ALIBABA CLOUD

阿里云

云服务器ECS

镜像

文档版本：20220713

阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.镜像概述 10
2.选择镜像 13
3.查找镜像 17
4.公共镜像 20
4.1. 公共镜像概述 20
4.2. 2022年 27
4.3. 已知问题 52
5.Alibaba Cloud Linux 66
5.1. Alibaba Cloud Linux概述 66
5.2. 镜像发布记录 70
5.2.1. Alibaba Cloud Linux 3镜像发布记录 70
5.2.2. Alibaba Cloud Linux 2镜像发布记录 79
5.3. 镜像使用说明 96
5.3.1. 在本地使用Alibaba Cloud Linux 3镜像 96
5.3.2. 在本地使用Alibaba Cloud Linux 2镜像 101
5.3.3. Alibaba Cloud Linux 2使用说明 104
5.3.4. 开启或关闭IPv6 106
5.3.5. 如何安装并启用高版本的curl 110
5.4. 安全 110
5.4.1. Alibaba Cloud Linux等保2.0三级版镜像概述 110
5.4.2. Alibaba Cloud Linux CIS安全基线 111
5.4.3. 订阅Alibaba Cloud Linux 2安全漏洞（CVE）公告 115
5.4.4. 基于YUM的安全更新操作（Alibaba Cloud Linux 3） 116
5.4.5. 基于YUM的安全更新操作（Alibaba Cloud Linux 2） 120
5.4.6. 处理Alibaba Cloud Linux安全更新提醒 124
5.4.7. 基于Docker使用Inclavare Containers机密容器 126

5.4.8. 使用Inclavare Containers实现远程证明 130
5.5. 内核热补丁 141
5.5.1. 内核热补丁概述 141
5.5.2. 内核热补丁操作说明 141
5.5.3. 内核热补丁管理工具livepatch-mgr使用说明 145
5.5.4. 内核热补丁知识库 151
5.6. 内核功能与接口 152
5.6.1. 内核功能与接口概述 152
5.6.2. Memcg Exstat功能 155
5.6.3. Memcg全局最低水位线分级 158
5.6.4. cgroup v1接口支持memcg QoS功能 160
5.6.5. Memcg后台异步回收 161
5.6.6. Memcg OOM优先级策略功能 163
5.6.7. THP reclaim功能 164
5.6.8. TCP-RT功能的配置说明 167
5.6.9. 修改TCP TIME-WAIT超时时间 173
5.6.10. 启用cgroup writeback功能 174
5.6.11. blk-iocost权重限速 176
5.6.12. Block IO限流增强监控接口 180
5.6.13. JBD2优化接口 182
5.6.14. 跨目录配额创建硬链接 183
5.6.15. 追踪IO时延 184
5.6.16. 检测文件系统和块层的IO hang 185
5.6.17. 在cgroup v1接口开启PSI功能 187
5.6.18. 在cgroup v1接口开启CPU Burst功能 188
5.6.19. Group Identity功能说明 190
5.6.20. /proc/meminfo文件中的统计信息变更说明 195
5.6.21. 增强容器资源可见性 196

5.6.22. SMC-R说明 198
5.6.23. 内核统一异常框架（UKFEF） 204
5.7. 操作系统迁移工具 208
5.7.1. CentOS 8迁移Alibaba Cloud Linux 3 208
5.7.2. CentOS 7迁移Alibaba Cloud Linux 2 212
5.8. 已知问题 214
5.9. Alibaba Cloud Linux知识库 215
5.10. Alibaba Cloud Linux FAQ 216
6.自定义镜像 219
6.1. 自定义镜像概述 219
6.2. 创建自定义镜像 220
6.2.1. 使用快照创建自定义镜像 220
6.2.2. 使用实例创建自定义镜像 223
6.2.3. 使用Packer创建自定义镜像 225
6.2.4. 使用Packer创建并导入本地镜像 227
6.2.5. 使用OOS创建自定义镜像 232
6.3. 导入镜像 233
6.3.1. 导入镜像流程 233
6.3.2. 使用工具检测镜像规范 234
6.3.3. 导入镜像必读 237
6.3.4. 安装cloud-init 241
6.3.5. 安装virtio驱动 252
6.3.6. 定制Linux自定义镜像 259
6.3.7. 转换镜像格式 264
6.3.8. 导入自定义镜像 267
6.4. 更新自定义镜像 271
6.5. 复制镜像 272
6.6. 共享或取消共享镜像 275

6.7. 导出镜像 277
6.8. 修改自定义镜像信息 279
6.9. 编辑自定义镜像标签 279
6.10. 删除自定义镜像 280
6.11. 自定义镜像检测项说明 281
7.社区镜像 283
7.1. 社区镜像概述 283
7.2. 发布社区镜像 283
7.3. 查找社区镜像 284
7.4. 使用社区镜像 285
7.5. 下架社区镜像 286
8.镜像市场 287
9.镜像族系 289
9.1. 镜像族系概述 289
9.2. 设置镜像族系 290
9.3. 通过镜像族系创建ECS实例 293
9.4. 弃用镜像或恢复可用镜像 294
10.镜像构建服务（ImageBuilder） 297
10.1. 镜像构建服务（ImageBuilder）概述 297
10.2. 镜像构建服务（ImageBuilder）指令集 298
10.3. 使用镜像构建服务（ImageBuilder） 300
10.3.1. 镜像构建服务（ImageBuilder）组件 300
10.3.2. 创建镜像模版 301
10.3.3. 查看与执行镜像模版 303
10.3.4. 删除镜像组件 304
10.3.5. 删除镜像模版 304
10.4. 镜像构建服务（ImageBuilder）最佳实践 304
11.更换操作系统 309

12.操作系统停止支持计划 310
13.常见问题 316
13.1. 镜像FAQ 316
13.2. 如何手动更新Windows实例的virtio驱动? 343
13.3. CentOS Linux停止维护后如何应对? 355
13.4. CentOS 8 EOL如何切换源? 357
13.5. CentOS 6 EOL如何切换源? 358
13.6. 阿里云针对CentOS EOL迁移方案 362
13.7. Ubuntu 16.04 LTS停止支持维护后如何继续安全更新? 364
13.8. 如何共享加密自定义镜像? 365
13.9. Linux自定义镜像如何适配NVMe系统盘? 368
13.10. 存量SUSE Linux Enterprise Server实例的镜像如何升级为商业... 380
13.11. Linux时间和时区说明 382
13.12. AMD实例的兼容性 384
13.13. 镜像常见格式 384
13.14. 如何为Linux服务器安装GRUB? 385
13.15. Windows Server半年渠道镜像与实例管理 387
13.16. 如何解决实例迁移后的宕机问题? 391
13.17. 如何收集操作系统宕机后的内核转储信息? 394
13.18. Red Hat云接入和Windows许可证 395
13.18.1. Red Hat云接入 395
13.18.1.1. Red Hat云接入概述 395
13.18.1.2. 步骤一：注册Red Hat云接入计划 397
13.18.1.3. 步骤二：创建RHEL镜像 398
13.18.1.4. （可选）步骤三：将镜像转换为受支持的格式 405
13.18.1.5. 步骤四：将镜像导入阿里云ECS 405
13.18.1.6. 步骤五：创建ECS实例并运行RHEL镜像 408
13.18.2. Windows许可证 409

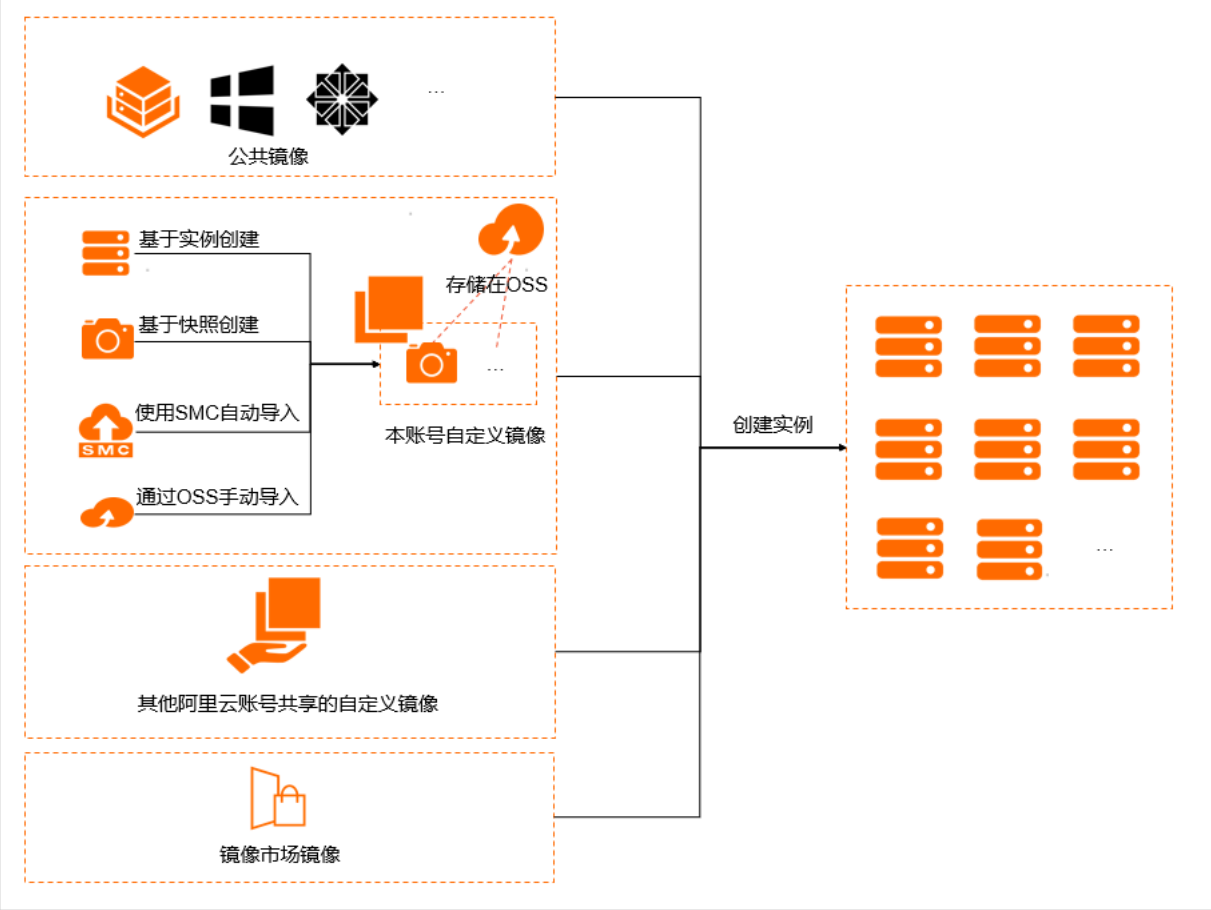
13.18.2.1. 微软许可证与软件保障 409
13.18.2.2. 申请许可移动性 411

1.镜像概述

ECS镜像提供了创建ECS实例所需的信息。创建ECS实例时，必须选择镜像。镜像文件相当于副本文件，该副本文件包含了一块或多块云盘中的所有数据，对于ECS实例而言，这些云盘可以是单块系统盘，也可以是系统盘加数据盘的组合。

镜像类型

ECS镜像根据来源不同，分为公共镜像、自定义镜像、共享镜像、镜像市场镜像和社区镜像。



- 公共镜像
  阿里云官方提供的镜像，皆是正版授权，安全性好，稳定性高。公共镜像包含了Windows Server系统镜像和主流的Linux系统镜像。更多信息，请参见公共镜像。
- 自定义镜像
  您使用实例或快照创建的镜像，或是您从本地导入的自定义镜像。更多信息，请参见自定义镜像。
- 共享镜像
  其他阿里云账号共享给您的镜像。共享镜像不会占用被共享者的镜像额度，也不会向被共享者收取快照容量等费用。更多信息，请参见共享镜像。
- 镜像市场镜像
  镜像市场的镜像根据供应商不同，可分为以下两种。
  - 由阿里云官方账号提供的镜像。
  - 由第三方服务商ISV（Independent Software Vendor）通过阿里云云市场授权提供的镜像。

  镜像市场的镜像包括操作系统和预装软件等，均经过服务商与阿里云严格测试，保证镜像内容的安全性。更多信息，请参见镜像市场。

- 社区镜像
  社区镜像是一种完全公开的镜像。您可以将制作好的自定义镜像发布为社区镜像供他人使用，也可以获取并使用他人发布的社区镜像。更多信息，请参见社区镜像概述。

镜像费用

使用镜像可能会产生费用，各类型镜像的费用如下表所示。

镜像类型	计费说明

公共镜像	公共镜像是阿里云官方提供的镜像，计费分为以下几种情况：
	• Windows Server：计费与实例规格大小有关，以创建实例时显示的信息为准。
	• Red Hat Enterprise Linux：收取镜像费用，镜像计费与实例规格大小有关，价格情况如下所示：
	  ○ 1 vCPU~4 vCPU：包月（291.00元/月）、包年（3,389.00元/年）、按量付费（0.43元/时）
	  ○ 5 vCPU及以上：包月（643.00元/月）、包年（7,433.00元/年）、按量付费（0.95元/时）
	• SUSE Linux Enterprise Server：收取镜像费用，镜像计费与实例规格大小有关，价格情况如下所示：
	  ○ 1 vCPU~2 vCPU：包月（159.00元/月）、包年（1,529.00元/年）、按量付费（0.41元/时）
	  ○ 3 vPU~4 vCPU：包月（326.00元/月）、包年（3,065.00元/年）、按量付费（0.82元/时）
	  ○ 5 vCPU及以上：包月（381.00元/月）、包年（3,670.00元/年）、按量付费（0.99元/时）
	• 其他：免费。

自定义镜像	自定义镜像是您使用实例或快照创建的镜像，或是您从本地导入的镜像。计费包括以下两部分：
	• 快照费用：生成自定义镜像的过程中，系统会自动生成一份快照，保有镜像会产生一定的快照费用。快照按快照容量和存储时长计费，更多信息，请参见快照计费。
	• 镜像费用：如果自定义镜像的最终来源为付费镜像且您使用了该自定义镜像，则需要收取镜像费用。
	  说明 如果您使用的自定义镜像为导入的Windows系统的自定义镜像，将以系统的许可证类型为依据进行计费。当许可证类型为阿里云（Aliyun）或自动（Auto）时，将收取镜像费用；当许可证类型为自带许可（BYOL）时，不收取镜像费用。关于许可证类型的更多信息，请参见自定义镜像支持的许可证类型。
	  例如：实例A使用了付费镜像A，则使用实例A创建自定义镜像后，您使用该自定义镜像创建实例，则除了快照费用外，需要再次支付镜像费用。

共享镜像	共享镜像是其他阿里云账号共享给您的镜像。如果该镜像的最终来源为付费镜像且您使用了该共享镜像，则收取镜像费用。 例如：源镜像A是付费镜像，用户A把该镜像共享给用户B后，用户B使用该共享镜像创建了实例，则用户B需要支付镜像费用。
镜像市场镜像	镜像市场镜像由镜像服务商ISV提供，费用以镜像市场购买页面为准。
社区镜像	免费。

更多计费信息，请参见镜像计费和镜像商业化FAQ。

选择和查找镜像

您可以基于地域、镜像类型、镜像费用、操作系统和内置软件等因素选择镜像。更多信息，请参见选择镜像。

如果您知道镜像的类型、名称、ID或对应的快照ID，您可以根据这些条件查找到特定镜像，进而创建实例或执行其他操作。更多信息，请参见查找镜像。

更换镜像

创建实例后，如果您需要更换实例的操作系统，可以通过更换系统盘来实现。

- 如果更换为公共镜像，请参见更换操作系统（公共镜像）。
- 如果更换为非公共镜像（如自定义镜像、镜像市场镜像或共享镜像），请参见更换操作系统（非公共镜像）。

使用限制

关于镜像的使用限制及配额，请参见镜像使用限制。

API操作

您也可以查看并使用镜像相关的API对镜像进行操作。更多信息，请参见镜像相关API。

2.选择镜像

创建ECS实例时，您必须选择镜像。本文旨在帮助您从众多镜像类型和操作系统中选择合适的镜像。
选择镜像时，您可能需要考虑以下几个因素：

- 地域
- 镜像类型和费用
- 操作系统
- 内置软件（如镜像中是否安装了MySQL等应用软件）

地域

镜像是一种地域性资源，您不能跨地域使用镜像创建实例。例如，在华北2地域创建实例时，您只能使用位于华北2地域的镜像。更多阿里云地域，请参见。

如需使用其他地域镜像创建实例，可先复制该镜像到当前地域，详情请参见复制镜像。

镜像类型和费用

ECS镜像根据来源不同，分为公共镜像、自定义镜像、共享镜像和镜像市场的镜像。不同类型镜像的简介和费用请参见镜像概述。

操作系统

选择操作系统时，您可能需要考虑以下方面：

- **选择系统架构（32位或64位）**

系统架构	适用内存	使用限制
32位	适用于4 GiB以下内存	○ 实例规格内存大于4 GiB时，无法使用32位操作系统。 ○ Windows 32位操作系统最高支持4核CPU。
64位	适用于4 GiB及以上内存	若您的应用需使用4 GiB以上内存或未来需扩充内存至4 GiB以上，请使用64位操作系统。

- **选择操作系统类型（Windows或Linux/类Unix系统）**

操作系统类型	登录方式	特点	适用场景
Windows	支持远程桌面方式	Windows系统的公共镜像内含正版已激活系统，默认不提供CD-ROM配置。	○ 适合运行Windows下开发的程序，如.NET等。 ○ 支持SQL Server等数据库（需自行安装）。
Linux/类Unix	支持SSH方式	○ 常用的服务器端操作系统，具备安全性和稳定性。 ○ 开源，轻松建立和编译源代码。	○ 一般用于高性能Web等服务器应用，支持常见的PHP、Python等编程语言。 ○ 支持MySQL等数据库（需自行安装)。

阿里云提供的Windows和Linux/类Unix系统的公共镜像列表，请参见公共镜像概述。

- **选择Windows系统版本**

建议您选择高版本Windows系统。相对低版本来说，高版本系统漏洞更少，并且IIS 7.5比IIS 6提供了更多功能以及更方便的控制台。
请您阅读以下注意事项并根据实际需要选择合适的硬件配置和Windows版本：

- vCPU为1核且内存为1 GiB的实例规格无法启动MySQL数据库。
- Windows实例用于建站、部署Web环境时，最少需要2 GiB内存。
- 为了保证性能体验，使用Windows 2008/2012系统时，建议您选择内存为2 GiB及以上的实例规格。
- 使用Windows Server 2016/2019系统必须选择内存为2 GiB及以上的实例规格，否则售卖页的公共镜像列表中不会出现Windows Server 2016/2019。
- 阿里云不再为Windows Server 2003系统镜像提供技术支持，详情请参见阿里云不再支持Windows Server 2003系统镜像。

- **选择Linux/类Unix系统的发行版**
  阿里云的Linux/类Unix公共镜像包含以下发行版：
  - **Aliyun Linux**
    Aliyun Linux是阿里云研发的Linux操作系统，旨在为ECS实例上的应用程序提供更加安全、稳定、高性能的运行环境。其中Aliyun Linux 2支持各种云场景负载，并支持各规格实例（除使用经典网络的实例和非I/O优化实例），详情请参见Alibaba Cloud Linux概述。
  - **Red Hat系列**
    - CentOS
    - Red Hat

    CentOS和Red Hat两种操作系统的特点和关系见下表：

操作系统	软件包格式	安装软件	费用	特点	两者关系
CentOS	rpm包	yum	免费使用	■ 稳定，但补丁更新速度慢于Red Hat。 ■ 支持在线升级，可即时更新系统。	■ CentOS是Red Hat的开源版本。 ■ 两者rpm包通用。 ■ 两者命令通用。
Red Hat			付费使用	稳定，可获得企业级技术支持。	

- **Debian系列**
  - Debian
  - Ubuntu

  Debian和Ubuntu两种操作系统的特点和关系见下表：

操作系统	软件包格式	安装软件	特点	两者关系
Debian	deb包	aptitude	系统相对稳定。	Ubuntu基于Debian开发，可简单认为Ubuntu是Debian的功能加强版。
Ubuntu		apt-get	■ 系统配置更人性化。 ■ 软件的更新更为激进。 ■ 新手友好度更高，易用性更好，更容易上手。	

- **SUSE系列**
  - SUSE Linux
  - OpenSUSE

  OpenSUSE和SUSE Linux的关系和对比见下表：

操作系统	两者对比	两者关系
OpenSUSE	■ OpenSUSE是社区版，SUSE Linux Enterprise是企业版。 ■ SUSE Linux Enterprise更成熟、稳定，官方源中软件与OpenSUSE相比较少。 ■ OpenSUSE软件版本更新，可扩展性强（可用于桌面或服务器），免费更新（也可购买官方技术支持）。 ■ SUSE Linux Enterprise更适用于工作、生产环境，娱乐功能较差，OpenSUSE可用于个人娱乐和其他较专业的用途。	■ SUSE Linux在版本10.2以后更名为OpenSUSE。 ■ OpenSUSE使用的内核与SUSE Linux相同。
SUSE Linux		

- **CoreOS**
  CoreOS是一款基于Linux内核的轻量级操作系统，为计算机集群的基础设施建设而生，专注于自动化，轻松部署，安全，可靠，规模化。作为一个操作系统，CoreOS提供了在应用容器内部署应用所需要的基础功能环境以及一系列用于服务发现和配置共享的内建工具。
- **FreeBSD**
  FreeBSD是一款类Unix操作系统，为专注于功能、速度和稳定性的平台提供。FreeBSD提供了先进的网络、性能、安全和兼容性功能，这些功能在其他操作系统甚至最好的商业操作系统中仍然缺失。详情请参见FreeBSD官方文档。

内置软件

镜像市场的镜像，通常在操作系统中预装了ECS实例的运行环境或软件应用，您可根据实际需要，购买相应的镜像创建实例。更多详情，请参见镜像市场。

下一步

- 使用镜像创建实例。详情请参见使用向导创建实例。
- 使用镜像更换操作系统。详情请参见更换操作系统。

3.查找镜像

如果您知道镜像的类型、名称、ID或对应的快照ID，可以根据这些条件查找到特定镜像，进而创建实例或执行其他操作。本文介绍查找镜像的方法和操作步骤。

查找方式

查找镜像方式包括：

- 通过ECS控制台查找镜像
  本文提供以下具体示例：
  - 示例一：查找位于华北2（北京）地域的Windows系统公共镜像。
  - 示例二：查找位于华东1（杭州）地域且镜像名称中包含MySQL的共享镜像。
  - 示例三：查找位于华南1（深圳）地域且快照ID为s-123****的自定义镜像。
  - 示例四：查找社区镜像的操作说明与示例，请参见查找社区镜像。
- 通过API查找镜像

通过ECS控制台查找镜像

您可在ECS控制台的**镜像**页面查找您所需要的镜像。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 选择镜像类型。
5. （可选）（可选）选择镜像族系。

   说明 仅自定义镜像支持选择镜像族系，默认为全部镜像，不筛选镜像族系。

6. 在搜索栏的下拉列表中，选择搜索项。

   说明
   - 自定义镜像、公共镜像和共享镜像：搜索项支持镜像名称、镜像ID和快照ID。
   - 镜像市场：搜索项支持镜像ID、实例ID和镜像商品名称。
   - 社区镜像：搜索项支持镜像名称、镜像ID和社区镜像OwnerId。

7. 在搜索栏的文本框中，输入相应的搜索值。
8. 单击图标进行搜索。

示例一

示例一：查找位于华北2（北京）地域的Windows系统公共镜像。

在**镜像**页面，完成如下配置：

1. 选择地域**华北2（北京）**。
2. 单击**公共镜像**。
3. 在搜索栏下拉列表中，选择**镜像名称**。

4. 在搜索栏文本框中，输入*win*。
5. 单击图标进行搜索。

示例二

示例二：查找位于华东1（杭州）地域且镜像名称中包含MySQL的共享镜像。

在**镜像**页面，完成如下配置：

1. 选择**华东1（杭州）**地域。
2. 单击**共享镜像**。
3. 在搜索栏下拉列表中，选择**镜像名称**。
4. 在搜索栏文本框中，输入*MySQL*。
5. 单击图标进行搜索。

示例三

示例三：查找位于华南1（深圳）地域且快照ID为s-123****的自定义镜像。

在**镜像**页面，完成如下配置：

1. 选择地域**华南1（深圳）**。
2. 单击**自定义镜像**。
3. 在搜索栏下拉列表中，选择**快照ID**。
4. 在搜索栏文本框中，输入*s-123****。
5. 单击图标进行搜索。

通过API查找镜像

您也可以通过OpenAPI开发者门户或阿里云CLI调用DescribeImages查找镜像。本文以OpenAPI开发者门户为例介绍调用API查找镜像的操作步骤。

1. 前往OpenAPI开发者门户。
2. 在**RegionId**下拉列表中，选择地域。
3. （可选）填写其他参数，例如镜像名称ImageName，镜像IDImageId等。

> **说明** 镜像ID的命名规则如下：
> - 公共镜像：以操作系统版本号、架构、语言和发布日期命名。例如，Windows Server 2008 R2企业版、64位英文系统的镜像ID为win2008r2_64_ent_sp1_en-us_40G_alibase_20190318.vhd。
> - 自定义镜像、镜像市场的镜像：以m开头。
> - 共享镜像：与被共享的自定义镜像ID相同。

4. 单击**发起调用**。
5. 单击**调试结果**。
   若查找到满足要求的镜像，会在**调试结果**标签页中返回镜像的详细信息，如镜像ID、描述、操作系统类型等。更多详情，请参见DescribeImages。

后续步骤

查找到满足要求的镜像后，您可能需要：

- 创建实例。具体操作，请参见使用向导创建实例。
- 共享镜像。具体操作，请参见共享或取消共享镜像。
- 复制镜像。具体操作，请参见复制镜像。
- 导出镜像。具体操作，请参见导出镜像。
- 删除镜像。具体操作，请参见删除自定义镜像。
- 修改镜像描述信息。具体操作，请参见修改自定义镜像信息。

相关文档

- DescribeImages

4.公共镜像

4.1. 公共镜像概述

公共镜像由阿里云官方提供，皆已正版授权，旨在为ECS实例上的应用程序提供安全、稳定的运行环境。本文介绍公共镜像类型、公共镜像列表以及Alibaba Cloud Linux系统镜像。

公共镜像类型

阿里云提供以下两种类型的公共镜像。除Windows Server、Red Hat Enterprise Linux和SUSE Linux Enterprise Server之外，您可免费使用其他公共镜像创建ECS实例。费用详情，请参见镜像费用。

公共镜像类型	描述	技术支持
Alibaba Cloud Linux镜像	阿里云针对ECS实例提供的定制化原生操作系统镜像。Alibaba Cloud Linux镜像均经过严格测试，确保镜像安全、稳定，保证您能够正常启动和使用镜像。	阿里云将为您在使用Alibaba Cloud Linux操作系统过程中遇到的问题提供技术支持。
第三方商业镜像及开源镜像合作的正版镜像	由阿里云严格测试并制作发布，确保镜像安全、稳定，保证您能正常启动和使用镜像。第三方公共镜像包括： • Windows系统：Windows Server • Linux系统：龙蜥（Anolis）OS、Ubuntu、CentOS、Redhat Enterprise Linux、Debian、OpenSUSE、SUSE Linux Enterprise Server、FreeBSD、CoreOS、Fedora CoreOS、Fedora、Rocky Linux和AlmaLinux等	请联系操作系统原厂或者开源社区获得技术支持。同时，阿里云将对问题的调查提供相应的技术协助。

Alibaba Cloud Linux镜像

Alibaba Cloud Linux是阿里云自主研发的Linux系统镜像，属于公共镜像。

操作系统类型	操作系统版本	描述
Alibaba Cloud Linux 3	• Alibaba Cloud Linux 3.2104 64位 • Alibaba Cloud Linux 3.2104 64位 快速启动版 • Alibaba Cloud Linux 3.2104 64位 SCC版 • Alibaba Cloud Linux 3.2104 64位 ARM版 • Alibaba Cloud Linux 3.2104 64位 UEFI版	支持多种阿里云实例规格，包括弹性裸金属服务器。Alibaba Cloud Linux 3中默认搭载了阿里云命令行工具及其他软件包，方便您的使用。 如果您要从其他Linux版本更换为Alibaba Cloud Linux 3，可以通过创建新实例或更换系统盘的方式进行更换。 更多信息，请参见Alibaba Cloud Linux概述及Alibaba Cloud Linux 3镜像发布记录。

操作系统类型	操作系统版本	描述
Alibaba Cloud Linux 2	• Alibaba Cloud Linux 2.1903 LTS 64位 • Alibaba Cloud Linux 2.1903 64位 快速启动版 • Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版 • Alibaba Cloud Linux 2.1903 LTS 64位 SCC版 • Alibaba Cloud Linux 2.1903 64位 UEFI版 • Alibaba Cloud Linux 2.1903 64位 可信版	支持多种阿里云实例规格，包括弹性裸金属服务器。Alibaba Cloud Linux 2中默认搭载了阿里云命令行工具及其他软件包，方便您的使用。 如果您要从其他Linux版本更换为Alibaba Cloud Linux 2，可以通过创建新实例或更换系统盘的方式进行更换。 更多信息，请参见Alibaba Cloud Linux概述及Alibaba Cloud Linux 2镜像发布记录。

第三方及开源公共镜像列表

阿里云会定期发布或更新公共镜像，请前往2022年页面查看详情。您也可以在ECS管理控制台相应地域的公共镜像列表页查看或查找可用的公共镜像。具体操作，请参见查找镜像。

阿里云提供的第三方商业镜像及开源公共镜像，如下表所示。

- Windows系统镜像

操作系统类型	操作系统版本
Windows Server 2019	○ Windows Server 2019 with Container 数据中心版 64位中文版 ○ Windows Server 2019 with Container 数据中心版 64位英文版 ○ Windows Server 2019 数据中心版 64位中文版 ○ Windows Server 2019 数据中心版 64位英文版
Windows Server 2016	○ Windows Server 2016 数据中心版 64位中文版 ○ Windows Server 2016 数据中心版 64位英文版
Windows Server 2012	○ Windows Server 2012 R2 数据中心版 64位中文版 ○ Windows Server 2012 R2 数据中心版 64位英文版
Windows Server Version ****（半年渠道）	○ Windows Server Version **** 数据中心版 64位中文版 ○ Windows Server Version **** 数据中心版 64位英文版 其中，****为半年渠道的最新版本。

说明 微软已经于2020年1月14日停止对Windows Server 2008和Windows Server 2008 R2操作系统提供支持。因此阿里云不再对使用上述操作系统的ECS实例提供技术支持。如果您有使用上述操作系统的ECS实例，请尽快更新至Windows Server 2012或以上版本。

- Linux系统镜像

操作系统类型	操作系统版本
Anolis OS	○ Anolis OS 8.4 ANCK 64 位 ○ Anolis OS 8.4 RHCK 64 位 ○ Anolis OS 8.4 ANCK 64 位 ARM版 ○ Anolis OS 8.4 RHCK 64 位 ARM版 ○ Anolis OS 8.2 ANCK 64 位 ○ Anolis OS 8.2 RHCK 64 位 ○ Anolis OS 8.2 ANCK 64 位 ARM版 ○ Anolis OS 8.2 RHCK 64 位 ARM版 ○ Anolis OS 7.9 ANCK 64位 ○ Anolis OS 7.9 RHCK 64位 ○ Anolis OS 7.9 ANCK 64 位 ARM版 ○ Anolis OS 7.9 RHCK 64 位 ARM版 ○ Anolis OS 7.7 ANCK 64位 ○ Anolis OS 7.7 RHCK 64位 ○ Anolis OS 7.7 ANCK 64位 ARM版 ○ Anolis OS 7.7 RHCK 64位 ARM版 关于Anolis OS的更多信息，请参见龙蜥（Anolis）OS。

操作系统类型	操作系统版本
CentOS	○ CentOS Stream 8 64位 ○ CentOS 8.5 64位 ○ CentOS 8.4 64位 ○ CentOS 8.4 64位 ARM版 ○ CentOS 8.4 64位 UEFI版 ○ CentOS 8.3 64位 ○ CentOS 8.3 64位 ARM版 ○ CentOS 8.3 64位 UEFI版 ○ CentOS 8.2 64位 ○ CentOS 8.2 64位 AMD版 ○ CentOS 8.1 64位 ○ CentOS 8.0 64位 ○ CentOS 7.9 64位 ○ CentOS 7.9 64位 AMD版 ○ CentOS 7.9 64位 UEFI版 ○ CentOS 7.8 64位 ○ CentOS 7.8 64位 可信版 ○ CentOS 7.8 64位 AMD版 ○ CentOS 7.7 64位 ○ CentOS 7.6 64位 ○ CentOS 7.5 64位 ○ CentOS 7.4 64位 ○ CentOS 7.3 64位 ○ CentOS 7.2 64位 ○ CentOS 6.10 64位 ○ CentOS 6.9 64位 ○ CentOS 6.8 32位 **说明** ○ CentOS官方已计划停止维护CentOS Linux项目，阿里云上CentOS Linux公共镜像来源于CentOS官方，当CentOS Linux停止维护后，阿里云将会同时停止对该操作系统的支持。具体应对措施，请参见CentOS Linux停止维护后如何应对？。 ○ CentOS 6和CentOS 8操作系统版本结束了生命周期（EOL），按照社区规则，CentOS 6/8的源地址内容已移除。如果您的业务过渡期仍需要使用CentOS 6/8操作系统中的一些安装包，则需要切换CentOS 6/8的源地址。具体操作，请参见CentOS 6 EOL如何切换源？和CentOS 8 EOL如何切换源？。 ○ 使用32位操作系统，请选择内存小于或等于4GiB的实例规格。更多信息，请参见选择镜像的操作系统。

操作系统类型	操作系统版本
CoreOS	○ CoreOS 2345.3.0 64位 ○ CoreOS 2303.4.0 64位 ○ CoreOS 2303.3.0 64位 ○ CoreOS 2247.6.0 64位 ○ CoreOS 2023.4.0 64位 ○ CoreOS 1745.7.0 64位 **说明** 根据Fedora CoreOS社区的公告，CoreOS Container Linux将于2020年5月26日停止提供更新。因此阿里云做出以下说明： ○ 自2020年5月26日起，阿里云将不再为CoreOS Container Linux提供技术协助，但不影响您已安装该操作系统的ECS实例的继续使用。 ○ 在2020年9月30日之后，您将无法使用阿里云提供的CoreOS Container Linux公共镜像创建新的ECS实例。 ○ 已安装的CoreOS Container Linux在2020年5月26日后仍可继续使用，但是由于该操作系统已经结束生命周期，不会继续提供安全补丁。出于安全因素的考虑，阿里云不推荐您继续使用CoreOS Container Linux镜像。 ○ Fedora CoreOS社区推荐使用Fedora CoreOS操作系统作为CoreOS Container Linux的替代，阿里云也将在近期上线Fedora CoreOS公共镜像。

操作系统类型	操作系统版本
Debian	○ Debian 11.2 64位 ○ Debian 11.1 64位 ○ Debian 11.0 64位 ○ Debian 10.11 64位 ○ Debian 10.10 64位 ○ Debian 10.10 64位 UEFI版 ○ Debian 10.9 64位 ○ Debian 10.9 64位 ARM版 ○ Debian 10.7 64位 ○ Debian 10.7 64位 AMD版 ○ Debian 10.6 64位 ○ Debian 10.5 64位 ○ Debian 10.4 64位 ○ Debian 10.3 64位 ○ Debian 10.2 64位 ○ Debian 9.13 64位 ○ Debian 9.13 64位 UEFI版 ○ Debian 9.12 64位 ○ Debian 9.11 64位 ○ Debian 9.9 64位 ○ Debian 9.8 64位 ○ Debian 9.6 64位 ○ Debian 8.11 64位 ○ Debian 8.9 64位
FreeBSD	○ FreeBSD 12.1 64位 ○ FreeBSD 11.4 64位 ○ FreeBSD 11.3 64位 ○ FreeBSD 11.2 64位
OpenSUSE	○ OpenSUSE 15.3 64位 ○ OpenSUSE 15.2 64位 ○ OpenSUSE 15.1 64位 ○ OpenSUSE 42.3 64位

操作系统类型	操作系统版本
Red Hat	○ Red Hat Enterprise Linux 8.5 64位 ○ Red Hat Enterprise Linux 8.4 64位 ○ Red Hat Enterprise Linux 8.3 64位 ○ Red Hat Enterprise Linux 8.2 64位 ○ Red Hat Enterprise Linux 8.1 64位 ○ Red Hat Enterprise Linux 8.0 64位 ○ Red Hat Enterprise Linux 7.9 64位 ○ Red Hat Enterprise Linux 7.9 64位 UEFI ○ Red Hat Enterprise Linux 7.8 64位 ○ Red Hat Enterprise Linux 7.7 64位 ○ Red Hat Enterprise Linux 7.6 64位 ○ Red Hat Enterprise Linux 7.5 64位 ○ Red Hat Enterprise Linux 7.4 64位 ○ Red Hat Enterprise Linux 6.10 64位 ○ Red Hat Enterprise Linux 6.9 64位 **说明** 使用Red Hat镜像前，请确认实例规格族是否支持。更多信息，请参见RHEL（Red Hat Enterprise Linux）镜像支持哪些实例规格族？。
SUSE Linux	○ SUSE Linux Enterprise Server 15 SP3 64位 ○ SUSE Linux Enterprise Server 15 SP2 64位 ○ SUSE Linux Enterprise Server 15 SP1 64位 ○ SUSE Linux Enterprise Server 12 SP5 64位 ○ SUSE Linux Enterprise Server 12 SP4 64位 ○ SUSE Linux Enterprise Server 12 SP3 64位 ○ SUSE Linux Enterprise Server 12 SP2 64位 ○ SUSE Linux Enterprise Server 11 SP4 64位 **说明** SUSE Linux Enterprise Server（SLES）公共镜像已于2021年10月30日正式开启收费。公告详情，请参见【其他】SUSE Enterprise Linux Server将于2021年10月30日开启收费。存量的SLES实例的镜像支持升级为商业版，以持续获得镜像更新与技术支持。具体操作，请参见存量SUSE Linux Enterprise Server实例的镜像如何升级为商业版？。

操作系统类型	操作系统版本
Ubuntu	○ Ubuntu 20.04 64位 ○ Ubuntu 20.04 64位 AMD版 ○ Ubuntu 20.04 64位 ARM版 ○ Ubuntu 20.04 64位 UEFI版 ○ Ubuntu 18.04 64位 ○ Ubuntu 18.04 64位 AMD版 ○ Ubuntu 18.04 64位 ARM版 ○ Ubuntu 18.04 64位 UEFI版 ○ Ubuntu 16.04 64位 ○ Ubuntu 16.04 32位 ○ Ubuntu 14.04 64位 ○ Ubuntu 14.04 32位 **说明** 使用32位操作系统，请选择内存小于或等于4GiB的实例规格。更多信息，请参见选择镜像的操作系统。
Fedora CoreOS	○ Fedora CoreOS 34.20210529.3.0_3 ○ Fedora CoreOS 33.20210217.3.0_3 使用该类镜像时，您需要注意： ○ 创建实例或更换系统盘时，登录凭证仅支持设置密钥对，且仅能使用实例第一次设置的密钥对登录实例，不支持更换或解绑该密钥对。 ○ 创建实例或更换系统盘后，不支持为实例重置密码。
Fedora	○ Fedora 34 64位 ○ Fedora 33 64位
Rocky Linux	Rocky Linux 8.5
AlmaLinux	AlmaLinux 8.5

4.2. 2022年

本章节以发布时间为顺序，介绍了云服务器ECS公共镜像在2022年的更新动态。

背景信息

- 如无特殊声明，镜像更新内容适用于云服务器ECS所有可用地域。
- 公共镜像适用于大多数实例规格族，但存在一部分实例规格族不适用，这些实例规格族只能选用指定的公共镜像。根据不同操作系统和实例规格族限制，镜像发布分类如下表所示。

Linux镜像	指定实例规格族使用的Linux镜像	Windows Server镜像
○ Anolis OS ○ AlmaLinux ○ CentOS ○ CoreOS（已停止更新） ○ Debian ○ Fedora CoreOS ○ Fedora ○ FreeBSD ○ OpenSUSE ○ Red Hat Enterprise Linux ○ Rocky Linux ○ SUSE Linux Enterprise Server ○ Ubuntu	○ ARM镜像 ○ AMD镜像 ○ UEFI镜像 ○ 可信镜像	○ Windows Server 2022 ○ Windows Server 2019 ○ Windows Server 2016 ○ Windows Server 2012 ○ Windows Server 2008 ○ Windows Server Version 2004 ○ Windows Server Version 1909 ○ Windows Server Version 1903 ○ Windows Server Version 1809

Anolis OS

版本	镜像ID	发布时间	发布内容
Anolis OS 8.4 RHCK	*anolisos_8_4_x64_20G_rhck_alibase_20220518.vhd*	2022-05-18	• 更新龙蜥（Anolis）OS 8.4 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.4版本 • 内核版本：4.18.0-348.23.1.an8_5.x86_64 • 更新最新软件包
Anolis OS 8.4 ANCK	*anolisos_8_4_x64_20G_anck_alibase_20220518.vhd*	2022-05-18	• 更新龙蜥（Anolis）OS 8.4 ANCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.4版本 • 内核版本：4.19.91-25.8.an8.x86_64 • 更新最新软件包
Anolis OS 7.9 RHCK	*anolisos_7_9_x64_20G_rhck_alibase_20220518.vhd*	2022-05-18	• 更新龙蜥（Anolis）OS 7.9 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 7.9版本 • 内核版本：3.10.0-1160.62.1.0.1.an7.x86_64 • 更新最新软件包

版本	镜像ID	发布时间	发布内容
Anolis OS 8.4 ANCK	*anolisos_8_4_x64_20G_anck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 8.4 ANCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.4版本 • 内核版本：4.19.91-25.8.an8.x86_64 • 更新最新软件包
Anolis OS 8.4 RHCK	*anolisos_8_4_x64_20G_rhck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 8.4 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.4版本 • 内核版本：4.18.0-348.20.1.an8_5.x86_64 • 更新最新软件包
Anolis OS 8.2 ANCK	*anolisos_8_2_x64_20G_anck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 8.2 ANCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.2版本 • 内核版本：4.18.0-348.20.1.an8_5.x86_64 • 更新最新软件包
Anolis OS 8.2 RHCK	*anolisos_8_2_x64_20G_rhck_alibase_20220415.vhd*	2022-04-15	• 更新龙蜥（Anolis）OS 8.2 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.2版本 • 内核版本：4.18.0-348.20.1.an8_5.x86_64 • 更新最新软件包
Anolis OS 7.9 RHCK	*anolisos_7_9_x64_20G_rhck_alibase_20220414.vhd*	2022-04-14	• 更新龙蜥（Anolis）OS 7.9 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 7.9版本 • 内核版本：3.10.0-1160.62.1.0.1.an7.x86_64 • 更新最新软件包

版本	镜像ID	发布时间	发布内容
Anolis OS 7.9 RHCK	*anolisos_7_9_x64_20G_rhck_alibase_20220316.vhd*	2022-03-16	• 更新龙蜥（Anolis）OS 7.9 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 7.9版本 • 内核版本：3.10.0-1160.59.1.0.1.an7.x86_64 • 更新最新软件包
Anolis OS 7.9 ANCK	*anolisos_7_9_x64_20G_anck_alibase_20220316.vhd*	2022-03-16	• 发布龙蜥（Anolis）OS 7.9 ANCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9版本 • 内核版本：4.19.91-25.7.an7.x86_64 • 更新最新软件包
Anolis OS 8.4 RHCK	*anolisos_8_4_x64_20G_rhck_alibase_20220119.vhd*	2022-01-19	• 更新龙蜥（Anolis）OS 8.4 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容新版CentOS 8.4版本 • 支持非root用户登录实例 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明 • 内核版本更新至：*kernel-4.18.0-348.2.1.an8_4.x86_64* • 适用地域：美国（弗吉尼亚）
Anolis OS 7.9 ANCK	*anolisos_7_9_x64_20G_anck_alibase_20220111.vhd*	2022-01-11	• 发布龙蜥（Anolis）OS 7.9 ANCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9版本 • 内核版本：4.19.91-25.2.an7.x86_64
Anolis OS 7.9 RHCK	*anolisos_7_9_x64_20G_rhck_alibase_20220110.vhd*	2022-01-10	• 更新龙蜥（Anolis）OS 7.9 RHCK基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9版本 • 内核版本：3.10.0-1160.an7.x86_64

历史版本更新记录，请参见Anolis OS。

AlmaLinux

版本	镜像ID	发布时间	发布内容

AlmaLinux 8.6	*almalinux_8_6_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.18.0-372.9.1.el8.x86_64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例
			• 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

AlmaLinux 9.0	*almalinux_9_0_x64_20G_alibase_20220628.vhd*	2022-06-28	• 首次发布AlmaLinux 9.0 64位公共镜像
			• 内核版本：5.14.0-70.13.1.el9_0.x86_64
			• 更新内容：
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例
			  ○ 开启Kdump服务

AlmaLinux 8.6	*almalinux_8_6_x64_20G_alibase_20220524.vhd*	2022-05-24	• 首次发布AlmaLinux 8.6 64位公共镜像 • 内核版本：4.18.0-372.9.1.el8.x86_64
AlmaLinux 8.5	*almalinux_8_5_x64_20G_alibase_20220426.vhd*	2022-04-26	• 内核版本：4.18.0-348.20.1.el8_5.x86_64 • 更新内容：更新最新补丁包

AlmaLinux 8.5	*almalinux_8_5_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：4.18.0-348.20.1.el8_5.x86_64
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2022-0847、CVE-2022-0492漏洞

版本	镜像ID	发布时间	发布内容

AlmaLinux 8.5	*almalinux_8_5_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：4.18.0-348.12.2.el8_5.x86_64
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2021-4034漏洞

AlmaLinux 8.5	*almalinux_8_5_x64_20G_alibase_20220110.vhd*	2022-01-10	• 内核版本：4.18.0-348.7.1.el8_5.x86_64
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2021-43527漏洞

历史版本更新记录，请参见AlmaLinux。

CentOS

版本	镜像ID	发布时间	发布内容
CentOS Stream 8	*centos_stream_8_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.18.0-394.el8.x86_64 • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡
CentOS 7.9	*centos_7_9_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：3.10.0-1160.66.1.el7.x86_64 • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

版本	镜像ID	发布时间	发布内容

CentOS Stream 9	*centos_stream_9_x64_20G_alibase_20220628.vhd*	2022-06-28	• 首次发布CentOS Stream 9 64位公共镜像
			• 内核版本：5.14.0-119.el9.x86_64
			• 更新内容：
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例

CentOS Stream 8	*centos_stream_8_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：4.18.0-383.el8.x86_64 • 更新内容：更新最新补丁包
CentOS 7.9	*centos_7_9_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：3.10.0-1160.66.1.el7.x86_64 • 更新内容：更新最新补丁包
CentOS 8.5	*centos_8_5_x64_20G_alibase_20220428.vhd*	2022-04-28	• 内核版本：4.18.0-348.7.1.el8_5.x86_64 • 更新内容：优化配置，支持开机DHCP IPv6地址
CentOS Stream 8	*centos_stream_8_x64_20G_alibase_20220426.vhd*	2022-04-26	• 内核版本：4.18.0-383.el8.x86_64 • 更新内容：更新最新补丁包
CentOS 7.9	*centos_7_9_x64_20G_alibase_20220426.vhd*	2022-04-26	• 内核版本：3.10.0-1160.62.1.el7.x86_64 • 更新内容：更新最新补丁包
CentOS 8.5	*centos_8_5_x64_20G_alibase_20220325.vhd*	2022-03-25	• 内核版本：4.18.0-348.7.1.el8_5.x86_64 • 更新内容： 优化GRUB配置文件
CentOS Stream 8	*centos_stream_8_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：4.18.0-365.el8.x86_64 • 更新内容：更新最新软件包
CentOS 7.9	*centos_7_9_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：3.10.0-1160.59.1.el7.x86_64 • 更新内容：更新最新软件包

版本	镜像ID	发布时间	发布内容
CentOS 8.5	*centos_8_5_x64_20G_alibase_20220303.vhd*	2022-03-03	• 内核版本：4.18.0-348.7.1.el8_5.x86_64 • 更新内容： ○ 源地址更改为使用vault源地址 ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
CentOS Stream 8	*centos_stream_8_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：4.18.0-348.2.1.el8_5.x86_64 • 更新内容： ○ 更新最新软件包 ○ 修复CVE-2021-4034漏洞
CentOS 7.9	*centos_7_9_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：3.10.0-1160.53.1.el7.x86_64 • 更新内容： ○ 更新最新软件包 ○ 修复CVE-2021-4034漏洞

历史版本更新记录，请参见CentOS。

CoreOS

说明 根据Fedora CoreOS社区的公告，CoreOS Container Linux将于2020年5月26日停止提供更新。因此阿里云做出以下说明：

- 自2020年5月26日起，阿里云将不再为CoreOS Container Linux提供技术协助，但不影响您已安装该操作系统的ECS实例的继续使用。
- 在2020年9月30日之后，您将无法使用阿里云提供的CoreOS Container Linux公共镜像创建新的ECS实例。
- 已安装的CoreOS Container Linux在2020年5月26日后仍可继续使用，但是由于该操作系统已经结束生命周期，不会继续提供安全补丁。出于安全因素的考虑，阿里云不推荐您继续使用CoreOS Container Linux镜像。
- Fedora CoreOS社区推荐使用Fedora CoreOS操作系统作为CoreOS Container Linux的替代，阿里云也将在近期上线Fedora CoreOS公共镜像。

历史版本更新记录，请参见CoreOS。

Debian

版本	镜像ID	发布时间	发布内容

版本	镜像ID	发布时间	发布内容
Debian 11.3	*debian_10_12_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.19.0-20-amd64 • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡
Debian 10.12	*debian_10_12_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.19.0-20-amd64 • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

Debian 11.3	*debian_11_3_x64_20G_alibase_20220531.vhd*	2022-05-31	• 内核版本：5.10.0-14-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例
			  ○ 增加内核cmdline参数 `crash_kexec_post_notifiers`

Debian 10.12	*debian_10_12_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：4.19.0-20-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例

Debian 11.3	*debian_11_3_x64_20G_alibase_20220510.vhd*	2022-05-10	• 首次发布Debian 11.3 64位公共镜像 • 内核版本：5.10.0-14-amd64

Debian 10.12	*debian_10_12_x64_20G_alibase_20220428.vhd*	2022-04-28	• 内核版本：4.19.0-20-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ 优化配置，支持开机DHCP IPv6地址

版本	镜像ID	发布时间	发布内容

Debian 9.13	*debian_9_13_x64_20G_alibase_20220428.vhd*	2022-04-28	• 内核版本：4.9.0-18-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ 优化配置，支持开机DHCP IPv6地址

Debian 10.12	*debian_10_12_x64_20G_alibase_20220328.vhd*	2022-03-28	• 首次发布Debian 10.12 64位公共镜像 • 内核版本：4.19.0-20-amd64

Debian 9.13	*debian_9_13_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：4.9.0-18-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ 修复CVE-2022-0847、CVE-2022-0492漏洞

Debian 11.2	*debian_11_2_x64_20G_alibase_20220308.vhd*	2022-03-08	• 内核版本：5.10.0-11-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ 修复CVE-2022-0847漏洞

Debian 11.2	*debian_11_2_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：5.10.0-11-amd64 • 更新内容：更新最新补丁包
Debian 10.11	*debian_10_11_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：4.19.0-18-amd64 • 更新内容：更新最新补丁包

Debian 9.13	*debian_9_13_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：4.9.0-17-amd64
			• 更新内容：
			  ○ 更新最新补丁包
			  ○ 修复CVE-2021-4034漏洞

历史版本更新记录，请参见Debian。

Fedora CoreOS

历史版本更新记录，请参见Fedora CoreOS。

Fedora

版本	镜像ID	发布时间	发布内容
Fedora 35 64位	*fedora_35_x64_20G_alibase_20220531.vhd*	2022-05-31	• 内核版本：5.17.9-200.fc35.x86_64 • 更新内容： ○ 更新最新补丁包 ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见 ○ 支持非root用户登录实例
Fedora 35 64位	*fedora_35_x64_20G_alibase_20220510.vhd*	2022-05-10	• 内核版本：5.17.6-200.fc35.x86_64 • 更新内容： ○ 更新最新补丁包 ○ 开启Kdump服务
Fedora 35 64位	*fedora_35_x64_20G_alibase_20220322.vhd*	2022-03-22	• 首次发布Fedora 35 64位公共镜像 • 内核版本：5.16.16-200.fc35.x86_64
Fedora 34 64位	*fedora_34_1_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：5.16.15-101.fc34.x86_64 • 更新最新补丁包
Fedora 34 64位	*fedora_34_1_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：5.16.5-100.fc34.x86_64 • 更新内容： ○ 更新最新补丁包 ○ 修复CVE-2021-4034漏洞

历史版本更新记录，请参见Fedora。

FreeBSD

版本	镜像ID	发布时间	发布内容
FreeBSD 12.3	*freebsd_12_3_x64_30G_alibase_20220331.vhd*	2022-03-31	内核版本：12.3-RELEAS
FreeBSD 13.0	*freebsd_13_0_x86_30G_alibase_20220324.vhd*	2022-03-24	• 首次发布FreeBSD 13.0 64位公共镜像 • 内核版本：13.0-RELEASE-p8

历史版本更新记录，请参见FreeBSD。

OpenSUSE

版本	镜像ID	发布时间	发布内容
Opensuse 15.3	*opensuse_15_3_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：5.3.18-150300.59.68-default • 更新内容：更新最新补丁包
Opensuse 15.3	*opensuse_15_3_x64_20G_alibase_20220426.vhd*	2022-04-26	• 内核版本：5.3.18-150300.59.63-default • 更新内容：更新最新补丁包

Opensuse 15.3	*opensuse_15_3_x64_20G_alibase_20220311.vhd*	2022-03-11	• 内核版本：5.3.18-150300.59.54-default
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2022-0847漏洞
			• 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

Opensuse 15.3	*opensuse_15_3_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：5.3.18-150300.59.46-default
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2021-4034漏洞

历史版本更新记录，请参见OpenSUSE。

Red Hat Enterprise Linux

阿里云提供的Red Hat Enterprise Linux公共镜像均源自阿里云云市场。该类镜像在搭配不同实例规格时价格也不同，您可以访问以下不同版本的Red Hat Enterprise Linux云市场镜像的详情页，以获取镜像的发布信息（镜像的适用地域、价格和使用指南等信息）。

> **说明**
> - Red Hat Enterprise Linux云市场镜像详情页提供的价格信息仅供参考，镜像实际价格请以资源购买页面的配置费用信息为准。
> - 已通过Red Hat Enterprise Linux认证的阿里云实例规格族信息，请参见RHEL（Red Hat Enterprise Linux）镜像支持哪些实例规格族？。

- Red Hat Enterprise Linux 8.5 64位
- Red Hat Enterprise Linux 8.4 64位
- Red Hat Enterprise Linux 8.3 64位
- Red Hat Enterprise Linux 8.2 64位
- Red Hat Enterprise Linux 8.1 64位

- Red Hat Enterprise Linux 8 64位
- Red Hat Enterprise Linux 7.9 64位
- Red Hat Enterprise Linux 7.9 64位 UEFI
- Red Hat Enterprise Linux 7.8 64位
- Red Hat Enterprise Linux 7.7 64位
- Red Hat Enterprise Linux 7.5 64位
- Red Hat Enterprise Linux 7.4 64位
- Red Hat Enterprise Linux 6.10 64位
- Red Hat Enterprise Linux 6.9 64位

Rocky Linux

版本	镜像ID	发布时间	发布内容
Rocky Linux 8.6	*rockylinux_8_6_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.18.0-372.9.1.el8.x86_64 • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

Rocky Linux 8.6	*rockylinux_8_6_x64_20G_alibase_20220524.vhd*	2022-05-24	• 首次发布Rocky Linux 8.6 64位公共镜像
			• 内核版本：4.18.0-372.9.1.el8.x86_64
			• 更新内容：
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例

Rocky Linux 8.5	*rockylinux_8_5_x64_20G_alibase_20220426.vhd*	2022-04-26	• 内核版本：4.18.0-348.20.1.el8_5.x86_64 • 更新内容：更新最新补丁包

Rocky Linux 8.5	*rockylinux_8_5_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：4.18.0-348.20.1.el8_5.x86_64
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2022-0847、CVE-2022-0492漏洞

版本	镜像ID	发布时间	发布内容
Rocky Linux 8.5	*rockylinux_8_5_x64_20G_alibase_20220214.vhd*	2022-02-14	• 内核版本：4.18.0-348.12.2.el8_5.x86_64 • 更新内容： ○ 更新最新软件包 ○ 修复CVE-2021-4034漏洞

历史版本更新记录，请参见Rocky Linux。

SUSE Linux Enterprise Server

阿里云提供的SUSE Linux Enterprise Server公共镜像均源自阿里云云市场。该类镜像在搭配不同实例规格时价格也不同，您可以访问以下不同版本的SUSE Linux Enterprise Server云市场镜像的详情页，以获取镜像的发布信息（镜像的适用地域、价格和使用指南等信息）。

> **说明** SUSE Linux Enterprise Server云市场镜像详情页提供的价格信息仅供参考，镜像实际价格请以资源购买页面的配置费用信息为准。

- SUSE Linux Enterprise Server 15 SP3
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP3

Ubuntu

版本	镜像ID	发布时间	发布内容
Ubuntu18.04	*ubuntu_18_04_x64_20G_alibase_20220629.vhd*	2022-06-29	• 内核版本：4.15.0-189-generic • 更新内容：更新最新补丁包 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡

版本	镜像ID	发布时间	发布内容

Ubuntu22.04	*ubuntu_22_04_x64_20G_alibase_20220628.vhd*	2022-06-28	• 首次发布Ubuntu 22.04 64位公共镜像
			• 内核版本：5.14.0-70.13.1.el9_0.x86_64
			• 更新内容：
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 支持非root用户登录实例
			  ○ 开启Kdump服务

Ubuntu20.04	*ubuntu_20_04_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：5.4.0-113-generic • 更新内容：更新最新补丁包
Ubuntu18.04	*ubuntu_18_04_x64_20G_alibase_20220524.vhd*	2022-05-24	• 内核版本：4.15.0-181-generic • 更新内容：更新最新补丁包
Ubuntu20.04	*ubuntu_20_04_x64_20G_alibase_20220428.vhd*	2022-04-28	• 内核版本：4.15.0-177-generic • 更新内容：更新最新补丁包
Ubuntu18.04	*ubuntu_18_04_x64_20G_alibase_20220428.vhd*	2022-04-28	• 内核版本：4.15.0-177-generic • 更新内容：更新最新补丁包

Ubuntu20.04	*ubuntu_20_04_x64_20G_alibase_20220331.vhd*	2022-03-31	• 内核版本：5.4.0-108-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2022-0492漏洞

Ubuntu18.04	*ubuntu_18_04_x64_20G_alibase_20220322.vhd*	2022-03-22	• 内核版本：4.15.0-173-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2022-0492漏洞

Ubuntu20.04	*ubuntu_20_04_x64_20G_alibase_20220215.vhd*	2022-02-15	• 内核版本：5.4.0-100-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 修复CVE-2021-4034漏洞

版本	镜像ID	发布时间	发布内容

Ubuntu18.04	*ubuntu_18_04_x64_20G_alibase_20220208.vhd*	2022-02-08	• 内核版本：4.15.0-169-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2021-4034漏洞

Ubuntu20.04	*ubuntu_20_04_x64_20G_alibase_20220110.vhd*	2022-01-10	• 内核版本：5.4.0-94-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 支持非root用户登录实例
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			• 适用地域：美国（弗吉尼亚）

历史版本更新记录，请参见Ubuntu。

ARM镜像

ARM镜像仅适用的实例规格族：ecs.g6r、ecs.c6r。

版本	镜像ID	发布时间	发布内容
Anolis OS 8.4 ANCK ARM版	*anolisos_8_4_arm64_20G_anck_alibase_20220519.vhd*	2022-05-19	• 更新龙蜥（Anolis）OS 8.4 ANCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.4 ARM64版本 • 内核版本：4.19.91-25.8.an8.aarch64 • 更新最新软件包
Anolis OS 8.4 RHCK ARM版	*anolisos_8_4_arm64_20G_rhck_alibase_20220519.vhd*	2022-05-19	• 更新龙蜥（Anolis）OS 8.4 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.4 ARM64版本 • 内核版本：4.18.0-348.23.1.an8_5.aarch64 • 更新最新软件包

版本	镜像ID	发布时间	发布内容
Anolis OS 7.9 RHCK ARM版	*anolisos_7_9_arm64_20G_rhck_alibase_20220518.vhd*	2022-05-18	• 更新龙蜥（Anolis）OS 7.9 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9 ARM版本 • 内核版本：4.18.0-193.28.1.an7.aarch64 • 更新最新软件包
Anolis OS 8.4 ANCK ARM版	*anolisos_8_4_arm64_20G_anck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 8.4 ANCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.4 ARM64版本 • 内核版本：4.19.91-25.8.an8.aarch64 • 更新最新软件包
Anolis OS 8.4 RHCK ARM版	*anolisos_8_4_arm64_20G_rhck_alibase_20220415.vhd*	2022-04-15	• 更新龙蜥（Anolis）OS 8.4 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.4 ARM64版本 • 内核版本：4.18.0-348.20.1.an8_5.aarch64 • 更新最新软件包
Anolis OS 8.2 ANCK ARM版	*anolisos_8_2_arm64_20G_anck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 8.2 ANCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.2 ARM版本 • 内核版本：4.19.91-25.8.an8.aarch64 • 更新最新软件包
Anolis OS 8.2 RHCK ARM版	*anolisos_8_2_arm64_20G_rhck_alibase_20220415.vhd*	2022-04-15	• 更新龙蜥（Anolis）OS 8.2 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 8.2 ARM版本 • 内核版本：4.18.0-348.20.1.an8_5.aarch64 • 更新最新软件包

版本	镜像ID	发布时间	发布内容
Anolis OS 7.9 RHCK ARM版	*anolisos_7_9_arm64_20G_rhck_alibase_20220413.vhd*	2022-04-13	• 更新龙蜥（Anolis）OS 7.9 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9 ARM版本 • 内核版本：4.18.0-193.28.1.an7.aarch64 • 更新最新软件包
Anolis OS 7.9 RHCK ARM版	*anolisos_7_9_arm64_20G_rhck_alibase_20220316.vhd*	2022-03-16	• 更新龙蜥（Anolis）OS 7.9 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9 ARM版本 • 内核版本：4.18.0-193.28.1.an7.aarch64 • 更新最新软件包
Anolis OS 7.9 ANCK ARM版	*anolisos_7_9_arm64_20G_anck_alibase_20220316.vhd*	2022-03-16	• 发布龙蜥（Anolis）OS 7.9 ANCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9 ARM版本 • 内核版本：4.19.91-25.7.an7.aarch64 • 更新最新软件包
Debian 11.2 ARM版	*debian_11_2_arm64_20G_alibase_20220308.vhd*	2022-03-08	• 发布Debian 11.2 ARM版镜像 • 内核版本：5.10.0-11-arm64 • 适用地域：华东1（杭州）、华北1（青岛）、华北6（乌兰察布）、西南1（成都）、中国（香港）、新加坡
Anolis OS 7.9 ANCK ARM版	*anolisos_7_9_arm64_20G_anck_alibase_20220111.vhd*	2022-01-11	• 发布龙蜥（Anolis）OS 7.9 ANCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9版本 • 内核版本：4.19.91-25.2.an7.aarch64
Anolis OS 7.9 RHCK ARM版	*anolisos_7_9_arm64_20G_rhck_alibase_20220110.vhd*	2022-01-10	• 更新龙蜥（Anolis）OS 7.9 RHCK ARM基础镜像。更多信息，请参见龙蜥（Anolis）OS • 兼容最新CentOS 7.9版本 • 内核版本：4.18.0-193.28.1.an7.aarch64

历史版本更新记录，请参见ARM镜像。

AMD镜像

历史版本更新记录，请参见AMD镜像。

UEFI镜像

UEFI镜像仅适用的实例规格族：ecs.g7、ecs.r7、ecs.c7、ecs.g7t、ecs.r7t、ecs.c7t。

版本	镜像ID	发布时间	发布内容
CentOS 8.4 UEFI版	*centos_8_4_uefi_x64_20G_scc_20220629.vhd*	2022-06-29	• 内核版本：4.18.0-305.3.1.el8.x86_64 • 更新内容： ○ 镜像基于 `centos_8_4_uefi_x64_20G_scc_20210727.vhd` 制作 ○ 新增以下配置，解决设备无空间的问题： ▪ soft nproc 65535 ▪ hard nproc 65535 ▪ hard memlock unlimited ▪ soft memlock unlimited ○ CentOS 8结束生命周期后，更新最新repo 源
CentOS 8.3 UEFI版	*centos_8_3_uefi_x64_20G_scc_20220629.vhd*	2022-06-29	• 内核版本：4.18.0-240.15.1.el8_3.x86_64 • 更新内容： ○ 镜像基于 `centos_8_3_uefi_x64_20G_scc_20210727.vhd` 制作 ○ 新增以下配置，解决设备无空间的问题： ▪ soft nproc 65535 ▪ hard nproc 65535 ▪ hard memlock unlimited ▪ soft memlock unlimited

版本	镜像ID	发布时间	发布内容

CentOS 7.9 UEFI版	*centos_7_9_uefi_x64_20G_scc_20220629.vhd*	2022-06-29	• 内核版本：3.10.0-1160.31.1.el7.x86_64
			• 更新内容：
			  ○ 镜像基于 `centos_7_9_uefi_x64_20G_scc_20210727.vhd` 制作
			  ○ 新增以下配置，解决设备无空间的问题：
			  ▪ soft nproc 65535
			  ▪ hard nproc 65535
			  ▪ hard memlock unlimited
			  ▪ soft memlock unlimited

CentOS 8.5 UEFI版	*centos_8_5_uefi_x64_20G_alibase_20220328.vhd*	2022-03-28	• 发布CentOS 8.5 64位UEFI版镜像 • 内核版本：4.18.0-348.7.1.el8_5.x86_64

Ubuntu 20.04 UEFI版	*ubuntu_20_04_uefi_x64_20G_alibase_20220324.vhd*	2022-03-24	• 内核版本：5.4.0-106-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
			  ○ 修复CVE-2021-4034、CVE-2022-0492漏洞

Anolis OS 8.4 RHCK UEFI版	*anolisos_8_4_x64_20G_rhck_uefi_alibase_20220328.vhd*	2022-03-28	• 发布Anolis OS 8.4 RHCK UEFI版本镜像
			• 内核版本：4.18.0-348.20.1.an8_5.x86_64
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 兼容最新CentOS 8.4 版本
			  ○ 启动切换为UEFI模式，而且仅支持该模式

版本	镜像ID	发布时间	发布内容

Anolis OS 8.4 ANCK UEFI版	*anolisos_8_4_x64_20G_anck_uefi_alibase_20220328.vhd*	2022-03-28	• 发布Anolis OS 8.4 ANCK UEFI版本镜像
			• 内核版本：4.19.91-25.7.an8.x86_64
			• 更新内容：
			  ○ 兼容最新CentOS 8.4 版本
			  ○ 启动切换为UEFI模式，而且仅支持该模式

Ubuntu 18.04 UEFI版	*ubuntu_18_04_uefi_x64_20G_alibase_20220330.vhd*	2022-03-30	• 内核版本：4.15.0-175-generic
			• 更新内容：
			  ○ 更新最新软件包
			  ○ 修复CVE-2021-4034、CVE-2022-0492漏洞

Debian 10.12 UEFI版	*debian_10_12_uefi_x64_20G_alibase_20220330.vhd*	2022-03-30	• 发布Debian 10.12 64位 UEFI版镜像 • 内核版本：4.19.0-20-amd64

历史版本更新记录，请参见UEFI镜像。

可信镜像

历史版本更新记录，请参见可信镜像。

Windows Server 2022

版本	镜像ID	发布时间	发布内容
Windows Server 2022 数据中心版	• 中文版：*win2022_21H2_x64_dtc_zh-cn_40G_alibase_20220616.vhd* • 英文版：*win2022_21H2_x64_dtc_en-us_40G_alibase_20220616.vhd*	2022-06-16	• 更新2022年06月份系统补丁：KB5014678、KB5013890 • 修复CVE-2022-30190、CVE-2022-30163、CVE-2022-30165、CVE-2022-30153等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）

版本	镜像ID	发布时间	发布内容
Windows Server 2022 数据中心版	• 中文版：*win2022_21H2_x64_dtc_zh-cn_40G_alibase_20220518.vhd* • 英文版：*win2022_21H2_x64_dtc_en-us_40G_alibase_20220518.vhd*	2022-05-18	• 更新2022年05月份系统补丁：KB5013944、KB5013630 • 修复CVE-2022-26937、CVE-2022-22017、CVE-2022-22012、CVE-2022-22019等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）
Windows Server 2022 数据中心版	• 中文版：*win2022_21H2_x64_dtc_zh-cn_40G_alibase_20220418.vhd* • 英文版：*win2022_21H2_x64_dtc_en-us_40G_alibase_20220418.vhd*	2022-04-18	• 更新2022年04月份系统补丁：KB5012604、KB5012123 • 修复CVE-2022-26809、CVE-2022-24491、CVE-2022-24500、CVE-2022-24541等漏洞
Windows Server 2022 数据中心版	• 中文版：*wincore_2022_x64_dtc_zh-cn_40G_alibase_20220311.vhd* • 英文版：*wincore_2022_x64_dtc_en-us_40G_alibase_20220311.vhd*	2022-03-11	• 新版本上线 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）
Windows Server 2022 数据中心版	• 中文版：*win2022_21H2_x64_dtc_zh-cn_40G_alibase_20220311.vhd* • 英文版：*win2022_21H2_x64_dtc_en-us_40G_alibase_20220311.vhd*	2022-03-11	• 新版本上线 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）

Windows Server 2019

版本	镜像ID	发布时间	发布内容
Windows Server 2019 with Container 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20220616.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_container_alibase_20220616.vhd*	2022-06-16	• 更新2022年06月份系统补丁：KB5014692、 KB5013888、KB5005112 • 修复CVE-2022-30190、CVE-2022-30163、CVE-2022-30136、CVE-2022-30165等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）

版本	镜像ID	发布时间	发布内容
Windows Server 2019 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_alibase_20220616.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_alibase_20220616.vhd*	2022-06-16	• 更新2022年06月份系统补丁：KB5014692、 KB5013888、KB5005112 • 修复CVE-2022-30190、CVE-2022-30163、CVE-2022-30136、CVE-2022-30165等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）
Windows Server 2019 with Container 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20220518.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_container_alibase_20220518.vhd*	2022-05-18	• 更新2022年05月份系统补丁：KB5013941、KB5013626、KB5005112 • 修复CVE-2022-26937、CVE-2022-22012、CVE-2022-22019等漏洞
Windows Server 2019 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_alibase_20220518.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_alibase_20220518.vhd*	2022-05-18	• 更新2022年05月份系统补丁：KB5013941、KB5013626、KB5005112 • 修复CVE-2022-26937、CVE-2022-22012、CVE-2022-22019等漏洞
Windows Server 2019 with Container 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20220418.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_container_alibase_20220418.vhd*	2022-04-18	• 更新2022年04月份系统补丁：KB5012647、KB5012119、KB5005112 • 修复CVE-2022-26809、CVE-2022-24491、CVE-2022-24541等漏洞
Windows Server 2019 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_alibase_20220418.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_alibase_20220418.vhd*	2022-04-18	• 更新2022年04月份系统补丁：KB5012647、KB5012119、KB5005112 • 修复CVE-2022-26809、CVE-2022-24491、CVE-2022-24541等漏洞
Windows Server 2019 with Container 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20220311.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_container_alibase_20220311.vhd*	2022-03-11	• 更新2022年03月份系统补丁：KB5011503、KB5009468 • 修复CVE-2022-21990、CVE-2022-23294、CVE-2022-24459等漏洞

版本	镜像ID	发布时间	发布内容
Windows Server 2019 数据中心版	• 中文版：*win2019_1809_x64_dtc_zh-cn_40G_alibase_20220311.vhd* • 英文版：*win2019_1809_x64_dtc_en-us_40G_alibase_20220311.vhd*	2022-03-11	• 更新2022年03月份系统补丁：KB5011503、KB5009468 • 修复CVE-2022-21990、CVE-2022-23294、CVE-2022-24459等漏洞

历史版本更新记录，请参见Windows Server 2019。

Windows Server 2016

版本	镜像ID	发布时间	发布内容
Windows Server 2016 数据中心版	• 中文版：*win2016_1607_x64_dtc_zh-cn_40G_alibase_20220616.vhd* • 英文版：*win2016_1607_x64_dtc_en-us_40G_alibase_20220616.vhd*	2022-06-16	• 更新2022年06月份系统补丁：KB5014702、 KB5014630、KB5014026 • 修复CVE-2022-30190、CVE-2022-30163、CVE-2022-30136、CVE-2022-30165等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）
Windows Server 2016 数据中心版	• 中文版：*win2016_1607_x64_dtc_zh-cn_40G_alibase_20220518.vhd* • 英文版：*win2016_1607_x64_dtc_en-us_40G_alibase_20220518.vhd*	2022-05-18	• 更新2022年05月份系统补丁：KB5013952、KB5013625、KB5014026 • 修复CVE-2022-26809、CVE-2022-22012、CVE-2022-22019等漏洞
Windows Server 2016 数据中心版	• 中文版：*win2016_1607_x64_dtc_zh-cn_40G_alibase_20220418.vhd* • 英文版：*win2016_1607_x64_dtc_en-us_40G_alibase_20220418.vhd*	2022-04-18	• 更新2022年04月份系统补丁：KB5012596、KB5012118、KB5011570 • 修复CVE-2022-26809、CVE-2022-24491、CVE-2022-24541等漏洞
Windows Server 2016 数据中心版	• 中文版：*win2016_1607_x64_dtc_zh-cn_40G_alibase_20220311.vhd* • 英文版：*win2016_1607_x64_dtc_en-us_40G_alibase_20220311.vhd*	2022-03-11	• 更新2022年03月份系统补丁：KB5011495、KB5010460、KB5011570 • 修复CVE-2022-21990、CVE-2022-23294、CVE-2022-24459等漏洞

历史版本更新记录，请参见Windows Server 2016。

Windows Server 2012

版本	镜像ID	发布时间	发布内容
Windows Server 2012 R2 数据中心版	• 中文版：*win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20220616.vhd* • 英文版：*win2012r2_9600_x64_dtc_en-us_40G_alibase_20220616.vhd*	2022-06-16	• 更新2022年06月份系统补丁：KB5014738、 KB5014633、KB5014025 • 修复CVE-2022-30190、CVE-2022-30163、CVE-2022-30136、CVE-2022-30165等漏洞 • 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、新加坡、美国（弗吉尼亚）
Windows Server 2012 R2 数据中心版	• 中文版：*win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20220518.vhd* • 英文版：*win2012r2_9600_x64_dtc_en-us_40G_alibase_20220518.vhd*	2022-05-18	• 更新2022年05月份系统补丁：KB5014011、KB5013631、KB5014025 • 修复CVE-2022-26937、CVE-2022-22012、CVE-2022-22019等漏洞
Windows Server 2012 R2 数据中心版	• 中文版：*win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20220418.vhd* • 英文版：*win2012r2_9600_x64_dtc_en-us_40G_alibase_20220418.vhd*	2022-04-18	• 更新2022年04月份系统补丁：KB5012670、KB5012124、KB5012672 • 修复CVE-2022-26809、CVE-2022-24491、CVE-2022-24541等漏洞
Windows Server 2012 R2 数据中心版	• 中文版：*win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20220311.vhd* • 英文版：*win2012r2_9600_x64_dtc_en-us_40G_alibase_20220311.vhd*	2022-03-11	• 更新2022年03月份系统补丁：KB5011564、KB5010462 • 修复CVE-2022-21990、CVE-2022-23294、CVE-2022-24459等漏洞

历史版本更新记录，请参见Windows Server 2012。

Windows Server 2008

历史版本更新记录，请参见Windows Server 2008。

Windows Server Version 2004

历史版本更新记录，请参见Windows Server Version 2004。

Windows Server Version 1909

历史版本更新记录，请参见Windows Server Version 1909。

Windows Server Version 1903

历史版本更新记录，请参见Windows Server Version 1903。

Windows Server Version 1809

历史版本更新记录，请参见Windows Server Version 1809。

4.3. 已知问题

本文介绍了不同发行平台的云服务器ECS镜像的已知问题、影响范围以及解决方法。

- Windows操作系统已知问题
  - Windows Server：2022年06月补丁导致Windows服务器网卡NAT、RRAS异常等问题
  - Windows Server：2022年01月补丁导致Windows域控服务器异常问题
  - 经典网络中Windows Server 2022镜像的实例无法自动激活问题
- Linux操作系统已知问题
  - Linux：部分高版本内核系统在部分实例规格上启动时可能出现Call Trace
  - Linux：高主频通用型实例规格族hfg6与部分Linux内核版本存在兼容性问题导致panic
  - Linux：pip操作时的超时问题
  - CentOS 8.0：公共镜像命名问题
  - CentOS 7：部分镜像ID变更可能引发的问题说明
  - CentOS 7：重启系统后主机名大写字母被修改
  - CentOS 6.8：装有NFS Client的实例异常崩溃的问题
  - Debian 9.6：经典网络配置问题
  - Fedora CoreOS：通过Fedora CoreOS自定义镜像创建的ECS实例中主机名不生效问题
  - OpenSUSE 15：内核升级可能导致启动hang的问题
  - Red Hat Enterprise Linux 8 64位：通过yum update命令更新内核版本不生效问题
  - SUSE Linux Enterprise Server：SMT Server连接失败问题
  - SUSE Linux Enterprise Server 12 SP5：内核升级可能导致启动hang的问题

Windows Server：2022年06月补丁导致Windows服务器网卡NAT、RRAS异常等问题

- 问题描述：根据微软官方2022年06月23日的公告，Windows终端在安装微软官方2022年06月的安全补丁后，会出现网络接口上启用了 NAT、RRAS服务器可能会失去连接、连接到服务器的设备也可能无法连接到Internet等风险。
- 影响范围：
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012

Windows Server 2012 R2和Windows Server 2012版本检查系统更新时，请务必选择①处的**检查更新**。①处连接的更新源为阿里云内部的Windows WSUS更新服务器，②处连接的更新源为微软官方的Internet Windows Update服务器。因为在特殊情况下，安全更新可能会带来潜在问题，为了预防发生此类情况，我们会检查收到的微软Windows安全更新，将通过检查的更新发布到内部WSUS更新服务器中。

- 解决方案：阿里云官方提供的WSUS服务中，已经将相关问题补丁剔除。为了确保您的操作系统不会受到相关影响，请您在Windows终端中检测是否已经安装了相关问题补丁。检测补丁的CMD命令如下，您需要根据不同的Windows Server版本运行匹配的检测命令。

```
Windows Server 2012 R2: wmic qfe get hotfixid | find "5014738"
Windows Server 2019: wmic qfe get hotfixid | find "5014692"
Windows Server 2016: wmic qfe get hotfixid | find "5014702"
Windows Server 2012: wmic qfe get hotfixid | find "5014747"
Windows Server 2022: wmic qfe get hotfixid | find "5014678"
```

如果检测结果中显示您已经安装了问题补丁，并且您的Windows服务器出现网卡NAT、RRAS异常等问题。建议您卸载相关问题补丁，以恢复终端至正常状态。卸载补丁的CMD命令如下，您需要根据不同的Windows Server版本运行匹配的卸载命令。

```
Windows Server 2012 R2: wusa /uninstall /kb:5014738
Windows Server 2019: wusa /uninstall /kb:5014692
Windows Server 2016: wusa /uninstall /kb:5014702
Windows Server 2012: wusa /uninstall /kb:5014747
Windows Server 2022: wusa /uninstall /kb:5014678
```

> **说明** 关于该问题的进一步更新以及操作指导，请以微软官方说明为准。更多信息，请参见RRAS Servers can lose connectivity if NAT is enabled on the public interface。

Windows Server：2022年01月补丁导致Windows域控服务器异常问题

- 问题描述：根据微软官方2022年01月13日的公告，Windows终端在安装微软官方2022年01月的安全补丁后，会出现域控服务器无法重启（或无限重启）问题、Hyper-V中的虚拟机（VM）可能无法启动、IPSec VPN连接可能失败等风险。
- 影响范围：
  - Windows Server 2022

- Windows Server, version 20H2
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Windows Server 2012 R2和Windows Server 2012版本检查系统更新时，请务必选择①处的**检查更新**。①处连接的更新源为阿里云内部的Windows WSUS更新服务器，②处连接的更新源为微软官方的Internet Windows Update服务器。因为在特殊情况下，安全更新可能会带来潜在问题，为了预防发生此类情况，我们会检查收到的微软Windows安全更新，将通过检查的更新发布到内部WSUS更新服务器中。

- 解决方案：阿里云官方提供的WSUS服务中，已经将相关问题补丁剔除。为了确保您的操作系统不会受到相关影响，请您在Windows终端中检测是否已经安装了相关问题补丁。检测补丁的CMD命令如下，您需要根据不同的Windows Server版本运行匹配的检测命令。

```
Windows Server 2012 R2: wmic qfe get hotfixid | find "5009624"
Windows Server 2019: wmic qfe get hotfixid | find "5009557"
Windows Server 2016: wmic qfe get hotfixid | find "5009546"
Windows Server 2012: wmic qfe get hotfixid | find "5009586"
Windows Server 2022: wmic qfe get hotfixid | find "5009555"
```

如果检测结果中显示您已经安装了问题补丁，并且您的Windows终端出现域控服务器无法使用或者虚拟机无法启动的问题。建议您卸载相关问题补丁，以恢复终端至正常状态。卸载补丁的CMD命令如下，您需要根据不同的Windows Server版本运行匹配的卸载命令。

```
Windows Server 2012 R2: wusa /uninstall /kb:5009624
Windows Server 2019: wusa /uninstall /kb:5009557
Windows Server 2016: wusa /uninstall /kb:5009546
Windows Server 2012: wusa /uninstall /kb:5009586
Windows Server 2022: wusa /uninstall /kb:5009555
```

> **说明** 关于该问题的进一步更新以及操作指导，请以微软官方说明为准。更多信息，请参见RRAS Servers can lose connectivity if NAT is enabled on the public interface。

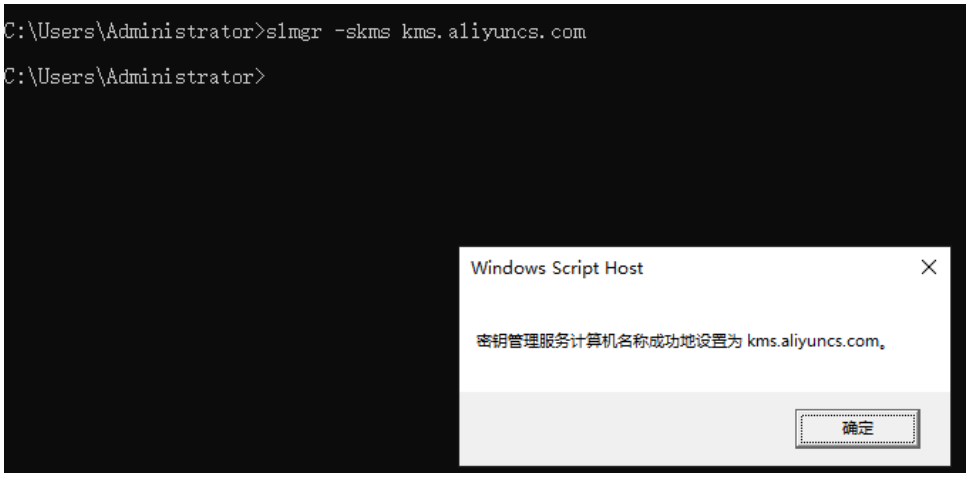
经典网络中Windows Server 2022镜像的实例无法自动激活问题

目前经典网络类型的Windows Server 2022镜像的实例无法实现自动激活，您需要按照如下操作完成激活。

1. 远程登录Windows实例。
   具体操作，请参见通过密码或密钥认证登录Windows实例。
2. 在Windows Server桌面，单击**开始** > **运行**，输入*cmd*，然后按回车键后进入命令行窗口。
3. 运行以下命令，配置KMS（Key Management Service）域名。

   ```
   slmgr -skms kms.aliyuncs.com
   ```

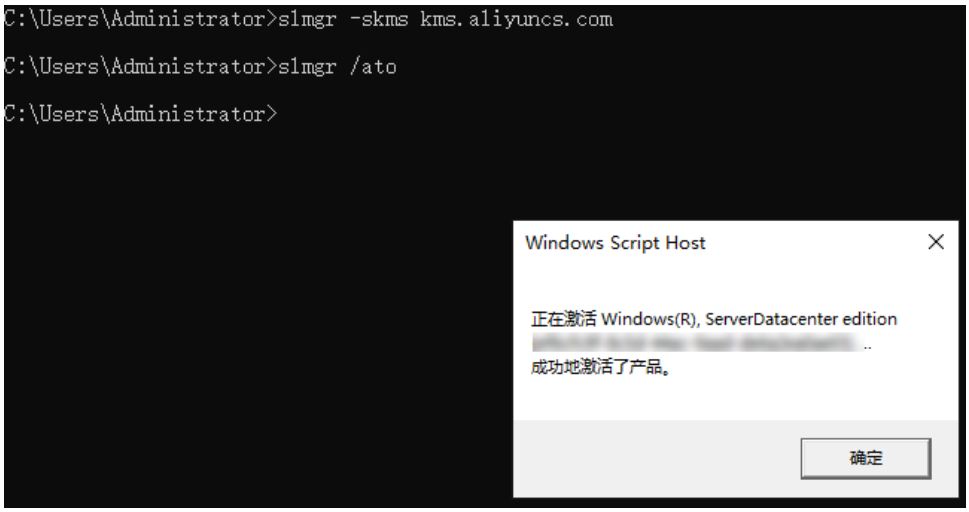
   系统显示类似如下，表示配置成功，然后单击**确定**。

4. 运行以下命令，激活KMS服务。

   ```
   slmgr /ato
   ```

   系统显示类似如下，表示激活成功，然后单击**确定**。

Linux：部分高版本内核系统在部分实例规格上启动时可能出现Call Trace

- 问题描述：部分高版本内核系统（例如 `4.18.0-240.1.1.el8_3.x86_64` 内核版本的RHEL 8.3、CentOS 8.3系统等），在部分实例规格（例如ecs.i2.4xlarge）上启动时可能出现如下所示的Call Trace：

```
Dec 28 17:43:45 localhost SELinux:  Initializing.
Dec 28 17:43:45 localhost kernel: Dentry cache hash table entries: 8388608 (order: 14, 67
108864 bytes)
Dec 28 17:43:45 localhost kernel: Inode-cache hash table entries: 4194304 (order: 13, 335
54432 bytes)
Dec 28 17:43:45 localhost kernel: Mount-cache hash table entries: 131072 (order: 8, 10485
76 bytes)
Dec 28 17:43:45 localhost kernel: Mountpoint-cache hash table entries: 131072 (order: 8,
1048576 bytes)
Dec 28 17:43:45 localhost kernel: unchecked MSR access error: WRMSR to 0x3a (tried to wri
te 0x000000000000****) at rIP: 0xffffffff8f26**** (native_write_msr+0x4/0x20)
Dec 28 17:43:45 localhost kernel: Call Trace:
Dec 28 17:43:45 localhost kernel:  init_ia32_feat_ctl+0x73/0x28b
Dec 28 17:43:45 localhost kernel:  init_intel+0xdf/0x400
Dec 28 17:43:45 localhost kernel:  identify_cpu+0x1f1/0x510
Dec 28 17:43:45 localhost kernel:  identify_boot_cpu+0xc/0x77
Dec 28 17:43:45 localhost kernel:  check_bugs+0x28/0xa9a
Dec 28 17:43:45 localhost kernel:  ? __slab_alloc+0x29/0x30
Dec 28 17:43:45 localhost kernel:  ? kmem_cache_alloc+0x1aa/0x1b0
Dec 28 17:43:45 localhost kernel:  start_kernel+0x4fa/0x53e
Dec 28 17:43:45 localhost kernel:  secondary_startup_64+0xb7/0xc0
Dec 28 17:43:45 localhost kernel: Last level iTLB entries: 4KB 64, 2MB 8, 4MB 8
Dec 28 17:43:45 localhost kernel: Last level dTLB entries: 4KB 64, 2MB 0, 4MB 0, 1GB 4
Dec 28 17:43:45 localhost kernel: FEATURE SPEC_CTRL Present
Dec 28 17:43:45 localhost kernel: FEATURE IBPB_SUPPORT Present
```

- 问题原因：这部分内核版本社区更新合入了尝试Write MSR的PATCH，但部分实例规格（例如ecs.i2.4xlarge）由于虚拟化版本不支持Write MSR，导致出现该Call Trace。
- 修复方案：该Call Trace不影响系统正常使用及稳定性，您可以忽略该报错。

Linux：高主频通用型实例规格族hfg6与部分Linux内核版本存在兼容性问题导致panic

- 问题描述：目前Linux社区的部分系统，例如CentOS 8、SUSE Linux Enterprise Server 15 SP2、OpenSUSE 15.2等系统。在高主频通用型实例规格族hfg6的实例中升级新版本内核可能出现内核错误（Kernel panic）。calltrace调试示例如下：

```
[    0.005000]  apic_timer_interrupt+0xf/0x20
[    0.005000]  </IRQ>
[    0.005000] RIP: 0010:smp_call_functi
[    0.005000] Code: 8b 4c 24 38 65 48 3
3 e2 01 75 f5 eb ca 8b 05 b1 37 c0 01 85
[    0.005000] RSP: 000 cfd80 EFLAGS: 00 ORIG_RAX: fff
[    0.005000] RAX: 000 RBX: fff RCX: 00000000
[    0.005000] RDX: 000 RSI: 000 RDI: 00000000
[    0.005000] RBP: fff R08: 000 R09: 00000000
[    0.005000] R10: fff R11: 000 R12: 00000000
[    0.005000] R13: fff R14: 000 R15: ffffffff
[    0.005000]  ? sort_range+0x20/0x20
[    0.005000]  ? poke_int3_handler+0xe0/0xe0
[    0.005000]  ? poke_int3_handler+0xe0/0xe0
[    0.005000]  ? poke_int3_handler+0xe0/0xe0
[    0.005000]  on_each_cpu+0x28/0x60
[    0.005000]  text_poke_bp_batch+0xcd/0x160
[    0.005000]  ? set_rq_offline+0x60/0x60
[    0.005000]  arch_jump_label_transform_apply+0x2e/0x50
[    0.005000]  static_key_slow_inc_cpuslocked+0x88/0x90
[    0.005000]  sched_cpu_activate+0xf1/0x100
[    0.005000]  ? refresh_zone_stat_thresholds+0x140/0x140
[    0.005000]  cpuhp_invoke_callback+0x8d/0x500
[    0.005000]  ? sort_range+0x20/0x20
[    0.005000]  cpuhp_thread_fun+0xb0/0x110
[    0.005000]  smpboot_thread_fn+0xc5/0x160
[    0.005000]  kthread+0x112/0x130
[    0.005000]  ? kthread_flush_work_fn+0x10/0x10
[    0.005000]  ret_from_fork+0x35/0x40
[    0.005000] Modules linked in:
[    0.005000] ---[ end trace 79c5ba462cfc4c1b ]---
[    0.005000] RIP: 0010:arch_scale_freq_tick+0x67/0x7e
```

- 问题原因：高主频通用型实例规格族hfg6与部分Linux内核版本存在兼容性问题。
- 修复方案：
  - SUSE Linux Enterprise Server 15 SP2和OpenSUSE 15.2系统目前最新版内核已经修复。变更提交（commit）内容如下，如果您升级的最新版内核包含此内容，则已兼容实例规格族hfg6。

```
commit 1e33d5975b49472e286bd7002ad0f689af33fab8
Author: Giovanni Gherdovich <ggherdovich@suse.cz>
Date:   Thu Sep 24 16:51:09 2020 +0200
    x86, sched: Bail out of frequency invariance if
    turbo_freq/base_freq gives 0 (bsc#1176925).
    suse-commit: a66109f44265ff3f3278fb34646152bc2b3224a5
commit dafb858aa4c0e6b0ce6a7ebec5e206f4b3cfc11c
Author: Giovanni Gherdovich <ggherdovich@suse.cz>
Date:   Thu Sep 24 16:16:50 2020 +0200
    x86, sched: Bail out of frequency invariance if turbo frequency
    is unknown (bsc#1176925).
    suse-commit: 53cd83ab2b10e7a524cb5a287cd61f38ce06aab7
commit 22d60a7b159c7851c33c45ada126be8139d68b87
Author: Giovanni Gherdovich <ggherdovich@suse.cz>
Date:   Thu Sep 24 16:10:30 2020 +0200
    x86, sched: check for counters overflow in frequency invariant
    accounting (bsc#1176925).
```

  - CentOS 8系统如果使用命令**yum update**升级到最新内核版本 `kernel-4.18.0-240` 及以上，在高主频通用型实例规格族hfg6的实例中，可能出现Kernel panic。如果发生该问题，请回退至上一个内核版本。

Linux：pip操作时的超时问题

- 问题描述：pip请求偶有超时或失败现象。
- 涉及镜像：CentOS、Debian、Ubuntu、SUSE、OpenSUSE、Alibaba Cloud Linux。
- 原因分析：阿里云提供了以下三个pip源地址。其中，默认访问地址为mirrors.aliyun.com，访问该地址的实例需能访问公网。当您的实例未分配公网IP时，会出现pip请求超时故障。
  - （默认）公网：mirrors.aliyun.com
  - 专有网络VPC内网：mirrors.cloud.aliyuncs.com
  - 经典网络内网：mirrors.aliyuncs.com
- 修复方案：您可采用以下任一方法解决该问题。
  - 方法一
    为您的实例分配公网IP，即为实例绑定一个弹性公网IP（EIP）。具体操作，请参见绑定ECS实例。
    包年包月实例还可通过升降配重新分配公网IP。具体操作，请参见包年包月实例升配规格。

- 方法二
  一旦出现pip响应延迟的情况，您可在ECS实例中运行脚本*fix_pypi.sh*，然后再重试pip操作。具体步骤如下：
  a. 远程连接实例。
     具体操作，请参见通过密码认证登录Linux实例。
  b. 运行以下命令获取脚本文件。
     ```
     wget http://image-offline.oss-cn-hangzhou.aliyuncs.com/fix/fix_pypi.sh
     ```
  c. 运行脚本。
     - 专有网络VPC实例：运行命令 `bash fix_pypi.sh "mirrors.cloud.aliyuncs.com"` 。
     - 经典网络实例：运行命令 `bash fix_pypi.sh "mirrors.aliyuncs.com"` 。
  d. 重试pip操作。

  *fix_pypi.sh*脚本内容如下：
  ```
  #!/bin/bash
  function config_pip() {
      pypi_source=$1
      if [[ ! -f ~/.pydistutils.cfg ]]; then
  cat > ~/.pydistutils.cfg << EOF
  [easy_install]
  index-url=http://$pypi_source/pypi/simple/
  EOF
      else
          sed -i "s#index-url.*#index-url=http://$pypi_source/pypi/simple/#" ~/.pydistuti
  ls.cfg
      fi
      if [[ ! -f ~/.pip/pip.conf ]]; then
      mkdir -p ~/.pip
  cat > ~/.pip/pip.conf << EOF
  [global]
  index-url=http://$pypi_source/pypi/simple/
  [install]
  trusted-host=$pypi_source
  EOF
      else
          sed -i "s#index-url.*#index-url=http://$pypi_source/pypi/simple/#" ~/.pip/pip.c
  onf
          sed -i "s#trusted-host.*#trusted-host=$pypi_source#" ~/.pip/pip.conf
      fi
  }
  config_pip $1
  ```

CentOS 8.0：公共镜像命名问题

- 问题描述：使用centos_8_0_x64_20G_alibase_20200218.vhd公共镜像创建了CentOS系统实例，远程连接实例后检查系统版本，您发现实际为CentOS 8.1。

```
root@ecshost:~$ lsb_release -a
LSB Version:    :core-4.1-amd64:core-4.1-noarch
Distributor ID:    CentOS
Description:    CentOS Linux release 8.1.1911 (Core)
Release:    8.1.1911
Codename:    Core
```

- 问题原因：该镜像出现在公共镜像列表中，已更新最新社区更新包，同时也升级了版本到8.1，所以实际版本是8.1。

- 涉及镜像ID：centos_8_0_x64_20G_alibase_20200218.vhd。
- 修复方案：如果您需要使用CentOS 8.0的系统版本，可以通过RunInstances等接口，设置 `ImageId=centos_8_0_x64_20G_alibase_20191225.vhd` 创建ECS实例。

CentOS 7：部分镜像ID变更可能引发的问题说明

- 问题描述：部分CentOS 7公共镜像更新了镜像ID，可能会影响到您自动化运维过程中获取镜像ID的策略。
- 涉及镜像：CentOS 7.5、CentOS 7.6
- 原因分析：CentOS 7.5和CentOS 7.6公共镜像在最新版本中使用的镜像ID格式为 `%OS类型%_%大版本号%_%小版本号%_%特殊字段%_alibase_%日期%.%格式%` 。例如，CentOS 7.5的镜像ID前缀由原 `centos_7_05_64` 更新为 `centos_7_5_x64` 。您需要根据镜像ID的变更自行调整可能受影响的自动化运维策略。关于镜像ID的更多信息，请参见2022年。

CentOS 7：重启系统后主机名大写字母被修改

- 问题描述：第一次重启ECS实例后，部分CentOS 7实例的主机名（hostname）存在大写字母变成小写字母的现象，如下表所示。

实例hostname示例	第一次重启后示例	后续是否保持小写不变
iZm5e1qe*****sxx1ps5zX	izm5e1qe*****sxx1ps5zx	是
ZZHost	zzhost	是
NetworkNode	networknode	是

- 涉及镜像：以下CentOS公共镜像，和基于以下公共镜像创建的自定义镜像。
  - centos_7_2_64_40G_base_20170222.vhd
  - centos_7_3_64_40G_base_20170322.vhd
  - centos_7_03_64_40G_alibase_20170503.vhd
  - centos_7_03_64_40G_alibase_20170523.vhd
  - centos_7_03_64_40G_alibase_20170625.vhd
  - centos_7_03_64_40G_alibase_20170710.vhd

- centos_7_02_64_20G_alibase_20170818.vhd
- centos_7_03_64_20G_alibase_20170818.vhd
- centos_7_04_64_20G_alibase_201701015.vhd

- 涉及Hostname类型：如果您的应用有hostname大小写敏感现象，重启实例后会影响业务。您可根据下面的修复方案修复以下类型的hostname。

hostname类型	是否受影响	何时受影响	是否继续阅读文档
在控制台或通过API创建实例时，hostname中有大写字母	是	第一次重启实例	是
在控制台或通过API创建实例时，hostname中全是小写字母	否	不适用	否
hostname中有大写字母，您登录实例后自行修改了hostname	否	不适用	是

- 修复方案：如果重启实例后需要保留带大写字母的hostname时，可按如下步骤操作。
  i. 远程连接实例。
     具体操作，请参见连接方式介绍。
  ii. 查看现有的hostname。

```
[root@izbp193*****3i161uynzzx ~]# hostname
izbp193*****3i161uynzzx
```

  iii. 运行以下命令固化hostname。

```
hostnamectl set-hostname --static iZbp193*****3i161uynzzX
```

  iv. 运行以下命令查看更新后的hostname。

```
[root@izbp193*****3i161uynzzx ~]# hostname
iZbp193*****3i161uynzzX
```

- 下一步：如果您使用的是自定义镜像，请更新cloud-init软件至最新版本后，再次创建自定义镜像。避免使用存在该问题的自定义镜像创建新实例后发生同样的问题。更多信息，请参见安装cloud-init和使用实例创建自定义镜像。

CentOS 6.8：装有NFS Client的实例异常崩溃的问题

- 问题描述：加载了NFS客户端（NFS Client）的CentOS 6.8实例出现超长等待状态，只能通过重启实例解决该问题。
- 问题原因：在2.6.32-696~2.6.32-696.10的内核版本上使用NFS服务时，如果通信延迟出现毛刺（glitch，电子脉冲），内核nfsclient会主动断开TCP连接。若NFS服务端（Server）响应慢，nfsclient发起的连接可能会卡顿在FIN_WAIT2状态。正常情况下，FIN_WAIT2状态的连接默认在一分钟后超时并被回收，nfsclient可以发起重连。但是，由于此类内核版本的TCP实现有缺陷，FIN_WAIT2状态的连接永远不会超时，因此nfsclient的TCP连接永远无法关闭，无法发起新的连接，造成用户请求卡死（hang死），永远无法恢复，只能通过重启ECS实例进行修复。
- 涉及镜像ID：centos_6_08_32_40G_alibase_20170710.vhd和centos_6_08_64_20G_alibase_20170824.vhd。
- 修复方案：您可以运行**yum update**命令升级系统内核至2.6.32-696.11及以上版本。

> **注意** 操作实例时，请确保您已经提前创建了快照备份数据。具体操作，请参见创建一个云盘快照。

Debian 9.6：经典网络配置问题

- 问题描述：无法Ping通使用Debian 9公共镜像创建的经典网络类型实例。
- 问题原因：因为Debian系统默认禁用了systemd-networkd服务，经典网络类型实例无法通过DHCP（Dynamic Host Configuration Protocol）模式自动分配IP。
- 涉及镜像ID：debian_9_06_64_20G_alibase_20181212.vhd。
- 修复方案：您需要依次运行下列命令解决该问题。

```
systemctl enable systemd-networkd
```

```
systemctl start systemd-networkd
```

Fedora CoreOS：通过Fedora CoreOS自定义镜像创建的ECS实例中主机名不生效问题

- 问题描述：当您选择Fedora CoreOS镜像创建了一台ECS实例A，通过实例A创建了一个自定义镜像，然后通过该自定义镜像新建了一台ECS实例B时，您为实例B设置的主机名不生效（登录实例B查看实例B的主机名与实例A的主机名相同）。
  例如，您有一台Fedora CoreOS操作系统的ECS实例（`实例A`），主机名为`test001`，然后您使用该实例对应的自定义镜像新建了一台ECS实例（`实例B`），并且在创建实例的过程中，将`实例B`的主机名设置为了`test002`。当您成功创建并远程连接`实例B`后，`实例B`的主机名仍然为`test001`。
- 问题原因：阿里云公共镜像提供的Fedora CoreOS镜像采用操作系统官方的Ignition服务进行实例初始化配置。Ignition服务是指Fedora CoreOS与Red Hat Enterprise Linux CoreOS在系统启动时进入initramfs期间用来操作磁盘的程序。ECS实例在首次启动时，Ignition中的`coreos-ignition-firstboot-complete.service`会根据*/boot/ignition.firstboot*文件（该文件为空文件）是否存在，判断是否进行实例的初始化配置。如果文件存在则进行初始化配置（其中包括配置主机名），并删除*/boot/ignition.firstboot*文件。由于创建Fedora CoreOS实例后至少启动了一次，则对应自定义镜像中*/boot/ignition.firstboot*文件已被删除。当您使用该自定义镜像新建ECS实例时，实例首次启动并不会进行初始化配置，对应的主机名称也不会发生变化。
- 修复方案：

> **说明** 为确保实例中数据安全，建议您在操作前先为实例创建快照。如果实例发生数据异常，可通过快照回滚云盘至正常状态。具体操作，请参见创建一个云盘快照。

当您基于Fedora CoreOS实例创建自定义镜像前，先使用`root`权限（管理员权限）在*/boot*目录下创建*/ignition.firstboot*文件。命令行操作说明如下：

i. 以读写方式重新挂载*/boot*。

```
sudo mount /boot -o rw,remount
```

ii. 创建*/ignition.firstboot*文件。

```
sudo touch /boot/ignition.firstboot
```

iii. 以只读方式重新挂载*/boot*。

```
sudo mount /boot -o ro,remount
```

关于Ignition相关的配置说明，请参见Ignition配置说明参考。

OpenSUSE 15：内核升级可能导致启动hang的问题

- 问题描述：OpenSUSE内核版本升级到 `4.12.14-lp151.28.52-default` 后，实例可能在某些CPU规格上启动hang，现已知的CPU规格为 `Intel® Xeon® CPU E5-2682 v4 @ 2.50GHz` 。对应的calltrace调试结果如下：

```
[    0.901281] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[    0.901281] CR2: ffffc90000d68000 CR3: 000000000200a001 CR4: 00000000003606e0
[    0.901281] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[    0.901281] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[    0.901281] Call Trace:
[    0.901281]  cpuidle_enter_state+0x6f/0x2e0
[    0.901281]  do_idle+0x183/0x1e0
[    0.901281]  cpu_startup_entry+0x5d/0x60
[    0.901281]  start_secondary+0x1b0/0x200
[    0.901281]  secondary_startup_64+0xa5/0xb0
[    0.901281] Code: 6c 01 00 0f ae 38 0f ae f0 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00
00 00 90 31 d2 65 48 8b 34 25 40 6c 01 00 48 89 d1 48 89 f0 <0f> 01 c8 0f 1f 84 00 00 00
00 00 0f 1f 84 00 00 00 00 00 ** **
```

- 问题原因：新内核版本与CPU Microcode不兼容，更多信息，请参见启动hang问题。
- 涉及镜像：opensuse_15_1_x64_20G_alibase_20200520.vhd。
- 修复方案：在*/boot/grub2/grub.cfg*文件中，以 `linux` 开头一行中增加内核参数 `idle=nomwait` 。文件修改的示例内容如下：

```
menuentry 'openSUSE Leap 15.1'  --class opensuse --class gnu-linux --class gnu --class os
$menuentry_id_option 'gnulinux-simple-20f5f35a-fbab-4c9c-8532-bb6c66ce****' {
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  20f5f35a-fbab-4c9c
-8532-bb6c66ce****
        else
          search --no-floppy --fs-uuid --set=root 20f5f35a-fbab-4c9c-8532-bb6c66ce****
        fi
        echo    'Loading Linux 4.12.14-lp151.28.52-default ...'
        linux   /boot/vmlinuz-4.12.14-lp151.28.52-default root=UUID=20f5f35a-fbab-4c9c-85
32-bb6c66ce****  net.ifnames=0 console=tty0 console=ttyS0,115200n8 splash=silent mitigati
ons=auto quiet idle=nomwait
        echo    'Loading initial ramdisk ...'
        initrd  /boot/initrd-4.12.14-lp151.28.52-default
}
```

Red Hat Enterprise Linux 8 64位：通过yum update命令更新内核版本不生效问题

- 问题描述：在Red Hat Enterprise Linux 8 64位操作系统的ECS实例中，运行**yum update**更新内核版本并重启实例后，发现内核版本仍为旧的内核版本。
- 问题原因：RHEL 8 64位操作系统中存储GRUB2环境变量的文件*/boot/grub2/grubenv*大小异常，该文件大小不是标准的1024字节，从而导致更新内核版本失败。
- 修复方案：您需要在更新内核版本后，将新的内核版本设置为默认启动版本。完整的操作说明如下所述：
  i. 运行以下命令，更新内核版本。
  ```
  yum update kernel -y
  ```
  ii. 运行以下命令，获取当前操作系统的内核启动参数。
  ```
  grub2-editenv list | grep kernelopts
  ```
  iii. 运行以下命令，备份旧的*/grubenv*文件。
  ```
  mv /boot/grub2/grubenv /home/grubenv.bak
  ```
  iv. 运行以下命令，生成一个新的*/grubenv*文件。
  ```
  grub2-editenv /boot/grub2/grubenv create
  ```
  v. 运行以下命令，把新的内核版本设置为默认启动版本。
  本示例中，更新后新的内核版本以 `/boot/vmlinuz-4.18.0-305.19.1.el8_4.x86_64` 为例。
  ```
  grubby --set-default /boot/vmlinuz-4.18.0-305.19.1.el8_4.x86_64
  ```
  vi. 运行以下命令，设置内核启动参数。
  其中，参数 `- set kernelopts` 需要手动设置，取值为步骤2中获取到的当前操作系统内核启动参数信息。
  ```
  grub2-editenv - set kernelopts="root=UUID=0dd6268d-9bde-40e1-b010-0d3574b4**** ro cra
  shkernel=auto net.ifnames=0 vga=792 console=tty0 console=ttyS0,115200n8 noibrs nosmt"
  ```
  vii. 运行以下命令，重启ECS实例至新的内核版本。
  ```
  reboot
  ```

SUSE Linux Enterprise Server：SMT Server连接失败问题

- 问题描述：您购买并使用阿里云付费镜像SUSE Linux Enterprise Server或SUSE Linux Enterprise Server for SAP时，会遇到SMT Server连接超时或异常的情况。当您尝试下载或更新组件时，返回类似于如下所示的报错信息：
  - `Registration server returned 'This server could not verify that you are authorized to access this service.' (500)`
  - `Problem retrieving the respository index file for service 'SMT-http_mirrors_cloud_aliyuncs_com' location ****`
- 涉及镜像：SUSE Linux Enterprise Server、SUSE Linux Enterprise Server for SAP
- 解决方案：您需要重新注册并激活SMT服务。
  i. 依次运行以下命令，重新注册并激活SMT服务。

```
SUSEConnect -d
SUSEConnect --cleanup
systemctl restart guestregister
```

ii. 运行以下命令，验证SMT服务的激活状态。

```
SUSEConnect -s
```

命令行返回示例如下，表示成功激活SMT服务。

```
[{"identifier":"SLES_SAP","version":"12.5","arch":"x86_64","status":"Registered"}]
```

SUSE Linux Enterprise Server 12 SP5：内核升级可能导致启动hang的问题

- 问题描述：SLES（SUSE Linux Enterprise Server）12 SP5之前的内核版本在升级至SLES 12 SP5，或SLES 12 SP5内部内核版本升级后，实例可能在某些CPU规格上启动hang。现已知的CPU规格为 `Intel® Xeon® CPU E5-2682 v4 @ 2.50GHz` 与 `Intel® Xeon® CPU E7-8880 v4 @ 2.20GHz` 。对应的calltrace调试结果如下：

```
[    0.901281] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[    0.901281] CR2: ffffc90000d68000 CR3: 000000000200a001 CR4: 00000000003606e0
[    0.901281] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[    0.901281] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[    0.901281] Call Trace:
[    0.901281]  cpuidle_enter_state+0x6f/0x2e0
[    0.901281]  do_idle+0x183/0x1e0
[    0.901281]  cpu_startup_entry+0x5d/0x60
[    0.901281]  start_secondary+0x1b0/0x200
[    0.901281]  secondary_startup_64+0xa5/0xb0
[    0.901281] Code: 6c 01 00 0f ae 38 0f ae f0 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00
00 00 90 31 d2 65 48 8b 34 25 40 6c 01 00 48 89 d1 48 89 f0 <0f> 01 c8 0f 1f 84 00 00 00
00 00 0f 1f 84 00 00 00 00 00 ** **
```

- 问题原因：新内核版本与CPU Microcode不兼容。
- 修复方案：在 `/boot/grub2/grub.cfg` 文件中，以 `linux` 开头一行中增加内核参数 `idle=nomwait` 。文件修改的示例内容如下：

```
menuentry 'SLES 12-SP5'  --class sles --class gnu-linux --class gnu --class os $menuentry
_id_option 'gnulinux-simple-fd7bda55-42d3-4fe9-a2b0-45efdced****' {
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd7bda55-42d3-4fe9
-a2b0-45efdced****
        else
          search --no-floppy --fs-uuid --set=root fd7bda55-42d3-4fe9-a2b0-45efdced****
        fi
        echo    'Loading Linux 4.12.14-122.26-default ...'
        linux   /boot/vmlinuz-4.12.14-122.26-default root=UUID=fd7bda55-42d3-4fe9-a2b0-45
efdced****  net.ifnames=0 console=tty0 console=ttyS0,115200n8 mitigations=auto splash=sil
ent quiet showopts idle=nomwait
        echo    'Loading initial ramdisk ...'
        initrd  /boot/initrd-4.12.14-122.26-default
}
```

5.Alibaba Cloud Linux

5.1. Alibaba Cloud Linux概述

Alibaba Cloud Linux是阿里云基于龙蜥社区（OpenAnolis）的龙蜥操作系统（Anolis OS）打造的操作系统发行版，在全面兼容RHEL/CentOS生态的同时，为云上应用程序提供安全、稳定、高性能的定制化运行环境，并针对云基础设施进行了深度优化，为您打造更好的云上操作系统体验。目前发行版本为Alibaba Cloud Linux 2与Alibaba Cloud Linux 3。
更多信息，请访问Alibaba Cloud Linux产品页。

适用范围

Alibaba Cloud Linux适用范围说明如下：

- 适用于多种实例规格族，包括弹性裸金属服务器。更多信息，请参见实例规格族。
  - 支持的实例vCPU范围为1 vCPU~768 vCPU。
  - 支持的实例内存范围为0.5 GiB~12288 GiB。
  - 不支持非I/O优化实例。
- 适用于各种云场景工作负载。例如数据库、云原生容器、数据分析、Web应用程序，以及生产环境中的其他工作负载。

费用

Alibaba Cloud Linux是免费镜像，但当您选用Alibaba Cloud Linux镜像创建ECS实例时，需要支付其他资源产生的费用，如vCPU、内存、存储、公网带宽和快照等。计费详情，请参见计费概述。

优势

与其他Linux系统相比，Alibaba Cloud Linux具有以下优势：

- 阿里云官方为Alibaba Cloud Linux提供长期免费的软件维护和技术支持。各版本生命周期请参见Alibaba Cloud Linux EOL计划。
- 与阿里云基础设施深度结合优化，持续提升系统的启动速度、运行时的性能。同时经过海量阿里巴巴和阿里云的产品打磨，提供优良的稳定性体验。
- 通过更新的Linux内核、用户态软件及工具包，为云上应用程序环境提供Linux社区的最新操作系统增强功能：
  - Alibaba Cloud Linux 3选择Linux kernel 5.10 LTS，同时默认搭载GCC 10.2、binutils 2.35、glibc 2.32等基础软件。
  - Alibaba Cloud Linux 2选择Linux kernel 4.19 LTS，同时提供GCC-7.3.1/8.2.1/9.1.1的devtoolset支持。devtoolset相关使用说明，请参见使用试验性支持的软件包。
- 兼容CentOS/RHEL生态，CentOS/RHEL中的大多数软件无需或仅需少量改造即可在Alibaba Cloud Linux中运行。
  - Alibaba Cloud Linux 3基于Anolis OS 8打造，兼容CentOS 8、RHEL 8生态。
  - Alibaba Cloud Linux 2基于Aonlis OS 7打造，兼容CentOS 7、RHEL 7生态。
- 提供安全漏洞监控与修复策略，持续保证系统安全。更多信息，请参见安全更新。

Alibaba Cloud Linux特性

- 默认搭载并启用阿里云云内核：

- Alibaba Cloud Linux2基于Linux kernel 4.19 LTS定制而成；Alibaba Cloud Linux 3基于Linux kernel 5.10 LTS定制而成。系统在持续增加适用于云场景的新特性的同时，持续改进内核性能并修复重大缺陷。更多信息，请参见Alibaba Cloud Linux 2镜像发布记录和Alibaba Cloud Linux 3镜像发布记录。
- 提供针对ECS实例环境定制优化的内核启动参数和系统配置参数。
- 提供操作系统崩溃后的内核转储（Kdump）能力，您可根据需要在线打开或者关闭该功能，无需重启操作系统。
- 提供内核热补丁升级（Live Patch）能力。 更多信息，请参见内核热补丁概述。

- 软件包预装和更新说明。
  - 用户态软件包保持与新版CentOS兼容。CentOS 7版本用户态软件包可直接在Alibaba Cloud Linux 2使用；CentOS 8版本用户态软件包可直接在Alibaba Cloud Linux 3使用。
  - 默认搭载阿里云CLI。
  - 软件包安全漏洞（CVE）修复在Alibaba Cloud Linux版本支持期限内会持续更新。更多信息，请参见Alibaba Cloud Linux 2安全公告和Alibaba Cloud Linux 3安全公告。Alibaba Cloud Linux提供自动化修复方案。具体操作，请参见基于YUM的安全更新操作（Alibaba Cloud Linux 2）。
- 大幅优化开机启动速度，提升运行时的系统性能，并增强系统稳定性。
  - 针对ECS实例环境大幅优化启动速度，在实际测试中，相比其他操作系统约减少60%的启动时间。
  - 优化调度、内存以及IO等子系统，在部分的开源基准测试（benchmark）中，相比其他操作系统约提升10%~30%性能。
  - 持续增强系统稳定性，在宕机数据统计结果中，相比其他操作系统减少约50%的宕机率。

Alibaba Cloud Linux镜像

发行版	镜像名称	最新版本镜像ID	镜像说明
	Alibaba Cloud Linux 3.2104 64位	*aliyun_3_x64_20G_alibase_20210910.vhd*	支持x86架构的默认标准镜像。

发行版	镜像名称	最新版本镜像ID	镜像说明
Alibaba Cloud Linux 3	Alibaba Cloud Linux 3.2104 64位 快速启动版	*aliyun_3_x64_20G_qboot_alibase_20211214.vhd*	该镜像支持Qboot（quick boot）快速启动，基于Alibaba Cloud Kernel，并直接从内核引导虚拟机启动的定制化镜像。使用该镜像创建的ECS实例相比其它镜像创建的ECS实例，启动速度得到了极大的提升，并且默认运行时与标准镜像完全一致。快速启动版镜像的相关说明如下： • 只对实例的初次启动加速，后续启动实例的速度将保持正常水准。 • 优化加速内存初始化的过程，模块化了启动耗时的鼠标等设备，加速内核引导速度。 • 使用最新的AliyunInit服务替代了CloudInit服务，降低了操作系统的初始化耗时。 • 该镜像的内核版本无法修改内核启动参数。 • 不支持的实例规格族：GPU计算型、GPU虚拟化型、FPGA计算型、NPU计算型、异构服务型、超级计算集群（SCC）、安全增强型等。
	Alibaba Cloud Linux 3.2104 64位 UEFI版	*aliyun_3_x64_20G_uefi_alibase_20210910.vhd*	基于x86架构默认标准镜像开发，仅支持UEFI启动模式。
	Alibaba Cloud Linux 3.2104 64位 ARM版	*aliyun_3_arm64_20G_alibase_20210910.vhd*	支持ARM架构的默认标准镜像。
	Alibaba Cloud Linux 3.2104 64位 SCC版	*aliyun_3_x64_20G_scc_alibase_20211018.vhd*	基于x86架构默认标准镜像开发，支持阿里云SCC实例的镜像版本，仅支持UEFI启动模式。
	Alibaba Cloud Linux 2.1903 LTS 64位	*aliyun_2_1903_x64_20G_alibase_20210726.vhd*	支持x86架构的默认标准镜像。

发行版	镜像名称	最新版本镜像ID	镜像说明
Alibaba Cloud Linux 2	Alibaba Cloud Linux 2.1903 LTS 64位 快速启动版	*aliyun_2_1903_x64_20G_qboot_alibase_20210726.vhd*	该镜像支持Qboot（quick boot）快速启动，基于Alibaba Cloud Kernel，并直接从内核引导虚拟机启动的定制化镜像。使用该镜像创建的ECS实例相比其它镜像创建的ECS实例，启动速度得到了极大的提升，并且默认运行时与标准镜像完全一致。快速启动版镜像的相关说明如下： • 只对实例的初次启动加速，后续启动实例的速度将保持正常水准。 • 优化加速内存初始化的过程，模块化了启动耗时的鼠标等设备，加速内核引导速度。 • 使用最新的AliyunInit服务替代了CloudInit服务，降低了操作系统的初始化耗时。 • 该镜像的内核版本无法修改内核启动参数。 • 不支持的实例规格族：GPU计算型、GPU虚拟化型、FPGA计算型、NPU计算型、异构服务型、超级计算集群（SCC）、安全增强型等。
	Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版	*aliyun_2_1903_x64_20G_dengbao_alibase_20210726.vhd*	基于x86架构默认标准镜像进行等保加固的镜像版本，该镜像符合等保2.0三级安全保护的基本要求。使用说明请参见Alibaba Cloud Linux等保2.0三级版镜像概述。
	Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版	*aliyun_2_1903_x64_20G_uefi_alibase_20210726.vhd*	基于x86架构默认标准镜像开发，仅支持UEFI启动模式。
	Alibaba Cloud Linux 2.1903 64位 可信版	*aliyun_2_1903_x64_20G_secured_alibase_20210325.vhd*	基于x86架构默认标准镜像开发，支持阿里云可信实例的镜像版本。
	Alibaba Cloud Linux 2.1903 64位 SCC版	*aliyun_2_1903_x64_20G_scc_alibase_20210806.vhd*	基于x86架构默认标准镜像开发，支持阿里云SCC实例的镜像版本，仅支持UEFI启动模式。

获取Alibaba Cloud Linux

您可通过下列方法获取并使用Alibaba Cloud Linux。

- ECS实例
  - 新创建ECS实例时选择**公共镜像**，并选择Alibaba Cloud Linux的相应版本。具体操作，请参见使用向导创建实例。
  - 已创建的ECS实例可通过更换系统盘，将现有操作系统更换为Alibaba Cloud Linux。具体操作，请参见更换操作系统（公共镜像）。

- 本地环境（基于KVM技术的虚拟化环境）
  直接下载Alibaba Cloud Linux虚拟机镜像并安装启动。更多信息，请参见在本地使用Alibaba Cloud Linux 2镜像或在本地使用Alibaba Cloud Linux 3镜像。

镜像发布记录

- Alibaba Cloud Linux 3镜像发布记录
- Alibaba Cloud Linux 2镜像发布记录

安全更新

Alibaba Cloud Linux CVE更新记录，请参见：

- Alibaba Cloud Linux 3安全公告
- Alibaba Cloud Linux 2安全公告

技术支持

阿里云为Alibaba Cloud Linux提供如下技术支持：

- 按各操作系统版本的生命周期（详情请参见Alibaba Cloud Linux EOL计划），提供免费安全更新和问题修复。您可以通过以下方式获得免费的技术支持：
  - 提交工单
  - 阿里云开发者社区
- 在保证repo源实时更新的同时，对基础镜像进行月度更新，更新内容包括新特性支持、安全更新、已知问题修复等。
- 在YUM源提供安全更新（Security Updates），运行**yum update**命令可更新至新版本。

联系我们

欢迎您通过钉钉（钉钉通讯客户端下载地址）加入Alibaba Cloud Linux技术交流群，与其他Alibaba Cloud Linux使用者交流经验、分享技术等。钉钉群号为23149462。

5.2. 镜像发布记录

5.2.1. Alibaba Cloud Linux 3镜像发布记录

本文以发布时间为顺序，介绍Alibaba Cloud Linux 3镜像的特性更新动态。

背景信息

- 如无特殊声明，更新内容适用于云服务器ECS所有可用地域。
- Alibaba Cloud Linux 3镜像适用于大多数实例规格族，但存在一部分镜像仅适用于部分实例规格族。更多信息，请参见仅适用部分实例规格族的镜像发布记录。

镜像发布记录

镜像ID	发布时间	发布内容

镜像ID	发布时间	发布内容

aliyun_3_2104_x64_20G_dengbao_alibase_20220601.vhd	2022-06-01	• 新增 `Alibaba Cloud Linux 3.2104 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220527.vhd*版本制作
		• 内核版本更新至*5.10.112-11.al8.x86_64*（**uname -r**命令回显结果）
		• 适用地域：华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_alibase_20220527.vhd	2022-05-27	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像到最新的软件版本 • 内核更新： ○ 版本更新至*5.10.112-11.al8.x86_64* ○ 修复内核缺陷（Bugfix）以及重要安全漏洞（CVE） ○ 支持以下阿里云自研技术： ■ 内核代码多副本特性 ■ 内核代码大页功能增强 ■ Kfence增加内存越界、UAF等问题定位能力 ○ 支持Hygon CSV2 机密虚拟机特性 ○ Guest OS最大支持256 CPU ○ SMC多场景下吞吐、时延性能提升，建联速度提升，多个稳定性、兼容问题修复 ○ Intel SPR支持AMX、vAMX、IPI虚拟化、UINTER、Intel_idle、TDX等特性 ○ AMD支持SEV-ES、ptdma、CPU frequency、k10temp、EDAC等特性 ○ 阿里倚天710支持特性：DDR PMU、PCIe PMU驱动支持、CMN-700、RAS ○ 支持coresight特性 ○ ARM架构支持ARM SPE perf memory profiling/c2c特性 ○ virtiofs支持文件级DAX ○ 支持smmu event polling特性
aliyun_3_x64_20G_qboot_alibase_20220527.vhd	2022-05-27	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220527.vhd*版本制作
aliyun_3_x64_20G_alibase_20220413.vhd	2022-04-13	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像到最新的软件版本 • 内核更新： ○ 版本更新至*5.10.84-10.4.al8.x86_64* ○ 修复重要安全漏洞CVE-2022-1016、CVE-2022-27666

镜像ID	发布时间	发布内容

aliyun_3_x64_20G_alibase_20220315.vhd	2022-03-15	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像到最新的软件版本
		• 修复软件包安全漏洞
		• 内核更新：
		  ○ 版本更新至*5.10.84-10.3.al8.x86_64*
		  ○ 修复CVE-2022-0435、CVE-2022-0847漏洞

aliyun_3_x64_20G_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像到最新的软件版本，修复软件包安全漏洞
		• RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
		• 内核更新：
		  ○ 版本更新至*5.10.84-10.2.al8.x86_64*
		  ○ 修复CVE-2022-0492、CVE-2021-4197、CVE-2022-0330、CVE-2022-22942、CVE-2022-0185漏洞
		  ○ 支持阿里云自研特性：
		  ■ 内核代码多副本特性
		  ■ 内核代码大页特性
		  ■ RDMA/SMC-R特性
		  ○ Intel SPR支持AMX/RAS/RCEC/Bus lock detect & Ratelimit support/uncore新特性
		  ○ Intel IceLake处理器增加MCA-R特性
		  ○ 使能Intel DSA功能
		  ○ virtio-net支持XDP socket特性
		  ○ 支持内核KTLS商密
		  ○ 支持内存越界、UAF等问题定位工具Kfence
		  ○ 优化内核SM4算法的avx/avx2指令集
		  ○ 支持Hygon CSV vm attestation功能
		  ○ 支持ARM SPE的perf c2c特性
		  ○ 支持i10nm_edac特性
		  ○ unevictable_pid功能移植
		  ○ 支持内存水位线调整
		  ○ 支持IO_Uring：adaptive sqpoll mode
		  ○ 支持huge vmalloc mappings

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_qboot_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220225.vhd*版本制作 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明

aliyun_3_x64_20G_alibase_20210910.vhd	2021-09-10	• 更新 `Alibaba Cloud Linux 3.2104 64位` 基础镜像到最新的软件版本，修复软件包安全漏洞
		• 新增并默认开启update-motd服务
		• 默认开启Kdump服务
		• 默认开启atd服务
		• 内核更新：
		  ○ 内核升级为主线稳定版5.10.60，当前内核版本为*5.10.60-9.al8.x86_64*
		  ○ 修复内核缺陷及重要安全漏洞
		  ○ 提供以下阿里云自研技术的支持：
		  ▪ eRDMA以及基于eRDMA的SMC-R技术
		  ▪ 资源隔离技术OOM优先级控制
		  ▪ Memory KIDLED技术
		  ▪ 资源隔离技术memcg zombie reaper
		  ▪ 富容器技术rich container
		  ▪ 资源隔离技术CPU Group Identity
		  ▪ UKFEF技术
		  ○ 支持Intel SPR CPU
		  ○ 支持AMD Milan cpupower
		  ○ ARM 64架构支持基于SEDI的NMI watchdog
		  ○ ARM 64架构支持MPAM
		  ○ ARM 64架构支持Memory hotplug
		  ○ 增强内核的快速启动技术
		  ○ 支持X86 SGX2
		  ○ virtio-net性能优化
		  ○ eBPF LSM技术支持
		  ○ KVM虚拟化的软硬件协同化（支持PV-qspinlock）

aliyun_3_x64_20G_qboot_alibase_20211214.vhd	2021-12-14	• 新增 `Alibaba Cloud Linux 3.2104 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210910.vhd*版本制作

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_alibase_20210425.vhd	2021-04-25	• 更新 `Alibaba Cloud Linux 3.2104 64位` 基础镜像 • 内核更新：版本更新至*5.10.23-5.al8.x86_64*

aliyun_3_x64_20G_alibase_20210415.vhd	2021-04-16	• `Alibaba Cloud Linux 3.2104 64位` 基础镜像发布上线
		• 内核说明：
		  ○ 基于Linux社区主线长期支持的*5.10*内核版本，初次采用的内核版本为*5.10.23-4.al8.x86_64*
		  ○ ARM64架构支持PV-Panic、PV-Unhalt、PV-Preempt特性
		  ○ ARM64架构支持内核热补丁
		  ○ 支持TCP-RT功能
		  ○ 支持Memcg后台异步回收
		  ○ cgroup v1接口支持memcg QoS及PSI功能
		  ○ 支持cgroup writeback功能
		  ○ 增强Block IO限流监控统计能力
		  ○ 优化ext4的JBD2的接口
		  ○ 优化阿里巴巴开源内核并修复缺陷，包括调度器、内存、文件系统与块层等多个子系统
		  ○ 增加CPU Burst支持。更多信息，请参见在cgroup v1接口开启CPU Burst功能
		• 镜像说明：
		  ○ 兼容CentOS 8、RHEL 8软件生态，修复软件包安全漏洞
		  ○ 支持GCC 10.2.1、glibc 2.32
		  ○ 支持Python 3.6、Python 2.7
		  ○ 支持Appstream新机制
		• 适用地域：华东1（杭州）

仅适用部分实例规格族的镜像发布记录

SCC镜像仅适用的实例规格族：sccg7、sccc7

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_scc_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 SCC版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220225.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_scc_alibase_20211018.vhd	2021-10-18	• 更新 `Alibaba Cloud Linux 3.2104 64位 SCC版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210910.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式
aliyun_3_x64_20G_scc_alibase_20210806.vhd	2021-08-06	• 新增 `Alibaba Cloud Linux 3.2104 64位 SCC版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210425.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 适用地域：华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）

SCC镜像

ARM镜像仅适用的实例规格族：ecs.g6r、ecs.c6r

镜像ID	发布时间	发布内容

aliyun_3_arm64_20G_alibase_20220526.vhd	2022-05-26	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 ARM版` 基础镜像到最新的软件版本
		• 内核更新：
		  ○ 版本更新至*5.10.112-11.al8.aarch64*
		  ○ 修复内核缺陷（Bugfix）以及重要安全漏洞（CVE）
		  ○ 支持以下阿里云自研技术：
		  ▪ 内核代码多副本特性
		  ▪ 内核代码大页功能增强
		  ▪ Kfence增加内存越界、UAF等问题定位能力
		  ○ 支持Hygon CSV2机密虚拟机特性
		  ○ Guest OS最大支持256 CPU
		  ○ SMC多场景下吞吐、时延性能提升，建联速度提升，多个稳定性、兼容问题修复
		  ○ Intel SPR支持AMX、vAMX、IPI虚拟化、UINTER、Intel_idle、TDX等特性
		  ○ AMD支持SEV-ES、ptdma、CPU frequency、k10temp、EDAC等特性
		  ○ 阿里倚天710支持特性：DDR PMU、PCIe PMU驱动支持、CMN-700、RAS
		  ○ 支持coresight特性
		  ○ ARM架构支持ARM SPE perf memory profiling/c2c特性
		  ○ virtiofs支持文件级DAX
		  ○ 支持smmu event polling特性

镜像ID	发布时间	发布内容
aliyun_3_arm64_20G_alibase_20220413.vhd	2022-04-13	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 ARM版` 基础镜像到最新的软件版本 • 内核更新： ○ 版本更新至*5.10.84-10.4.al8.aarch64* ○ 修复重要安全漏洞CVE-2022-1016、CVE-2022-27666
aliyun_3_arm64_20G_alibase_20220315.vhd	2022-03-15	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 ARM版` 基础镜像到最新的软件版本 • 修复软件包安全漏洞 • 内核更新： ○ 版本更新至*5.10.84-10.3.al8.aarch64* ○ 修复CVE-2022-0435、CVE-2022-0847漏洞
aliyun_3_arm64_20G_alibase_20220225.vhd	2022-02-25	• RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明 • 内核更新： ○ 版本更新至*5.10.84-10.2.al8.aarch64* ○ 修复CVE-2022-0492、CVE-2021-4197、CVE-2022-0330、CVE-2022-22942、CVE-2022-0185漏洞 ○ 支持阿里云自研特性： ■ 内核代码多副本特性 ■ 内核代码大页特性 ■ RDMA/SMC-R特性 ○ Intel SPR支持AMX/RAS/RCEC/Bus lock detect & Ratelimit support/uncore新特性 ○ Intel IceLake处理器增加MCA-R特性 ○ 使能Intel DSA功能 ○ virtio-net支持XDP socket特性 ○ 支持内核KTLS商密 ○ 支持内存越界、UAF等问题定位工具Kfence ○ 优化内核SM4算法的avx/avx2指令集 ○ 支持Hygon CSV vm attestation功能 ○ 支持ARM SPE的perf c2c特性 ○ 支持i10nm_edac特性 ○ unevictable_pid功能移植 ○ 支持内存水位线调整 ○ 支持IO_Uring：adaptive sqpoll mode ○ 支持huge vmalloc mappings

镜像ID	发布时间	发布内容
aliyun_3_arm64_20G_alibase_20210910.vhd	2021-09-10	• 更新 `Alibaba Cloud Linux 3.2104 64位 ARM版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210910.vhd*版本制作
aliyun_3_arm64_20G_alibase_20210709.vhd	2021-07-09	• 新增 `Alibaba Cloud Linux 3.2104 64位 ARM版` 镜像 • 支持接入云安全中心 • 适用地域：华东1（杭州）

ARM镜像

UEFI镜像仅适用的实例规格族：ecs.c7、ecs.g7、ecs.r7、ecs.c7t、ecs.g7t、ecs.r7t、ecs.ebmc7a、ecs.ebmg7a、ecs.ebmr7a

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_uefi_alibase_20220527.vhd	2022-05-27	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 UEFI版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220527.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式
aliyun_3_x64_20G_uefi_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 3.2104 LTS 64位 UEFI版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 LTS 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20220225.vhd*版本制作 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
aliyun_3_x64_20G_uefi_alibase_20210910.vhd	2021-09-10	• 更新 `Alibaba Cloud Linux 3.2104 64位 UEFI版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210910.vhd*版本制作 • 适用地域：华东1（杭州）、华东2（上海）、华北2（北京）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、新加坡

镜像ID	发布时间	发布内容
aliyun_3_x64_20G_uefi_alibase_20210425.vhd	2021-04-25	• 新增 `Alibaba Cloud Linux 3.2104 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 3.2104 64位` 基础镜像的*aliyun_3_x64_20G_alibase_20210425.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 适用地域：华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）

UEFI镜像

5.2.2. Alibaba Cloud Linux 2镜像发布记录

本文以发布时间为顺序，介绍Alibaba Cloud Linux 2镜像的特性更新动态。

背景信息

- 如无特殊声明，更新内容适用于云服务器ECS所有可用地域。
- Alibaba Cloud Linux 2镜像适用于大多数实例规格族，但存在一部分实例规格族不适用。这些实例规格族只能选用指定的公共镜像，详情请参见仅适用部分实例规格族的镜像发布记录。

镜像发布记录

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20220525.vhd	2022-05-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本
		• 内核更新：
		  ○ 版本更新至*4.19.91-26.al7*
		  ○ 修复内核缺陷（Bugfix）以及重要安全漏洞（CVE）
		  ○ 支持以下阿里云自研技术：
		  ▪ 混部资源隔离Group Identity特性
		  ▪ 多租户容器网络QoS隔离特性
		  ▪ 冷slab内存监测与回收特性
		  ▪ UKFEF特性
		  ○ 支持Megaraid_sas设备驱动
		  ○ virtio-net支持XDP socket特性
		  ○ 支持基于EROFS实现RAFS v6格式
		  ○ Livepatch支持static key
		  ○ 支持SMR zoned设备
		  ○ ext4 delalloc buffer写性能优化
		  ○ 支持KUnit测试框架
		  ○ ARM架构支持Kdump crashkernel分配4 GB以上内存
		  ○ ARM架构支持CMN PMU特性
		  ○ 支持perf c2c功能

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_qboot_alibase_20220525.vhd	2022-05-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220525.vhd*版本制作

aliyun_2_1903_x64_20G_dengbao_alibase_20220525.vhd	2022-05-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220525.vhd*版本制作
		• 内核版本更新至*4.19.91-26.al7.x86_64*（uname -r命令回显结果）

aliyun_2_1903_x64_20G_alibase_20220413.vhd	2022-04-13	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本
		• 兼容最新CentOS 7.9版本
		• 内核更新：
		  ○ 版本更新至*4.19.91-25.8.al7.x86_64*
		  ○ 修复重要安全漏洞CVE-2022-1016、CVE-2022-27666

aliyun_2_1903_x64_20G_alibase_20220408.vhd	2022-04-08	• 版本更新至*4.19.91-25.7.al7.x86_64* • 更新最新软件包
aliyun_2_1903_x64_20G_alibase_20220225.vhd	2022-02-25	内核更新： • 版本更新至*4.19.91-25.6.al7.x86_64*（uname -r命令回显结果） • 修复CVE-2022-0492、CVE-2021-4197、CVE-2022-0330、CVE-2022-22942、CVE-2021-4155漏洞 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_qboot_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220225.vhd*版本制作 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明

aliyun_2_1903_x64_20G_dengbao_alibase_20211220.vhd	2021-12-20	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20211216.vhd*版本制作
		• 内核版本更新至*4.19.91-25.1.al7.x86_64*（**uname -r**命令回显结果）
		• 适用地域：华北1（青岛）、华北2（北京）、华东1（杭州）、西南1（成都）、中国（香港）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20211216.vhd	2021-12-16	内核更新：
		• 版本更新至*4.19.91-25.1.al7.x86_64*（uname -r命令回显结果）
		• 修复内核缺陷（Bugfix）以及重要安全漏洞（CVE）
		• ARM64架构支持Kata-container
		• 支持IO_uring sqthread调度策略与优先级配置
		• 增加AMD Milan平台CPUPower功能
		• Virtio-fs：
		  ○ 性能优化提升
		  ○ 支持fuse DAX功能
		  ○ 支持fuse CACHE_DIR/CACHE_SYMLINK特性
		• crypto：优化内核SM4算法的avx/avx2指令集
		• 支持阿里云自研特性：
		  ○ 富容器功能
		  ○ 代码段透明大页

aliyun_2_1903_x64_20G_qboot_alibase_20211216.vhd	2021-12-16	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20211216.vhd*版本制作

aliyun_2_1903_x64_20G_alibase_20210726.vhd	2021-07-26	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.9版本，修复软件包安全漏洞
		• 内核更新：
		  ○ 版本更新至*4.19.91-24.1.al7.x86_64*（uname -r命令回显结果）
		  ○ 修复重要安全漏洞
		  ○ 更新PCIe驱动

aliyun_2_1903_x64_20G_qboot_alibase_20210726.vhd	2021-07-26	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210726.vhd*版本制作

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_dengbao_alibase_20210726.vhd	2021-07-26	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210726.vhd*版本制作
		• 内核版本更新至*4.19.91-24.1.al7.x86_64*（**uname -r**命令回显结果）
		• 适用地域：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华东1（杭州）、华东2（上海）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

aliyun_2_1903_x64_20G_alibase_20210630.vhd	2021-06-30	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.9版本，修复软件包安全漏洞
		• 内核更新：
		  ○ 版本更新至*4.19.91-24.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 修复内核缺陷及重要安全漏洞
		  ○ 支持x86 FSGSBASE特性
		  ○ 支持AMD Milan架构
		  ○ 支持RDMA NET Namespace特性
		  ○ 支持ZSR特性
		  ○ 支持CPU资源隔离Group Identity特性
		  ○ 支持ARM64 MPAM特性
		  ○ 支持Hisilicon、PHYTIUM、Zhaoxin架构
		  ○ 在*/proc/<pid>/status*以及*/proc/<pid>/smap*中加入了进程的THP使能信息
		• 适用地域：华东1（杭州）、华北1（青岛）、华北2（北京）、西南1（成都）、中国（香港）、新加坡

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20210325.vhd	2021-03-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.9版本，修复软件包安全漏洞
		• 修复CVE-2021-3156漏洞，即Linux sudo权限漏洞。更多信息，请参见漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156）
		• 默认的网络配置服务切换为network-scripts
		• 增大net.ipv4.tcp_max_tw_buckets参数值
		• 在initramfs增加了NVME驱动
		• 默认开启Kdump服务
		• 内核更新：
		  ○ 版本更新至*4.19.91-23.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 修复内核缺陷及重要安全漏洞
		  ○ 支持Intel SGX
		  ○ 支持网络诊断工具Ping Trace
		  ○ 支持在单机多实例的场景下轻量级创建cgroup，有效减少cgroup的创建时间
		  ○ 支持Intel IceLake MCA

aliyun_2_1903_x64_20G_qboot_alibase_20210325.vhd	2021-03-25	• 更新 `Alibaba Cloud Linux 2.1903 64位` **快速启动版** 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210325.vhd*版本制作 • 适用地域：华东1（杭州）、华北2（北京）、华北3（张家口）、华南1（深圳）、中国（香港）、新加坡、马来西亚（吉隆坡）、美国（弗吉尼亚）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_dengbao_alibase_20210325.vhd	2021-03-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210325.vhd*版本制作
		• 内核版本：*4.19.91-23.al7.x86_64*（**uname -r**命令回显结果）
		• 适用地域：华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

aliyun_2_1903_x64_20G_qboot_alibase_20210218.vhd	2021-02-18	• 更新 `Alibaba Cloud Linux 2.1903 64位 快速启动版` 镜像 • 默认的网络配置服务切换为network-scripts • 修复CVE-2021-3156漏洞，即Linux sudo权限漏洞。更多信息，请参见漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156） • 适用地域：华东1（杭州）、华南1（深圳）、华北2（北京）、华北3（张家口）、中国（香港）、新加坡、马来西亚（吉隆坡）、美国（弗吉尼亚）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_dengbao_alibase_20210218.vhd	2021-02-18	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 默认的网络配置服务切换为network-scripts
		• 修复CVE-2021-3156漏洞，即Linux sudo权限漏洞。更多信息，请参见漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156）
		• 内核版本：*4.19.91-22.2.al7.x86_64*（uname -r命令回显结果）
		• 适用地域：华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20210120.vhd	2021-01-20	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.9版本，修复软件包安全漏洞
		• 新增并默认开启update-motd服务
		• 默认开启rhel-loadmodules服务
		• 增加vring_force_dma_api启动参数
		• 内核更新：
		  ○ 版本更新至*4.19.91-22.2.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 修复内核缺陷及重要安全漏洞
		  ○ 同步社区最新的ext4文件系统，增强稳定性
		  ○ 默认开启RAID支持
		  ○ 增加Dragonfly Enclaves特性支持
		  ○ 增加Intel IceLake PMU Topdown性能调试支持
		  ○ 优化增强IO_Uring Buffer读能力
		  ○ 优化增强blk-throttle
		  ○ 增加SM2国密算法支持以及SM2-with-SM3的标准X509格式证书支持
		  ○ 增加blk-mq batch request支持
		  ○ 增加PCIe Error recover特性支持
		  ○ 优化Swap，大大提升内存超卖稳定性
		  ○ 增加Alibaba Cloud Linux容器增强技术支持
		  ○ 增加CPU Burst支持，更多信息，请参见在cgroup v1接口开启CPU Burst功能

aliyun_2_1903_x64_20G_qboot_alibase_20210120.vhd	2021-01-20	• 更新 `Alibaba Cloud Linux 2.1903 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210120.vhd*版本制作 • 适用地域：华东1（杭州）、华南1（深圳）、华北2（北京）、华北3（张家口）、中国（香港）、新加坡、马来西亚（吉隆坡）、美国（弗吉尼亚）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_dengbao_alibase_20210120.vhd	2021-01-20	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210120.vhd*版本制作
		• 内核版本：*4.19.91-22.2.al7.x86_64*（uname -r命令回显结果）
		• 适用地域：华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

aliyun_2_1903_x64_20G_dengbao_alibase_20200925.vhd	2020-09-25	• 新增 `Alibaba Cloud Linux 2.1903 LTS 64位 等保2.0三级版` 镜像
		• 该镜像是根据*GB/T22239-2019信息安全技术网络安全等级保护基本要求*进行等保加固的镜像，您使用本镜像无需额外配置即可满足以下等保合规要求：
		  ○ 身份鉴别
		  ○ 访问控制
		  ○ 安全审计
		  ○ 入侵防范
		  ○ 恶意代码防范
		  详情请参见Alibaba Cloud Linux等保2.0三级版镜像概述
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200904.vhd*版本制作
		• 内核版本：*4.19.91-22.2.al7.x86_64*（uname -r命令回显结果）
		• 适用地域：华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20200904.vhd	2020-09-04	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.8版本，修复软件包安全漏洞
		• */etc/redhat-release*的信息从Aliyun Linux release 7.2 LTS (Hunting Beagle)变更成Alibaba Cloud Linux (Aliyun Linux) release 2.1903 LTS (Hunting Beagle)
		• 优化*/etc/image-id*标识镜像类型
		• 默认开启tuned服务
		• 内核更新：
		  ○ 版本更新至*4.19.91-21.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 修复内核重要缺陷及安全漏洞
		  ○ 修复IO_Uring缺陷及功能增加
		  ○ 增加THP fork优化，提升大内存进程创建速度
		  ○ 增加AEP设备安全操作支持
		  ○ 增加阿里巴巴自研特性TCP-RT支持
		  ○ 增加virtio-mem特性支持
		  ○ 增强Intel® IceLake处理器电源管理、PCIe Gen4、RAS等功能
		  ○ 增加Intel® Speed Select Technology技术支持

aliyun_2_1903_x64_20G_qboot_alibase_20200904.vhd	2020-09-04	• 更新 `Alibaba Cloud Linux 2.1903 64位 快速启动版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200904.vhd*版本制作 • 适用地域：华东1（杭州）、华南1（深圳）、华北3（张家口）、中国（香港）

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20200529.vhd	2020-05-29	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.8版本，修复软件包安全漏洞
		• 增加*/etc/image-id*标识
		• 默认关闭tuned服务
		• 内核更新：
		  ○ 版本更新至*4.19.91-19.1.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 开源阿里云内核对调度、内存QoS指标统计内核接口支持，提供调度、内存相关SLI细粒度监控能力
		  ○ 开源阿里云内核memcg OOM（Out-Of-Memory）优先级控制接口支持，增强系统OOM时重要进程保护措施
		  ○ 增加AMD QoS支持
		  ○ 增加virtio pmem驱动支持
		  ○ 增加free page reporting特性支持，增强Hypervisor对Guest OS空闲内存感知能力，高效管理利用物理内存资源
		  ○ 优化Memory compaction，有效缓解内存碎片化，提升系统内存使用效率
		  ○ 修复内核重要缺陷及安全漏洞

aliyun_2_1903_x64_20G_alibase_20200324.vhd	2020-03-24	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.8版本，修复软件包安全漏洞
		• 新增支持通过yum获取安全漏洞（CVE）更新
		• 正式发布Alibaba Cloud Linux 2的LTS版本，并更新*/etc/alinux-release*为Aliyun Linux release 2.1903 LTS (Hunting Beagle)
		• 默认开启tuned服务
		• 内核更新：
		  ○ 版本更新至*4.19.91-18.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 增加NVMe设备支持
		  ○ 默认开启THP以提升应用性能
		  ○ 增加IO_Uring技术
		  ○ 开启Intel_idle及guest halt polling，以提升guest CPU效能
		  ○ 开启ftrace syscalls以增强bpftrace工具的能力
		  ○ 开源了多个阿里云内部内核优化和缺陷修复，包含调度器、内存、文件系统与块层等多个子系统
		  ○ 修复内核安全漏洞

镜像ID	发布时间	发布内容

aliyun_2_1903_x64_20G_alibase_20200221.vhd	2020-02-21	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本，兼容最新CentOS 7.8版本，修复软件包安全漏洞
		• 默认开启IPv6支持
		• 内核更新：
		  ○ 版本更新至*4.19.81-17.1.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 支持Intel Cooper Lake CPU和Ice Lake CPU
		  ○ 完善对AMD CPU和ARM64 CPU架构的支持
		  ○ 支持持久化内存（presistent memory）
		  ○ 支持IO Cost（基于IO消耗模型、按比例分配的blkio cgroup controller），更多信息，请参见blk-iocost权重限速
		  ○ 支持基于cgroup v1接口的PSI（pressure stall information）功能，更多信息，请参见在cgroup v1接口开启PSI功能
		  ○ 开源了多个阿里云内部内核优化和缺陷修复，包含调度器、内存、文件系统与块层等多个子系统
		  ○ 修复内核安全漏洞

aliyun_2_1903_x64_20G_alibase_20200114.qboot.vhd	2020-01-14	• 新增 `Alibaba Cloud Linux 2.1903 64位 快速启动版` 镜像
		• 内核更新：
		  ○ 版本更新至*4.19.81-17.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 支持qboot快速启动
		• 适用地域：华北2（北京）、华东1（杭州）、中国（香港）

aliyun_2_1903_64_20G_alibase_20190829.vhd	2019-08-29	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本
		• 内核更新：
		  ○ 版本更新至*4.19.57-15.1.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 修复Spectre-V1 SWAPGS问题
		  ○ 修复DM bio splitting问题
		  ○ 修改TCP拥塞控制默认算法为CUBIC
		  ○ 网络配置统一为10-eth0.network

镜像ID	发布时间	发布内容

aliyun_2_1903_64_20G_alibase_20190619.vhd	2019-06-19	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本
		• 内核更新：
		  ○ 版本更新至*4.19.43-13.2.al7.x86_64*（uname -r命令回显结果）
		  ○ 支持基于cgroup v1版本接口的cgroup writeback特性
		  ○ 支持策略路由
		  ○ 开启INET_DIAG内核配置项，以支持iproute2套件的ss命令
		  ○ 支持可配置的内核接口net.ipv4.tcp_tw_timeout
		  ○ 修复了以下网络相关缺陷（CVE）：
		  ■ CVE-2019-11477
		  ■ CVE-2019-11478
		  ■ CVE-2019-11479

aliyun-2.1903-x64-20G-alibase-20190507.vhd	2019-05-07	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像到最新的软件版本 • 修复启动ECS实例后时间同步延迟的问题 • 内核版本更新至*4.19.34-11.al7.x86_64*（uname -r命令回显结果），更新系统内核，修复若干问题
aliyun-2.1903-x64-20G-alibase-20190327.vhd	2019-03-27	• `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像发布上线 • 初次采用的内核版本为*4.19.24-9.al7.x86_64*（uname -r命令回显结果）

仅适用部分实例规格族的镜像发布记录

SCC镜像仅适用的实例规格族：sccg7、sccc7

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_scc_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 SCC版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220225.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_scc_alibase_20211216.vhd	2021-12-16	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 SCC版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20211216.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式
aliyun_2_1903_x64_20G_scc_alibase_20210806.vhd	2021-08-06	• 新增 `Alibaba Cloud Linux 2.1903 64位 SCC版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210726.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 适用地域：华东1（杭州）、华东2（上海）、华北2（北京）、华南1（深圳）

SCC镜像

UEFI镜像仅适用的实例规格族：ecs.c7、ecs.g7、ecs.r7、ecs.c7t、ecs.g7t、ecs.r7t、ecs.ebmc7a、ecs.ebmg7a、ecs.ebmr7a

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_uefi_alibase_20220525.vhd	2022-05-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220525.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式
aliyun_2_1903_x64_20G_uefi_alibase_20220225.vhd	2022-02-25	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20220225.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • RTC（Real Time Clock）时钟使用UTC时间标准。更多信息，请参见Linux时间和时区说明
aliyun_2_1903_x64_20G_uefi_alibase_20211216.vhd	2021-12-16	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20211216.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_uefi_alibase_20210726.vhd	2021-07-26	• 更新 `Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210726.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 适用地域：华东1（杭州）、华东2（上海）、华北2（北京）、华南1（深圳）、新加坡
aliyun_2_1903_x64_20G_uefi_alibase_20210325.vhd	2021-03-25	• 更新 `Alibaba Cloud Linux 2.1903 64位 UEFI版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210325.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 适用地域：华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）

UEFI镜像

可信镜像仅适用的实例规格族：ecs.g6t、ecs.c6t

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_secured_alibase_20210325.vhd	2021-03-25	• 更新 `Alibaba Cloud Linux 2.1903 64位 可信版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210325.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 内核更新：版本更新至*4.19.91-23.al7.x86_64*（uname -r命令回显结果）
aliyun_2_1903_x64_20G_secured_alibase_20210218.vhd	2021-02-18	• 更新 `Alibaba Cloud Linux 2.1903 64位 可信版` 镜像 • 默认的网络配置服务切换为network-scripts • 修复CVE-2021-3156漏洞，即Linux sudo权限漏洞。更多信息，请参见漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156） • 启动切换为UEFI模式，而且仅支持该模式 • 内核更新：版本更新至*4.19.91-22.2.al7.x86_64*（uname -r命令回显结果）

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_secured_alibase_20210120.vhd	2021-01-20	• 更新 `Alibaba Cloud Linux 2.1903 64位 可信版` 镜像 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210120.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 内核更新：版本更新至*4.19.91-22.2.al7.x86_64*（**uname -r**命令回显结果）
aliyun_2_1903_x64_20G_secured_alibase_20200904.vhd	2020-09-04	• 更新 `Alibaba Cloud Linux 2.1903 64位 可信版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200904.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式 • 增加可信功能

aliyun_2_1903_x64_20G_secured_alibase_20200622.vhd	2020-06-22	• 新增 `Alibaba Cloud Linux 2.1903 64位 可信版` 镜像
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200529.vhd*版本制作
		• 启动切换为UEFI模式，而且仅支持该模式
		• 增加可信功能
		• 内核更新：
		  ○ 版本更新至*4.19.91-19.2.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 增加AMD IOMMU支持

可信镜像

AMD镜像仅适用的实例规格族：ecs.ebmg6a、ecs.ebmc6a、ecs.ebmr6a

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_uefi_alibase_20210218.vhd	2021-02-18	• 更新 `Alibaba Cloud Linux 2.1903 64位 AMD版` 镜像到最新的软件版本 • 默认的网络配置服务切换为network-scripts • 修复CVE-2021-3156漏洞，即Linux sudo权限漏洞。更多信息，请参见漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156） • 启动切换为UEFI模式，而且仅支持该模式

镜像ID	发布时间	发布内容
aliyun_2_1903_x64_20G_uefi_alibase_20210120.vhd	2021-01-20	• 更新 `Alibaba Cloud Linux 2.1903 64位 AMD版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20210120.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式
aliyun_2_1903_x64_20G_uefi_alibase_20200904.vhd	2020-09-04	• 更新 `Alibaba Cloud Linux 2.1903 64位 AMD版` 镜像到最新的软件版本 • 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200904.vhd*版本制作 • 启动切换为UEFI模式，而且仅支持该模式

aliyun_2_1903_x64_20G_uefi_alibase_20200616.vhd	2020-06-16	• 新增 `Alibaba Cloud Linux 2.1903 64位 AMD版` 镜像
		• 该镜像基于 `Alibaba Cloud Linux 2.1903 LTS 64位` 基础镜像的*aliyun_2_1903_x64_20G_alibase_20200529.vhd*版本制作
		• 启动切换为UEFI模式，而且仅支持该模式
		• 内核更新：
		  ○ 版本更新至*4.19.91-19.2.al7.x86_64*（**uname -r**命令回显结果）
		  ○ 增加AMD IOMMU支持

AMD镜像

5.3. 镜像使用说明

5.3.1. 在本地使用Alibaba Cloud Linux 3镜像

Alibaba Cloud Linux 3提供了多种格式的本地镜像，并内置cloud-init。本文介绍如何在本地使用Alibaba Cloud Linux 3镜像。

背景信息

Alibaba Cloud Linux 3镜像目前只支持KVM虚拟机。镜像本身不可直接启动虚拟机，需要配置引导镜像。

例如，本文示例中，本地环境为CentOS操作系统，使用Alibaba Cloud Linux 3镜像创建了KVM虚拟机，使用cloud-init初始化虚拟机系统设置，然后使用NoCloud数据源在本地建立相关配置文件，以虚拟磁盘的形式挂载到KVM虚拟机中进行设置，并启动虚拟机。cloud-init的相关信息请参见cloud-init官网 - 阿里云数据源说明文档。

步骤一：本地下载Alibaba Cloud Linux 3镜像

在本地下载Alibaba Cloud Linux 3镜像，下载地址为Alibaba Cloud Linux 3 On-premise Image，目前提供vhd与qcow2格式的本地镜像。

步骤二：本地生成seed.img引导镜像

该镜像为引导镜像，需要配置网络、账号、YUM源等信息。通常情况下该镜像的名称设置为seed.img，您可以使用其他名称，但不建议您这样做。

> **注意** seed.img镜像只包含cloud-init启动所需要的配置文件，不包含Alibaba Cloud Linux 3系统文件。

您可以通过以下两种方式生成seed.img镜像。

- Alibaba Cloud Linux 3预先提供了seed.img镜像文件，下载地址为Alibaba Cloud Linux 3 On-premise Image，在页面列表选择*seed.img*下载镜像。
  该引导镜像中的配置信息是不可修改的，因此不适用于所有场景。在使用之前请确保您已了解镜像文件的内容。
- 使用NoCloud数据源手动生成seed.img镜像，操作步骤如下。

1. 在本地同一级目录下，创建 `meta-data` 和 `user-data` 两个配置文件。
   i. 新建名为 `seed` 的目录，并进入该目录。

   ```
   mkdir seed
   cd seed/
   ```

   ii. 创建 `meta-data` 配置文件。

   文件内容示例如下，您可以根据需要修改相关配置信息。

   ```
   #cloud-config
   #vim:syntax=yaml
   local-hostname: alinux-host
   ```

   iii. 创建 `user-data` 配置文件。

   文件内容示例如下，您可以根据需要修改相关配置信息。

```
#cloud-config
#vim:syntax=yaml
# 添加一个名为alinux的账号，并且可以执行sudo命令。
users:
  - default
  - name: alinux
    sudo: ['ALL=(ALL)   ALL']
    plain_text_passwd: aliyun
    lock_passwd: false
# 添加Alibaba Cloud Linux 3的YUM源。
yum_repos:
    alinux3-module:
        name: alinux3-module
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/module/$basearch/
        enabled: 1
        gpgcheck: 1
        gpgkey: https://mirrors.aliyun.com/alinux/$releasever/RPM-GPG-KEY-ALINUX-3
    alinux3-updates:
        name: alinux3-updates
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/updates/$basearch/
        enabled: 1
        gpgcheck: 1
        gpgkey: https://mirrors.aliyun.com/alinux/$releasever/RPM-GPG-KEY-ALINUX-3
    alinux3-plus:
        name: alinux3-plus
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/plus/$basearch/
        enabled: 1
        gpgcheck: 1
        gpgkey: https://mirrors.aliyun.com/alinux/$releasever/RPM-GPG-KEY-ALINUX-3
    alinux3-powertools:
        name: alinux3-powertools
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/powertools/$basearch
/
        gpgcheck: 1
        enabled: 1
        gpgkey: https://mirrors.aliyun.com/alinux/$releasever/RPM-GPG-KEY-ALINUX-3
    alinux3-os:
        name: alinux3-os
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/os/$basearch/
        gpgcheck: 1
        enabled: 1
        gpgkey: https://mirrors.aliyun.com/alinux/$releasever/RPM-GPG-KEY-ALINUX-3
```

2. 本地安装 `cloud-utils` 软件包。

```
yum install -y cloud-utils
```

3. 在 `seed` 目录下，执行以下命令生成 `seed.img` 镜像。

```
cloud-localds seed.img user-data meta-data
```

步骤三：启动虚拟机

您可以使用以下任一方式启动KVM虚拟机，成功启动后，使用 `user-data` 配置文件中的账号信息登录虚拟机。

- 使用libvirt工具启动KVM虚拟机。
  i. 在本地创建一个xml配置文件。示例文件的名称为 `alinux3.xml` ，内容如下。 您可以依据需求修改xml配置文件。

```
<domain type='kvm'>
    <name>alinux3</name>
    <memory>1048576</memory><!-- 1 GB内存。 -->
    <vcpu>1</vcpu>
    <cpu mode='host-passthrough'><!-- 需要在对应架构的服务器上启动实例。 -->
    </cpu>
    <os>
        <type arch='x86_64'>hvm</type><!-- 如果是ARM64架构的服务器，则需设置为arch='aarch
64'。 -->
        <boot dev='hd'/>
    </os>
    <clock sync="localtime"/>
    <on_poweroff>destroy</on_poweroff>
    <on_reboot>restart</on_reboot>
    <on_crash>restart</on_crash>
    <devices>
        <emulator>/usr/bin/qemu-kvm</emulator><!-- 请根据不同的操作系统设置对应的kvm路径。
例如：Ubuntu对应的kvm路径是/usr/bin/kvm。 -->
        <disk type='file' device='disk'><!-- 请根据镜像格式设置下面的type参数：qcow2对应t
ype='qcow2'、vhd对应type='vpc'。 -->
            <driver name='qemu' type='qcow2' cache='none' dataplane='on' io='native'/
> <!-- 如果要创建qcow2快照，需要关闭dataplane。 -->
            <source file='path'/> <!-- 填写Alibaba Cloud Linux 3镜像的绝对路径。 -->
            <target dev='vda' bus='virtio'/>
        </disk>
        <!-- 加入seed.img的信息。 -->
        <disk type='file' device='disk'>
            <driver name='qemu' type='raw'/>
            <source file='/path/to/your/seed.img'/> <!-- 填写seed镜像的绝对路径。 -->
            <target dev='vdb' bus='virtio'/>
        </disk>
        <interface type='network'>
            <source network='default'/>
            <model type='virtio'/>
        </interface>
        <console type='pty'>
            <target type='virtio' port='0'/>
        </console>
        <video>
            <model type='cirrus' vram='9216' heads='1'/>
            <alias name='video0'/>
        </video>
        <input type='tablet' bus='usb'/>
        <input type='mouse' bus='ps2'/>
        <graphics type='vnc' port='-1' autoport='yes'/>
    </devices>
</domain>
```

ii. 使用 `virsh` 命令启动虚拟机，命令示例如下。

> **说明** libvirt工具默认使用普通用户启动，请确认镜像文件及所在路径对普通用户是否具有相应的操作权限。

```
virsh define alinux3.xml
virsh start KVMName     # 请修改为KVM虚拟机的真实名称。
```

- 使用 `qemu-kvm` 命令行启动KVM虚拟机。您需要在命令行中追加如下参数信息，其中 `file` 参数信息修改为seed.img镜像真实的绝对路径。

  ```
  -drive file=/path/to/your/seed.img,if=virtio,format=raw
  ```

  关于虚拟化配置的更多信息，请参见Red Hat官方说明。
- 使用图形界面（virt-manager）启动KVM虚拟机。在启动虚拟机之前，您需要在本地找到KVM虚拟机的配置文件，在文件内添加seed.img镜像文件的绝对路径。

5.3.2. 在本地使用Alibaba Cloud Linux 2镜像

Alibaba Cloud Linux 2提供了多种格式的本地镜像，并内置cloud-init。本文介绍如何在本地使用Alibaba Cloud Linux 2镜像。

背景信息

Alibaba Cloud Linux 2镜像目前只支持KVM虚拟机。镜像本身不可直接启动虚拟机，需要配置引导镜像。本文中本地环境为CentOS操作系统，使用Alibaba Cloud Linux 2创建了KVM虚拟机，并使用cloud-init初始化虚拟机系统设置。cloud-init的相关信息，请参见cloud-init官网 - 阿里云数据源说明文档。然后使用NoCloud数据源在本地建立相关配置文件，以虚拟磁盘的形式挂载到KVM虚拟机中进行设置，并启动虚拟机。

本文适用于对KVM虚拟机有一定了解的用户。

步骤一：本地下载Alibaba Cloud Linux 2镜像

在本地下载Alibaba Cloud Linux 2镜像，下载地址为Alibaba Cloud Linux 2 On-premise Image，目前提供vhd与qcow2格式的本地镜像。

步骤二：本地生成seed.img引导镜像

该镜像为引导镜像，需要配置网络、账号、YUM源等信息。通常情况下该镜像的名称设置为seed.img，您可以使用其他名称，但不建议您这样做。

> **注意** seed.img镜像只包含cloud-init启动所需要的配置文件，不包含Alibaba Cloud Linux 2系统文件。

您可以通过以下两种方式生成seed.img镜像。

- Alibaba Cloud Linux 2预先提供了seed.img镜像文件，下载地址为Alibaba Cloud Linux 2 On-premise Image，在页面列表选择*seed.img*下载镜像。
  该引导镜像中的配置信息是不可修改的，因此不适用于所有场景。在使用之前请确保您对该镜像文件有一定的了解。
- 使用NoCloud数据源手动生成seed.img镜像，操作步骤如下。

1. 在本地同一级目录下，创建 `meta-data` 和 `user-data` 两个配置文件。
   i. 新建名为 `seed` 的目录，并进入该目录。

   ```
   mkdir seed
   cd seed/
   ```

ii. 创建 `meta-data` 配置文件。

文件内容示例如下，您可以根据需要修改相关配置信息。

```
#cloud-config
#vim:syntax=yaml
local-hostname: alinux-host
```

iii. 创建 `user-data` 配置文件。

文件内容示例如下，您可以根据需要修改相关配置信息。

```
#cloud-config
#vim:syntax=yaml
# 添加一个名为alinux的账号，并且可以执行sudo命令。
users:
  - default
  - name: alinux
    sudo: ['ALL=(ALL)   ALL']
    plain_text_passwd: aliyun
    lock_passwd: false
# 添加Alibaba Cloud Linux 2的YUM源。
yum_repos:
    base:
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/os/$basearch/
        enabled: true
        gpgcheck: true
        gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
        name: Aliyun Linux - $releasever - Base - mirrors.aliyun.com
    updates:
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/updates/$basearch/
        enabled: true
        gpgcheck: true
        gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
        name: Aliyun Linux - $releasever - Updates - mirrors.aliyun.com
    extras:
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/extras/$basearch/
        enabled: true
        gpgcheck: true
        gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
        name: Aliyun Linux - $releasever - Extras - mirrors.aliyun.com
    plus:
        baseurl: https://mirrors.aliyun.com/alinux/$releasever/plus/$basearch/
        enabled: true
        gpgcheck: true
        gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
        name: Aliyun Linux - $releasever - Plus - mirrors.aliyun.com
```

2. 本地安装 `cloud-utils` 软件包。

```
yum install -y cloud-utils
```

3. 在 `seed` 目录下，执行以下命令生成 `seed.img` 镜像。

```
cloud-localds seed.img user-data meta-data
```

步骤三：启动虚拟机

您可以使用以下任意一种方式启动KVM虚拟机，成功启动虚拟机后，使用 `user-data` 配置文件中的账号信息登录虚拟机。

- 使用libvirt工具启动KVM虚拟机。
  i. 在本地创建一个xml配置文件。示例文件的名称为 `alinux2.xml` ，内容如下。 您可以依据需求修改xml配置文件。

```
<domain type='kvm'>
    <name>alinux2</name>
    <memory>1048576</memory> <!-- 1 GB内存。 -->
    <vcpu>1</vcpu>
    <os>
        <type arch='x86_64'>hvm</type>
        <boot dev='hd'/>
    </os>
    <clock sync="localtime"/>
    <on_poweroff>destroy</on_poweroff>
    <on_reboot>restart</on_reboot>
    <on_crash>restart</on_crash>
    <devices>
        <emulator>/usr/bin/qemu-kvm</emulator><!-- 请根据不同的操作系统设置对应的kvm路径。例如：Ubuntu对应的kvm路径是/usr/bin/kvm -->
        <disk type='file' device='disk'><!-- 请根据镜像格式设置下面的type参数：qcow2对应type='qcow2'、vhd对应type='vpc'。 -->
            <driver name='qemu' type='qcow2' cache='none' dataplane='on' io='native'/> <!-- 如果要创建qcow2快照，需要关闭dataplane。 -->
            <source file='path'/> <!-- 填写Alibaba Cloud Linux 2镜像的绝对路径。 -->
            <target dev='vda' bus='virtio'/>
        </disk>
        <!-- 加入seed.img的信息。 -->
        <disk type='file' device='disk'>
            <driver name='qemu' type='raw'/>
            <source file='/path/to/your/seed.img'/> <!-- 填写seed镜像的绝对路径。 -->
            <target dev='vdb' bus='virtio'/>
        </disk>
        <interface type='network'>
            <source network='default'/>
            <model type='virtio'/>
        </interface>
        <console type='pty'>
            <target type='virtio' port='0'/>
        </console>
        <video>
            <model type='cirrus' vram='9216' heads='1'/>
            <alias name='video0'/>
        </video>
        <input type='tablet' bus='usb'/>
        <input type='mouse' bus='ps2'/>
        <graphics type='vnc' port='-1' autoport='yes'/>
    </devices>
</domain>
```

ii. 使用 `virsh` 命令启动虚拟机，命令示例如下。

> **说明** libvirt工具默认使用普通用户启动，请确认镜像文件及所在路径对普通用户是否具有相应的操作权限。

```
virsh define alinux2.xml
virsh start KVMName     # 请修改为KVM虚拟机的真实名称。
```

- 使用 `qemu-kvm` 命令行启动KVM虚拟机。您需要在命令行中追加如下参数信息，其中 `file` 参数信息修改为seed.img镜像真实的绝对路径。

  ```
  -drive file=/path/to/your/seed.img,if=virtio,format=raw
  ```

  关于libvirt和qemu-kvm命令的使用详情，请参见Red Hat官方说明。
- 使用图形界面（virt-manager）启动KVM虚拟机。在启动虚拟机之前，您需要在本地找到KVM虚拟机的配置文件，在文件内添加seed.img镜像文件的绝对路径。

5.3.3. Alibaba Cloud Linux 2使用说明

本文主要介绍在Alibaba Cloud Linux 2操作系统中查看系统或内核参数、设置内核转储功能的操作步骤，同时提供了Debuginfo包、源码包以及实验性软件包的获取方式。

查看或修改参数

- 查看或修改系统参数
  Alibaba Cloud Linux 2在配置文件*/etc/sysctl.d/50-aliyun.conf*中更新了下列内核配置参数，运行sysctl命令，可查看或修改Alibaba Cloud Linux 2运行时的系统参数。

系统参数	说明
`kernel.hung_task_timeout_secs = 240`	延长内核hung_task超时秒数，避免频繁的hung_task提示。
`kernel.panic_on_oops = 1`	允许内核发生Oops错误时抛出Kernel Panic异常，如果配置了Kdump则可自动捕获崩溃详情。
`kernel.watchdog_thresh = 50`	延长hrtimer、NMI、Soft Lockup以及Hard Lockup等事件的阈值，避免可能出现的内核误报。
`kernel.hardlockup_panic = 1`	允许内核发生Hard Lockup错误时抛出Kernel Panic异常，如果配置了Kdump则可自动捕获崩溃详情。

- 查看内核参数
  Alibaba Cloud Linux 2更新了下列内核参数，运行 `cat /proc/cmdline` 命令，可查看Alibaba Cloud Linux 2运行时的内核参数。

内核参数	说明
`crashkernel=0M-2G:0M,2G-8G:192M,8G-:256M`	为内核转储（Kdump）功能预留的内存空间。
`cryptomgr.notests`	关闭crypto在内核启动时的自检行为，加快启动速度。

内核参数	说明
`cgroup.memory=nokmem`	关闭Memory Cgroup的内核内存统计功能，避免出现潜在的内核不稳定问题。
`rcupdate.rcu_cpu_stall_timeout=300`	延长RCU CPU Stall Detector的超时阈值为300秒，避免内核误报。

开启或关闭内核转储（Kdump）功能

Alibaba Cloud Linux 2提供了Kdump服务。开启该服务后可捕获内核错误，方便您分析内核崩溃现象。

> **说明** 所选实例规格的内存小于或等于2 GiB时，无法使用Kdump服务。

- 依次运行以下命令可以开启Kdump服务。

```
# 先开启Kdump服务
sudo systemctl enable kdump.service
# 重启Kdump服务
sudo systemctl restart kdump.service
```

- 依次运行以下命令可以将Kdump服务预留的内存地址空间归还给操作系统，并彻底关闭Kdump服务。

```
# 先更改/sys/kernel/kexec_crash_size文件配置
sudo sh -c 'echo 0 > /sys/kernel/kexec_crash_size'
# 关闭Kdump服务
sudo systemctl disable kdump.service
# 停止Kdump服务
sudo systemctl stop kdump.service
```

> **说明** Kdump服务预留的内存地址空间归还给操作系统后，必须重启操作系统才可再次开启Kdump服务。

获取Debuginfo包和源码包

- 依次运行以下命令可以获取Debuginfo包。

```
# 先安装yum-utils
sudo yum install -y yum-utils
# 安装Debuginfo包，其中<packageName>为您预期安装的软件包名称
sudo debuginfo-install -y <packageName>
```

- 依次运行以下命令可以获取源码包。

```
# 先安装源码
sudo yum install -y alinux-release-source
# 安装yum-utils
sudo yum install -y yum-utils
# 安装源码包，其中<sourcePackageName>为您预期安装的软件包名称
sudo yumdownloader --source <sourcePackageName>
```

使用试验性支持的软件包

试验性支持的软件包指由阿里云官方提供，但未经严格测试，不保证质量的软件包。Alibaba Cloud Linux 2提供了普通试验性软件包和SCL插件方式支持的试验性软件包。

- 普通试验性软件包
  - `Golang 1.12`
  - `Golang 1.13`

  依次运行以下命令可以安装软件包。

```
# 先开启YUM仓库支持
sudo yum install -y alinux-release-experimentals
# 安装普通试验性软件包，其中<packageName>为您预期安装的软件包名称
sudo yum install -y <packageName>
```

- SCL插件方式支持的开发工具包
  - 基于 `GCC-7.3.1` 的开发工具包（devtoolset-7）
  - 基于 `GCC-8.2.1` 的开发工具包（devtoolset-8）
  - 基于 `GCC-9.1.1` 的开发工具包（devtoolset-9）

  依次运行以下命令可以安装软件包。

```
# 先安装scl-utils
sudo yum install -y scl-utils
# 打开YUM仓库支持
sudo yum install -y alinux-release-experimentals
# 从YUM源安装您需要的软件包，以下示例命令同时安装了SCL插件方式支持的所有开发工具包
sudo yum install -y devtoolset-7-gcc devtoolset-7-gdb devtoolset-7-binutils devtoolset-7-
make
sudo yum install -y devtoolset-8-gcc devtoolset-8-gdb devtoolset-8-binutils devtoolset-8-
make
sudo yum install -y devtoolset-9-gcc devtoolset-9-gdb devtoolset-9-binutils devtoolset-9-
make
```

安装成功后，您即可使用高版本的GCC以及相关工具。示例命令如下：

```
# 先查看现有的SCL，需要指定库名，本示例命令中，库名为devtoolset-7
scl -l devtoolset-7
# 运行相关的SCL软件
scl enable devtoolset-7 'gcc --version'
```

5.3.4. 开启或关闭IPv6

本文主要介绍如何开启或关闭Alibaba Cloud Linux 2操作系统中的IPv6。

前提条件

- 选用的实例规格必须支持IPv6，详情请参见实例规格族。
- 创建的实例必须在支持开通IPv6网段的地域下，并搭建了IPv6专有网络，详情请参见搭建IPv6专有网络。

背景信息

Alibaba Cloud Linux 2镜像在 `aliyun-2.1903-x64-20G-alibase-20190829.vhd` 及之前的版本未开启IPv6，从 `aliyun_2_1903_x64_20G_alibase_20200221.vhd` 版本开始默认开启了IPv6。

本文所有操作步骤均是在ECS实例内进行，远程连接实例的方式请参见连接方式概述ECS远程连接操作指南。

暂时开启IPv6

在镜像 `aliyun_2_1903_64_20G_alibase_20190619.vhd` 及之前的版本中，*/etc/systemd/network/*目录下的*.network*文件只配置了 `DHCP=ipv4` ，您可以按照以下步骤修改文件内容来暂时开启IPv6。

> **注意** 实例一旦停止或重启，开启IPv6的相关配置会失效。

1. 运行以下命令进入*/etc/systemd/network/*目录。

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

2. 使用命令 `ls` 查询该目录下的*.network*文件。

   本文以*50-dhcp.network*文件为例。

```
[root@alinux2 network]# ls
50-dhcp.network
```

3. 修改文件*50-dhcp.network*内容。

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

4. 按*i*进入编辑模式。

   将 `[Network]` 下的信息修改为 `DHCP=yes` 。

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

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

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

5. 运行以下命令开启IPv6。
   - 开启所有网络接口。

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

   - 开启指定网络接口示例。

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

6. 重启systemd-networkd服务使配置生效。

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

持久开启IPv6

以下操作步骤将持久化开启IPv6，实例重启后配置仍然生效。

1. 修改 `/etc/sysctl.conf` 配置文件。

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

2. 按进入编辑模式。使用以下任一方式修改文件内容。
   - 删除下列配置信息。

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

   - 修改对应的配置信息为如下内容。

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

     如果需要开启指定网络接口，修改信息示例如下。

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

   修改完成后按*Esc*键，并输入 `:wq` 后按下回车键，保存并退出。
3. 验证 `/etc/sysctl.conf` 配置信息是否与initramfs中的 `/etc/sysctl.conf` 存在差异。

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

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

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

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

5. 重启实例。

   ```
   sudo reboot
   ```

6. 执行 `ifconfig` 命令判断是否已开启IPv6。

   如果网络配置信息包含以下信息，表示IPv6已开启。

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

暂时关闭IPv6

以下命令将暂时关闭IPv6。

> **注意** 实例一旦停止或重启，关闭IPv6的相关配置会失效。

- 关闭所有网络接口。

  ```
  sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
  sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
  ```

- 关闭指定网络接口示例。

```
sudo sysctl -w net.ipv6.conf.eth0.disable_ipv6=1
```

持久关闭IPv6

以下操作步骤将持久化关闭IPv6，实例重启后配置仍然生效。您可以通过以下任一方式关闭IPv6。

- 通过以下任一命令行参数持久化关闭IPv6。

```
sudo grubby --args="ipv6.disale_ipv6=1" --update-kernel=/boot/vmlinuz-$(uname -r)
```

```
sudo grubby --args="ipv6.disale=1" --update-kernel=/boot/vmlinuz-$(uname -r)
```

> **说明** 参数 `--args="ipv6.disale_ipv6=1"` 与 `--args="ipv6.disale=1"` 均能实现关闭IPv6的功能，区别在于设置 `--args="ipv6.disale_ipv6=1"` 参数只关闭网络接口IPv6；而设置 `--args="ipv6.disale=1"` 参数直接禁用了IPv6的内核模块，详情请参见Linux内核IPv6说明。

- 通过修改*/etc/sysctl.conf*文件持久化关闭IPv6。

1. 修改 `/etc/sysctl.conf` 配置文件。

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

2. 按i进入编辑模式，将对应的配置信息修改为如下所示。

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

如果需要关闭指定网络接口，修改示例如下。

```
net.ipv6.conf.eth0.disable_ipv6=1
```

3. 重启实例。

```
sudo reboot
```

4. 执行 `ifconfig` 命令判断是否已关闭IPv6。

如果网络配置信息没有包含以下信息，表示IPv6已关闭。

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

支持多网卡配置

如果您需要配置多个IPv6地址，可以参见下述方式进行配置。

1. 运行以下命令进入 `/etc/systemd/network/` 目录。

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

2. 使用命令 `ls` 查询该目录下的 `.network` 文件。

例如， `10-eth0.network` 文件。

3. 使用命令 `cp` 复制一个新的配置文件。

例如：

```
cp 10-eth0.network 20-dhcp.network
```

4. 运行以下命令修改配置文件。

```
sed -i 's/^Name.*$/Name=*/g' /etc/systemd/network/20-dhcp.network
```

5. 重启systemd-networkd服务使配置生效。

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

5.3.5. 如何安装并启用高版本的curl

Alibaba Cloud Linux 2默认的curl版本为7.29.0。当您的业务需要使用更高版本的curl时，可以根据本文的操作步骤安装并启用 `curl-7.61.1` 。

背景信息

Alibaba Cloud Linux 2基于兼容性问题的考虑，不支持直接在系统中升级curl，因此提供了安装并启用 `curl-7.61.1` 版本的方式。

操作步骤

1. 运行以下命令，安装阿里云exp源。

```
sudo yum install -y alinux-release-experimentals
```

2. 依次运行以下命令，安装curl及依赖包。
   i. 安装curl。

   ```
   sudo yum install -y httpd24-curl
   ```

   ii. 安装curl的依赖包httpd24-libcurl-devel。

   ```
   sudo yum install -y httpd24-libcurl-devel
   ```

3. 运行以下命令，启用curl。

```
source /opt/rh/httpd24/enable
```

4. 运行以下命令，查看curl版本。

```
curl --version
```

如下图所示，表示已成功安装 `curl-7.61.1` 。

```
[root@test ~]# curl --version
curl 7.61.1 (x86_64-koji-linux-gnu) libcurl/7.61.1 NSS/3.44 zlib/1.2.7 libssh2/1.8.0 nghttp2/1.7.1
Release-Date: 2018-09-05
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtsp scp sftp smb smbs smtp smtps telnet tftp
Features: AsynchDNS IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz HTTP2 UnixSockets HTTPS-proxy
```

5.4. 安全

5.4.1. Alibaba Cloud Linux等保2.0三级版镜像概述

Alibaba Cloud Linux等保2.0三级版镜像是基于Alibaba Cloud Linux默认标准镜像进行等保加固的镜像版本，该镜像符合等保2.0三级安全保护的基本要求。

什么是等保2.0三级版镜像

阿里云根据国家信息安全部发布的*GB/T22239-2019信息安全技术网络安全等级保护基本要求*中对操作系统提出的一些等级保护要求，推出自研云原生操作系统Alibaba Cloud Linux等保2.0三级版镜像。您使用本镜像可满足以下等保合规要求：

- 身份鉴别
- 访问控制
- 安全审计
- 入侵防范
- 恶意代码防范

关于等保合规检查规则的更多信息，请参见Alibaba Cloud Linux等保2.0三级版镜像检查规则说明。

优势

使用等保2.0三级版镜像，您可以获得以下优势：

- 节省成本：Alibaba Cloud Linux等保2.0三级版镜像是完全免费提供使用的。
- 节省人力：云安全中心提供基线检查策略，系统将自动判断实例是否达到了等保合规的要求。
- 节省时间：您可以通过已完成等保加固的自定义镜像，批量创建ECS实例。

计费

Alibaba Cloud Linux等保2.0三级版是免费镜像，但当您选用等保2.0三级版镜像创建ECS实例时，需要支付其他资源产生的费用，如vCPU、内存、存储、公网带宽和快照等。计费详情，请参见计费概述。

应用场景

当您的云上业务需要满足*GB/T22239-2019信息安全技术网络安全等级保护基本要求*时，由于等保合规要求复杂，技术要求高。您可以选择Alibaba Cloud Linux等保2.0三级版镜像创建对应的ECS实例，以快速满足网络安全等级保护2.0规定的要求。

使用说明

相关操作	说明
使用Alibaba Cloud Linux等保2.0三级版镜像	您可以在创建ECS实例时，选择使用Alibaba Cloud Linux 2或者Alibaba Cloud Linux 3等保2.0三级版镜像。当您成功创建对应的ECS实例后，第一次远程连接该实例时，需要立即完成等级保护加固的配置。
配置Alibaba Cloud Linux等保2.0三级版镜像基线检查策略	阿里云已为Alibaba Cloud Linux 2和Alibaba Cloud Linux 3等保2.0三级版镜像提供了等保合规的基线检查标准和扫描程序，您可以通过云安全中心完成相关操作。
使用等保加固后的自定义镜像批量创建实例	当您的业务需要多台Alibaba Cloud Linux 2或者Alibaba Cloud Linux 3等保2.0三级版镜像的ECS实例时，您可以通过已完成等保加固的自定义镜像批量创建实例。该方式将节省每一台实例都需要完成等保加固配置的时间。

使用等保2.0三级版镜像常见的问题及解决方案，请参见Alibaba Cloud Linux等保2.0三级版镜像FAQ。

5.4.2. Alibaba Cloud Linux CIS安全基线

Alibaba Cloud Linux安全基线已经通过CIS认证，CIS发布了Alibaba Cloud Linux CIS Benchmarks。本文主要介绍Alibaba Cloud Linux CIS Benchmarks及下载方式。

背景信息

CIS全称为Center for Internet Security，即互联网安全中心。CIS是一个具有几十年历史的知名非营利信息安全组织，致力于采用线上社区的模式与大公司、政府、学术机构一起打造优秀的安全实践解决方案（即各种Benchmarks）。更多信息，请参见CIS官网。目前多数Linux操作系统发行版已提供了CIS Benchmarks，例如：Alibaba Cloud Linux、CentOS、Ubuntu等。基于CIS Benchmarks提供的优秀安全实践解决方案，已成为云上操作系统安全的重要评判标准之一。

Alibaba Cloud Linux 2安全基线在2019年08月16日正式通过了CIS的全部认证流程，CIS对外发布*CIS Aliyun Linux 2 Benchmark v1.0.0*。Alibaba Cloud Linux 3安全基线在2022年02月06日正式通过了CIS的全部认证流程，CIS对外发布*CIS Alibaba Cloud Linux 3 benchmark v1.0.0*。Alibaba Cloud Linux是中国第一个完成CIS认证的操作系统。

Alibaba Cloud Linux CIS Benchmarks说明

关于Alibaba Cloud Linux CIS Benchmarks的说明信息如下：

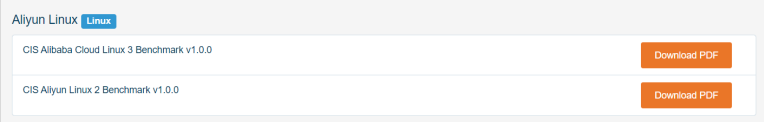
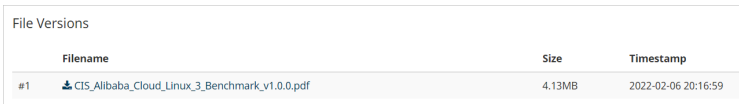
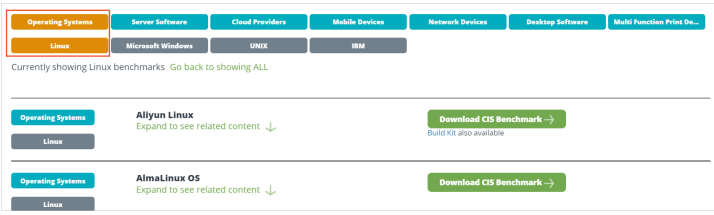
- Alibaba Cloud Linux CIS Benchmarks从初始设置（Initial Setup）、服务（Services）、网络配置（Network Configuration）、日志与审计（Logging and Auditing）、访问，认证和授权（Access, Authentication and Authorization）、系统维护（System Maintenance）六个方面的200余项提供了具体的安全建议。其中：
  - *CIS Aliyun Linux 2 Benchmark v1.0.0*共204项。
  - *CIS Alibaba Cloud Linux 3 benchmark v1.0.0*共266项。
- 每一项包含了安全等级（Profile Applicability）、计分规则（Scoring Information）、描述（Description）、基本原理（Rationale）、影响（Impact）、审计（Audit）、修复方法（Remediation）以及参考（References）等具体内容。其中按照每一项所处的安全等级分为Level 1和Level 2。Level 1与Level 2的主要区别如下：
  - Level 1表示此条目是安全加固的基础项，且不会带来较大的性能影响。
  - Level 2表示此条目适用于安全性更高的场景，且可能会对系统带来一定的性能开销。
- 从计分规则（Scoring Information）的维度出发，*CIS Aliyun Linux 2 Benchmark*分为 `Scored` 和 `Not Scored` 两类。*CIS Alibaba Cloud Linux 3 Benchmark*分为 `Automated` 和 `Manual` 两类。具体说明如下：
  - `Scored` 与 `Automated` ：表示此条目为计分项。如果验证系统为安全，则加分；如果验证系统不安全，则减分。
  - `Not Scored` 与 `Manual` ：表示此条目不作为计分项。无论验证系统是否安全，均不增减计分。

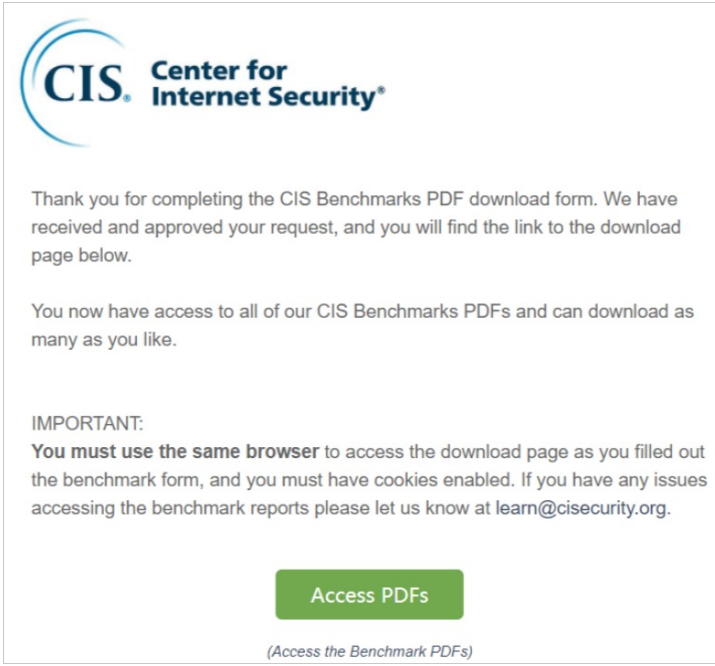
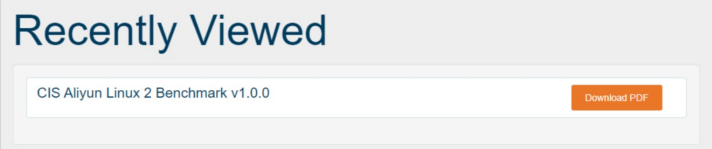
> **说明** 您在使用Alibaba Cloud Linux CIS Benchmarks时，可根据自身实际需求，灵活选择合适的安全加固项，以提高您的Alibaba Cloud Linux的安全性。此外，您也可以参考Alibaba Cloud Linux CIS Benchmarks来提高其他兼容的操作系统的安全性。

下载Alibaba Cloud Linux CIS Benchmarks

您可以通过多种方式下载Alibaba Cloud Linux CIS Benchmarks，具体说明如下表所示。

下载方式	具体操作说明

下载方式	具体操作说明
通过CIS下载页直接下载CIS Benchmarks	访问CIS下载页，然后根据您的Alibaba Cloud Linux版本选择下载对应的CIS Benchmarks。具体说明如下： ● 如果您的操作系统版本为Alibaba Cloud Linux 2（原Aliyun Linux 2），请找到*CIS Aliyun Linux 2 Benchmark v1.0.0*，然后单击**Download PDF**。 ● 如果您的操作系统版本为Alibaba Cloud Linux 3，请找到*CIS Alibaba Cloud Linux 3 Benchmark v1.0.0*，然后单击**Download PDF**。 
通过注册CIS账号下载CIS Benchmarks	根据您的Alibaba Cloud Linux版本选择访问以下PDF下载页： **说明** 以下PDF下载页需要注册CIS账号并登录CIS。如果您已拥有CIS账号，直接根据页面提示登录CIS即可。如果您未拥有CIS账号，请在页面单击**Register Now!**并根据页面提示完成账号注册，之后使用新账号登录CIS。登录CIS后，您还可以参与CIS社区的讨论与开发。 ● 如果您的操作系统版本为Alibaba Cloud Linux 2（原Aliyun Linux 2），请访问CIS Aliyun Linux 2 Benchmark v1.0.0 PDF下载页，然后在如下图所示的位置下载相应的CIS Benchmark。 ● 如果您的操作系统版本为Alibaba Cloud Linux 3，请访问CIS Alibaba Cloud Linux 3 benchmark v1.0.0 PDF页面，然后在如下图所示的位置下载相应的CIS Benchmark。 
	您可以通过CIS官网设置邮箱信息，然后通过指定邮箱接收并下载相应的CIS Benchmark。具体操作说明如下： 1. 访问CIS Benchmarks官方主页。 2. 在如下图所示的区域，单击**Operating Systems**，然后单击**Linux**。  3. 找到Aliyun Linux CIS Benchmark，然后单击**Download CIS Benchmark→**。

下载方式	具体操作说明
通过邮件下载CIS Benchmarks	4. 在**FREE BENCHMARKS**区域，填写个人信息以及邮箱地址，然后单击**Get Free Benchmarks Now**。 5. 登录邮箱并查看邮件。 CIS的邮件可能会有几分钟延迟，成功收到邮件后，邮件内容如下图所示。  6. 单击**Access PDFs**，然后找到对应的CIS Benchmark。 ○ 如果您的操作系统版本为Alibaba Cloud Linux 2（原Aliyun Linux 2），请找到*CIS Aliyun Linux 2 Benchmark v1.0.0*，然后单击**Download PDF**。 ○ 如果您的操作系统版本为Alibaba Cloud Linux 3，请找到*CIS Alibaba Cloud Linux 3 Benchmark v1.0.0*，然后单击**Download PDF**。 以Alibaba Cloud Linux 2为例，下载页面信息如下图所示。 

相关链接

CIS提供了Alibaba Cloud Linux CIS Benchmarks使用说明供您参考：

- CIS Aliyun Linux 2 Benchmark v1.0.0
- CIS Alibaba Cloud Linux 3 Benchmark v1.0.0

5.4.3. 订阅Alibaba Cloud Linux 2安全漏洞（CVE）公告

软件包安全漏洞（CVE）修复在Alibaba Cloud Linux 2版本支持期限内会持续更新，您可以利用浏览器插件，订阅Alibaba Cloud Linux 2 CVE公告，方便快捷地查看CVE更新情况。

背景信息

本文以Google Chrome浏览器为示例，安装RSS Feed Reader插件用于订阅Alibaba Cloud Linux 2 CVE更新记录。您也可以自行选择其它常用的浏览器插件订阅Alibaba Cloud Linux 2 CVE更新记录。

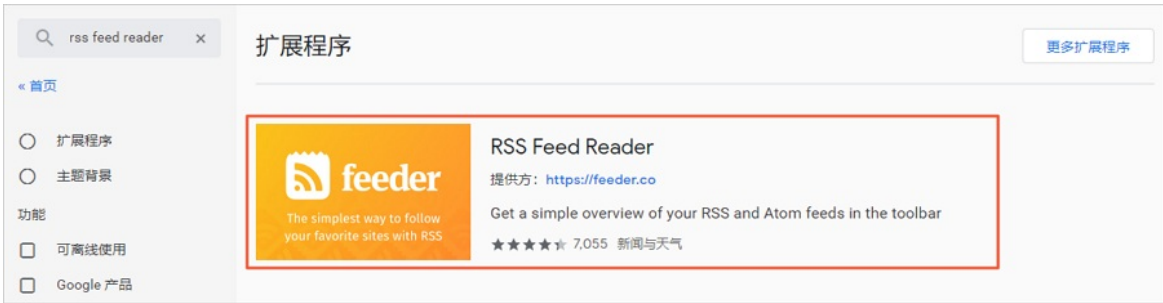
Alibaba Cloud Linux 2 安全中心简介

阿里云操作系统团队为保障Alibaba Cloud Linux 2发行版的系统安全性，会紧密跟进Linux业界与社区发现的各种软件问题及安全漏洞（CVE），并及时提供修复策略到Yum Repositories，用于修复软件缺陷、增强安全功能以及修补安全漏洞。最终通过安全中心实时公告出安全漏洞修复策略。

（可选）安装RSS Feed Reader插件

如果您的Google Chrome浏览器未安装RSS Feed Reader插件，需要先安装插件。

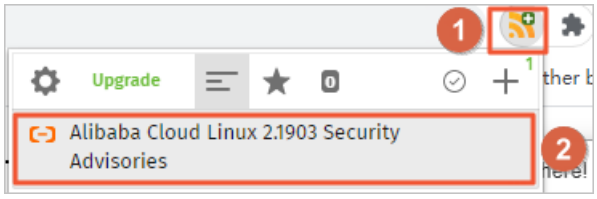
1. 在本地物理主机中打开Google Chrome浏览器。
2. 在顶部书签栏，单击**应用**，然后单击**Chrome 网上应用店**。
3. 在**chrome 网上应用店**页面的左上角，单击搜索栏并输入 `rss feed reader` 进行搜索。
4. 在搜索结果中，单击**RSS Feed Reader**插件，进入详情页。



5. 在**RSS Feed Reader**详情页，单击**添加至 Chrome**，然后单击**添加至扩展程序**。
   当详情页中的**添加至 Chrome**变更为**从 Chrome 中删除**时，表示已成功添加插件至扩展程序。

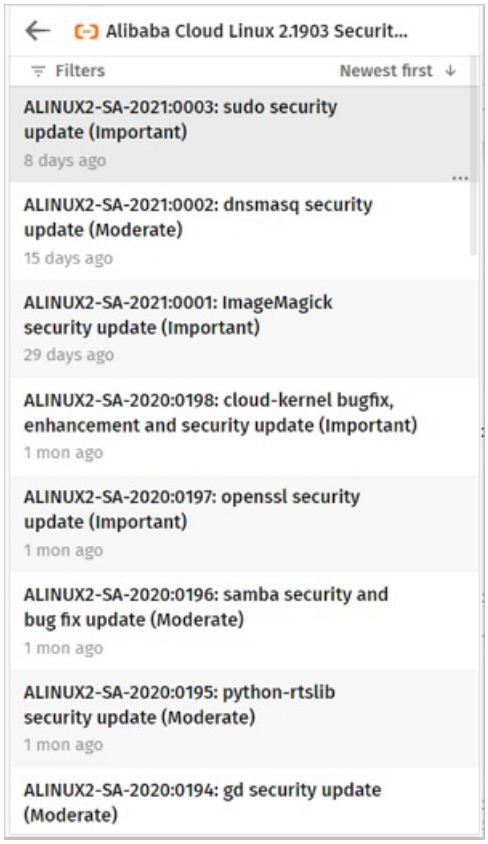
订阅公告Alibaba Cloud Linux 2 安全漏洞（CVE）公告

1. 订阅Alibaba Cloud Linux 2 CVE更新记录。
   i. 使用Google Chrome浏览器访问Alibaba Cloud Linux 2 CVE更新记录。
   ii. 单击页面右上角的 RSS 图标。
   iii. 等待弹出对话框后，单击**Subscribe**。
   当对话框中的**Subscribe**变更为**Following**时，表示成功订阅。
2. 通过RSS Feed Reader插件查看Alibaba Cloud Linux 2 CVE更新记录。



i. 在Google Chrome浏览器右上角，单击RSS Feed Reader插件图标（图中①所示）。

ii. 单击**Alibaba Cloud Linux 2.1903 Security Advisories**（图中②所示）。
更新记录展示结果如下所示：



5.4.4. 基于YUM的安全更新操作（Alibaba Cloud Linux 3）

本文主要介绍如何使用yum查询、检查以及安装Alibaba Cloud Linux 3操作系统的安全更新。

前提条件

已创建了操作系统为Alibaba Cloud Linux 3的ECS实例。具体操作，请参见创建方式导航。

背景信息

Alibaba Cloud Linux 3发行版为保障系统的安全性，会紧密跟进业界与社区发现的软件问题及安全漏洞（CVE），及时更新包括内核在内的软件包、修复软件缺陷、修补安全漏洞以及增强安全功能。关于Alibaba Cloud Linux 3安全更新记录，请参见Alibaba Cloud Linux 3安全公告。

Alibaba Cloud Linux 3安全更新根据CVE的通用漏洞评估方法（CVSS3）的评分，将安全更新分为以下四个等级：

- Critical：高风险，必须更新

- Important：较高风险，强烈建议更新
- Moderate：中等风险，推荐更新
- Low：低风险，可选更新

查询安全更新

查询安全更新的yum命令格式如下。

```
yum updateinfo <command> [option]
```

命令内参数的取值说明如下。

变量名称	取值
<command>	• `list`：查询可用的安全更新列表。 • `info` *<update_id>*：查询指定的安全更新详情。其中参数*<update_id>*的取值为Alibaba Cloud Linux 3安全公告中的Advisory ID。
[option]	• `--sec-severity=`*<SEVS>*：指定安全更新级别，参数*<SEVS>*为指定的安全更新级别。 说明 您可以指定多个安全更新的级别，以半角逗号（,）分隔，区分大小写。 格式说明： ○ 如果只指定一个安全更新级别进行查询，示例格式为 `--sec-severity=Moderate`。 ○ 如果同时指定多个安全更新级别进行查询，示例格式为 `--sec-severity={Moderate,Important}`。 • `--cve=`*<CVE ID>*：指定CVE ID。CVE ID可从Alibaba Cloud Linux 3安全公告中获取。

查询安全更新的命令使用示例如下。

- 运行**yum updateinfo --help**命令可以获取命令的帮助信息。
- 运行以下命令，查询当前全部可用的安全更新信息。

  ```
  yum updateinfo
  ```

  查询结果示例如下所示：

  ```
  Last metadata expiration check: 0:06:42 ago on Wed 02 Jun 2021 03:05:30 AM EDT.
  Updates Information Summary: available
      3 Security notice(s)
          2 Important Security notice(s)
          1 Moderate Security notice(s)
  ```

- 运行以下命令，查询当前可用的安全更新列表。

  ```
  yum updateinfo list
  ```

  查询结果示例如下所示：

```
Last metadata expiration check: 0:09:05 ago on Wed 02 Jun 2021 03:05:30 AM EDT.
ALINUX3-SA-2021:0008 Moderate/Sec.  gnutls-3.6.14-7.1.al8.x86_64
ALINUX3-SA-2021:0029 Important/Sec. gnutls-3.6.14-8.1.al8.x86_64
ALINUX3-SA-2021:0028 Important/Sec. libldb-2.1.3-3.1.al8.x86_64
ALINUX3-SA-2021:0029 Important/Sec. nettle-3.4.1-4.1.al8.x86_64
```

- 命令 `yum updateinfo info <update_id>` 可以查询指定安全更新的内容，使用示例如下。
  例如，*<update_id>*的取值为 `ALINUX3-SA-2021:0008` ，则需要运行以下命令。

  ```
  yum updateinfo info ALINUX3-SA-2021:0008
  ```

  查询结果示例如下所示：

  ```
  Last metadata expiration check: 0:11:58 ago on Wed 02 Jun 2021 03:05:30 AM EDT.
  ================================================================================
    ALINUX3-SA-2021:0008: gnutls security and bug fix update (Moderate)
  ================================================================================
    Update ID: ALINUX3-SA-2021:0008
         Type: security
      Updated: 1969-12-31 19:00:00
         CVEs: CVE-2020-24659
  Description: Package updates are available for Alibaba Cloud Linux 3 that fix the followi
  ng vulnerabilities:
             :
             : CVE-2020-24659:
             : An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL
  pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpect
  ed timing, and then an invalid second handshake occurs. The crash happens in the applicat
  ion's error handling path, where the gnutls_deinit function is called after detecting a h
  andshake failure.
             :
     Severity: Moderate
  ```

- 运行以下命令，指定安全更新级别进行查询。

  ```
  yum updateinfo list --sec-severity=Moderate
  ```

  查询结果示例如下所示：

  ```
  Last metadata expiration check: 0:05:25 ago on Mon 07 Jun 2021 09:08:25 AM EDT.
  ALINUX3-SA-2021:0008 Moderate/Sec. gnutls-3.6.14-7.1.al8.x86_64
  ```

检查安全更新

命令 `yum check-update --security` 可以检查系统当前可用的安全更新信息。可以在命令后追加参数 `--sec-severity=<SEVS>` 来检查指定级别的安全更新，参数*<SEVS>*为指定的安全更新级别。

> **说明** 您可以指定多个安全更新的级别，以半角逗号（,）分隔，区分大小写。

检查安全更新的使用示例如下。

- 示例一：运行以下命令，检查所有安全更新信息。

  ```
  yum check-update --security
  ```

查询结果示例如下所示：

```
Last metadata expiration check: 0:08:41 ago on Wed 02 Jun 2021 05:24:55 PM CST.
nss.x86_64                        3.53.1-17.1.al8                 alinux3-updates
nss-softokn.x86_64                3.53.1-17.1.al8                 alinux3-updates
nss-softokn-freebl.x86_64         3.53.1-17.1.al8                 alinux3-updates
nss-sysinit.x86_64                3.53.1-17.1.al8                 alinux3-updates
nss-util.x86_64                   3.53.1-17.1.al8                 alinux3-updates
perl-Errno.x86_64                 1.28-417.2.al8                  alinux3-updates
perl-IO.x86_64                    1.38-417.2.al8                  alinux3-updates
```

- 示例二：运行以下命令，检查高风险和较高风险的安全更新信息。

```
yum check-update --security  --sec-severity={Critical,Important}
```

查询结果示例如下所示：

```
Last metadata expiration check: 0:10:23 ago on Wed 02 Jun 2021 05:24:55 PM CST.
gnutls.x86_64                      3.6.14-8.2.al8              alinux3-updates
nss.x86_64                         3.53.1-17.1.al8             alinux3-updates
nss-softokn.x86_64                 3.53.1-17.1.al8             alinux3-updates
nss-softokn-freebl.x86_64          3.53.1-17.1.al8             alinux3-updates
nss-sysinit.x86_64                 3.53.1-17.1.al8             alinux3-updates
nss-util.x86_64                    3.53.1-17.1.al8             alinux3-updates
perl-Errno.x86_64                  1.28-417.2.al8              alinux3-updates
perl-IO.x86_64                     1.38-417.2.al8              alinux3-updates
```

安装安全更新

您可以通过命令 `yum upgrade` 指定安全更新级别或者CVE ID，安装安全更新。

- 命令 `yum upgrade --security` 可以安装安全更新，可在该命令后追加参数 `--sec-severity=<SEVS>` 来安装指定级别的安全更新，*<SEVS>*为指定的安全更新级别。

> **说明** 您可以指定多个安全更新的级别，以半角逗号（,）分隔，区分大小写。

操作示例：
运行以下命令，安装高风险和较高风险的安全更新。

```
yum upgrade --security --sec-severity={Critical,Image}
```

安装过程中的回显信息示例如下所示：

```
Last metadata expiration check: 0:06:43 ago on Wed 02 Jun 2021 03:51:48 AM EDT.
Dependencies resolved.
================================================================================
 Package              Arch       Version              Repository          Size
================================================================================
Upgrading:
...
Transaction Summary
================================================================================
Upgrade  12 Packages
Total download size: 3.9 M
Is this ok [y/N]:
```

- 命令 `yum upgrade -cve=<CVE ID>` 可以安装指定CVE的安全更新，参数 `-cve=<CVE ID>` 为指定的CVE ID。

  > **说明** 您可以指定多个CVE ID，以半角逗号（,）分隔，区分大小写。

  操作示例：
  运行以下命令，安装 `CVE-2020-24659` 安全更新。

  ```
  yum upgrade --cve=CVE-2020-24659
  ```

  安装过程中的回显信息示例如下所示：

  ```
  Last metadata expiration check: 0:02:44 ago on Wed 02 Jun 2021 04:17:27 AM EDT.
  Dependencies resolved.
  ==========================================================================================
   Package        Architecture   Version                 Repository              Size
  ==========================================================================================
  Upgrading:
  ...
  Transaction Summary
  ==========================================================================================
  Upgrade  1 Package
  Total download size: 1.0 M
  Is this ok [y/N]
  ```

5.4.5. 基于YUM的安全更新操作（Alibaba Cloud Linux 2）

本文主要介绍如何使用yum查询、检查以及安装Alibaba Cloud Linux 2操作系统的安全更新。

背景信息

Alibaba Cloud Linux 2发行版为保障系统的安全性，会紧密跟进业界与社区发现的软件问题及安全漏洞（CVE），及时更新包括内核在内的软件包，修复软件缺陷，以及修补安全漏洞，增强安全功能。Alibaba Cloud Linux 2安全更新记录请参见Alibaba Cloud Linux 2安全公告。

Alibaba Cloud Linux 2安全更新根据CVE的通用漏洞评估方法（CVSS3）的评分，将安全更新分为以下四个等级：

- Critical：高风险，必须更新
- Important：较高风险，强烈建议更新
- Moderate：中等风险，推荐更新
- Low：低风险，可选更新

查询安全更新

查询安全更新的yum命令格式如下。

```
yum updateinfo <command> [option]
```

命令内参数的取值说明如下。

变量名称	取值
command	• `list` ：查询可用的安全更新列表。 • `info <update_id>` ：查询指定的安全更新详情。其中参数 `<update_id>` 的取值为Alibaba Cloud Linux 2安全公告中的Advisory ID。
option	• `--sec-severity=<SEVS>` 或 `--secseverity=<SEVS>` ：指定安全更新级别，参数 `<SEVS>` 为指定的安全更新级别。 **注意** 安全更新级别的取值严格区分大小写。 • `--cve=<CVES>` ：指定CVE ID。CVE ID可从Alibaba Cloud Linux 2安全公告中获取。

查询安全更新的命令使用示例如下。

- 命令 `yum updateinfo --help` 可以获取命令的帮助信息。
- 命令 `yum updateinfo` 可以查询当前全部可用的安全更新信息，使用示例如下。

```
# yum updateinfo
Loaded plugins: fastestmirror
Determining fastest mirrors
base
| 3.1 kB  00:00:00
extras
| 2.5 kB  00:00:00
plus
| 2.5 kB  00:00:00
updates
| 2.9 kB  00:00:00
(1/6): extras/2.1903/x86_64/primary_db
| 149 kB  00:00:00
(2/6): base/2.1903/x86_64/group_gz
| 101 kB  00:00:00
(3/6): updates/2.1903/x86_64/updateinfo
|  81 kB  00:00:00
(4/6): plus/2.1903/x86_64/primary_db
| 1.5 MB  00:00:00
(5/6): base/2.1903/x86_64/primary_db
| 4.9 MB  00:00:00
(6/6): updates/2.1903/x86_64/primary_db
| 6.1 MB  00:00:00
Updates Information Summary: updates
    17 Security notice(s)
         7 Important Security notice(s)
         6 Moderate Security notice(s)
         4 Low Security notice(s)
updateinfo summary done
```

- 命令 `yum updateinfo list` 可以查询当前可用的安全更新列表，使用示例如下。

```
# yum updateinfo list
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
ALINUX2-SA-2019:0055 Moderate/Sec.  binutils-2.27-41.base.1.al7.x86_64
ALINUX2-SA-2019:0058 Low/Sec.       curl-7.29.0-54.1.al7.x86_64
ALINUX2-SA-2019:0059 Low/Sec.       elfutils-default-yama-scope-0.176-2.1.al7.n
...
```

- 命令 `yum updateinfo info <update_id>` 可以查询指定安全更新的内容，使用示例如下。

```
# yum updateinfo info ALINUX2-SA-2020:0005
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
==============================================================================
  ALINUX2-SA-2020:0005: nss, nss-softokn, nss-util security update (Important)
==============================================================================
  Update ID : ALINUX2-SA-2020:0005
    Release : Alibaba Cloud Linux 2.1903
       Type : security
     Status : stable
     Issued : 2020-01-03
       CVEs : CVE-2019-11729
            : CVE-2019-11745
Description : Package updates are available for Alibaba Cloud Linux 2.1903 that fix
            : the following vulnerabilities:
            :
            : CVE-2019-11729:
            : Empty or malformed p256-ECDH public keys may
            : trigger a segmentation fault due values being
            : improperly sanitized before being copied into
            : memory and used. This vulnerability affects
            : Firefox ESR < 60.8, Firefox < 68, and Thunderbird
            : < 60.8.
            :
            : CVE-2019-11745:
            : When encrypting with a block cipher, if a call to
            : NSC_EncryptUpdate was made with data smaller than
            : the block size, a small out of bounds write could
            : occur. This could have caused heap corruption and
            : a potentially exploitable crash. This
            : vulnerability affects Thunderbird < 68.3, Firefox
            : ESR < 68.3, and Firefox < 71.
            :
   Severity : Important
updateinfo info done
```

检查安全更新

命令 `yum check-update --security` 可以检查系统当前可用的安全更新信息。可以在命令后追加参数 `--secseverity=<SEVS>` 来检查指定级别的安全更新，参数 `<SEVS>` 为指定的安全更新级别。

> **注意** 您可以指定多个安全更新的级别，以逗号（,）分隔，严格区分大小写。

检查安全更新的使用示例如下。

- 示例一。

```
# yum check-update --security |grep available
49 package(s) needed for security, out of 183 available
```

- 示例二。

```
# yum check-update --security --secseverity=Critical,Important |grep available
30 package(s) needed for security, out of 183 available
```

安装安全更新

您可以使用命令 `yum upgrade` 通过以下任意一种方式安装安全更新。

- 命令 `yum upgrade --security` 可以安装安全更新，可在该命令后追加参数 `--secseverity=<SEVS>` 来安装指定级别的安全更新，参数 `<SEVS>` 为指定的安全更新级别。

  > **注意** 您可以指定多个安全更新的级别，以逗号（,）分隔，严格区分大小写。

  该命令的使用示例如下。

```
# yum upgrade --security --secseverity=Critical,Important
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
...
[snipped]
...
Transaction Summary
================================================================================================
=================================================================================
Upgrade  30 Packages (+1 Dependent package)
Total download size: 91 M
Is this ok [y/d/N]:
```

- 命令 `yum upgrade -cves=<CVES>` 可以安装指定CVE的安全更新，参数 `<CVES>` 为指定的CVE ID。

  > **注意** 您可以指定多个CVE ID，以逗号（,）分隔，严格区分大小写。

  该命令的使用示例如下。

```
# yum upgrade --cve=CVE-2019-11729,CVE-2019-11745
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
...
[snipped]
...
Dependencies Resolved
=====================================================================================
================================================================================
 Package                                          Arch                          Vers
ion                                     Repository                          Size
=====================================================================================
================================================================================
Updating:
 nss                                              x86_64                        3.44
.0-7.1.al7                              updates                            854 k
 nss-softokn                                      x86_64                        3.44
.0-8.1.al7                              updates                            330 k
 nss-softokn-freebl                               x86_64                        3.44
.0-8.1.al7                              updates                            225 k
 nss-sysinit                                      x86_64                        3.44
.0-7.1.al7                              updates                             65 k
 nss-tools                                        x86_64                        3.44
.0-7.1.al7                              updates                            528 k
 nss-util                                         x86_64                        3.44
.0-4.1.al7                              updates                             79 k
Updating for dependencies:
 nspr                                             x86_64                        4.21
.0-1.1.al7                              updates                            127 k
Transaction Summary
=====================================================================================
================================================================================
Upgrade  6 Packages (+1 Dependent package)
Total download size: 2.2 M
Is this ok [y/d/N]:
```

说明 通过命令`man yum`可知，`yum upgrade`命令等同于`yum update --obsoletes`。因配置文件*/etc/yum.conf*中默认开启了`obsoletes`，所以`yum upgrade`也等同于`yum update`。

5.4.6. 处理Alibaba Cloud Linux安全更新提醒

Alibaba Cloud Linux操作系统中默认安装并开启了update-motd服务，当系统检测有可用的安全更新时，会在您登录ECS实例时显示安全更新的提醒。本文介绍如何处理这类Alibaba Cloud Linux的安全更新。

背景信息

Alibaba Cloud Linux发行版为保障系统的安全性，会紧密跟进业界与社区发现的软件问题及安全漏洞（CVE），及时更新包括内核在内的软件包，从而修复软件缺陷、修补安全漏洞并增强安全功能。Alibaba Cloud Linux的安全更新记录，请参见Alibaba Cloud Linux 2安全公告和Alibaba Cloud Linux 3安全公告。

为了更好地提醒您关注安全更新相关信息，Alibaba Cloud Linux操作系统内安装并默认安装并开启了 `update-motd` 服务，该服务会周期性的调用**yum check-update**命令（Alibaba Cloud Linux 2）或者**dnf updateinfo**命令（Alibaba Cloud Linux 3），用于检查并获取系统当前可用的安全更新。当您通过终端远程登录ECS实例时，系统会通过登录提示界面（motd）展示安全更新的提醒信息。例如：

- Alibaba Cloud Linux 2提醒信息示例如下：

```
3 package(s) needed for security, out of 3 available
Run "yum update" to apply all updates.
```

- Alibaba Cloud Linux 3提醒信息示例如下：

```
Updates Information Summary: available
    8 Security notice(s)
        1 Critical Security notice(s)
        1 Important Security notice(s)
        6 Moderate Security notice(s)
Run "dnf upgrade-minimal --security" to apply all updates.
```

以上提醒示例中：

- Alibaba Cloud Linux 2的提醒信息表示当前操作系统存在3个可更新的安全漏洞。
- Alibaba Cloud Linux 3的提醒信息表示当前操作系统存在1个高风险漏洞、1个较高风险漏洞及6个中等风险漏洞。

Alibaba Cloud Linux安全更新根据CVE的通用漏洞评估方法（CVSS3）的评分，将安全更新分为以下四个等级：

- Critical：高风险，强烈建议更新。
- Important：较高风险，强烈建议更新。
- Moderate：中等风险，推荐更新。
- Low：低风险，可选更新。

更多信息， 请参见检查安全更新（Alibaba Cloud Linux 2）或检查安全更新（Alibaba Cloud Linux 3）。

操作建议

您可以根据实际的业务需求，选择更新所有漏洞或者更新部分漏洞。

操作	说明
全量更新	运行以下命令，您可以安装操作系统提醒中所有的安全更新。 `yum upgrade --security`
部分更新	您可以结合业务实际需求，选择性安装安全更新。具体操作，请参见安装安全更新（Alibaba Cloud Linux 2）或安装安全更新（Alibaba Cloud Linux 3）。

相关操作

您可以通过**systemctl**命令管理 `update-motd` 服务。具体说明如下：

- 启动 `update-motd` 服务。

```
systemctl start update-motd
```

- 停止 `update-motd` 服务。

```
systemctl stop update-motd
```

- 重启 `update-motd` 服务。

```
systemctl restart update-motd
```

- 查看 `update-motd` 服务状态。

```
systemctl status update-motd
```

5.4.7. 基于Docker使用Inclavare Containers机密容器

Inclavare Containers是工业界首个面向机密计算场景的开源容器运行时，它在基于硬件的可信执行环境中启动受保护的容器，以防止不受信任的实体（例如：云服务商）访问您的敏感数据。在基于SGX的机密计算环境中，您可以基于Inclavare Containers灵活、便捷地部署机密容器。本文主要为您介绍如何在Docker中基于Inclavare Containers部署和使用机密容器（简称Inclavare Containers机密容器）。

前提条件

- 已创建一台使用Alibaba Cloud Linux镜像的安全增强型实例。
  创建安全增强型实例时，您需要选择特定的镜像以生效安全特性。更多信息，请参见创建安全增强型实例。例如，创建ECS实例时，实例规格选择安全增强型ecs.g7t、公共镜像选择Alibaba Cloud Linux 3.2104 64位 UEFI版进行创建。
- 在已创建的安全增强型实例中构建SGX加密计算环境。具体操作，请参见构建SGX加密计算环境。

背景信息

在Docker中虽然可以使用常规技术部署和使用机密容器，但需要您掌握机密计算领域的专业知识，并按照SGX SDK应用开发规范开发和构建镜像。而Inclavare Containers能帮您省去这些复杂过程，降低机密计算的使用门槛，灵活对接不同类型的Enclave运行时形态，同时保持和普通容器一样的使用体验。更多信息，请参见inclavare-containers。

操作导航

在Alibaba Cloud Linux操作系统中基于Docker使用Inclavare Containers机密容器的操作步骤如下：

- 步骤一：搭建Inclavare Containers机密容器运行环境
- 步骤二：为Docker配置OCI运行时rune
- 步骤三：构建Inclavare Containers机密容器镜像
- 步骤四：使用Inclavare Containers机密容器

步骤一：搭建Inclavare Containers机密容器运行环境

1. 登录安全增强型实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 安装rune。

   rune是符合OCI Runtime规范的命令行工具，用于在容器里创建和运行Enclave。更多信息，请参见rune和runtime-container。
   不同发行版的Alibaba Cloud Linux安装命令也不同，具体说明如下：

   - 如果您使用的是Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版操作系统，需运行以下命令安装rune：

```
yum-config-manager --add-repo https://mirrors.openanolis.org/inclavare-containers/ali
nux2-repo && \
  rpm --import https://mirrors.openanolis.org/inclavare-containers/alinux2-repo/RPM-G
PG-KEY-rpm-sign && \
  yum install -y rune
```

- 如果您使用的是Alibaba Cloud Linux 3.2104 64位 UEFI版操作系统，需运行以下命令安装rune：

```
yum-config-manager --add-repo https://mirrors.openanolis.org/inclavare-containers/ali
nux3-repo && \
  rpm --import https://mirrors.openanolis.org/inclavare-containers/alinux3-repo/RPM-G
PG-KEY-rpm-sign && \
  yum install -y rune
```

3. 运行以下命令，查看rune是否安装成功。

```
which rune
```

返回结果如下所示，表示rune已安装成功。

```
/usr/local/bin/rune
```

4. 运行以下命令，安装Occlum软件栈。

Occlum是Inclavare Containers当前支持的Enclave运行时，而Inclavare Containers需要Enclave运行时的配合才能运行机密容器。更多信息，请参见occlum。

```
yum install -y occlum-pal
```

5. 运行以下命令，查看Occlum是否安装成功。

```
ls /opt/occlum/build/lib
```

返回结果如下所示，表示Occlum已安装成功。

```
libocclum-pal.so.0.21.0
```

步骤二：为Docker配置OCI运行时rune

1. 安装社区版Docker。

不同发行版的Alibaba Cloud Linux安装社区版Docker操作不同，说明如下：

> **说明** 以下部署Docker的教程中提供了两种安装Docker的方式，请注意您需要选择安装社区版Docker（docker-ce）。

- 如果您使用的是Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版操作系统，具体操作，请参见部署并使用Docker（Alibaba Cloud Linux 2）。
- 如果您使用的是Alibaba Cloud Linux 3.2104 64位 UEFI版操作系统，具体操作，请参见部署并使用Docker（Alibaba Cloud Linux 3）。

2. 为Docker配置OCI运行时rune。

i. 运行以下命令，在Docker配置文件中添加rune的相关配置。

例如，系统内的Docker配置文件*/etc/docker/daemon.json*。

```
mkdir -p /etc/docker && \
cat << EOF > /etc/docker/daemon.json
{
 "runtimes": {
  "rune": {
   "path": "/usr/local/bin/rune",
   "runtimeArgs": []
   }
  }
}
EOF
```

ii. 运行以下命令，重启Docker守护进程。

```
systemctl restart docker
```

iii. 运行以下命令，检查rune容器运行时是否成功配置。

```
docker info | grep rune
```

- 如果您使用的是Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版操作系统，返回结果如下所示，表示rune容器运行时成功配置。

```
Runtimes: rune io.containerd.runc.v2 io.containerd.runtime.v1.linux runc
```

- 如果您使用的是Alibaba Cloud Linux 3.2104 64位 UEFI版操作系统，返回结果如下所示，表示rune容器运行时成功配置。

```
Runtimes: io.containerd.runc.v2 io.containerd.runtime.v1.linux runc rune
```

步骤三：构建Inclavare Containers机密容器镜像

1. 运行以下命令，启动Occlum开发镜像。

该操作是为了确保后续构建机密容器镜像的步骤都在Occlum开发镜像里进行。关于Occlum开发镜像的更多信息，请参见occlum 0.21.0。

```
mkdir "$HOME/rune_workdir" && \
docker run -it --privileged \
    -v /dev/sgx_enclave:/dev/sgx/enclave \
    -v /dev/sgx_provision:/dev/sgx/provision \
    -v "$HOME/rune_workdir":/root/rune_workdir \
    occlum/occlum:0.21.0-ubuntu18.04
```

2. 运行以下命令，编写测试用的Hello World代码。

```
cd /root/rune_workdir && \
cat << EOF > hello_world.c
#include <stdio.h>
#include <unistd.h>
void main(void)
{
    while (1) {
        printf("Hello World!\n");
        fflush(stdout);
        sleep(5);
    }
}
EOF
```

3. 构建并打包Hello World可信应用。
   i. 运行以下命令，使用Occlum工具链编译程序。

   ```
   occlum-gcc -o hello_world hello_world.c
   ```

   ii. 运行以下命令，初始化Occlum instance。

   ```
   occlum new occlum_instance
   ```

   iii. 运行以下命令，生成Occlum FS image和Occlum SGX Enclave。

   ```
   cd occlum_instance && \
       cp ../hello_world image/bin/ && \
       openssl genrsa -aes128 -out occlum_key.pem -3 3072 && \
       occlum build --sign-key occlum_key.pem
   ```

   运行命令后，请根据如下提示信息设置合适的保护密码，密码将用于加密保护签名私钥。

   ```
   Enter pass phrase for occlum_key.pem:
   Verifying - Enter pass phrase for occlum_key.pem:
   ```

   iv. 运行以下命令，设置Production Enclave。

   Occlum默认会生成Debug Enclave，因此在实际业务环境中，你需要参考以下命令将Enclave设置为Production Enclave。关于Debug Enclave和Production Enclave的区别，请参见debugging-intel-sgx-enclaves-in-windows-737361.pdf。

   ```
   sed -i 's/"debuggable": true/"debuggable": false/g' Occlum.json
   ```

   当您运行以上命令修改Occlum.json配置文件后，您还需要重新执行以下命令生成Production Enclave。

   ```
   occlum build --sign-key occlum_key.pem
   ```

   v. 运行以下命令，打包Hello World可信应用，并将可信应用拷贝到*rune_workdir*目录。

   ```
   occlum package occlum_instance.tar.gz && \
       cp occlum_instance.tar.gz /root/rune_workdir
   ```

4. 构建机密容器镜像。

i. 运行以下命令，退出Occlum开发镜像。

```
exit
```

ii. 运行以下命令，编写Dockerfile。

```
cd "$HOME/rune_workdir" && \
cat << EOF >Dockerfile
FROM scratch
ADD occlum_instance.tar.gz /
ENTRYPOINT ["/bin/hello_world"]
EOF
```

iii. 运行以下命令，构建机密容器镜像。

```
docker build . -t occlum-app
```

步骤四：使用Inclavare Containers机密容器

运行以下命令，运行Inclavare Containers机密容器，并查看容器运行日志。

```
docker run -it --rm --runtime=rune \
  -e ENCLAVE_TYPE=intelSgx \
  -e ENCLAVE_RUNTIME_PATH=/opt/occlum/build/lib/libocclum-pal.so.0.21.0 \
  -e ENCLAVE_RUNTIME_ARGS=occlum_instance \
  -e ENCLAVE_RUNTIME_LOGLEVEL="off" \
  -e OCCLUM_RELEASE_ENCLAVE=1 \
  occlum-app
```

以上命令中相关参数说明如下：

- ENCLAVE_TYPE：指定要使用的Enclave硬件类型，当前验证环境请选择类型为intelSgx。
- ENCLAVE_PATH：指定要启动的Enclave运行时PAL的路径。
- ENCLAVE_ARGS：指定Enclave运行时PAL的特定参数。如果有多个参数，需用半角逗号（,）分隔。
- ENCLAVE_RUNTIME_LOGLEVEL：指定Enclave运行时的日志等级。
- OCCLUM_RELEASE_ENCLAVE：指定Enclave类型。设置为0表示为Debug Enclave，设置为1表示为Production Enclave。

输出结果如下所示，如果容器日志每隔5s打印一行 `Hello World!` ，则表示Inclavare Containers环境安装成功且机密容器也被正常运行。

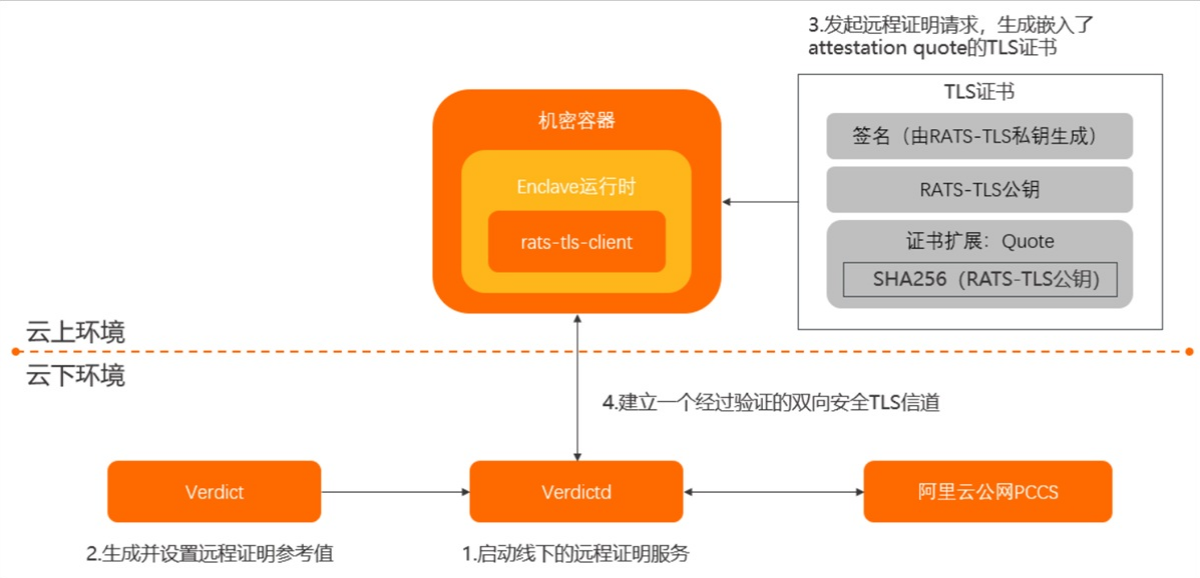
```
Hello World!
Hello World!
Hello World!
```

5.4.8. 使用Inclavare Containers实现远程证明

Inclavare Containers实现了一个针对云场景的通用且跨平台的远程证明架构。该架构能够向您证明其敏感的工作负载是运行在基于机密技术硬件的可信执行加密环境（Trusted Execution Environment，简称TEE）中的。本文介绍如何使用Inclavare Containers实现远程证明。

背景信息

远程证明以关联了带有硬件可执行环境的Quote的TLS证书为信任根，确保通信双方的通信信道的安全性是完全基于硬件可信执行环境的。具体工作流程和架构图如下图所示。



当您想验证机密容器工作负载是否运行在基于机密技术硬件的可信执行加密环境上时，可以启动云上的rats-tls-client客户端发送验证请求给Verdictd。具体工作流程如下：

1. 启动运行在用户侧可信环境中的Verdictd服务，作为线下的远程证明验证者。
2. Verdict生成并设置远程证明参考值，然后将其上传到Verdictd运行环境中。
3. 云上的rats-tls-client客户端向Verdictd发起远程证明请求，将机密容器提供的硬件可执行环境信息和敏感信息发送给Verdictd。
4. Verdictd检查度量值信息，检查云上的工作负载是否运行在预期的可信环境中，从而完成整个远程证明流程。

其中涉及的主要组件及功能说明如下表所示。

组件名称	角色	功能
机密容器	工作负载	在Enclave运行时中运行客户端程序rats-tls-client。该程序获取HW-TEE（即机密容器）中运行程序的度量值，基于RATS-TLS向Verdictd发起远程证明请求。更多信息，请参见rats-tls。
Verdictd	线下的远程证明验证者	运行在用户侧可信环境中的服务。职责是调用阿里云公网PCCS和Verdict检查运行在HW-TEE中程序度量值信息，以完成整个远程证明流程。更多信息，请参见Verdictd。
Verdict	线下的参考值提供者	运行在用户侧可信环境中的程序，它也是Verdictd的配置程序。作用是配置Verdictd认可的、运行在HW-TEE程序度量值的参考值，以判定在HW-TEE环境中的运行程序是符合预期的或者程序是没有被篡改过的。更多信息，请参见Verdict。

组件名称	角色	功能
阿里云证书缓存服务PCCS（Provisioning Certificate Caching Service）	远程证明服务	阿里云SGX远程证明服务完全兼容Intel® SGX ECDSA远程证明服务和Intel® SGX SDK，因此阿里云vSGX实例（即g7t、c7t或r7t等实例规格族的简称）能够通过远程证明来获得远程提供商或生产者的信任。更多信息，请参见Intel® SGX ECDSA远程证明服务和Intel® SGX SDK。

本教程中示例资源分配如下：

- 使用Alibaba Cloud Linux的UEFI版公共镜像的安全增强型实例模拟云上的rats-tls-client客户端。
- 使用CentOS 8.2公共镜像的ECS实例模拟运行远程证明验证者Verdictd的线下主机。

注意事项：

- Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版和Alibaba Cloud Linux 3.2104 64位 UEFI版公共镜像均可使用Inclavare Containers实现远程证明。部分需要区分操作系统版本的命令将在下文的具体步骤中说明。
- 仅中国内地地域支持阿里云SGX远程证明服务。关于地域的更多信息，请参见地域和可用区。

操作导航

使用Inclavare Containers实现远程证明的操作步骤如下：

- 步骤一：准备工作
- 步骤二：安装云上的机密容器工作负载
- 步骤三：安装并启动线下的Verdictd
- 步骤四：配置远程证明参考值
- 步骤五：验证远程证明是否成功

步骤一：准备工作

1. 创建一台使用Alibaba Cloud Linux的UEFI版公共镜像的安全增强型实例。

   该实例将模拟云上的rats-tls-client客户端。创建安全增强型实例时，您需要选择特定的支持安全特性的镜像。具体操作，请参见创建安全增强型实例。

   > **说明** 创建实例时，请为实例选择专有网络VPC与交换机，并绑定公网IP地址，使实例开通公网访问能力。

2. 在已创建的安全增强型实例中构建SGX加密计算环境。

   具体操作，请参见构建SGX加密计算环境。

3. 创建一台使用CentOS 8.2公共镜像的ECS实例。

   该实例将模拟运行远程证明验证者Verdictd的线下主机。创建ECS实例的具体操作，请参见使用向导创建实例。关于Verdictd的更多信息，请参见Verdictd。

   > **说明** 创建实例时，请为实例选择专有网络VPC与交换机，并绑定公网IP地址，使实例开通公网访问能力。

4. 添加CentOS 8.2实例的安全组规则，在安全组入方向放行1111端口。

   具体操作，请参见添加安全组规则。

步骤二：安装云上的机密容器工作负载

1. 远程连接使用Alibaba Cloud Linux的UEFI版公共镜像的安全增强型实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 运行以下命令，安装机密容器rats-tls-sgx。

   rats-tls-sgx安装包中提供了sample程序和库文件，用于基于硬件可执行环境建立安全通信信道。更多信息，请参见rats-tls。

   - 云上环境为Alibaba Cloud Linux 3.2104 64位 UEFI版系统，运行以下命令：

     ```
     yum-config-manager --add-repo https://mirrors.openanolis.org/inclavare-containers/alinux3-repo && \
       rpm --import https://mirrors.openanolis.org/inclavare-containers/alinux3-repo/RPM-GPG-KEY-rpm-sign && \
       yum install -y rats-tls-sgx
     ```

   - 云上环境为Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统，运行以下命令：

     ```
     yum-config-manager --add-repo https://mirrors.openanolis.org/inclavare-containers/alinux2-repo && \
       rpm --import https://mirrors.openanolis.org/inclavare-containers/alinux2-repo/RPM-GPG-KEY-rpm-sign && \
       yum install -y rats-tls-sgx
     ```

3. 运行以下命令，查看rats-tls-sgx是否安装成功。

   ```
   ls /usr/share/rats-tls/samples
   ```

   返回结果示例如下，表示rats-tls-sgx已安装成功。

   ```
   rats-tls-client  rats-tls-server  sgx_stub_enclave.signed.so
   ```

步骤三：安装并启动线下的Verdictd

1. 远程连接使用CentOS 8.2公共镜像的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 切换CentOS 8源地址。

   CentOS 8操作系统版本结束了生命周期（EOL），按照社区规则，CentOS 8的源地址*http://mirror.centos.org/centos/8/*内容已移除，您在阿里云上继续使用默认配置的CentOS 8的源会发生报错。如果您需要使用CentOS 8系统中的一些安装包，则需要手动切换源地址。具体操作，请参见CentOS 8 EOL如何切换源？。

3. 运行以下命令，安装SGX PSW环境。

   Verdictd在验证嵌有SGX认证信息的TLS证书过程中，需要依赖SGX PSW提供的动态库。更多信息，请参见SGX PSW。

```
yum install -y yum-utils && \
    wget -c https://download.01.org/intel-sgx/sgx-linux/2.13/distro/centos8.2-server/sg
x_rpm_local_repo.tgz && \
    tar xzf sgx_rpm_local_repo.tgz && \
    yum-config-manager --add-repo sgx_rpm_local_repo && \
    yum makecache && rm -f sgx_rpm_local_repo.tgz && \
    yum install --nogpgcheck -y libsgx-dcap-quote-verify \
    libsgx-dcap-default-qpl libsgx-dcap-ql \
    libsgx-uae-service
```

4. 配置阿里云PCCS公网URL。

   阿里云SGX远程证明服务采用区域化部署，您可以通过访问实例所在地域的阿里云SGX远程证明服务来获得最佳的稳定性。您需要手动修改*/etc/sgx_default_qcnl.conf*文件以适配实例所在地域的阿里云SGX远程证明服务。

   > **说明** 仅中国内地地域支持阿里云SGX远程证明服务。关于地域的更多信息，请参见地域和可用区。

   - 如果实例已分配公网IP，则需要对*/etc/sgx_default_qcnl.conf*的内容做以下修改。您可以使用vi或vim编辑器修改文档。使用编辑器的示例命令为 `vi /etc/sgx_default_qcnl.conf` 或 `vim /etc/sgx_default_qcnl.conf` 。

     ```
     # PCCS server address
     PCCS_URL=https://sgx-dcap-server.<Region-ID>.aliyuncs.com/sgx/certification/v3/
     # To accept insecure HTTPS cert, set this option to FALSE
     USE_SECURE_CERT=TRUE
     ```

     其中，*<Region-ID>*为变量，您需要替换为实例所属的地域信息。例如实例所属华东1（杭州），则*<Region-ID>*需要替换为 `cn-hangzhou` 。

   - 如果实例只有VPC内网IP，则需要对*/etc/sgx_default_qcnl.conf*的内容做以下修改。您可以使用vi或vim编辑器修改文档。使用编辑器的示例命令为 `vi /etc/sgx_default_qcnl.conf` 或 `vim /etc/sgx_default_qcnl.conf` 。

     ```
     # PCCS server address
     PCCS_URL=https://sgx-dcap-server-vpc.<Region-ID>.aliyuncs.com/sgx/certification/v3/
     # To accept insecure HTTPS cert, set this option to FALSE
     USE_SECURE_CERT=TRUE
     ```

     其中，*<Region-ID>*为变量，您需要替换为实例所属的地域信息。例如实例所属华东1（杭州），则*<Region-ID>*需要替换为 `cn-hangzhou` 。

5. 运行以下命令，安装Verdictd软件栈。

   Verdictd在验证嵌有SGX认证信息的TLS证书过程中，需要依赖rats-tls-host库文件。

```
yum-config-manager --add-repo https://mirrors.openanolis.cn/inclavare-containers/rpm-re
po/ && \
    rpm --import https://mirrors.openanolis.cn/inclavare-containers/rpm-repo/RPM-GPG-KE
Y-rpm-sign && \
    yum install -y rats-tls-host verdictd
```

6. 运行以下命令，查看Verdictd是否安装成功。

```
which verdictd verdict
```

返回结果示例如下，表示Verdictd已安装成功。

```
/usr/local/bin/verdictd
/usr/local/bin/verdict
```

7. 运行以下命令，查看rats-tls-host是否安装成功。

```
ls /usr/share/rats-tls/samples
```

返回结果示例如下，表示rats-tls-host已安装成功。

```
rats-tls-client  rats-tls-server
```

8. 运行以下命令，启动线下的Verdictd服务。

```
verdictd --client-api 127.0.0.1:10001 --listen 0.0.0.0:1111 --mutual --attester nullatt
ester --verifier sgx_ecdsa --tls openssl --crypto openssl
```

> **说明** 当Verdictd启动后，Verdictd在端口监听地址 `0.0.0.0:1111` 监听来自远程认证客户端rats-tls-client的远程证明请求，同时在端口监听地址 `127.0.0.1:10001` 监听来自Verdict的配置policy的相关请求。

在后续的操作步骤中，您需要始终保持Verdictd服务为运行状态。因此您需要始终保持当前远程连接ECS实例的终端页面为正常的连接状态。

步骤四：配置远程证明参考值

1. 新建一个终端远程连接使用CentOS 8.2公共镜像的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

   > **说明** 新建终端时，您需要保证已启动Verdictd服务的终端未关闭或未断开连接，即当前共有两个终端同时远程连接的使用CentOS 8.2公共镜像的ECS实例。

2. 使用Verdict工具配置Verdictd的SGX OPA的参考值，从而实现只能启动特定SGX Enclave的目标。

   Open Policy Agent（OPA）是一个开源的通用策略引擎，可以统一整个堆栈的策略执行。具体信息，请参见OPA。

i. 运行以下命令，导出SGX OPA参考值文件。

```
verdict --client-api 127.0.0.1:10001 --export-opa-reference sgxData
```

导出的*sgxData*内容如下：

```
cat sgxData
{
    "mrEnclave": [],
    "mrSigner": [],
    "productId": 0,
    "svn": 0
}
```

默认参考值文件*sgxData*的参数解析如下：

- mrEnclave：SGX Enclave的mrEnclave会被添加到参考值mrEnclave数组中。
- mrSigner：SGX Enclave的mrSigner会被添加到参考值mrSigner数组中。
- productId：用于确保SGX Enclave的productId大于等于参考值productId。
- svn：用于确保SGX Enclave的svn大于等于参考值svn。

ii. 获取SGX OPA参考值。

在实际业务环境中，云上部署的应用是您自己生成的，您需要根据自己的可信应用获得应用的参考值。下面以如何获得云上部署的sgx_stub_enclave.signed.so参考值为例，介绍如何获得SGX OPA参考值：

a. 运行以下命令，下载云上部署的应用。

- 云上环境为Alibaba Cloud Linux 3.2104 64位 UEFI版系统，运行以下命令：

```
wget https://mirrors.openanolis.cn/inclavare-containers/alinux3-repo/rats-tls
-sgx-0.6.5-1.al8.x86_64.rpm
```

- 云上环境为Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统，运行以下命令：

```
wget https://mirrors.openanolis.cn/inclavare-containers/alinux2-repo/rats-tls
-sgx-0.6.5-1.al7.x86_64.rpm
```

b. 运行以下命令，解压缩已下载的rpm包。

- 云上环境为Alibaba Cloud Linux 3.2104 64位 UEFI版系统，运行以下命令：

```
rpm2cpio rats-tls-sgx-0.6.5-1.al8.x86_64.rpm | cpio -div
```

- 云上环境为Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统，运行以下命令：

```
rpm2cpio rats-tls-sgx-0.6.5-1.al7.x86_64.rpm | cpio -div
```

c. 运行以下命令，下载并安装sgx_sign工具。

```
export SGX_SDK_VERSION=2.14 && \
    export SGX_SDK_RELEASE_NUMBER=2.14.100.2 && \
    wget -c https://download.01.org/intel-sgx/sgx-linux/$SGX_SDK_VERSION/distro
/centos8.2-server/sgx_linux_x64_sdk_$SGX_SDK_RELEASE_NUMBER.bin && \
    chmod +x sgx_linux_x64_sdk_$SGX_SDK_RELEASE_NUMBER.bin && \
    echo -e 'no\n/opt/intel\n' | ./sgx_linux_x64_sdk_$SGX_SDK_RELEASE_NUMBER.bi
n && \
    rm -f sgx_linux_x64_sdk_$SGX_SDK_RELEASE_NUMBER.bin
```

d. 运行以下命令，使用sgx_sign工具dump Enclave的元数据文件和Enclave签名数据结构（即SIGSTRUCT）。

```
/opt/intel/sgxsdk/bin/x64/sgx_sign dump -enclave usr/share/rats-tls/samples/sgx
_stub_enclave.signed.so-dumpfile metadata.txt -cssfile sigstruct.bin
```

e. 运行以下命令，获取mrEnclave的base64编码。

```
dd skip=960 count=32 if=sigstruct.bin of=mrenclave.binary bs=1 && \
    cat mrenclave.binary | base64
```

返回结果示例如下：

- Alibaba Cloud Linux 3.2104 64位 UEFI版系统

```
zqs/chEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA=
```

- Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统

```
+PLc9QPrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw=
```

f. 运行以下命令，获取mrSigner的base64编码。

```
grep -A 2 -i "mrsigner->value" metadata.txt | awk -F ":" 'NR==2,NR==3 {print $1
}' | xargs echo -n | sed 's/[[:space:]]//g;s/0x//g' | xxd -r -p | base64
```

返回结果示例如下：

```
g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=
```

g. 运行以下命令，获取productId值。

```
dd skip=1024 count=2 if=sigstruct.bin of=productId.binary bs=1 && \
    od -An -tx2 productId.binary
```

以本节下载的rats-tls-sgx-0.6.5-1.al8.x86_64.rpm为例，返回结果示例如下：

```
0000
```

h. 运行以下命令，获取svn值。

```
dd skip=1026 count=2 if=sigstruct.bin of=svn.binary bs=1 && \
    od -An -tx2 svn.binary
```

以本节下载的rats-tls-sgx-0.6.5-1.al8.x86_64.rpm为例，返回结果示例如下：

```
0000
```

iii. 运行以下命令，根据SGX OPA参考值生成evidence文件。

根据已获得的SGX OPA参考值，生成evidence文件。该文件是一个包含stub_enclave evidence信息的JSON文件，其作用是测试更新后的*sgxData*参考值文件是否可以工作。

- 云上环境为Alibaba Cloud Linux 3.2104 64位 UEFI版系统，运行以下命令：

```
cat <<- EOF >evidence
{
    "mrEnclave": "zqs/chEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA=",
    "mrSigner": "g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=",
    "productId": 0,
    "svn": 0
}
EOF
```

- 云上环境为Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统，运行以下命令：

```
cat <<- EOF >evidence
{
    "mrEnclave": "+PLc9QPrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw=",
    "mrSigner": "g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=",
    "productId": 0,
    "svn": 0
}
EOF
```

iv. 运行以下命令，更新SGX OPA参考值本地文件。

根据已获得的SGX OPA参考值更新*sgxData*文件。

- 云上环境为Alibaba Cloud Linux 3.2104 64位 UEFI版系统，运行以下命令：

```
cat <<- EOF >./sgxData
{
    "mrEnclave": ["zqs/chEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA="],
    "mrSigner": ["g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4="],
    "productId": 0,
    "svn": 0
}
EOF
```

- 云上环境为Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统，运行以下命令：

```
cat <<- EOF >./sgxData
{
    "mrEnclave": ["+PLc9QPrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw="],
    "mrSigner": ["g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4="],
    "productId": 0,
    "svn": 0
}
EOF
```

v. （可选）运行以下命令测试更新后的参考值本地文件。

如果您需要测试本地更新后的参考值文件，例如新参考值文件格式是否正确、新添加的参考值是否可以工作等问题，可以选择执行该步骤。

```
verdict --client-api 127.0.0.1:10001 --test-opa-local-reference sgxPolicy.rego ./sg
xData ./evidence
```

命令内参数说明如下：

- `--test-opa-local-reference` ：表示测试本地的参考值文件。
- `sgxPolicy.rego` ：表示测试使用的OPA策略文件的名字，命令中必须设置为 `sgxPolicy.rego` 。
- `./sgxData` ：被测试的文件，即更新后的参考值文件。
- `./evidence` ：由Shell脚本生成，包含 `stub_enclave` 的evidence信息的JSON文件。该文件的作用是测试更新后的*sgxData*参考值文件是否可以正常工作。

测试成功的返回结果如下：

- Alibaba Cloud Linux 3.2104 64位 UEFI版系统

```
[root@test ~]# verdict --client-api 127.0.0.1:10001 --test-opa-local-reference sgxPolicy.rego ./sgxData ./evidence
[2022-02-25T07:23:16Z INFO  verdict] Connect to Verdictd with addr: 127.0.0.1:10001
[2022-02-25T07:23:16Z INFO  verdict::opa] OPA Test local reference: policy name: sgxPolicy.rego, reference file:./s
gxData, input file:./evidence
[2022-02-25T07:23:16Z INFO  verdict::opa] TestOpa status is: "{\"allow\":true,\"parseInfo\":{\"mrEnclave\":[\"zqs/c
hEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA=\",[\"zqs/chEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA=\"]],\"mrSigner\":[\"g9cZ5
33qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=\",[\"g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=\"]],\"productId\":[0,0],\
"svn\":[0,0]}}"
```

- Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统

```
[[redacted] verdict --client-api 127.0.0.1:10001 --test-opa-l
ocal-reference sgxPolicy.rego ./sgxData ./evidence
[2022-03-04T12:18:57Z INFO  verdict] Connect to Verdictd with addr: 127.0.0.1:10001
[2022-03-04T12:18:57Z INFO  verdict::opa] OPA Test local reference: policy name: sg
xPolicy.rego, reference file:./sgxData, input file:./evidence
[2022-03-04T12:18:57Z INFO  verdict::opa] TestOpa status is: "{\"allow\":true,\"par
seInfo\":{\"mrEnclave\":[\"+PLc9QPrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw=\",[\"+PLc9Q
PrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw=\"]],\"mrSigner\":[\"g9cZ533qyhRw9rr2Kk13QwPI
mdtpAg+ccO4d/AjHzp4=\",[\"g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4=\"]],\"produc
tId\":[0,0],\"svn\":[0,0]}}"
```

vi. 运行以下命令，上传参考值文件。

当参考值文件更新完毕后，您可以把本地的最新参考值文件上传到Verdictd。

```
verdict --client-api 127.0.0.1:10001 --set-opa-reference sgxData ./sgxData
```

返回结果如下图所示：

```
[root@test ~]# verdict --client-api 127.0.0.1:10001 --set-opa-reference sgxData ./sgxData
[2022-02-25T07:24:05Z INFO  verdict] Connect to Verdictd with addr: 127.0.0.1:10001
[2022-02-25T07:24:05Z INFO  verdict::opa] set_opa_reference status is: "OK"
```

此时，您运行**cat /opt/verdictd/opa/sgxData**命令可以查看到参考值文件已经被更新。如下所示：

- Alibaba Cloud Linux 3.2104 64位 UEFI版系统

```
cat /opt/verdictd/opa/sgxData
{
    "mrEnclave": ["zqs/chEBBNrInHlSCDO+0eV/pnlAB5qieF3M0hKfekA="],
    "mrSigner": ["g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4="],
    "productId": 0,
    "svn": 0
}
```

- Alibaba Cloud Linux 2.1903 LTS 64位 UEFI版系统

```
cat /opt/verdictd/opa/sgxData
{
    "mrEnclave": ["+PLc9QPrEZ6ad9e3BgihgOINOVPYvIj0v/ixt2Kbwyw="],
    "mrSigner": ["g9cZ533qyhRw9rr2Kk13QwPImdtpAg+ccO4d/AjHzp4="],
    "productId": 0,
    "svn": 0
}
```

步骤五：验证远程证明是否成功

1. 远程连接使用Alibaba Cloud Linux的UEFI版公共镜像的安全增强型实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

   > **说明** 您需要继续保持已启动Verdictd服务的终端未关闭或未断开连接。

2. 运行以下命令，远程证明客户端rats-tls-client程序向线下的Verdictd服务发起远程证明请求，进而检测云上的工作负载是否运行在基于硬件的可信执行环境中。

```
cd /usr/share/rats-tls/samples/ && \
./rats-tls-client -a sgx_ecdsa -v nullverifier -t openssl -c openssl -i <Verdictd服务所在实例的公网IP地址> -p 1111 --mutual --verdictd
```

   其中，*<Verdictd服务所在实例的公网IP地址>*为变量，您需要替换为Verdictd服务所在实例的公网IP地址。

   返回结果如下所示，表示远程证明已成功。

```
[                                    ]# cd /usr/share/rats-tls/samples/ && \
> ./rats-tls-client -a sgx_ecdsa -v nullverifier -t openssl -c openssl -i                -p 1111 --mutual --verdictd
    - Welcome to RATS-TLS sample client program for Intel SGX
[INFO] load_enclave()@L49: Success to load enclave with enclave id 2
[INFO] rtls_crypto_wrapper_select()@L67: the crypto wrapper 'openssl' selected
[INFO] rtls_attester_select()@L75: the enclave attester 'sgx_ecdsa' selected
[INFO] rtls_verifier_select()@L73: the enclave verifier 'nullverifier' selected
[INFO] rtls_tls_wrapper_select()@L68: the tls wrapper 'openssl' selected
[WARN] openssl_extract_x509_extensions()@L275: Unhandled evidence type nullverifier
[WARN] openssl_extract_x509_extensions()@L275: Unhandled evidence type nullverifier
[INFO] ecall_rtls_client_startup()@L247: Server: Hello and welcome to RATS-TLS!
```

5.5. 内核热补丁

5.5.1. 内核热补丁概述

Alibaba Cloud Linux为内核的高危安全漏洞（CVE）以及重要的错误修复（Bugfix）提供了热补丁支持，您无需重启服务器即可对操作系统内核更新补丁，以获取内核的稳定与安全。本文主要介绍内核热补丁以及内核热补丁的优势与限制。

功能简介

您可以通过内核热补丁为Alibaba Cloud Linux操作系统内核即时更新补丁。内核热补丁由以下组件构成：

- 补丁RPM包：RPM包包含补丁的内核模块（ko文件）以及补丁的描述文件，内核通过加载该补丁中的内核模块，对内核进行问题修复。
- kpatch工具：管理各补丁中内核模块的命令行工具。
- kpatch系统服务：内核热补丁的系统守护进程（systemd），该服务在操作系统初始化阶段加载各补丁的内核模块，用于对内核进行问题修复。

功能优势

内核热补丁可以在保证服务器的安全性与稳定性（无需重启服务器和任何业务相关的任务进程、无需等待长时运行的任务完成、无需用户注销登录、无需进行业务迁移）的前提下，平滑且快速地为内核更新高危安全漏洞或重要错误修复的补丁。

功能限制

您需要注意内核热补丁方式存在以下限制：

- 适用于Alibaba Cloud Linux操作系统，并且：
  - Alibaba Cloud Linux 2.1903的内核版本不能低于**kernel-4.19.24-9.al7.x86_64**。
  - Alibaba Cloud Linux 3.1903的内核版本不能低于**5.10.23-4.al8.x86_64**。
- 对于每次迭代的Alibaba Cloud Linux操作系统内核版本，阿里云提供一年的内核热补丁支持，超过支持期限后，您需要将操作系统的内核版本升级至最新版。
- 不是所有的高危安全漏洞或重要错误修复都可以通过热补丁的方式修复，该方式主要为了减少因更新补丁而产生的重启服务器操作，但不能完全避免重启服务器。热补丁主要修复范围为：严重及以上级别的CVE漏洞、严重级别的错误修复。
- 热补丁不是通用的内核升级解决方案，仅适用于在不方便对服务器立即重启时，为内核更新高危安全漏洞或重要错误修复的补丁。
- 在更新补丁过程中以及补丁生效后，不能使用SystemTap或者kprobe工具对补丁涉及的函数进行测试或跟踪。否则补丁将失效。

相关操作

获取、启动或禁用Alibaba Cloud Linux的内核热补丁的具体操作，请参见内核热补丁操作说明。

5.5.2. 内核热补丁操作说明

您可以通过本文了解获取Alibaba Cloud Linux内核热补丁的方式，以及如何在Alibaba Cloud Linux实例内启用、禁用内核热补丁或禁用kpatch系统服务。

背景信息

内核热补丁的相关操作说明如下：

- 如何获取内核热补丁以及如何查看热补丁的具体信息，请参见获取内核热补丁。
- 如果您需要在操作系统中启用内核热补丁，具体操作，请参见启用内核热补丁。
- 如果操作系统中已启用的内核热补丁存在问题，您可以禁用该补丁。具体操作，请参见禁用内核热补丁。
- 如果操作系统中已启用了内核热补丁，但您需要在重启服务器时，使操作系统不自动加载所有的热补丁的内核模块，您可以禁用kpatch系统服务。具体操作，请参见禁用kpatch系统服务。

获取内核热补丁

每一个内核热补丁均通过RPM包发布，您可以通过以下任一方式获取热补丁的安装包：

- Alibaba Cloud Linux CVE公告平台
  i. 访问CVE公告平台。
  所有已发布的热补丁都将在CVE公告平台上公示，您可以访问不同发行版本的CVE公告平台进行查看。
  - Alibaba Cloud Linux 2.1903 Security Advisories
  - Alibaba Cloud Linux 3 Security Advisories

  ii. 单击**Advisory ID**列名，重新排序列表内的信息，将热补丁的相关更新展示在最上方。
  以 `HOTFIX` 开头的**Advisory ID**为内核热补丁，重新排序后如下图所示：

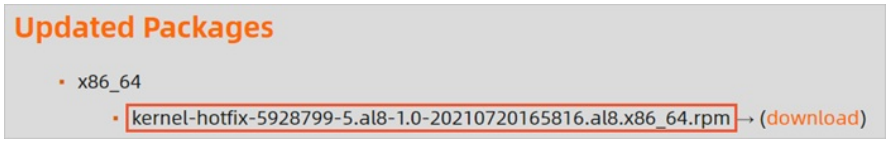
Updated Date	Affected Packages	Advisory ID	Severity	CVE ID(s)
2021-07-28	kernel-hotfix-5928799-5.al8	HOTFIX-SA-2021:0026	High	• CVE-2021-22555
2021-07-28	kernel-hotfix-5928799-4.al8	HOTFIX-SA-2021:0025	High	• CVE-2021-22555
2021-07-28	kernel-hotfix-5956925-6.al8	HOTFIX-SA-2021:0024	High	• CVE-2021-33909
2021-07-28	kernel-hotfix-5956925-5.al8	HOTFIX-SA-2021:0023	High	• CVE-2021-33909
2021-07-28	kernel-hotfix-5956925-4.al8	HOTFIX-SA-2021:0022	High	• CVE-2021-33909

  关于CVE公告平台中的信息说明，如下表所示。

列信息	说明
Affected Packages	表示内核热补丁的具体包名。名称以 `kernel-hotfix-` 为前缀，以Alibaba Cloud Linux操作系统的子版本号信息为后缀。 您可以通过名称后缀确认该热补丁是否适用于您的Alibaba Cloud Linux操作系统。例如： ■ **Affected Packages**的信息为 `kernel-hotfix-5928799-5.al8` 。 ■ 您在Alibaba Cloud Linux 3操作系统中运行**uname -r**命令的回显结果为 `5.10.23-5.al8.x86_64` 。 Alibaba Cloud Linux 3子版本号信息均为 `5.al8` ，则表示该热补丁适用于您的Alibaba Cloud Linux 3操作系统。 **说明** Alibaba Cloud Linux 2操作系统的版本号均为al7。

列信息	说明
Advisory ID	表示热补丁的发布序号。分为安全漏洞（CVE）和错误修复（Bugfix）两类热补丁，命名有如下区别： ■ 安全漏洞补丁以 `HOTFIX-SA-` 为前缀。 ■ 错误修复补丁以 `HOTFIX-BA-` 为前缀。 您可以单击热补丁的**Advisory ID**查看补丁的详细信息，并支持下载热补丁的RPM包。
CVE ID(s)	表示具体修复的安全漏洞（CVE）ID号。如果是错误修复热补丁，则**CVE ID(s)**列的内容为空。

iii. 单击**Advisory ID**列下对应的热补丁发布序号，进入热补丁详情页。
在该页面，您可以查看热补丁的详细信息，以及热补丁RPM包对应的名称。



补丁RPM包的格式为 `kernel-hotfix-{hotfix_id}-{操作系统子版本号}-{hotfix版本号}-{hotfix制作时间戳}.{操作系统大版本号}.{体系架构}.rpm` 。
例如上图所示的格式RPM包名称说明：

- 5928799：热补丁的ID。
- 5.al8：匹配的Alibaba Cloud Linux 3子版本号，您的Alibaba Cloud Linux 3操作系统的内核版本需要与该版本一致，才可以使用该热补丁。操作系统的内核版本信息可以在ECS实例内运行**uname -r**查看。
- 1.0：热补丁的RPM包版本号。
- 20210720165816：热补丁的制作时间为2021年07月20日16时58分16秒。部分历史版本的热补丁中该字段可能为无效的值。
- al8：匹配的Alibaba Cloud Linux 3版本号。Alibaba Cloud Linux 3操作系统的版本号均为al8。

  > **说明** Alibaba Cloud Linux 2操作系统的版本号均为al7。

- x86_64：适用的操作系统的体系架构为x86_64。

- yum源
  您可以通过**yum list** 命令查询相应的内核热补丁安装包。具体操作，请参见启用内核热补丁。

启用内核热补丁

1. 远程连接需要热补丁的Alibaba Cloud Linux实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 运行以下命令，安装kpatch工具。

```
sudo yum -y install kpatch
```

3. 安装热补丁。

i. 运行以下命令，查看操作系统的内核版本信息。

```
sudo uname -r
```

本示例中，查询结果如下所示。可以确认该操作系统的子版本号为 `5.al8` 。

```
5.10.23-5.al8.x86_64
```

ii. 使用yum list命令查询适用于该操作系统的内核热补丁。

命令格式为：

```
sudo yum list | grep "kernel-hotfix" | grep "<操作系统的子版本号>"
```

本示例中，操作系统的子版本号为 `5.al8` ，需要运行以下命令：

```
sudo yum list | grep "kernel-hotfix" | grep "5.al8"
```

回显结果示例，如下所示：

```
kernel-hotfix-5928799-5.al8.x86_64           1.0-20210720165816.al8
alinux3-plus
kernel-hotfix-5956925-5.al8.x86_64           1.0-20210726171200.al8
alinux3-plus
```

iii. 安装指定的热补丁。

本示例中，以 `kernel-hotfix-5928799-5.al8.x86_64` 为例，说明如何通过yum命令安装热补丁。

> **说明** 通过yum安装热补丁时，不需要指定RPM包文件的后缀 `.rpm` 。

```
sudo yum -y install kernel-hotfix-5928799-5.al8.x86_64
```

4. 运行以下命令，通过kpatch工具查看系统补丁的状态。

```
sudo kpatch list
```

回显结果如下所示，表示内核热补丁安装成功且已经生效。

```
Loaded patch modules:
kpatch_5928799 [enabled]
Installed patch modules:
kpatch_5928799 (5.10.23-5.al8.x86_64)
```

禁用内核热补丁

如果您已启用的热补丁存在问题（例如热补丁未生效），可以通过以下步骤禁用内核热补丁以解决问题。本示例将使用yum命令完成操作。

1. 运行以下命令，查看可禁用的热补丁包。

```
sudo yum list installed | grep kernel-hotfix
```

回显结果示例，如下所示：

```
kernel-hotfix-5928799-5.al8.x86_64  1.0-20210720165816.al8            @alinux3-plus
```

2. 运行以下命令，删除存在问题的热补丁包。

   本示例中，以 `kernel-hotfix-5928799-5.al8.x86_64` 为例。

```
sudo yum -y remove kernel-hotfix-5928799-5.al8.x86_64
```

3. 运行以下命令，确认存在问题的热补丁包已经被删除。

```
sudo kpatch list
```

   回显结果如下所示，表示没有已安装并生效的热补丁。

```
Loaded patch modules:
Installed patch modules:
```

禁用kpatch系统服务

如果您的热补丁已安装并且已生效，但您需要在重启服务器时，使操作系统不自动加载所有的热补丁的内核模块，您可以通过以下操作步骤禁用kpatch系统服务。

1. 运行以下命令，查看kpatch系统服务是否已启动。

```
sudo systemctl is-enabled kpatch.service
```

   回显结果为 `enabled` ，表示kpatch系统服务已启动。

2. 运行以下命令，禁用kpatch系统服务。

```
sudo systemctl disable kpatch.service
```

   回显结果如下所示，表示已禁用kpatch系统服务。

```
Removed symlink /etc/systemd/system/multi-user.target.wants/kpatch.service.
```

3. 运行以下命令，查看kpatch系统服务状态。

```
sudo systemctl status kpatch.service
```

   回显结果如下所示，表示kpatch系统服务已禁用。

```
 kpatch.service - "Apply kpatch kernel patches"
   Loaded: loaded (/usr/lib/systemd/system/kpatch.service; disabled; vendor preset: dis
abled)
```

> **说明** 如有需要，您可以运行sudo systemctl enable kpatch.service命令，重新启用kpatch系统服务。

5.5.3. 内核热补丁管理工具livepatch-mgr使用说明

livepatch-mgr是Alibaba Cloud Linux操作系统提供的内核热补丁管理工具，您可以在Alibaba Cloud Linux操作系统中使用livepatch-mgr查看、安装或卸载内核热补丁。

背景信息

Alibaba Cloud Linux发行版为保障系统的稳定与安全，会紧密跟进Linux业界与社区发现的各种软件问题及安全漏洞（CVE），及时更新包括内核在内的软件包，修复软件缺陷（Bugfix）并修补安全漏洞（CVE）。Alibaba Cloud Linux的安全更新记录，请参见：

- Alibaba Cloud Linux 2.1903 Security Advisories
- Alibaba Cloud Linux 3 Security Advisories

您可以基于安全更新记录，选择冷补丁或热补丁的方式更新软件包，本文主要提供内核热补丁管理工具livepatch-mgr的使用说明。

安装并查看livepatch-mgr工具

1. 远程连接需要热补丁的Alibaba Cloud Linux实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

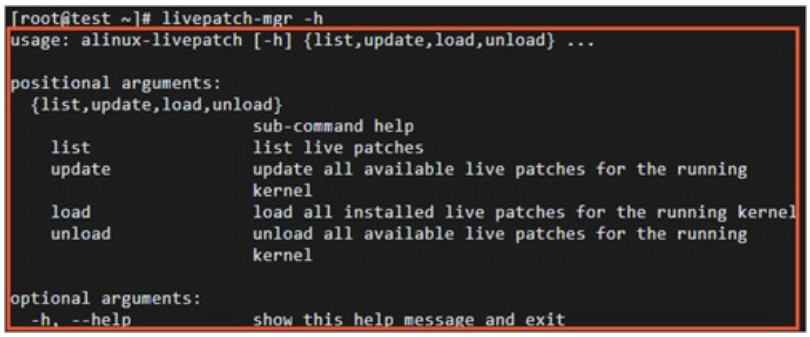
2. 运行以下命令，安装内核热补丁管理工具livepatch-mgr。

```
yum install livepatch-mgr -y
```

3. 安装完成后，运行以下命令，查看livepatch-mgr支持的功能。

```
livepatch-mgr -h
```

   命令行返回结果如下图所示：



   livepatch-mgr提供了4个子命令，每个子命令支持的功能说明如下：

   - **update**：安装并使能适用于本主机的热补丁。命令的具体使用说明，请参见安装并使能热补丁。
   - **list**：查询本主机的热补丁相关信息。命令的具体使用说明，请参见查询热补丁信息。
   - **load**：加载（使能）已安装在本主机的热补丁。命令的具体使用说明，请参见加载（使能）热补丁。
   - **unload**：卸载已安装在本主机的热补丁。命令的具体使用说明，请参见卸载热补丁。

安装并使能热补丁

安装并使能本主机适用的所有热补丁命令如下：

```
livepatch-mgr update
```

同时，livepatch-mgr工具提供了 `--bugfix` 、 `--security` 以及 `-cve=<CVEs>` 参数，供您在不同的场景下选择使用。具体说明如下：

- 安装并使能本主机适用的Bugfix类热补丁。

```
livepatch-mgr update --bugfix
```

- 安装并使能本主机适用的CVE类热补丁。

```
livepatch-mgr update --security
```

- 安装并使能指定的CVE类热补丁。

```
livepatch-mgr update -cve=<CVEs>
```

变量*<CVEs>*表示可以指定一个或多个CVE ID，当指定多个CVE ID时，需要使用半角逗号（,）间隔，且严格区分变量值的大小写。例如：

```
livepatch-mgr update -cve=CVE-2021-33909,CVE-2021-22555
```

> **说明** CVE ID的获取请参见Alibaba Cloud Linux 2.1903 Security Advisories或Alibaba Cloud Linux 3 Security Advisories。

以 `livepatch-mgr update` 命令为例，安装并使能本主机适用的所有热补丁的返回结果如下：

```
已加载插件：fastestmirror, langpacks, releasever-adapter, update-motd
Loading mirror speeds from cached hostfile
正在解决依赖关系
--> 正在检查事务
---> 软件包 kernel-hotfix-4121479-21.al7.x86_64.0.1.0-1.al7 将被 安装
--> 解决依赖关系完成
依赖关系解决
================================================================================
 Package                              架构         版本              源          大小
================================================================================
正在安装：
 kernel-hotfix-4121479-21.al7      x86_64      1.0-1.al7        plus      244 k
事务概要
================================================================================
安装  1 软件包
总下载量：244 k
安装大小：1.0 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  正在安装     : kernel-hotfix-4121479-21.al7-1.0-1.al7.x86_64                1/1
installing /var/khotfix/4.19.91-21.al7.x86_64/4121479/kpatch-4121479.ko (4.19.91-21.al7.x86
_64)
loading patch module: /var/khotfix/4.19.91-21.al7.x86_64/4121479/kpatch-4121479.ko
  验证中       : kernel-hotfix-4121479-21.al7-1.0-1.al7.x86_64                1/1
已安装：
  kernel-hotfix-4121479-21.al7.x86_64 0:1.0-1.al7
完毕！
```

查询热补丁信息

列出本主机适用的所有热补丁命令如下：

```
livepatch-mgr list
```

同时，livepatch-mgr工具提供了 `--installed` 、 `--bugfix` 、 `--security` 、 `--running` 以及 `--available` 参数，供您在不同的场景下选择使用。具体说明如下：

- 列出本主机已安装的热补丁。

```
livepatch-mgr list --installed
```

- 列出本主机已安装的Bugfix类热补丁。

```
livepatch-mgr list --installed --bugfix
```

- 列出本主机已安装的CVE类热补丁。

```
livepatch-mgr list --installed --security
```

- 列出本主机正在生效的所有热补丁。

```
livepatch-mgr list --running
```

- 列出本主机正在生效的Bugfix类热补丁。

```
livepatch-mgr list --running --bugfix
```

- 列出本主机正在生效的CVE类热补丁。

```
livepatch-mgr list --running --security
```

- 列出本主机可用的所有热补丁。

```
livepatch-mgr list --available
```

- 列出本主机可用的Bugfix类热补丁。

```
livepatch-mgr list --available --bugfix
```

- 列出本主机可用的CVE类热补丁。

```
livepatch-mgr list --available --security
```

以 `livepatch-mgr list` 命令为例，列出本主机适用的所有热补丁的返回结果如下。根据返回结果可以将查询到的热补丁分为三类：

- Loaded patch modules：已加载（使能）的热补丁
- Installed patch modules：已安装的热补丁
- Available and not installed patch modules：可用且未安装的热补丁

```
Loaded patch modules:
               5692820 fix_trace_buffer_out_bound
CVE-2021-33909 5956925  seq_file: disallow extremely large seq buffer allocations;
               4375449  ovl: fix dentry leak in ovl_get_redirect;
               5260815  ext4: Avoid freeing inodes on dirty list;
               5000697  mm, compaction: make capture control handling safe wrt interrupts;
CVE-2021-22555 5928799  netfilter: x_tables: fix compat match/target pad out-of-bound write
;
               4121479  fix XDP socket queue descriptor entries overflow;
Installed patch modules:
               5692820 fix_trace_buffer_out_bound
CVE-2021-33909 5956925  seq_file: disallow extremely large seq buffer allocations;
               4375449  ovl: fix dentry leak in ovl_get_redirect;
               5260815  ext4: Avoid freeing inodes on dirty list;
               5000697  mm, compaction: make capture control handling safe wrt interrupts;
CVE-2021-22555 5928799  netfilter: x_tables: fix compat match/target pad out-of-bound write
;
               4121479  fix XDP socket queue descriptor entries overflow;
Available and not installed patch modules:
CVE-2020-14386 kernel-hotfix-3768348-21.al7.x86_64 Using tp_reserve to calculate netoff can
overflow as tp_rese...(more)
               kernel-hotfix-5902278-21.al7.x86_64  We notice that hung task happens in a c
onner but practical ...(more)
```

加载（使能）热补丁

加载本主机中已安装的所有热补丁命令如下：

```
livepatch-mgr load
```

同时，livepatch-mgr工具提供了 `--security` 、 `--bugfix` 、 `load <目标热补丁标识>` 参数，供您在不同的场景下选择使用。具体说明如下：

- 加载本主机中已安装的CVE类热补丁。

  ```
  livepatch-mgr load --security
  ```

- 加载本主机中已安装的Bugfix类热补丁。

  ```
  livepatch-mgr load --bugfix
  ```

- 加载本主机中某一具体的热补丁。

  ```
  livepatch-mgr load <目标热补丁标识>
  ```

  变量*<目标热补丁标识>*表示支持通过热补丁中的内核模块（ko文件）绝对路径或模块名称指定要加载的热补丁信息。例如：

  - 通过热补丁中内核模块（ko文件）的绝对路径指定热补丁包，命令使用示例如下：

    ```
    livepatch-mgr load /var/khotfix/4.19.91-21.al7.x86_64/5956925/kpatch-5956925.ko
    ```

    返回结果示例：

    ```
    loading kernel-hotfix-5956925
    loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5956925/kpatch-5956925.ko
    ```

- 通过热补丁的模块名称（不带*.ko*后缀）指定热补丁包，命令使用示例如下：

  ```
  livepatch-mgr load kpatch-5260815
  ```

  返回结果示例：

  ```
  loading kernel-hotfix-5260815
  loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5260815/kpatch-5260815.ko
  ```

- 通过热补丁的模块名称（带*.ko*后缀）指定热补丁包，命令使用示例如下：

  ```
  livepatch-mgr load kpatch-4121479.ko
  ```

  返回结果示例：

  ```
  loading kernel-hotfix-4121479
  loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/4121479/kpatch-4121479.ko
  ```

以 `livepatch-mgr load` 命令为例，加载本主机中已安装的所有热补丁的返回结果如下所示：

```
loading kernel-hotfix-5956925-23.x86_64
loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5956925/kpatch-5956925.ko
loading kernel-hotfix-5902278-23.x86_64
loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5902278/kpatch-5902278.ko
loading kernel-hotfix-5260815-23.x86_64
loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5260815/kpatch-5260815.ko
loading kernel-hotfix-5928799-23.x86_64
loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5928799/kpatch-5928799.ko
loading kernel-hotfix-5577959-23.x86_64
loading patch module: /var/khotfix/4.19.91-23.al7.x86_64/5577959/kpatch-5577959.ko
```

卸载热补丁

卸载本主机中已安装的所有热补丁命令如下：

```
livepatch-mgr unload
```

同时，livepatch-mgr工具提供了 `--security` 、 `--bugfix` 、 `unload <目标热补丁标识>` 参数，供您在不同的场景下选择使用。具体说明如下：

- 卸载本主机中CVE类热补丁。

  ```
  livepatch-mgr unload --security
  ```

- 卸载本主机中Bugfix类热补丁。

  ```
  livepatch-mgr unload --bugfix
  ```

- 卸载本主机中某一具体的热补丁。

  ```
  livepatch-mgr unload <目标热补丁标识>
  ```

  变量*<目标热补丁标识>*表示支持通过热补丁中的内核模块（ko文件）绝对路径或模块名称指定要卸载的热补丁信息。例如：

- 通过热补丁中内核模块（ko文件）的绝对路径指定热补丁包，命令使用示例如下：

  ```
  livepatch-mgr unload /var/khotfix/4.19.91-21.al7.x86_64/5928799/kpatch-5928799.ko
  ```

  返回结果示例：

  ```
  unoading kernel-hotfix-5928799
  disabling patch module: kpatch_5928799
  unloading patch module: kpatch_5928799
  ```

- 通过热补丁的模块名称（不带*.ko*后缀）指定热补丁包，命令使用示例如下：

  ```
  livepatch-mgr unload kpatch_5692820
  ```

  返回结果示例：

  ```
  unoading kernel-hotfix-5692820
  disabling patch module: kpatch_5692820
  unloading patch module: kpatch_5692820
  ```

- 通过热补丁的模块名称（带*.ko*后缀）指定热补丁包，命令使用示例如下：

  ```
  livepatch-mgr unload kpatch_5000697.ko
  ```

  返回结果示例：

  ```
  unoading kernel-hotfix-5000697
  disabling patch module: kpatch_5000697
  unloading patch module: kpatch_5000697
  ```

以 `livepatch-mgr unload` 命令为例，卸载本主机中已安装的所有热补丁的返回结果示例如下：

```
unloading kernel-hotfix-5956925-23.x86_64
disabling patch module: kpatch_5956925
unloading patch module: kpatch_5956925
unloading kernel-hotfix-5902278-23.x86_64
disabling patch module: kpatch_5902278
unloading patch module: kpatch_5902278
unloading kernel-hotfix-5260815-23.x86_64
disabling patch module: kpatch_5260815
unloading patch module: kpatch_5260815
unloading kernel-hotfix-5928799-23.x86_64
disabling patch module: kpatch_5928799
unloading patch module: kpatch_5928799
unloading kernel-hotfix-5577959-23.x86_64
disabling patch module: kpatch_5577959
unloading patch module: kpatch_5577959
```

5.5.4. 内核热补丁知识库

本文提供Alibaba Cloud Linux内核热补丁相关的故障排查与解决方案。

- Alibaba Cloud Linux 2
  - Alibaba Cloud Linux 2系统的CVE-2021-33909安全漏洞内核热补丁修复方案
  - Alibaba Cloud Linux 2系统的CVE-2021-22555安全漏洞内核热补丁修复方案

- Alibaba Cloud Linux 2系统的ECS实例中Page Fault异常导致系统宕机
- Alibaba Cloud Linux 2系统的ECS实例中SGX驱动在特定情况下存在内存泄露问题
- Alibaba Cloud Linux 2系统的ECS实例中断处理释放内存页时由于访问空指针导致系统宕机
- Alibaba Cloud Linux 2系统的ECS实例中使用已释放的文件系统inode导致系统宕机
- Alibaba Cloud Linux 2系统的ECS实例OverlayFS的dentry泄漏导致系统宕机
- Alibaba Cloud Linux 2系统的ECS实例中打开Ftrace的Filter功能后异常导致系统宕机

- Alibaba Cloud Linux 3
  - Alibaba Cloud Linux 3系统的ECS实例中rq->nr_running在throttle场景下统计异常

5.6. 内核功能与接口

5.6.1. 内核功能与接口概述

如果您对Linux的内核系统有一定的了解，并且需要使用Linux内核功能，可以通过本文了解Alibaba Cloud Linux已支持的内核功能与接口。

内存

文档链接	支持版本	说明
Memcg Exstat功能	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2所支持的Memcg Exstat功能，相较于社区版内核额外在cgroup v1接口支持了memory.events、memory.events.local及memory.stat接口，并增加了memcg全局最低水位调整产生的延迟统计和后台异步回收产生的延迟统计。
Memcg全局最低水位线分级	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2新增了memcg全局最低水位线分级功能。在global wmark_min的基础上，将资源消耗型任务的global wmark_min上移，使其提前进入直接内存回收。将时延敏感型业务的global wmark_min下移，使其尽量避免直接内存回收。这样当资源消耗型任务瞬间申请大量内存的时候，会通过上移的global wmark_min将其短时间抑制，避免时延敏感型业务发生直接内存回收。等待全局kswapd回收一定量的内存后，再解除资源消耗型任务的短时间抑制。
cgroup v1接口支持memcg QoS功能	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	内存子系统服务质量（memcg QoS）可以用来控制内存子系统（memcg）的内存使用量的保证（锁定）与限制。在社区版内核中只有cgroup v2接口支持该功能，Alibaba Cloud Linux 2中新增cgroup v1接口支持memcg QoS的相关功能。
Memcg后台异步回收	• Alibaba Cloud Linux 2内核版本4.19.81-17.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2增加了memcg粒度的后台异步回收功能。该功能的实现不同于全局kswapd内核线程的实现，并没有创建对应的memcg kswapd内核线程，而是采用了workqueue机制来实现。

文档链接	支持版本	说明
Memcg OOM优先级策略功能	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7及以上 • Alibaba Cloud Linux 3内核版本5.10.60-9.al8及以上	Alibaba Cloud Linux 2和Alibaba Cloud Linux 3新增memcg OOM优先级策略功能。该功能在进行OOM操作时，会首先判定cgroup的优先级，选择低优先级的cgroup进行OOM操作。
THP reclaim功能	• Alibaba Cloud Linux 2内核版本4.19.91-24.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2增加了THP reclaim功能，用于解决因透明大页THP带来的内存问题（例如OOM）。

网络

文档链接	支持版本	说明
SMC-R说明	Alibaba Cloud Linux 3内核版本5.10.60-9.al8.x86_64及以上	Alibaba Cloud Linux 3操作系统增加了对SMC-R的支持，基于阿里云弹性RDMA技术，实现对TCP应用透明无损的替换，为内存数据库、RPC、大文件传输等场景提供相比TCP更好的性能。
TCP-RT功能的配置说明	• Alibaba Cloud Linux 2内核版本4.19.91-21.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2支持TCP层的服务监控功能（TCP-RT）。TCP-RT本质是一种trace方式。通过在内核TCP协议栈中相应的位置设置埋点，可以在单个连接上只有一个并发请求与响应的场景下识别出请求与响应，进而获取请求在协议栈中接收的时间及服务进程处理过程中的耗时等数据信息。此外，TCP-RT还支持在内核系统中做统计分析，定期输出指定连接的统计信息。
修改TCP TIME-WAIT超时时间	• Alibaba Cloud Linux 2内核版本4.19.43-13.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	在Linux的内核中，TCP/IP协议的TIME-WAIT状态持续60秒且无法修改。但在某些场景下，例如TCP负载过高时，适当调小该值有助于提升网络性能。因此Alibaba Cloud Linux 2新增内核接口，用于修改TCP TIME-WAIT超时时间。

存储

文档链接	支持版本	说明
启用cgroup writeback功能	• Alibaba Cloud Linux 2内核版本4.19.36-12.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2对内核接口cgroup v1增加了控制群组回写（cgroup writeback）功能。该功能使您在使用内核接口cgroup v1时，可以对缓存异步I/O (Buffered I/O) 进行限速。

文档链接	支持版本	说明
blk-iocost权重限速	• Alibaba Cloud Linux 2内核版本4.19.81-17.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2支持基于成本模型（cost model）的权重限速功能，即blk-iocost功能。该功能是对内核中IO子系统（blkcg）基于权重的磁盘限速功能的进一步完善。
Block IO限流增强监控接口	• Alibaba Cloud Linux 2内核版本4.19.81-17.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	为了更方便地监控Linux block IO限流，Alibaba Cloud Linux 2增加相关接口，用于增强block IO限流的监控统计能力。
JBD2优化接口	• Alibaba Cloud Linux 2内核版本4.19.81-17.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	JBD2作为ext4文件系统的内核线程，在使用过程中常会遇到影子状态（BH_Shadow），影响系统性能。为解决使用JBD2过程中出现的异常，Alibaba Cloud Linux 2对JBD2进行了优化。
跨目录配额创建硬链接	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	默认情况下，ext4文件系统中存在约束，不允许跨目录配额创建硬链接。但在实际中，某些特定场景有创建硬链接的需求，因此Alibaba Cloud Linux 2提供定制接口，该接口能够绕过ext4文件系统中的约束，实现跨目录配额创建硬链接。
追踪IO时延	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2优化了IO时延分析工具iostat的原始数据来源/proc/diskstats接口，增加了对设备侧的读、写及特殊IO（discard）等耗时的统计，此外还提供了一个方便追踪IO时延的工具bcc。
检测文件系统和块层的IO hang	• Alibaba Cloud Linux 2内核版本4.19.91-18.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	IO hang是指在系统运行过程中，因某些IO耗时过长而引起的系统不稳定甚至宕机。为了准确检测出IO hang，Alibaba Cloud Linux 2扩展核心数据结构，增加了在较小的系统开销下，快速定位并检测IO hang的功能。

监控

文档链接	支持版本	说明
内核统一异常框架（UKFEF）	Alibaba Cloud Linux 3内核版本5.10.60-9.al8.x86_64及以上	Alibaba Cloud Linux 3在内核版本5.10.60-9.al8.x86_64增加了UKFEF（Unified Kernel Fault Event Framework），用于统计可能导致风险的系统异常事件，并统一格式输出事件报告。

文档链接	支持版本	说明
在cgroup v1接口开启PSI功能	• Alibaba Cloud Linux 2内核版本4.19.81-17.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2为cgroup v1接口提供了PSI功能。PSI（Pressure Stall Information）是一个可以监控CPU、内存及IO性能异常的内核功能。

调度

文档链接	支持版本	说明
在cgroup v1接口开启CPU Burst功能	• Alibaba Cloud Linux 2内核版本4.19.91-22.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2为cgroup v1接口提供了CPU Burst功能。CPU Burst功能允许容器被CPU限流时，突发使用CPU资源，进而提升容器性能、降低系统的延迟指标。
Group Identity功能说明	• Alibaba Cloud Linux 2内核版本4.19.91-24.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2支持Group Identity功能，您可以通过该功能为每一个CPU cgroup设置不同的身份标识，以区分不同CPU cgroup中进程任务的优先级。

兼容性

文档链接	支持版本	说明
/proc/meminfo文件中的统计信息变更说明	• Alibaba Cloud Linux 2内核版本4.19.91-22.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2操作系统在内核4.19.91-22.al7.x86_64及其之后的版本中，*/proc/meminfo*文件内的匿名页状态统计信息 `Active(anon)` 和 `Inactive(anon)` 发生了变化。如果您的应用程序正在使用该统计信息，统计信息的变化会导致变更前后查询到的数据不一致。

其他

文档链接	支持版本	说明
增强容器资源可见性	• Alibaba Cloud Linux 2内核版本4.19.91-22.2.al7.x86_64及以上 • Alibaba Cloud Linux 3所有内核版本	Alibaba Cloud Linux 2在内核层面提供了容器资源视图功能的相关接口，实现对容器资源的可见性增强。

5.6.2. Memcg Exstat功能

本文主要介绍Alibaba Cloud Linux 2在 `4.19.91-18.al7` 内核版本开始支持的Memcg Exstat（Extend/Extra）功能。

背景信息

Alibaba Cloud Linux 2所支持的Memcg Exstat功能，相较于社区版内核额外提供了以下memcg统计项：

- 在cgroup v1接口支持了memory.events、memory.events.local及memory.stat接口。
- 增加memcg全局最低水位调整产生的延迟统计。
- 增加memcg后台异步回收产生的延迟统计。

功能概述

Alibaba Cloud Linux 2内核功能均基于内核接口来实现，本节主要介绍各个功能对应的接口实现方式。

功能	说明
memory events统计	在社区版内核的cgroup v2接口中存在memory.events和memory.events.local两个接口，能够查询memcg内发生特定事件的次数统计信息。接口详情请参见内核文档cgroup-v2.rst。 Alibaba Cloud Linux 2在cgroup v1接口新增了memory.events和memory.events.local接口。 **说明** memcg根组目录下不存在对应的接口文件。

memory workingset统计	在社区版内核的cgroup v2接口中存在memory.stat接口，该接口提供了 `workingset refault` 、 `workingset activate` 及 `workingset nodereclaim` 三个统计项，接口详情请参见内核文档cgroup-v2.rst。
	Alibaba Cloud Linux 2在cgroup v1接口新增了memory.stat接口，并支持查询 `workingset refault` 、 `workingset activate` 、 `workingset nodereclaim` 及 `workingset restore` 四个统计项。 新增的统计项 `workingset restore` 官方说明，请参见如下内容。
	`+ workingset_restore`
	`+ Number of restored pages which have been detected as an active`
	`+ workingset before they got reclaimed.`

功能	说明
memcg全局最低水位调整产生延迟统计	Alibaba Cloud Linux 2支持memcg全局最低水位线分级功能，详情请参见Memcg全局最低水位线分级。 Alibaba Cloud Linux 2在memcg.exstat接口中，提供了memcg超过偏移后的全局最低水位线导致的抑制时间统计，即统计项 `wmark_min_throttled_ms` 。 **说明** 该统计项将递归到父组，且memcg根组目录下不存在该接口文件。 统计说明： • 统计输出文件：*memory.exstat* • 统计输出项：`wmark_min_throttled_ms` • 统计输出单位：ms
memcg后台异步回收产生延迟统计	Alibaba Cloud Linux 2支持memcg后台异步回收功能，即memcg kswapd特性，详情请参见Memcg后台异步回收。 Alibaba Cloud Linux 2在memcg.exstat接口中，提供了memcg后台异步回收产生的延迟统计（包含回收过程中的阻塞时间和实际工作时间），即统计项 `wmark_reclaim_work_ms` 。 **说明** 该统计项将递归到父组，且memcg根组目录下不存在该接口文件。 统计说明： • 统计输出文件：*memory.exstat* • 统计输出项：`wmark_reclaim_work_ms` • 统计输出单位：ms

功能使用示例

本示例在memcg的挂载点（一般情况下为*/sys/fs/cgroup/memory*）创建测试文件，确认该memcg文件内包含memory.events、memory.events.local及memory.exstat三个控制接口，并确认memory.stat控制接口内包含 `workingset` 统计项。

1. 运行以下命令创建测试文件。

```
mkdir /sys/fs/cgroup/memory/test
```

2. 分别查询memory.events、memory.events.local及memory.exstat接口。
   i. 运行以下命令查询memory.events接口。

```
cat /sys/fs/cgroup/memory/test/memory.events
```

   查询结果示例如下所示。

```
low 0
high 0
max 0
oom 0
oom_kill 0
```

ii. 运行以下命令查询memory.events.local接口。

```
cat /sys/fs/cgroup/memory/test/memory.events.local
```

查询结果示例如下所示。

```
low 0
high 0
max 0
oom 0
oom_kill 0
```

iii. 运行以下命令查询memory.exstat接口。

```
cat /sys/fs/cgroup/memory/test/memory.exstat
```

查询结果示例如下所示。

```
wmark_min_throttled_ms 0
wmark_reclaim_work_ms 0
```

3. 运行以下命令确认memory.stat接口中是否包含 `workingset` 统计项。

```
cat /sys/fs/cgroup/memory/test/memory.stat | grep workingset
```

返回结果示例如下所，表示已包含 `workingset` 统计项。

```
workingset_refault 0
workingset_activate 0
workingset_restore 0
workingset_nodereclaim 0
total_workingset_refault 0
total_workingset_activate 0
total_workingset_restore 0
total_workingset_nodereclaim 0
```

5.6.3. Memcg全局最低水位线分级

本文介绍Alibaba Cloud Linux 2在 `4.19.91-18.al7` 内核版本新增的memcg全局最低水位线分级功能。

背景信息

在Linux内核中，全局内存回收对系统性能影响很大。当时延敏感型业务和资源消耗型任务共同部署时，资源消耗型任务时常会瞬间申请大量的内存，使得系统的空闲内存触及全局最低水位线（global wmark_min），引发系统所有任务进入直接内存回收的慢速路径，引发时延敏感型业务的性能抖动。在此场景下，无论是全局kswapd后台回收还是memcg后台回收，都将无法处理该问题。

基于上述场景下的问题，Alibaba Cloud Linux 2新增了memcg全局最低水位线分级功能。在global wmark_min的基础上，将资源消耗型任务的global wmark_min上移，使其提前进入直接内存回收。将时延敏感型业务的global wmark_min下移，使其尽量避免直接内存回收。这样当资源消耗型任务瞬间申请大量内存的时候，会通过上移的global wmark_min将其短时间抑制，避免时延敏感型业务发生直接内存回收。等待全局kswapd回收一定量的内存后，再解除资源消耗型任务的短时间抑制。

功能接口说明

实现memcg全局最低水位线分级功能的接口为memory.wmark_min_adj。该接口的值，表示基于全局最低水位线（global wmark_min）所作出的调整（adjustment）百分比。取值范围：-25 ~ 50，取值范围说明如下：

- 该接口创建时，继承父组的值（值为0），即默认值为0。
- 取值范围中的负值是基于调整范围 `[0, WMARK_MIN]` 的百分比，其中 `WMARK_MIN` 表示global wmark_min的值，例如：

  ```
  memory.wmark_min_adj=-25, memcg WMARK_MIN is "WMARK_MIN + (WMARK_MIN - 0) * (-25%)"
  ```

  > **说明** 负值也表示global wmark_min下移，即提高时延敏感型业务的内存子系统服务质量（memcg QoS）。

- 取值范围中的正值是基于调整范围 `[WMARK_MIN, WMARK_LOW]` 的百分比，其中 `WMARK_MIN` 和 `WMARK_LOW` 分别表示global wmark_min和global wmark_low的值，例如：

  ```
  memory.wmark_min_adj=50, memcg WMARK_MIN is "WMARK_MIN + (WMARK_LOW - WMARK_MIN) * 50%"
  ```

  > **说明** 正值也表示global wmark_min上移，即降低资源消耗型任务的内存子系统服务质量（memcg QoS）。

- 当偏移后的global wmark_min被触发后，会执行抑制操作，抑制操作的时间和超出的内存使用为线性比例关系。抑制时间的取值范围：1ms ~ 1000ms。

> **说明** memcg根组目录下不存在该接口文件。

接口注意事项

在多层级目录的memcg中，有一个 `effective memory.wmark_min_adj` 的概念，即最终生效的memory.wmark_min_adj值。具体规则是在memcg层级路径上遍历取最大值（中间节点的默认值0除外）。例如，有以下层级关系示例。

```
        root
        / \
       A   D
      / \
     B   C
    / \
   E   F
```

则各层级设置的接口值与最终生效的接口值，对应关系如下所示。

层级	各层级设置的接口值	最终生效的接口值
A	-10	-10
B	-25	-10
C	0	0
D	50	50
E	-25	-10
F	50	50

说明

- 运行命令 `cat /sys/fs/cgroup/memory/<memcg path>/memory.wmark_min_adj` 输出的值为最终生效的值，其中变量 `<memcg path>` 是memcg的根路径。
- 本功能建议配合较高的全局最低水位线（global wmark_min）来使用，例如将global wmark_min值设置为2 GB或更高，您可以通过*/proc/sys/vm/min_free_kbytes*进行设置。

功能配置示例

示例一：为时延敏感型业务所在memcg配置全局最低水位线分级。

1. 运行命令 `mkdir /sys/fs/cgroup/memory/test-lc` 创建测试文件。
2. 运行命令 `echo -25 > /sys/fs/cgroup/memory/test-lc/memory.wmark_min_adj` 向接口写入值 `-25`，提高时延敏感型业务的memcg QoS。

示例二：为资源消耗型任务所在memcg配置全局最低水位线分级。

1. 运行命令 `mkdir /sys/fs/cgroup/memory/test-be` 创建测试文件。
2. 运行命令 `echo 25 > /sys/fs/cgroup/memory/test-be/memory.wmark_min_adj` 向接口写入值 `25`，降低资源消耗型任务的memcg QoS。

5.6.4. cgroup v1接口支持memcg QoS功能

内存子系统服务质量（memcg QoS）可以用来控制内存子系统（memcg）的内存使用量的保证（锁定）与限制，在社区版内核中只有 `cgroup v2` 接口支持该功能。Alibaba Cloud Linux 2在 `4.19.91-18.al7` 内核版本，新增 `cgroup v1` 接口支持memcg QoS的相关功能。

背景信息

在Alibaba Cloud Linux 2内核中，`cgroup v1` 接口中默认开启 `memcg QoS` 功能。关于 `memcg QoS` 的更多信息，您可以参见内核文档 `Documentation/admin-guide/cgroup-v2.rst`。内核文档通过Alibaba Cloud Linux 2的Debuginfo包和源码包获取，如何获取请参见Alibaba Cloud Linux 2使用说明。

注意事项

使用 `cgroup v1` 接口的memcg QoS功能时，建议将任务放置在memcg的叶子节点中，例如，*/sys/fs/cgroup/memory/<intermediate node>/<leaf node>/tasks*路径下。

接口说明

本节介绍Alibaba Cloud Linux 2内核中 `cgroup v1` 接口实现memcg QoS功能的相关接口。

接口	描述
memory.min	绝对锁定内存，即使系统没有可回收的内存，也不会回收该接口锁定的内存。读写说明如下： ● 读该接口可以查看memcg锁定的内存大小。 ● 写该接口可以设置memcg锁定的内存大小。
memory.low	相对锁定内存，如果系统没有其他可回收的内存，该接口锁定的内存也会被回收一部分。读写说明如下： ● 读该接口可以查看memcg锁定的内存大小。 ● 写该接口可以设置memcg锁定的内存大小。
memory.high	限制memcg的内存使用，读写说明如下： ● 读该接口可以查看memcg的使用限制。 ● 写该接口可以设置memcg的使用限制。

接口示例

在memcg的挂载目录下，例如*/sys/fs/cgroup/memory/*路径下，创建测试memcg，确认该memcg内包含memory.min、memory.low和memory.high三个接口。

示例命令如下。

```
mkdir /sys/fs/cgroup/memory/test
ls /sys/fs/cgroup/memory/test | grep -E "memory.(min|low|high)"
```

返回结果示例。

```
memory.high
memory.low
memory.min
```

5.6.5. Memcg后台异步回收

Alibaba Cloud Linux 2在 `4.19.81-17.al7` 内核版本增加了内存子系统（memcg）后台异步回收功能。本文介绍实现memcg后台异步回收功能的接口。

背景信息

在社区内核系统中，系统分配内存并在相应memcg中的统计达到memcg设定的内存上限时，会触发memcg级别的直接内存回收。直接内存回收是发生在内存分配上下文的同步回收，因此会影响当前进程的性能。

为了解决这个问题，Alibaba Cloud Linux 2增加了memcg粒度的后台异步回收功能。该功能的实现不同于全局kswapd内核线程的实现，并没有创建对应的memcg kswapd内核线程，而是采用了workqueue机制来实现，并在cgroup v1和cgroup v2两个接口中，均新增了4个memcg控制接口。

注意事项：

- 当前memcg的内存分配，可能会递归触发父组的后台异步回收。
- 触发memcg后台异步回收时，会从当前被触发的memcg开始，自上而下做层级回收。

- 当memory.high接口被配置，并且memory.high的值比memory.limit_in_bytes接口的值小的时候，接口memory.wmark_high和memory.wmark_low水位线的计算将基于memory.high而不是memory.limit_in_bytes。

memcg后台异步回收功能接口说明

接口	说明
memory.wmark_ratio	该接口用于设置是否启用memcg后台异步回收功能，以及设置异步回收功能开始工作的memcg内存水位线。单位是相对于memcg limit的百分之几。取值范围：0~100 • 默认值为0，该值也表示禁用memcg后台异步回收功能。 • 取值为非0时，表示开启memcg后台异步回收功能并设置对应的水位线。
memory.wmark_high	只读接口，说明如下： • 当memcg内存使用超过该接口的值时，后台异步回收功能启动。 • 该接口的值由 `(memory.limit_in_bytes * memory.wmark_ratio / 100)` 计算获得。 • memcg后台异步回收功能被禁用时，memory.wmark_high默认为一个极大值，从而达到永不触发后台异步回收功能的目的。 • memcg根组目录下不存在该接口文件。
memory.wmark_low	只读接口，说明如下： • 当memcg内存使用低于该接口的值时，后台异步回收结束。 • 该接口的值由 `memory.wmark_high - memory.limit_in_bytes * memory.wmark_scale_factor / 10000` 计算得出。 • memcg根组目录下不存在该接口文件。
memory.wmark_scale_factor	该接口用于控制memory.wmark_high和memory.wmark_low之间的间隔。单位是相对于memcg limit的万分之几。取值范围：1~1000 • 该接口在创建时，会继承父组的值（该值为50），该值也是默认值，即memcg limit的千分之五。 • memcg根组目录不存在该接口文件。

接口配置示例

1. 创建测试文件。

```
mkdir /sys/fs/cgroup/memory/test/
```

2. 为内存使用量限制接口memory.limit_in_bytes设置值。

   本示例限制为1 G。

```
echo 1G > /sys/fs/cgroup/memory/test/memory.limit_in_bytes
```

3. 配置memory.wmark_ratio接口。

   本示例设置异步回收功能开始工作的memcg内存水位线为memcg limit的百分之九十五。

```
echo 95 > /sys/fs/cgroup/memory/test/memory.wmark_ratio
```

4. 运行以下命令查看memory.wmark_scale_factor接口的值。

```
cat /sys/fs/cgroup/memory/test/memory.wmark_scale_factor
```

默认值为memcg limit的千分之五。 接口值返回示例： `50` 。

5. 此时分别查看memory.wmark_high和memory.wmark_low接口的值。

对应的查看结果为如下所示时，即为配置正确。

- 运行以下命令：

```
cat /sys/fs/cgroup/memory/test/memory.wmark_high
```

得到的接口值反馈示例： `1020051456` 。

- 运行以下命令：

```
cat /sys/fs/cgroup/memory/test/memory.wmark_low
```

得到的接口值返回示例： `1014685696` 。

5.6.6. Memcg OOM优先级策略功能

在Alibaba Cloud Linux 2内核版本 `4.19.91-18.al7` 和Alibaba Cloud Linux 3内核版本 `5.10.60-9.al8` 新增内存子系统（memcg）内存溢出OOM（Out Of Memory）优先级策略功能。本文主要介绍实现memcg OOM优先级策略功能的接口，以及接口的示例说明。

背景信息

在现有内核系统中，内存紧张情况下内核会遍历cgroup，选择耗用内存较多的cgroup进行内存回收，甚至在回收失败的情况下直接OOM，并停止当前cgroup下的所有任务。这对于当前cgroup包含的核心业务来说，会造成很大的影响。为此我们希望这类包含核心业务的cgroup占有的内存不被回收，或者cgroup下的任务在OOM中可以存活下来，以便让内核去选择其他的cgroup进行内存回收或者OOM。

为了解决这个问题，Alibaba Cloud Linux增加了memcg OOM优先级配置功能。该功能在进行OOM操作时，会首先判定cgroup的优先级，选择低优先级的cgroup进行OOM操作。

memcg OOM优先级接口功能说明

接口	说明
`memory.use_priority_oom`	该接口用于设置是否启用memcg OOM优先级策略功能，取值为0或者1。该接口不会继承，默认值为0。 • 取值为0时，表示禁用memcg OOM优先级策略功能。 • 取值为1时，表示开启memcgOOM优先级策略功能。
`memory.priority`	该接口提供13个级别的memcg优先级以支持不同重要程度的业务。取值范围为0~12，数值越大表示优先级越高。该接口不会继承，默认值为0。 • 实现一定程度的内存QoS，此处需要说明的优先级值非全局变量，只能在同父cgroup下的兄弟节点进行比较。 • 对于优先级相等的兄弟节点来说，会按照组的内存使用量来排序选择内存使用最大的进行OOM操作。

接口配置示例

按如下所示创建6个cgroup子节点A、 B、 C、 D、 E、 F，开启 `memory.use_priority_oom` 接口，并通过 `memory.priority` 接口设置OOM的优先级。

```
                root
                /  \
               A    B
              / \  /  \
             C   D E   F
```

则各层级设置的接口值，对应关系如下所示：

- A：10
- B：8
- C：5
- D：6
- E：7
- F：8

当在root中进行OOM操作时，它首先迭代查找它的两个子节点A和B，由于B的优先级值低于A，所以会选择B节点作为下一个迭代cgroup继续进行迭代，最终会在子节点E上进行OOM操作，因为它的优先级比其他的兄弟节点低。

5.6.7. THP reclaim功能

Alibaba Cloud Linux 2在内核版本4.19.91-24.al7增加了THP reclaim功能，用于解决因透明大页THP带来的内存问题（例如OOM）。本文介绍实现THP reclaim功能的接口，以及接口的示例操作说明。

背景信息

Linux操作系统的内存采用分页管理模式，其中的THP（Transparent Huge Page）是指内核中2 MiB或1 GiB大小的大页面（普通的小页面大小为4 KiB），一般被称为透明大页。基于应用程序使用到的内存范围越来越大，地址转换产生的开销变得不可忽视。因此，当服务器上的应用程序申请内存时，内核会根据进程的实际情况动态分配透明大页，透明大页可以减少TLB（Translation Lookaside Buffer） Miss的出现概率，从而提升应用程序的性能。

THP在带来性能提升的同时，也产生了一定副作用，即可能产生Memory bloating（内存膨胀）问题。该问题产生的原因说明：透明大页申请释放的粒度为2 MiB（即512个小页面），相较于小页面，透明大页更容易产生内存碎片，进而导致内核分配的内存容量大于实际需要的内存容量。

Memory bloating可能引发OOM（Out Of Memory）。例如，一个应用程序实际需要使用2个小页面，即8 KiB内存，但是内核分配了1个透明大页。此时，除去应用程序实际需要的内存（2个小页面），透明大页剩下的内存（510个小页面）大小均为0。最终可能会因RSS（Resident Set Size）内存用量增加而导致OOM。

为解决THP可能引发的内存问题。Alibaba Cloud Linux 2增加了memcg粒度的THP reclaim功能。在内核回收内存时，该功能会把透明大页拆分为小页面，并将其中的全零页面（zero subpage）回收，从而避免内存的快速膨胀引发OOM。但您需要注意，由于THP reclaim功能会将透明大页拆分为小页面，所以相较于2 MiB大小的透明大页，THP reclaim功能会在一定程度上造成内存性能的回退。

接口说明

实现THP reclaim功能的接口说明，如下表所述：

接口	说明

接口	说明
`memory.thp_reclaim`	开启或关闭THP reclaim功能。支持以下配置项： • reclaim：开启THP reclaim功能。 • swap：预留配置项，目前暂无实际功能。 • disable：关闭THP reclaim功能。 THP reclaim功能默认为关闭状态，即接口默认值为disable。
`memory.thp_reclaim_stat`	查看THP reclaim功能当前的状态。接口内的参数说明如下： • queue_length：当前被THP reclaim管理的透明大页数量。 • split_hugepage：累计拆分的透明大页数量。 • reclaim_subpage：累计回收的全零页面（zero subpage）数量。 该接口的参数值按照NUMA node的顺序（node0、node1）从左到右排列。
`memory.thp_reclaim_ctrl`	控制THP reclaim功能的触发机制。目前支持以下配置项： • threshold：默认值为16。表示当透明大页中的全零页面（zero subpage）数量超过该值时，会触发THP reclaim功能。 • reclaim：用于主动触发THP reclaim功能。
`/sys/kernel/mm/transparent_hugepage/reclaim`	THP reclaim功能的全局配置接口。支持以下配置项： • memcg：该接口的默认配置项。表示每个memory cgroup按照各自的配置开启或关闭THP reclaim，即以每个memory cgroup中的 `memory.thp_reclaim` 接口配置为准。 • reclaim：强制开启所有memory cgroup的THP reclaim功能。 • swap：预留配置项，目前暂无实际功能。 • disable：强制关闭所有memory cgroup的THP reclaim功能。

接口配置的操作说明

本示例操作中，将创建一个名为*test*的memory cgroup，以*test*为例介绍THP reclaim接口的操作说明。

1. 运行以下命令，创建一个名为*test*的memory cgroup。

```
mkdir /sys/fs/cgroup/memory/test/
```

2. 运行以下命令，开启*test*的THP reclaim功能。

```
echo reclaim > /sys/fs/cgroup/memory/test/memory.thp_reclaim
```

3. 运行以下命令，确认*test*的THP reclaim功能成功开启。

```
cat /sys/fs/cgroup/memory/test/memory.thp_reclaim
```

返回结果如下图所示，被 `[]` 包裹的配置项为生效配置项，`[reclaim]` 表示*test*的THP reclaim功能已开启。

```
[root@test ~]# cat /sys/fs/cgroup/memory/test/memory.thp_reclaim
[reclaim] swap disable
```

4. 运行以下命令，通过THP reclaim功能的全局配置接口强制开启THP reclaim功能。

```
echo reclaim > /sys/kernel/mm/transparent_hugepage/reclaim
```

如果您想强制关闭THP reclaim功能，可运行以下命令：

```
echo disable > /sys/kernel/mm/transparent_hugepage/reclaim
```

> **说明** THP reclaim功能的全局配置接口 `/sys/kernel/mm/transparent_hugepage/reclaim` 在设置为强制开启（ `reclaim` ）或强制关闭（ `disable` ）时，接口生效的优先级会高于各个memory cgroup中的 `memory.thp_reclaim` 接口，但不会影响各个memory cgroup中 `memory.thp_reclaim` 接口的配置。

5. 运行以下命令，配置*test*的 `memory.thp_reclaim_ctrl` 接口的 `threshold` 配置项。

```
echo "threshold 32" >  /sys/fs/cgroup/memory/test/memory.thp_reclaim_ctrl
```

此时，如果透明大页中的全零页面数量超过32，则会触发THP reclaim的全零页面回收功能。

6. 主动触发THP reclaim的全零页面回收功能。

主动触发后，THP reclaim会把所有超过 `threshold` 配置的全零页面回收。配置项 `reclaim` 存在以下配置方式：

> **说明** 该配置项的调用方式为同步调用，并且为只写配置项，即您只能向 `memory.thp_reclaim_ctrl` 接口写入 `reclaim` 以主动触发THP reclaim的全零页面回收功能，但不能通过cat命令查看到 `reclaim` 配置项。

- 运行以下命令，会主动触发当前memory cgroup的THP reclaim的全零页面回收功能。

```
echo "reclaim 1" >  /sys/fs/cgroup/memory/test/memory.thp_reclaim_ctrl
```

- 运行以下命令，会主动递归触发当前memory cgroup以及该cgroup下所有子cgroup的THP reclaim的全零页面回收功能。

```
echo "reclaim 2" >  /sys/fs/cgroup/memory/test/memory.thp_reclaim_ctrl
```

除了通过 `reclaim` 主动触发THP reclaim的全零页面回收功能。THP reclaim还会伴随内存回收而触发：

  - 内存出现OOM时，会触发THP reclaim的全零页面回收功能。
  - 当memory cgroup触发memory后台异步回收时，会触发THP reclaim的全零页面回收功能。关于memory后台异步回收的更多信息，请参见Memcg后台异步回收。

7. 运行以下命令，查看*test*的THP reclaim功能状态。

```
cat  /sys/fs/cgroup/memory/test/memory.thp_reclaim_stat
```

返回结果示例如下：

```
queue_length         14
split_hugepage      523
reclaim_subpage 256207
```

C语言代码测试样例

本章节基于C语言提供了进程申请透明大页的代码测试样例。您可以通过以下测试样例，查看到THP reclaim功能在开启与关闭时的区别。

1. 运行以下命令，为内存使用量限制接口 `memory.limit_in_bytes` 设置1 GiB的限制。

```
echo 1G > /sys/fs/cgroup/memory/test/memory.limit_in_bytes
```

设置后，您可以运行以下命令查看 `memory.limit_in_bytes` 接口的值。

```
cat /sys/fs/cgroup/memory/test/memory.limit_in_bytes
```

查看结果如下图所示：

```
[root@test ~]# echo 1G > /sys/fs/cgroup/memory/test/memory.limit_in_bytes
[root@test ~]# cat /sys/fs/cgroup/memory/test/memory.limit_in_bytes
1073741824
[root@test ~]#
```

2. 运行以下命令，关闭memcg后台异步回收功能。

关于memory后台异步回收的更多信息，请参见Memcg后台异步回收。

```
echo 0 > /sys/fs/cgroup/memory/test/memory.wmark_ratio
```

3. 分别在开启或关闭THP reclaim功能的前提下，运行以下C语言代码进行测试，并查看测试结果。

```
// 申请1 G内存（即512个透明大页），其中10个透明大页包含部分全零页面。
#define HUGEPAGE_SIZE 4096 * 512
int main()
{
        int i, thp = 512;
        char *addr;
        posix_memalign((void **)&addr, HUGEPAGE_SIZE, HUGEPAGE_SIZE * thp);
        for (i = 0; i < 10; i++) {
                memset(addr, 0xc, HUGEPAGE_SIZE >> 1);
                addr += HUGEPAGE_SIZE;
        }
        for (; i < thp; i++) {
                memset(addr, 0xc, HUGEPAGE_SIZE);
                addr += HUGEPAGE_SIZE;
        }
        pause();
        return 0;
}
```

测试结果根据THP reclaim功能的开启状态有所不同：

- 在THP reclaim功能关闭时，进程申请最后一个透明大页会发生OOM。
- 在THP reclaim功能开启时，进程申请透明大页过程中，THP reclaim会把前序申请的透明大页拆分为小页，并回收其中的全零页面，最终不会发生OOM。

5.6.8. TCP-RT功能的配置说明

Alibaba Cloud Linux 2在内核版本kernel-4.19.91-21.al7开始支持TCP层的服务监控功能（TCP-RT）。

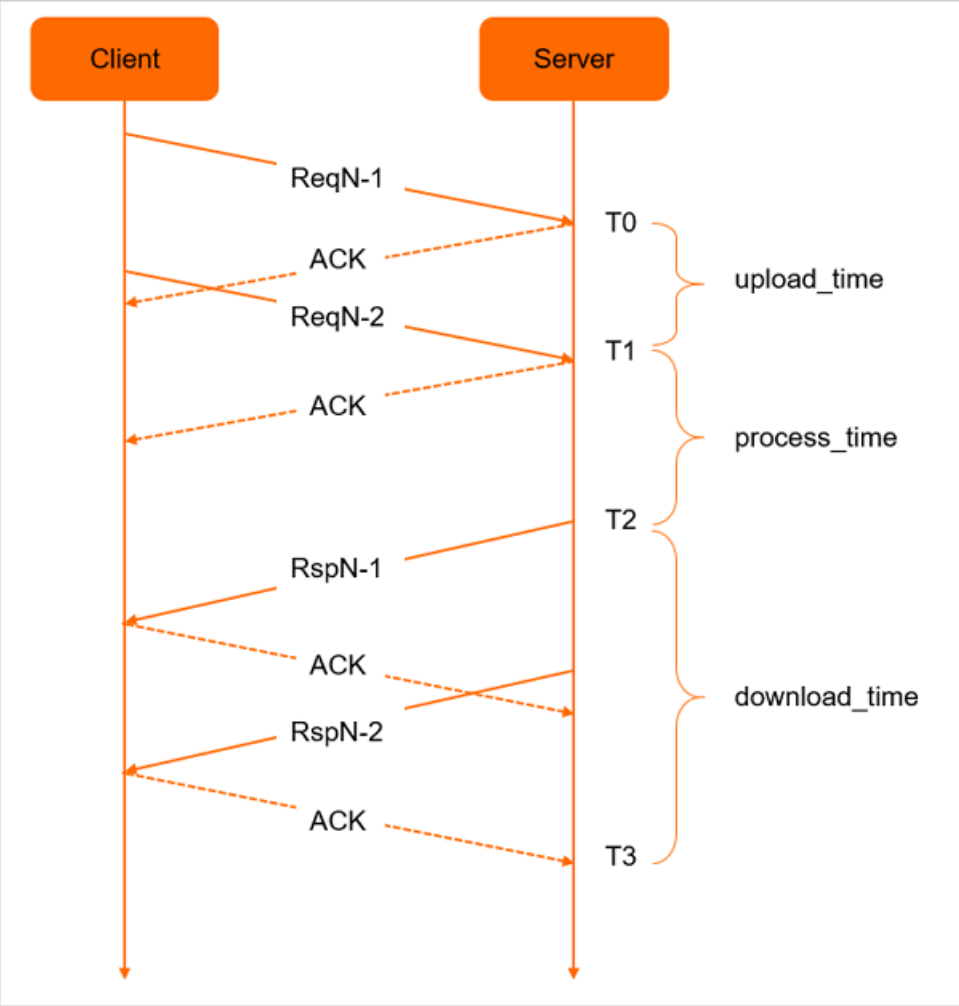
背景信息

TCP-RT本质是一种trace方式。通过在内核TCP协议栈中相应的位置设置埋点，可以在单个连接上只有一个并发请求与响应的场景下识别出请求与响应，进而获取请求在协议栈中接收的时间及服务进程处理过程中的耗时等数据信息。此外，TCP-RT还支持在内核系统中做统计分析，定期输出指定连接的统计信息。

TCP-RT适用于在一个连接上只有一个并发请求与响应的服务。例如：HTTP/1.1协议的Web服务、MySQL数据库服务、Redis服务等。

功能原理

当TCP的服务场景为一个并发的请求与响应时，各个阶段如下图所示。



在上图中，客户端（Client）向服务端（Server）发送的第N个请求（request）表示为ReqN。该请求由 `ReqN-1` 和 `ReqN-2` 两个数据包组成。服务端收到第一个包的时间被记录为T0，第二个包的时间被记录为T1。服务端收到请求后进行处理，完成处理后会向客户端发送两个响应的数据包 `RspN-1` 和 `RspN-2` ，服务端发送第一个包的时间被记录为T2。客户端收到响应包后会发送确认信息ACK给服务器，服务端收到最后一个ACK的时间被记录为T3。

TCP-RT基于以上的时间点的记录，可以计算出以下有意义的信息：

- upload_time：用户请求上传所使用的时间。
- process_time：服务端的处理时间。服务端从收到最后一个请求的数据包开始，到服务端向客户端开始发送响应的数据包为止，这段时间为服务端的处理时间。
- download_time：数据下载时间。从服务端开始向客户端发送响应的数据包开始，到服务端收到客户端最后一个ACK为止，这段时间为数据下载时间。对于下载比较大的数据响应，该信息的获取较为重要。

信息输出说明

TCP-RT在内核态采集TCP服务的相关参数并输出，下表说明了文件的输出方式与输出时间点。

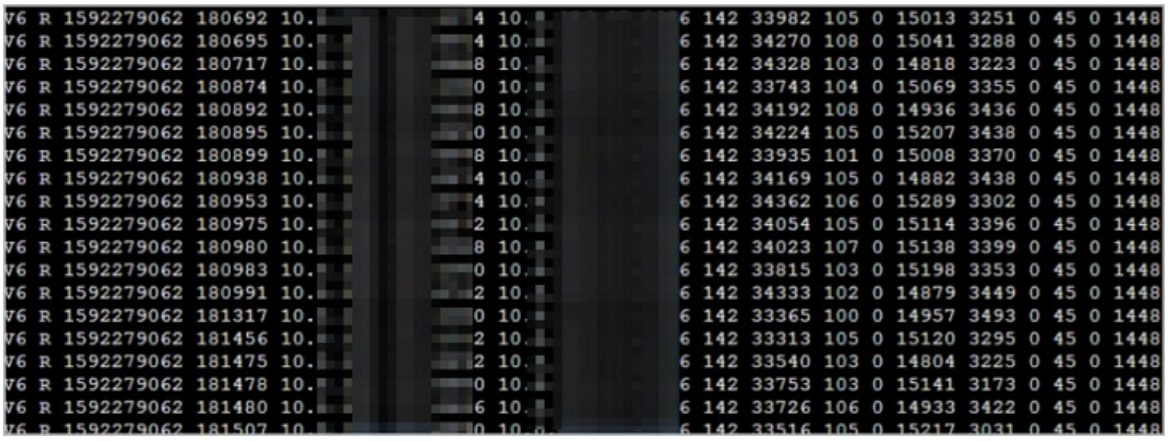
文件类型	输出方式	输出时间
log文件	以debugfs的方式输出到*/sys/kernel/debug/tcp-rt*路径下的 `rt-network-log*` 为名称的文件中。 该类文件特征如下： • 文件名称的后缀为CPU内核的序号。例如：32核的服务器，输出的log文件为 `rt-network-log0` 到 `rt-network-log31` 。 • 文件大小最大为2 MB，当数据超过该限制后，旧数据会被清除。 • debugfs方式输出的log文件是一次性的，当您读取一次文件数据后，读取部分的数据就被清除了。	• 时间一：在TCP连接上，当上一个任务（一次请求/响应为一个任务）完成后下一个任务开始时，输出上一个任务的信息。 • 时间二：在连接关闭时，输出信息。 在TCP-RT输出信息之后，应用层可以立即读取到数据。
stats文件	该数据是基于端口（服务端端口或客户端端口）进行数据汇总后，输出到*/sys/kernl/debug/tcp-rt*路径下的 `rt-network-stats` 文件中。	定时输出。默认为一分钟输出一次。

输出格式说明

本章节主要介绍输出的log与stats文件格式说明。

> **说明** 下文中描述的TASK与TCP生命周期释义：
> - TASK表示一次完整的请求+响应（request+response）。
> - TCP生命周期中包含多个TASK。

- log文件格式说明
  在log文件中，每条记录的每一列都对应了不同的信息。log文件内容示例如下图所示。



```
V6 R 1592279062 180692 10.[redacted]4 10.[redacted]6 142 33982 105 0 15013 3251 0 45 0 1448
V6 R 1592279062 180695 10.[redacted]4 10.[redacted]6 142 34270 108 0 15041 3288 0 45 0 1448
V6 R 1592279062 180717 10.[redacted]8 10.[redacted]6 142 34328 103 0 14818 3223 0 45 0 1448
V6 R 1592279062 180874 10.[redacted]0 10.[redacted]6 142 33743 104 0 15069 3355 0 45 0 1448
V6 R 1592279062 180892 10.[redacted]8 10.[redacted]6 142 34192 108 0 14936 3436 0 45 0 1448
V6 R 1592279062 180895 10.[redacted]0 10.[redacted]6 142 34224 105 0 15207 3438 0 45 0 1448
V6 R 1592279062 180899 10.[redacted]8 10.[redacted]6 142 33935 101 0 15008 3370 0 45 0 1448
V6 R 1592279062 180938 10.[redacted]4 10.[redacted]6 142 34169 105 0 14882 3438 0 45 0 1448
V6 R 1592279062 180953 10.[redacted]4 10.[redacted]6 142 34362 106 0 15289 3302 0 45 0 1448
V6 R 1592279062 180975 10.[redacted]2 10.[redacted]6 142 34054 105 0 15114 3396 0 45 0 1448
V6 R 1592279062 180980 10.[redacted]8 10.[redacted]6 142 34023 107 0 15138 3399 0 45 0 1448
V6 R 1592279062 180983 10.[redacted]0 10.[redacted]6 142 33815 103 0 15198 3353 0 45 0 1448
V6 R 1592279062 180991 10.[redacted]2 10.[redacted]6 142 34333 102 0 14879 3449 0 45 0 1448
V6 R 1592279062 181317 10.[redacted]0 10.[redacted]6 142 33365 100 0 14957 3493 0 45 0 1448
V6 R 1592279062 181456 10.[redacted]2 10.[redacted]6 142 33313 105 0 15120 3295 0 45 0 1448
V6 R 1592279062 181475 10.[redacted]2 10.[redacted]6 142 33540 103 0 14804 3225 0 45 0 1448
V6 R 1592279062 181478 10.[redacted]0 10.[redacted]6 142 33753 103 0 15141 3173 0 45 0 1448
V6 R 1592279062 181480 10.[redacted]6 10.[redacted]6 142 33726 106 0 14933 3422 0 45 0 1448
V6 R 1592279062 181507 10.[redacted]0 10.[redacted]6 142 33516 105 0 15217 3031 0 45 0 1448
```

  按照每一条记录值从左到右的顺序。参数说明如下：
  - 版本号，目前为V6。
  - 记录场景标识，目前分为R、E、W、N、P五种类型。说明如下：
    - R：请求到本地服务器的情况下，在一个TCP服务中完成一次请求+响应产生一条该记录。
    - E：连接关闭的情况下，产生一条该记录。
    - W：连接在发送数据过程中被关闭的情况下，产生一条该记录。
    - N：连接在接收数据过程中被关闭的情况下，产生一条该记录。
    - P：本地服务器请求对端服务器的情况下，在一个TCP服务中完成一次请求+响应产生一条该记录。

- TASK开始时间，开始时间的秒部分。
- TASK开始时间，开始时间的微秒部分。
- TCP连接的对端IP地址。
- TCP连接的对端端口。
- TCP连接的本地IP地址。
- TCP连接的本地端口。

以上参数后面衔接不同记录场景标识的不同参数。说明如下表所示。

记录场景标识	参数说明
R	该记录是TASK正常启动和关闭的记录，每个TCP连接可以有多个R记录。 ○ TASK发送的数据量。单位：Byte ○ TASK总耗时。即从TCP服务收到客户端请求到收到客户端发送的ACK确认信息之间的时间间隔。单位：us ○ TASK最小的TCP RTT（Round Trip Time）。单位：us ○ TASK重传发送的TCP报文段（TCP segment）数量。 ○ TASK序号。TCP建立后的第一个TASK序号为1。 ○ TASK服务延时。即 `最后一个请求的segment到达` 与 `第一个响应的segment发送` 之间的时间间隔。单位：us ○ TASK上送延时。即 `第一个请求segment到达` 与 `最后一个请求segment到达` 之间的时间间隔。单位：us ○ TASK接收的数据量。单位：Byte ○ TASK过程是否发生接收乱序。参数值说明：1表示发生；0表示没有发生。 ○ TASK过程中TCP使用的最大报文长度（MSS）。单位：Byte
P	该记录是TASK正常启动和关闭的记录，每个TCP服务可以有多个P记录。P是V6版本中新增的记录，表述的是客户端对外请求时的信息。只有配置了选项 `pports` 或 `pports_range` 时才有该记录。 ○ TASK发送的数据量。单位：Byte ○ TASK总耗时。从本地服务器发送数据开始到最后一次收到对端响应的时间。单位：us ○ TASK最小的TCP RTT（Round Trip Time）。单位：us ○ TASK重传发送的TCP报文段（TCP segment）数量。 ○ TASK序号。TCP建立后的第一个TASK序号为1。 ○ TASK服务时间。即从请求发送完成到收到第一个响应的时间。单位：us ○ TASK响应接收时间。从接收到第一个响应包到最后一个响应包之间的时间。单位：us ○ TASK接收响应的总大小。单位：Byte ○ TASK过程是否发生接收乱序。参数值说明：1表示发生；0表示没有发生。 ○ TASK过程中TCP使用的最大报文长度（MSS）。单位：Byte

记录场景标识	参数说明
E	该记录是TCP被关闭的记录。每个TCP连接都有1个E记录，配置了选项 `pports` 或 `pports_range` 的连接也会有该记录。 ○ 最后一个TASK的序号。 ○ TCP生命周期中发送的数据量。单位：Byte ○ TCP发送响应但是没有收到ACK的数据量。参数值说明：没有则为0。单位：Byte ○ TCP生命周期中接收的数据量。单位：Byte ○ TASK重传发送的TCP报文段（TCP segment）数量。 ○ TCP生命周期中最小的TCP RTT（Round Trip Time）。单位：us
N	该记录时在TASK请求接收报文段（segment）过程中，TCP被关闭场景的记录。每个TCP连接可能有1个N记录或没有。 ○ 最后一个TASK的序号。 ○ 最后一个TASK的耗时，因为是被关闭，所以只有接收时间，没有发送时间。单位：us ○ TCP生命周期中接收的数据量。单位：Byte ○ TASK过程是否发生接收乱序。参数值说明：1表示发生；0表示没有发生。 ○ TASK过程中TCP使用的最大报文长度（MSS）。单位：Byte
W	该记录是在TASK响应发送的报文段（segment）过程中，TCP被关闭场景的记录。每个TCP连接可能有1个W记录或没有。 ○ 最后一个TASK的响应已发送数据量。单位：Byte ○ 最后一个TASK的耗时，因为是被关闭，所以发送时间是不完整的。单位：us ○ 最后一个TASK最小的TCP RTT（Round Trip Time）。单位：us ○ 最后一个TASK重传发送的TCP报文段（TCP segment）数量。 ○ 最后一个TASK的序号。 ○ 最后一个TASK服务延时。单位：us ○ 最后一个TASK上送延时。单位：us ○ 最后一个TASK发送响应但是没有收到ACK确认信息的数据量。参数值说明：没有则为0。单位：Byte ○ 最后一个TASK过程中TCP使用的最大报文长度（MSS）。单位：Byte

说明 在上表涉及TASK发送数据量的这类信息中，如果是连接的最后一个TASK，正常处理会减去关闭连接（fin）占用的一个 `snd_nxt` 值。而如果连接是异常关闭的，例如一个TASK完成之后收到了异常终止报文（reset）并且连接也是以响应 `reset` 结束的，则实际发送的数据量会大于这里显示值一个字节。正常情况下，该类值都是正确的，并且异常的情况下只误差一个字节。

- stats文件格式说明
  按照每一条记录值从左到右的顺序。参数说明如下：
  - 记录输出时的时间戳。
  - 保留字段，目前唯一值为 `all` 。
  - 端口号。
  - R记录中TASK总耗时的平均值。

- R记录中TASK服务延时的平均值。
- 丢包千分数（‰）。
- RTT的平均值。单位：us
- 请求发送的数据中，被关闭的TASK数量的千分数（‰）。
- TASK发送的数据量的平均值。
- TASK上送延时的平均值。
- TASK接收的数据量的平均值。
- 参与统计的TASK的数量。

功能使用

您可以通过以下操作使用TCP-RT。

1. 加载与配置模块。

   您可以用以下任一方式加载与配置模块：

   - 模块加载时直接配置参数。
     例如：`modprobe tcp_rt lports=80`。
   - 先加载模块，然后进行配置。
     a. 运行以下命令加载模块。

     ```
     modprobe tcp_rt
     ```

b. 模块加载后，在*/sys/module/tcp_rt/parameters/*路径下，运行命令进行配置，参数配置说明与配置命令如下表所示。

参数	说明	默认值	配置命令
stats	控制是否输出stats。取值范围：0表示否；1表示是。	0	`echo 0 > stats`
stats_interval	stats输出时间间隔。单位：s	60	`echo 60 > stats_interval`
lports	控制采集的本地服务器端口，最多6个。	无	`echo 80,800,8080 > lports`
pports	TCP连接的对端端口。	无	`echo 80,800,8080 > pports`
lports_range	本地服务器端口范围，两个为一组，配置命令中表示80-100和1000-2000。	无	`echo 80,100,1000,2000 >lports_range`
pports_range	TCP连接的对端端口范围，两个为一组，配置命令中表示80-100和1000-2000。	无	`echo 80,100,1000,2000 >pports_range`
log_buf_num	每一个log文件最大大小为 `log_buf_num * 256 k` 。只在加载模块的时候可以配置。	8	`modprobe tcp_rt log_buf_num=10`
stats_buf_num	每一个stats文件最大大小为 `stats_buf_num * 16 k` 。只在加载模块的时候可以配置。	8	`modprobe tcp_rt stats_buf_num=10`

2. 卸载模块。

   i. 运行以下命令，停用 `tcp-rt` 模块，保证不会有新的连接使用TCP-RT。

   ```
   echo 1 > /sys/kernel/debug/tcp-rt/deactivate
   ```

   ii. 运行以下命令判断是否所有连接均未使用 `tcp-rt` 模块。

   ```
   lsmod
   ```

   当输出结果中 `tcp-rt` 模块 `Used by` 为 `0` 时，表示没有连接使用 `tcp-rt` 。

   iii. 当所有连接都不使用 `tcp-rt` 模块后，运行以下命令卸载 `tcp-rt` 模块。

   ```
   rmmod tcp_rt
   ```

5.6.9. 修改TCP TIME-WAIT超时时间

在Linux的内核中，TCP/IP协议的TIME-WAIT状态持续60秒且无法修改。但在某些场景下，例如TCP负载过高时，适当调小该值有助于提升网络性能。因此Alibaba Cloud Linux 2从内核版本4.19.43-13.al7开始，新增内核接口用于修改TCP TIME-WAIT超时时间。本文主要介绍该接口的使用方法。

背景信息

TCP/IP协议的TIME-WAIT状态是指应用关闭用于通信的套接口（socket）之后，TCP/IP协议栈保持socket处于打开状态。该状态默认持续60秒，用来保证完成服务器和客户端的数据传输。当处于TIME-WAIT状态的连接数过多时，可能会影响到网络性能。因此Alibaba Cloud Linux 2提供了可修改TIME-WAIT超时时间的接口，用于在特定场景提高网络性能。例如，高并发业务场景。该接口的取值范围为[1, 600]，单位为秒。如果不修改该接口，TIME-WAIT超时时间的默认值保持60秒不变。

注意事项

将TCP TIME-WAIT超时时间修改为小于60秒与TCP/IP协议quiet time概念相违背，可能导致您的系统将旧数据当做新数据接收，或者复制的新数据当做旧数据拒绝。因此请在网络专家建议下调整。了解TCP/IP协议quiet time的相关概念，请参见IETF RFC 793标准。

配置方法

您可以通过以下两种方式修改TIME-WAIT超时时间，其中参数*[$TIME_VALUE]*为您修改的TIME-WAIT超时时间。

- 通过 `sysctl` 命令修改TIME-WAIT超时时间。

```
sysctl -w "net.ipv4.tcp_tw_timeout=[$TIME_VALUE]"
```

- 以root权限使用 `echo` 命令，将值修改到 `/proc/sys/net/ipv4/tcp_tw_timeout` 接口中。

```
echo [$TIME_VALUE] > /proc/sys/net/ipv4/tcp_tw_timeout
```

例如，在Nginx配置7层代理等存在大量短连接的场景下，阿里云推荐您将TIME-WAIT超时时间修改为5s。运行以下任一命令修改超时时间：

> **说明** 服务器中是否存在大量短连接，您可以运行 `netstat -ant | grep TIME_WAIT | wc -l` 命令进行判断。

```
sysctl -w "net.ipv4.tcp_tw_timeout=5"
```

```
echo 5 > /proc/sys/net/ipv4/tcp_tw_timeout
```

5.6.10. 启用cgroup writeback功能

Alibaba Cloud Linux 2在内核版本4.19.36-12.al7中，对内核接口cgroup v1新增了控制群组回写（cgroup writeback）功能。该功能使您在使用内核接口cgroup v1时，可以对缓存异步I/O (Buffered I/O) 进行限速。

背景信息

控制群组（control group）简称为cgroup，分为v1和v2两个版本，详情请参见什么是控制群组。本文介绍如何启用cgroup v1的cgroup writeback功能，并对进程进行Buffered I/O限速。

使用限制

在启用cgroup writeback功能之后，您可以先确认内存子系统（memcg）和IO子系统（blkcg）的映射关系是否符合下文所述的规则，再对进程进行Buffered I/O限速。

cgroup writeback功能需要memcg和blkcg协同工作，完成Buffered I/O的限速，但是内核接口cgroup v1的各个控制子系统间默认不协同工作。因此需要通过一定的规则把memcg和blkcg连接起来，规则为：通过任意一个memcg必须可以找到与之唯一对应的blkcg。即memcg和blkcg的映射关系可以是一对一或多对一，不可以是一对多或多对多。

例如，存在进程A和B，对它们进行Buffered I/O限速，需要遵循以下约束。

- 如果A和B分属不同的memcg，它们可以映射到不同的blkcg，只需各自一一对应。例如：A属于 `memcg1` ， `blkcg1` ；B属于 `memcg2` ， `blkcg0` 。
- 如果A和B分属不同的memcg，它们也可以映射到同一个blkcg。例如：A属于 `memcg1` ，B属于 `memcg2` ，A和B都属于 `blkcg2` 。
- 如果A和B属于相同的memcg，那么它们只能映射到同一个blkcg。例如：A和B均属于 `memcg0` ，它们同时属于 `blkcg3` 。

为了避免出现意外情况，建议您在启用cgroup writeback功能后，对进程进行Buffered I/O限速前，优先设置blkcg的 `cgroup.procs` 接口，向该接口写入一个进程ID来保证blkcg映射的唯一性。同时您也可以通过工具查看memcg和blkcg的映射关系，详情请参见确认memcg和blkcg的映射关系。
在实际运维中，可能出现进程移动到其它cgroup的情况。根据上述规则，如果进程在memcg之间移动，不会出现问题，但如果进程在blkcg之间移动，将会出现异常情况。为了避免产生异常，该功能的代码中定义了规则：一旦工作中的blkcg内的进程发生blkcg间的移动，则将映射关系直接指向root blkcg。由于一般情况是不在root blkcg设置限流阈值，所以当映射关系直接指向root blkcg时，限速功能会失效。

> **注意** 内核代码虽定义了规则避免出现意外，但您需要在实际操作中尽量避免将进程在blkcg间移动。

开启cgroup writeback功能

cgroup v1接口中的cgroup writeback功能默认是关闭的，按照以下步骤开启该功能。

1. 通过命令 `grubby` 内添加 `cgwb_v1` 字段开启该功能。

   本示例中内核版本为 `4.19.36-12.al7.x86_64` ，您在操作中需要更换为实际的内核版本，内核版本的查看命令为 `uname -a` 。

   ```
   sudo grubby --update-kernel="/boot/vmlinuz-4.19.36-12.al7.x86_64" --args="cgwb_v1"
   ```

2. 重启系统使功能生效。

   ```
   sudo reboot
   ```

3. 使用以下命令读取内核文件 `/proc/cmdline` ，确认内核命令行参数中带有 `cgwb_v1` 字段。此时，blkcg下的 `blkio.throttle.write_bps_device` 及 `blkio.throttle.write_iops_device` 接口能够对Buffered I/O进行限速。

   ```
   cat /proc/cmdline | grep cgwb_v1
   ```

确认memcg和blkcg的映射关系

当您对进程进行Buffered I/O限速之前，您可以使用以下任意一种方式诊断memcg和blkcg的映射关系是否为一对一或多对一。

- 查看memcg与blkcg映射关系。

  ```
  sudo cat /sys/kernel/debug/bdi/bdi_wb_link
  ```

  返回结果示例如下，该示例表示memcg和blkcg符合一对一的映射规则。

```
memory     <--->     blkio
memcg1:   35 <---> blkcg1:   48
```

- 使用ftrace内核监测工具。
  i. 开启ftrace工具。

```
sudo bash -c "echo 1 > /sys/kernel/debug/tracing/events/writeback/insert_memcg_blkcg_link/enable"
```

  ii. 查看信息输出接口。

```
sudo cat /sys/kernel/debug/tracing/trace_pipe
```

  输出内容示例如下，其中 `memcg_ino=35 blkcg_ino=48` 表示memcg和blkcg符合一对一的映射规则。

```
<...>-1537  [006] ....    99.511327: insert_memcg_blkcg_link: memcg_ino=35 blkcg_ino=48 old_blkcg_ino=0
```

验证cgroup writeback是否生效

本示例将模拟出两个产生I/O的进程，用于验证cgroup writeback功能是否有效。

> **说明**
> - 由于 `dd` 命令的反馈速度较快，结果使用 `iostat` 命令查看。
> - 由于 `dd` 命令为顺序写入，顺序IO回刷时，会生成1 MB数据再回刷，因此设置阈值时，`blkio.throttle.write_bps_device` 不得小于1 MB(1048576)。如果设置值小于1 MB，可能会引发IO hang。

1. 模拟出两个产生I/O的进程，并按照限制条件优先设置blkcg的 `cgroup.procs` 接口。

```
sudo mkdir /sys/fs/cgroup/blkio/blkcg1
sudo mkdir /sys/fs/cgroup/memory/memcg1
sudo bash -c "echo $$ > /sys/fs/cgroup/blkio/blkcg1/cgroup.procs"    # $$为您的进程ID
sudo bash -c "echo $$ > /sys/fs/cgroup/memory/memcg1/cgroup.procs"    # $$为您的进程ID
```

2. 使用blkcg下的 `blkio.throttle.write_bps_device` 接口对Buffered I/O进行限速。

```
sudo bash -c "echo 254:48 10485760 > /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.write_bps_device"    # 通过设备号配置磁盘的回写限流bps为10 M
```

3. 使用不带参数 `oflag=sync` 的 `dd` 命令产生缓存异步I/O。

```
sudo dd if=/dev/zero of=/mnt/vdd/testfile bs=4k count=10000
```

4. 使用iostat工具查询结果。查看输出列 `wMB/s` ，如果被限制到10 MB/s，则表示cgroup writeback功能已生效。

```
iostat -xdm 1 vdd
```

5.6.11. blk-iocost权重限速

Alibaba Cloud Linux 2在内核版本4.19.81-17.al7.x86_64开始支持基于成本模型（cost model）的权重限速功能，即blk-iocost功能。该功能是对内核中IO子系统（blkcg）基于权重的磁盘限速功能的进一步完善，在Alibaba Cloud Linux 2内核中，该功能同时支持cgroup v1和v2接口。本文主要介绍实现该功能的接口。

接口说明

接口	描述	配置项说明
cost.qos	可读可写接口，接口文件只存在于blkcg根组。在cgroup v1中，该接口文件完整名称为 `blkio.cost.qos` ，在cgroup v2中，该接口文件完整名称为 `io.cost.qos` 。该接口主要实现blk-iocost功能以及基于延迟（latency）权重限制I/O服务质量（Qos）的速率。 当实现blk-iocost功能之后，内核按延迟数值统计以下比例：超过读写延迟 `rlat|wlat` 的请求占所有请求的比例。当该比例超过读写延迟百分比 `rpct|wpct` 时，内核认为设备达到饱和状态，会降低往磁盘发送请求的速率。默认情况下， `rlat|wlat` 的值为0，表示该功能未启用。	每行配置以设备的Major号和Minor号开头（格式为 `MAJ:MIN` ），后边衔接其他配置项，说明如下。 • enable：是否开启blk-iocost controller，即开启blk-iocost功能。默认值0为关闭状态，修改值为1时开启功能。 • ctrl：控制模式，可选值为 `auto` 或者 `user` 。使用 `auto` 时，内核自动探测设备类型并使用内置参数；使用 `user` ，则需要输入以下QoS控制参数。 • rpct：读延迟百分比，取值范围为[0,100]。 • rlat：读延迟，单位为us。 • wpct：写延迟百分比，取值范围为[0,100]。 • wlat：写延迟，单位为us。 • min：最小速率调整比例，取值范围为[1,10000]。 • max：最大速率调整比例，取值范围为[1,10000]。

接口	描述	配置项说明

cost.model	可读可写接口，只存在于blkcg根组。在cgroup v1中，该接口文件完整名称为 `blkio.cost.model` ，在cgroup v2中，该接口文件完整名称为 `io.cost.model` 。该接口用于设置成本模型（cost model）。	每行配置以设备的Major号和Minor号开头（格式为 `MAJ:MIN` ），后边衔接其他配置项，说明如下。
		• ctrl：控制模式，可选值为 `auto` 或 `user` ，表示是否使用用户输入模型参数。
		• model：模型参数，当前只实现了一种模型 `linear` 。当模型参数为 `linear` 时，定义如下建模参数。
		  ○ [r|w]bps：最大顺序IO带宽。
		  ○ [r|w]seqiops：顺序IOPS（Input/Output Operations Per Second）。
		  ○ [r|w]randiops：随机IOPS（Input/Output Operations Per Second）。
		说明 以上参数可以使用内核源码中的*tools/cgroup/iocost_coef_gen.py*脚本来生成，然后写入cost.model接口文件内设置成本模型。

cost.weight	可读可写接口，只存在blkcg的子组中。在cgroup v1中，该接口文件完整名称为 `blkio.cost.weight` ，在cgroup v2中，该接口文件完整名称为 `io.cost.weight` 。该接口用于配置子组的权重，范围为[1,10000]，默认值为100。该接口可以为每个设备配置权重，也可以修改该整个子组的默认权重。	• 为接口设置权重值 `<weight>` ：表示修改blkcg的默认权重。 • 为接口设置端口号和权重值 `MAJ:MIN <weight>` ：表示修改设备上的blkcg的权重。

注意事项

在ECS实例中使用blk-iocost功能启动 `ctrl=auto` 配置项时，如果对应的云盘为高效云盘、SSD云盘、ESSD云盘或NVMe SSD本地盘类型时，需要手动将对应磁盘的 `rotational` 属性设置为0。

```
echo 0 > /sys/block/[$DISK_NAME]/queue/rotational    #[$DISK_NAME]为磁盘名称
```

示例一

使用*cost.qos*接口为设备 `254：48` 开启blk-iocost功能，并且当读写延迟 `rlat|wlat` 的请求有95%超过5 ms时，认为磁盘饱和。内核将进行磁盘发送请求速率的调整，调整区间为最低降至原速率的50%，最高升至原速率的150%。cgroup v1接口和cgroup v2接口命令分别如下。

- cgroup v1 接口。

```
echo "254:48 enable=1 ctrl=user rpct=95.00 rlat=5000 wpct=95.00 wlat=5000 min=50.00 max=1
50.00" > /sys/fs/cgroup/blkio/blkio.cost.qos
```

- cgroup v2接口。

```
echo "254:48 enable=1 ctrl=user rpct=95.00 rlat=5000 wpct=95.00 wlat=5000 min=50.00 max=1
50.00" > /sys/fs/cgroup/io.cost.qos
```

示例二

使用 `cost.model` 在设备 `254: 48` 上使用用户输入的 `linear` 建模参数设置模型。cgroup v1接口和cgroup v2接口命令分别如下。

- cgroup v1接口。

```
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698 rrandiops=110036 wbps=
1063126016 wseqiops=135560 wrandiops=130734" > /sys/fs/cgroup/blkio/blkio.cost.model
```

- cgroup v2接口。

```
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698 rrandiops=110036 wbps=
1063126016 wseqiops=135560 wrandiops=130734" > /sys/fs/cgroup/io.cost.model
```

示例三

使用 `cost.weight` 接口将blkcg1的默认权重修改为50，然后设置blkcg1在设备 `254:48` 上的权重为50，cgroup v1接口和cgroup v2接口命令分别如下。

- cgroup v1接口。

```
echo "50" > /sys/fs/cgroup/blkio/blkcg1/blkio.cost.weight     # 将默认权重修改为50
echo "254:48 50" > /sys/fs/cgroup/blkio/blkcg1/blkio.cost.weight     #将设备上的权重设置为50
```

- cgroup v2接口。

```
echo "50" > /sys/fs/cgroup/cg1/io.cost.weight     # 将默认权重修改为50
echo "254:48 50" > /sys/fs/cgroup/cg1/io.cost.weight     #将设备上的权重设置为50
```

常用监测工具

- iocost monitor脚本
  内核源码中的 `tools/cgroup/iocost_monitor.py` 脚本基于drgn调试器直接获取内核参数进行IO性能数据的监控输出。关于drgn的详情请参见drgn。脚本使用方式如下。
  执行以下命令监测磁盘*vdd*的IO性能数据。

```
./iocost_monitor.py vdd
```

  返回结果示例如下。

```
vdd RUN  per=500.0ms cur_per=3930.839:v14620.321 busy= +1 vrate=6136.22% params=hdd
                          active     weight      hweight% inflt% dbt  delay usages%
blkcg1                       *     50/   50   9.09/  9.09   0.00   0  0*000 009:009:009
blkcg2                       *    500/  500  90.91/ 90.91   0.00   0  0*000 089:091:092
```

- cgroup v1接口下的blkio.cost.stat cost.stat接口

Alibaba Cloud Linux 2内核提供了在cgroup v1接口下的blk-iocost统计接口，该接口文件中记录了每个受控制的设备的QoS数据。查看该接口文档的命令如下。

```
cat /sys/fs/cgroup/blkio/blkcg1/blkio.cost.stat
```

返回结果示例如下。

```
254:48 is_active=1 active=50 inuse=50 hweight_active=5957 hweight_inuse=5957 vrate=159571
```

- ftrace监测工具
  Alibaba Cloud Linux 2内核提供了blk-iocost相关的ftrace工具，您可以进行内核侧的分析。使用方式如下。
  i. 将 `enable` 属性设置为1，开启ftrace工具。

  ```
  echo 1 > /sys/kernel/debug/tracing/events/iocost/enable
  ```

  ii. 查看信息输出接口。

  ```
  cat /sys/kernel/debug/tracing/trace_pipe
  ```

  返回结果示例如下。

  ```
      dd-1593  [008] d...   688.565349: iocost_iocg_activate: [vdd:/blkcg1] now=6890652
  89:57986587662878 vrate=137438 period=22->22 vtime=0->57986365150756 weight=50/50 hwe
  ight=65536/65536
      dd-1593  [008] d.s.   688.575374: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.608369: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
      dd-1594  [006] d...   688.620002: iocost_iocg_activate: [vdd:/blkcg2] now=6891199
  46:57994099611644 vrate=137438 period=22->26 vtime=0->57993412421644 weight=250/250 h
  weight=65536/65536
  <idle>-0     [008] d.s.   688.631367: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.642368: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.653366: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.664366: iocost_ioc_vrate_adj: [vdd] vrate=137438->13743
  8 busy=0 missed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  ```

5.6.12. Block IO限流增强监控接口

为了更方便地监控Linux block IO限流，Alibaba Cloud Linux 2在内核版本4.19.81-17.al7增加相关接口，用于增强block IO限流的监控统计能力。本文主要介绍新增接口及使用示例。

背景信息

很多场景中您会用到Linux block IO限流（bps/iops），特别是在支持控制群组回写（cgroup writeback）后，IO限流使用场景更加广泛。提高block IO限流的监控能力能使您更方便进行IO限流相关操作，因此Alibaba Cloud Linux 2新增了Block IO限流增强监控接口。

接口说明

接口	描述
blkio.throttle.io_service_time	该接口表示从block IO限流层开始下发到IO完成的耗时。单位：ns
blkio.throttle.io_wait_time	该接口表示在block IO限流层被限流的耗时。单位：ns
blkio.throttle.io_completed	该接口表示已完成的IO个数，用于计算block IO限流层的平均时延。单位：个
blkio.throttle.total_io_queued	该接口表示历史发生限流的IO总个数，通过周期性的监控可以计算出当前周期发生限流的IO个数，从而辅助分析IO时延是否与限流有关。单位：个
blkio.throttle.total_bytes_queued	该接口表示历史发生限流的IO总字节数，同blkio.throttle.total_io_queued，只是以IO大小的形式展现。单位：字节

以上接口的路径为*/sys/fs/cgroup/blkio/<cgroup>/*，其中 `<cgroup>` 为控制群组。

示例

您可以通过增强block IO限流的监控统计能力的接口获取某个磁盘上的平均IO时延。本示例中通过监控磁盘*vdd*两个时间点的平均写IO时延，时间间隔为5 s，进而统计出磁盘*vdd*的平均IO时延。示例参数说明如下。

参数	说明
write_wait_time<N>	获取在block IO限流层被限流的耗时。
write_service_time<N>	获取从block IO限流层开始下发到IO完成的耗时。
write_completed<N>	获取已完成的IO个数。

1. 在T1时刻获取监控数据。

```
write_wait_time1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_wait_time | grep
-w "254:48 Write" | awk '{print $3}'`
write_service_time1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_service_time |
grep -w "254:48 Write" | awk '{print $3}'`
write_completed1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_completed | grep
-w "254:48 Write" | awk '{print $3}'`
```

2. 等待5 s后，在T2时刻获取监控数据。

```
write_wait_time2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_wait_time | grep
-w "254:48 Write" | awk '{print $3}'`
write_service_time2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_service_time |
grep -w "254:48 Write" | awk '{print $3}'`
write_completed2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_completed | grep
-w "254:48 Write" | awk '{print $3}'`
```

3. 统计5 s内的平均IO时延。

   平均IO时延的计算规则：（T2时刻的总IO耗时 - T1时刻的总IO耗时）/（T2时刻已完成的IO个数 - T1时

刻已完成的IO个数）。

```
avg_delay = `echo "((write_wait_time2 + write_service_time2) - (write_wait_time1+write_
service_time1)) / (write_completed2 - write_completed1)" | bc`
```

5.6.13. JBD2优化接口

JBD2作为ext4文件系统的内核线程，在使用过程中常会遇到影子状态（BH_Shadow），影响系统性能。为解决使用JBD2过程中出现的异常，Alibaba Cloud Linux 2在内核版本4.19.81-17.al7对JBD2进行了优化。本文主要介绍优化JBD2的接口。

背景信息

ext4作为最常用的日志文件系统之一，更新日志（journal）的内核线程为JBD2，JBD2对ext4文件系统而言，是一个全局资源。您在使用过程中，可能出现JBD2内核线程对缓存尝试获取访问权限时，发生缓存页处于影子状态（BH_Shadow），从而引发JBD2持续等待缓存页回写到磁盘的时间过长的情况，该情况会影响系统性能。因此Alibaba Cloud Linux 2针对特定场景进行了优化，增加了内核接口 `force_copy` ，允许用户启用优化功能，以强制进行缓存页拷贝，从而减少在缓存页处于影子状态的等待。同时，为了辅助分析文件系统相关的服务质量（QoS）中的问题，Alibaba Cloud Linux 2增加了一个JBD2的相关信息统计接口 `stats` 。

接口说明

接口	描述
force_copy	接口位于*/proc/fs/jbd2/<device>-8/force_copy*，其中变量 `device` 指块存储设备名。当设置force_copy接口后，系统强制进行数据拷贝操作，从而减少处于BH_Shadow时的等待。 **注意** 设置该接口后会额外消耗一定的内存。
stats	接口位于*/proc/fs/jbd2/<device>-8/stats*。用于辅助确认文件系统的QoS中的问题是否因JBD2引发。

接口示例

`force_copy` 和 `stats` 接口示例如下。

- `force_copy` 接口默认为关闭状态。将接口设置为1表示调用该接口；设置为0表示关闭该接口。

  ```
  echo 1 > /proc/fs/jbd2/nvme0n1-8/force_copy    # 调用接口
  ```

- 使用以下命令查看 `stats` 接口。

  ```
  cat /proc/fs/jbd2/nvme0n1-8/stats
  ```

  返回结果如下。

  ```
  337 336 65536 0 14837 1701504 16 0 20058 5 33082732 605 942 1000 1000
  ```

  返回结果中，各域说明如下。

域	描述
第1个域	事务ID。
第2个域	请求的事务数。
第3个域	最大事务缓存。
第4个域	事务等待时间。
第5个域	事务请求延迟。
第6个域	事务运行时间。
第7个域	事务锁住时间。
第8个域	事务刷新时间。
第9个域	事务logging时间。
第10个域	平均提交时间。
第11个域	事务包含的原子操作handle个数。
第12个域	事务包含的块数。
第13个域	事务已记录的块数。
第14个域	HZ（内核配置中的时间常量）。
第15个域	HZ转化为ms。

5.6.14. 跨目录配额创建硬链接

默认情况下，ext4文件系统中存在约束，不允许跨目录配额创建硬链接。但在实际中，某些特定场景有创建硬链接的需求，因此Alibaba Cloud Linux 2提供定制接口，该接口能够绕过ext4文件系统中的约束，实现跨目录配额创建硬链接。本文主要介绍实现该功能的接口及接口示例。

背景信息

Linux系统支持三种模式的磁盘配额，分别为：user quota、group quota以及project quota。前两种是针对用户和组的，最后的project quota提供一种更细粒度的磁盘配额，细化到文件系统的目录和文件，使用project id将不同的目录和文件进行标记并限制。本文介绍的功能便是指在ext4文件系统中跨不同的project id目录创建硬链接。

接口说明

*/proc/sys/fs/hardlink_cross_projid*该接口默认值为0，该情况下不允许跨目录配额创建硬链接。当设置值为1时，则可以绕过ext4文件系统的约束，实现跨目录配额创建硬链接。

您可以参考内核文档 `Documentation/sysctl/fs.txt` 中对该接口的相关说明。内核文档通过Alibaba Cloud Linux 2的Debuginfo包和源码包获取，如何获取请参见Alibaba Cloud Linux 2使用说明。

示例

您可以查看默认情况下接口*/proc/sys/fs/hardlink_cross_projid*的值。

```
cat /proc/sys/fs/hardlink_cross_projid
```

返回结果为 `0` ，表明当前不允许跨目录配额创建硬链接。
您可以通过以下命令将默认值0修改为1，实现跨目录配额创建硬链接。

```
echo 1 > /proc/sys/fs/hardlink_cross_projid
```

5.6.15. 追踪IO时延

Alibaba Cloud Linux 2优化了IO时延分析工具iostat的原始数据来源 `/proc/diskstats` 接口，增加了对设备侧的读、写及特殊IO（discard）等耗时的统计，此外还提供了一个方便追踪IO时延的工具bcc。本文将分别介绍优化后的 `/proc/diskstats` 接口以及bcc工具。

接口说明

*/proc/diskstats*接口在Alibaba Cloud Linux 2中可查询磁盘IO信息、设备侧的读耗时、设备侧的写耗时及设备侧discard耗时。

示例：以root权限查询*/proc/diskstats*接口。

```
cat /proc/diskstats
```

返回结果示例如下。

```
254       0 vda 6328 3156 565378 2223 1610 424 25160 4366 0 1358 5332 0 0 0 0 2205 3347 0
```

返回结果中，最后三个域为Alibaba Cloud Linux 2新增域，域说明如下。

域	描述
第16个域	设备侧的读耗时，单位为ms。
第17个域	设备侧的写耗时，单位为ms。
第18个域	设备侧的discard耗时，单位为ms。

> **说明** 其他域的说明，您可以参考内核文档 `Documentation/iostats.txt` 中对该接口的相关说明。内核文档通过Alibaba Cloud Linux 2的Debuginfo包和源码包获取，如何获取请参见Alibaba Cloud Linux 2使用说明。

bcc工具

Alibaba Cloud Linux 2提供一个方便用户追踪IO时延的工具bcc。您需要先下载该工具才能使用，下载命令如下。

```
yum install -y bcc-tools
```

您可以通过以下两种命令查看bcc工具的说明。

- 通过以下命令获取bcc工具说明。

```
/usr/share/bcc/tools/alibiolatency -h
```

说明展示。

```
usage: alibiolatency [-h] [-d DEVICE] [-i [DIS_INTERVAL]]
                     [-t [AVG_THRESHOLD_TIME]] [-T [THRESHOLD_TIME]] [-r]
Summarize block device I/O latency
optional arguments:
  -h, --help            show this help message and exit
  -d DEVICE, --device DEVICE
                        inspect specified device
  -i [DIS_INTERVAL], --dis_interval [DIS_INTERVAL]
                        specify display interval
  -t [AVG_THRESHOLD_TIME], --avg_threshold_time [AVG_THRESHOLD_TIME]
                        display only when average request process time is
                        greater than this value
  -T [THRESHOLD_TIME], --threshold_time [THRESHOLD_TIME]
                        dump request life cycle when single request process
                        time is greater than this value
  -r, --dump_raw        dump every io request life cycle
examples:
    ./alibiolatency          # summarize block I/O latency(default display interval is 2s
)
    ./alibiolatency -d sda3  # inspect specified device /dev/sda3
    ./alibiolatency -i 2     # specify display interval, 2s
    ./alibiolatency -t 10    # display only when average request process time is greater
than 10ms
    ./alibiolatency -T 20    # dump request life cycle when single request process time i
s greater than 20ms
    ./alibiolatency -r       # dump every io request life cycle
```

- 通过 `man` 命令获取bcc工具说明。

```
man bcc-alibiolatency
```

5.6.16. 检测文件系统和块层的IO hang

IO hang是指在系统运行过程中，因某些IO耗时过长而引起的系统不稳定甚至宕机。为了准确检测出IO hang，Alibaba Cloud Linux 2扩展核心数据结构，增加了在较小的系统开销下，快速定位并检测IO hang的功能。本文主要介绍实现该功能的接口以及接口操作示例。

接口说明

接口	描述
/sys/block/<device>/queue/hang_threshold	该接口能够查看和修改用于检测IO hang的阈值，单位为ms，默认值为5000。
/sys/block/<device>/hang	该接口能够输出对应设备上超过IO hang阈值的读写IO个数。
/sys/kernel/debug/block/<device>/rq_hang	该接口能够获取IO hang的详细信息。

接口	描述
/proc/<pid>/wait_res	该接口能够获取进程正在等待的资源信息。
/proc/<pid>/task/<tid>/wait_res	该接口能够获取线程正在等待的资源信息。

以上接口中变量说明如下。

变量名	说明
<device>	块存储设备名。
<pid>	进程ID。
<tid>	线程ID。

示例一

您可以根据需求调用接口 `/sys/block/<device>/queue/hang_threshold` 修改用于检测IO hang的阈值。本示例中将默认阈值5000 ms修改为10000 ms。

1. 将磁盘*vdb*下的用于检测IO hang的阈值修改为10000 ms。

```
echo 10000 > /sys/block/vdb/queue/hang_threshold
```

2. 查看修改结果。

```
cat /sys/block/vdb/queue/hang_threshold
```

返回结果示例。

```
10000
```

示例二

您可以调用接口 `/sys/block/<device>/hang` 查询磁盘上产生IO hang的读写IO个数。本示例查询的磁盘为*vdb*。

查询命令如下。

```
cat /sys/block/vdb/hang
```

返回结果示例。

```
0        1      # 左边参数表示产生IO hang的读IO的个数，右边参数表示产生IO hang的写IO的个数
```

示例三

您可以调用接口 `/sys/kernel/debug/block/<device>/rq_hang` 获取产生IO hang的详细信息。本示例中的磁盘为*vdb*。

查询命令如下。

```
cat /sys/kernel/debug/block/vdb/rq_hang
```

返回结果示例如下。

```
ffff9e50162fc600 {.op=WRITE, .cmd_flags=SYNC, .rq_flags=STARTED|ELVPRIV|IO_STAT|STATS, .sta
te=in_flight, .tag=118, .internal_tag=67, .start_time_ns=1260981417094, .io_start_time_ns=1
260981436160, .current_time=1268458297417, .bio = ffff9e4907c31c00, .bio_pages = { ffffc859
60686740 }, .bio = ffff9e4907c31500, .bio_pages = { ffffc85960639000 }, .bio = ffff9e4907c3
0300, .bio_pages = { ffffc85960651700 }, .bio = ffff9e4907c31900, .bio_pages = { ffffc85960
608b00 }}
```

上述示例显示了IO的详细信息，从信息中获取到IO请求开始时间 `io_start_time_ns` 已被赋值。表明该IO请求未被及时处理，从而导致IO耗时过长。

示例四

您可以调用接口 `/proc/<pid>/wait_res` 获取进程正在等待的资源信息。本示例所查询的进程ID为 `577` 。

查询命令如下。

```
cat /proc/577/wait_res
```

返回结果示例。

```
1 0000000000000000 4310058496 4310061448    #示例值依次对应Field 1 Field 2 Field 3 Field 4
```

返回结果示例中参数说明如下。

参数	说明
Field 1	等待的资源类型。1表示文件系统中的缓存页（page），2表示块层bio。
Field 2	等待的资源（page/bio）地址。
Field 3	等待资源开始时间。
Field 4	读取该文件的当前时间，与Field 3的差值即为在该资源上等待的耗时。

5.6.17. 在cgroup v1接口开启PSI功能

在Linux的内核中PSI功能只支持cgroup v2接口。为了您在使用cgroup v1接口时，也可以通过PSI功能监控CPU、内存及IO性能异常等信息。Alibaba Cloud Linux 2在内核版本4.19.81-17.al7中为cgroup v1接口提供了PSI功能。本文主要介绍如何在cgroup v1接口开启PSI功能并查询相关信息。

背景信息

PSI（Pressure Stall Information）是一个可以监控CPU、内存及IO性能异常的内核功能。有关PSI功能的详细信息，您可以通过内核文档 `Documentation/accounting/psi.txt` 了解，内核文档包含在Alibaba Cloud Linux 2的Debuginfo包和源码包内，下载Debuginfo包和源码包请参见Alibaba Cloud Linux概述。

为cgroup v1接口开启PSI功能

默认情况下cgroup v1接口的PSI功能为关闭状态。按照以下步骤开启PSI功能。

1. 运行 `grubby` 命令，修改启动参数。

参数 `args` 中默认为 `"psi=1"` ，表示cgroup v2启用PSI功能。将参数修改为 `"psi=1 psi_v1=1"` ，表示Alibaba Cloud Linux 2为cgroup v1接口开启PSI功能。 本示例中内核版本为 `4.19.81-17.al7.x86_64` ，您在操作中需要更换为实际的内核版本，内核版本的查看命令为 `uname -a` 。

```
sudo grubby --update-kernel="/boot/vmlinuz-4.19.81-17.al7.x86_64" --args="psi=1 psi_v1=1"
```

2. 重启系统使该功能生效。

```
sudo reboot
```

确认cgroup v1接口的PSI功能已启用

系统重启后，您可以执行命令，确认内核 `/proc/cmdline` 中已启用cgroup v1接口的PSI功能。

```
cat /proc/cmdline | grep "psi=1 psi_v1=1"
```

查询CPU、内存及IO的监控数据

当您开启cgroup v1接口的PSI功能时，CPU、内存及IO的PSI监控数据均会输出到cpuacct控制器下，您可以通过以下命令查看详细的监控数据。

```
cat /sys/fs/cgroup/cpuacct/cpu.pressure
cat /sys/fs/cgroup/cpuacct/memory.pressure
cat /sys/fs/cgroup/cpuacct/io.pressure
```

5.6.18. 在cgroup v1接口开启CPU Burst功能

Alibaba Cloud Linux 2在内核版本4.19.91-22.al7中为cgroup v1接口提供了CPU Burst功能。CPU Burst功能允许容器被CPU限流时，突发使用CPU资源，进而提升容器性能、降低系统的延迟指标。本文介绍如何在cgroup v1接口开启CPU Burst功能，以及如何查询CPU Burst的统计数据。

背景信息

在容器服务中，容器允许使用的CPU资源被内核的CFS Bandwidth Controller（带宽控制器）限流。当您在cgroup v1接口开启CPU Burst功能后，CPU Burst功能允许容器突发使用限流之外的CPU资源。该功能既可以保证容器运行的服务质量，又不降低容器部署密度。

> **说明** 突发是指允许容器超过CPU限流使用额外的CPU资源。

关于CPU Burst的详细信息，您可以通过Alibaba Cloud Linux 2内核文档进行了解。Alibaba Cloud Linux 2内核文档存储在Debuginfo包和源码包内，路径为*Documentation/scheduler/sched-bwc.rst*。下载Debuginfo包和源码包的具体操作，请参见Alibaba Cloud Linux 2使用说明。

功能原理

CPU Burst功能允许突发使用的CPU资源依赖于日常的资源积累。比如，容器在日常运行中使用的CPU资源未超过CPU限流，则空余的CPU资源将会被积累。后续当容器运行需要大量CPU资源时，将通过CPU Burst功能突发使用CPU资源，这部分突发使用的资源来源于已积累的资源。以休假体系作为类比：

假如您每年休假时间为4天（CPU限流），未休的假期可以存放起来后续使用，但存放上限为4天（CPU Burst）。当您第一年、第二年各只休了1天的假期，那么没有休息的6天假期可以存放起来。当第三年的时候，理论上您可以休息共计10天的假期，但因为有存放上限（CPU Burst），则实际可以休息至多8天的假期。

开启CPU Burst功能

1. 检查cgroup v1接口中的CPU Burst功能的全局开关是否已打开。

```
cat /proc/sys/kernel/sched_cfs_bw_burst_enabled
```

返回结果说明：

- 如果返回结果为 `1` ，则表示CPU Burst功能的全局开关已打开。

> **说明** 默认情况下，cgroup v1接口中的CPU Burst功能的全局开关为打开状态。

- 如果返回结果不为 `1` ，则表示CPU Burst功能的全局开关已关闭。您可以运行以下命令打开全局开关：

```
echo 1 > /proc/sys/kernel/sched_cfs_bw_burst_enabled
```

2. 在具体的子cgroup中开启CPU Burst功能。

默认情况下，cgroup v1接口中的CPU Burst功能在各个子cgroup中均未开启。具体的开启方式如下：

i. 进入子cgroup路径下，检查CFS Bandwidth Controller限流是否处于生效状态。

```
cd /sys/fs/cgroup/cpu/子cgroup目录名称/
cat cpu.cfs_period_us
cat cpu.cfs_quota_us
```

如果 `cpu.cfs_quota_us` 对应的返回结果为正整数，则表示CFS Bandwidth Controller限流处于生效状态，进而在启用CPU Burst功能后，容器才可以获得超出CPU限流的CPU资源。

ii. 检查当前默认的CPU Burst设置。

```
cat cpu.cfs_burst_us
```

返回结果的默认值为 `0` ，表示CPU Burst功能未开启。

iii. 设置 `cpu.cfs_burst_us` 的值以开启CPU Burst功能。

您可以设置一个适用的正整数启用CPU Burst功能，且这个正整数表示子cgroup突发额外使用的CPU资源的上限。本文通过以下示例场景，介绍如何开启CPU Burst功能。

a. 配置CFS Bandwidth Controller带宽控制器默认的 `cpu.cfs_quota_us` 与 `cpu.cfs_period_us` 。
以下配置，将CPU资源的使用周期（ `cpu.cfs_period_us` ）设置为100ms，每个周期中的CPU限流（ `cpu.cfs_quota_us` ）设置为400ms，则子cgroup将会持续获得4个CPU资源（ `cpu.cfs_quota_us` / `cpu.cfs_period_us` ）。

```
echo 400000 > cpu.cfs_quota_us
echo 100000 > cpu.cfs_period_us
```

b. 配置 `cpu.cfs_burst_us` 以开启CPU Burst功能。
以下配置，将CPU Burst的值设置为600ms，表示开启了CPU Burst功能，且允许子cgroup可以突发额外使用最多6个CPU资源（ `cpu.cfs_burst_us` / `cpu.cfs_period_us` ）。

```
echo 600000 > cpu.cfs_burst_us
```

查询CPU Burst的统计数据

1. 进入待查询数据的子cgroup路径下。

```
cd /sys/fs/cgroup/cpu/子cgroup目录名称/
```

2. 查看统计数据。

```
cat cpu.stat
```

返回结果中，主要的信息说明如下：

- `nr_burst` 数据：当前子cgroup触发CPU Burst的次数。
- `burst_time` 数据：当前子cgroup突发使用CPU资源的时间。

5.6.19. Group Identity功能说明

Alibaba Cloud Linux 2从内核版本kernel-4.19.91-24.al7开始支持Group Identity功能，您可以通过该功能为每一个CPU cgroup设置不同的身份标识，以区分不同CPU cgroup中进程任务的优先级。

背景信息

> **注意** 当内核版本是kernel-4.19.91-25.1.al7时，Alibaba Cloud Linux 2使用Group Identity功能时会出现宕机现象。请先升级内核版本至kernel-4.19.91-25.6.al7或更高版本。具体操作，请参见相关问题。

在业务的混合部署（延迟敏感型和计算型任务混合部署在同一台实例）场景中，Linux内核调度器需要为高优先级任务赋予更多的调度机会以最小化调度延迟，并需要把低优先级任务对内核调度带来的影响降到最低。基于该场景，Alibaba Cloud Linux 2提供了Group Identity功能，为CPU cgroup新增了配置调度优先级的接口，且不同优先级的任务具有以下特点：

- 高优先级任务的唤醒延迟最小化。
- 低优先级任务不对高优先级任务造成性能影响。主要体现在：
  - 低优先级任务的唤醒不会对高优先级任务造成性能影响。
  - 低优先级任务不会通过SMT调度器共享硬件unit而对高优先级任务造成性能影响。

功能原理

Group Identity功能可以对每一个CPU cgroup设置身份标识，以区分cgroup中的任务优先级。Group Identity核心是双红黑树设计，在CFS（Completely Fair Scheduler）调度队列的单红黑树基础上，新增了一颗低优先级的红黑树，用于存放低优先级任务。

系统内核在调度包含具有身份标识的任务时，会根据不同的优先级做相应处理。具体说明如下表：

身份标识（按优先级由高到低排序）	说明

身份标识（按优先级由高到低排序）	说明
`ID_HIGHCLASS`	高优先级任务，相较于低于其优先级的任务会有更多的资源抢占机会。 CFS调度器在调度高优先级任务时，会有以下行为的变化： • 如果当前运行的是低优先级任务，当高优先级任务被唤醒时，可无条件进行资源抢占。 • 如果当前运行的是普通优先级任务，当高优先级任务被唤醒时vruntime小于普通优先级任务，则高优先级任务可以无视原有调度策略（任务在CPU上运行的时间小于最小运行时间时不可以进行资源抢占），进行资源抢占。 • 在排队运行任务的场景中，如果当前运行的是普通或低优先级的任务，当高优先级任务的vruntime小于当前任务时，高优先级任务可以无视原有调度策略（任务在CPU上运行的时间小于最小运行时间时不可以进行资源抢占），进行资源抢占。
`ID_NORMAL`	普通优先级任务，相较于低于其优先级的任务会有更多的资源抢占机会。 CFS调度器在调度普通优先级任务时，会有以下行为的变化： • 如果当前运行的是低优先级任务，当普通优先级任务被唤醒时，可无条件进行资源抢占。 • 在排队运行任务的场景中，如果当前运行的是低优先级任务，当普通优先级任务vruntime小于低优先级任务时，普通优先级任务可以无视原有调度策略（任务在CPU上运行的时间小于最小运行时间时不可以进行资源抢占），进行资源抢占。
`ID_UNDERCLASS`	低优先级任务。 CFS调度器在调度低优先级任务时，会有以下行为的变化： 如果对端的SMT调度器运行了SMT驱逐者（`ID_SMT_EXPELLER`）任务，则低优先级任务无法被调度至CPU上，即等同于被踢出了任务运行队列。

以上身份标识的作用范围遵从CPU cgroup的资源管理策略：

- 在同一层级的cgroup中的任务，身份标识的优先级生效。
- 相对于父层级的cgroup，任务身份标识的优先级不生效；相对于子层级的cgroup，任务身份标识的优先级生效。
- 同优先级的身份标识之间的资源竞争基本服从CFS调度器的策略，但需要注意`ID_UNDERCLASS`、`ID_NORMAL`身份标识的任务没有最小运行时间的保障。

其他身份标识说明：

身份标识	说明
`ID_SMT_EXPELLER`	SMT驱逐者，当其被调度到CPU上运行时，驱逐SMT对端CPU上的`ID_UNDERCLASS`身份标识的任务。
`ID_IDLE_SEEKER`	表示当任务被唤醒时，会在调度器策略范围内最大限度的尝试找到空闲CPU（Idle CPU）。
`ID_IDLE_SAVER`	与内核参数`sched_idle_saver_wmark`结合使用，您可以通过`sched_idle_saver_wmark`自行配置空闲时长水位线。 当`ID_IDLE_SAVER`身份标识的任务被唤醒时，只会尝试找到高于该水位线的空闲CPU，不会尝试找到低于该水位线的空闲CPU。

接口说明

- 身份标识配置接口
  Group Identity提供了两个用于设置任务身份标识的接口：`/sys/fs/cgroup/cpu/$cg/cpu.identity` 与 `/sys/fs/cgroup/cpu/$cg/cpu.bvt_warp_ns` 。其中变量*$cg*表示任务实际所在的子cgroup目录节点。
  在使用身份标识配置接口前，您需要注意：
  - `cpu.bvt_warp_ns` 接口是快捷配置接口，写入后会转换为identity。
  - `cpu.identity` 接口与 `cpu.bvt_warp_ns` 接口都是对cgroup的identity做更改。
  - `cpu.identity` 接口写入后会覆盖 `cpu.bvt_warp_ns` 接口上次的写入值，但不会在 `cpu.bvt_warp_ns` 接口中体现。
  - `cpu.bvt_warp_ns` 接口写入后会覆盖 `cpu.identity` 接口上次的写入值，但不会在 `cpu.identity` 接口中体现。
  - 您只需要使用任一接口设置任务的身份标识，不建议同时设置两个接口。
  - 如果您不熟悉操作系统内核的相关操作，不建议使用 `cpu.identity` 接口。

  接口说明如下：

接口	说明
`cpu.identity`	默认取值为0，表示身份标识为 `ID_UNDERCLASS` 。 该接口是一个位段，一共有5个比特位，该接口各个比特位的取值说明如下： ○ 空值：表示身份标识为 `ID_NORMAL` 。 ○ 比特位0：表示身份标识为 `ID_UNDERCLASS` 。 ○ 比特位1：表示身份标识为 `ID_HIGHCLASS` 。 ○ 比特位2：表示身份标识为 `ID_SMT_EXPELLER` 。 ○ 比特位3：表示身份标识为 `ID_IDLE_SAVER` 。 ○ 比特位4：表示身份标识为 `ID_IDLE_SEEKER` 。 例如，如果设置一个cgroup的身份标识为 `ID_HIGHCLASS` 和 `ID_IDLE_SEEKER` ，那么将比特位1和4置为1，其他比特位置为0，得到的二进制表示为：10010，转化为十进制为：18，则执行 `echo 18 > /sys/fs/cgroup/cpu/$cg/cpu.identity` 即可完成写入。
`cpu.bvt_warp_ns`	默认取值为0，表示身份标识为 `ID_NORMAL` 。该接口的取值说明如下： ○ 2：表示同时具有身份标识 `ID_SMT_EXPELLER` 、 `ID_IDLE_SEEKER` 、 `ID_HIGHCLASS` ，对应的identity值为22。 ○ 1：表示同时具有身份标识 `ID_HIGHCLASS` 、 `ID_IDLE_SEEKER` ，对应的identity值为18。 ○ 0：表示身份标识为 `ID_NORMAL` ，对应的identity值为0。 ○ -1：表示同时具有身份标识 `ID_UNDERCLASS` 、 `ID_IDLE_SAVER` ，对应的identity值为9。 ○ -2：表示同时具有身份标识 `ID_UNDERCLASS` 、 `ID_IDLE_SAVER` ，对应的identity值为9。

- 调度特性开关配置接口

运行以下命令，您可以通过 `sched_features` 接口查看到内核调度特性的默认配置。

```
cat /sys/kernel/debug/sched_features
```

具体说明如下：

调度特性	说明	默认值
`ID_IDLE_AVG`	该特性与 `ID_IDLE_SAVER` 身份标识配合，把 `ID_UNDERCLASS` 任务的运行时间计入空闲时长，防止只有 `ID_UNDERCLASS` 任务运行时仍保留空闲CPU（Idle CPU）的问题，避免资源浪费。	`ID_IDLE_AVG` ：表示特性为启用状态。
`ID_RESCUE_EXPELLEE`	该特性作用于负载均衡场景，如果任务无法找到可用的CPU资源，则正在进行驱逐 `ID_UNDERCLASS` 任务的CPU会成为负载均衡的目标。用于帮助 `ID_UNDERCLASS` 任务尽快摆脱被驱逐的状态。	`ID_RESCUE_EXPELLEE` ：表示特性为启用状态。
`ID_EXPELLEE_NEVER_HOT`	该特性被启用后，正在被驱逐的任务在判断是否需要迁移至其他CPU时，不会因为热缓存的原因而造成拒绝迁移。用于帮助 `ID_UNDERCLASS` 任务尽快摆脱被驱逐的状态。	`NO_ID_EXPELLEE_NEVER_HOT` ：表示特性为关闭状态。
`ID_LOOSE_EXPEL`	该特性被启用后，CPU不会在每次选择任务时更新驱逐状态，而是根据内核参数 `sched_expel_update_interval` 设置的时间自动更新。该特性的开关仅影响CPU选择任务时的状态更新，不影响处理IPI中断的更新。	`NO_ID_LOOSE_EXPEL` ：表示特性为关闭状态。
`ID_LAST_HIGHCLASS_STAY`	该特性被启用后，CPU上最后一个运行的 `ID_HIGHCLASS` 任务不会被迁移至其他CPU上。	`ID_LAST_HIGHCLASS_STAY` ：表示特性为启用状态。
`ID_EXPELLER_SHARE_CORE`	○ 该特性开启时允许 `ID_SMT_EXPELLER` 的任务优先选择已经有 `ID_SMT_EXPELLER` 任务的物理核，该特性关闭时则不允许。 ○ 该特性关闭时可以尽可能的把 `ID_SMT_EXPELLER` 的任务分散到各个物理核上，从而避免 `ID_SMT_EXPELLER` 任务之间的相互干扰。	`ID_EXPELLER_SHARE_CORE` ：表示特性为启用状态。

- 用于sysctl配置内核参数的接口
  Group Identity的部分功能的实现需要以内核参数的取值作为参考。相关内核参数的具体说明如下表：

内核参数	说明	单位	默认值
`/proc/sys/kernel/sched_expel_update_interval`	CPU在选择任务时，驱逐状态的自动更新时间间隔。仅在 `ID_LOOSE_EXPEL` 特性开启时生效。	ms	10
`/proc/sys/kernel/sched_expel_idle_balance_delay`	CPU在驱逐状态下，`idle balance` 的最小时间间隔。取值为-1时表示不允许进行 `idle balance` 。当CPU上均为 `ID_UNDERCLASS` 任务且任务在被驱逐时，CPU的状态可以理解为空闲状态，在该状态下CPU会进行 `idle balance` 以提高负载均衡的效果，但会对 `ID_UNDERCLASS` 任务造成损伤。通过设置 `sched_expel_idle_balance_delay` 参数可以缓解该问题。	ms	-1
`/proc/sys/kernel/sched_idle_saver_wmark`	设置CPU空闲时间的水位线。当 `ID_IDLE_SAVER` 任务被唤醒时，只会尝试找到高于该水位线的空闲CPU，不会尝试找到低于该水位线的空闲CPU。	ns	0

信息输出说明

在使用Group Identity功能期间，您可以运行以下命令，查看多维度的参数信息。

```
cat /proc/sched_debug
```

输出的参数说明如下：

参数	说明
`nr_high_running`	当前CPU上运行的 `ID_HIGHCLASS` 任务数量。
`nr_under_running`	当前CPU上运行的 `ID_UNDERCLASS` 任务数量。
`nr_expel_immune`	当前CPU上运行的非 `ID_UNDERCLASS` 任务数量。
`smt_expeller`	当前CPU是否有 `ID_SMT_EXPELLER` 任务在运行。参数值为1表示有；参数值为0表示无。
`on_expel`	SMT调度器的对端是否有 `ID_SMT_EXPELLER` 任务在运行。参数值为1表示有；参数值为0表示无。
`high_exec_sum`	当前CPU上 `ID_HIGHCLASS` 任务的累计运行时间。
`under_exec_sum`	当前CPU上 `ID_UNDERCLASS` 任务的累计运行时间。

参数	说明
`h_nr_expel_immune`	当前 `cfs_rq` 上运行的非 `ID_UNDERCLASS` 任务数量。
`expel_start`	CPU在驱逐任务的开始阶段，两个红黑树结构的最小虚拟运行时间的差距。
`expel_spread`	由于CPU驱逐状态造成的两个红黑树结构最小虚拟运行时间的累计差距。
`min_under_vruntime`	低优先级红黑树结构的最小虚拟运行时间。

相关问题

问题：如何将内核版本从kernel-4.19.91-25.1.al7升级至kernel-4.19.91-25.6.al7或更高版本？

解决方案：

1. 远程登录ECS实例。
   具体操作，请参见通过密码或密钥认证登录Linux实例。
2. 运行以下命令，查询内核版本。

   ```
   uname -r
   ```

3. 运行以下命令，升级内核版本。

   ```
   yum update kernel
   ```

4. 运行以下命令，重启ECS实例至新的内核版本。

   ```
   reboot
   ```

5.6.20. /proc/meminfo文件中的统计信息变更说明

Alibaba Cloud Linux 2操作系统在内核4.19.91-22.al7.x86_64及其之后的版本中，*/proc/meminfo*文件内的匿名页状态统计信息 `Active(anon)` 和 `Inactive(anon)` 发生了变化。如果您的应用程序正在使用该统计信息，统计信息的变化会导致变更前后查询到的数据不一致。本文将对本次变化进行详细说明。

变更原因

Linux kernel社区在最新的版本中对匿名页的回收进行了优化，分配的匿名页默认放置的位置由active LRU变更为了inactive LRU，因此对*/proc/meminfo*文件内的统计信息 `Active(anon)` 和 `Inactive(anon)` 的数据产生了影响。社区合入信息如下所示：

- 社区合入版本：Linux Kernel 5.10
- 社区合入commit：b518154e59aab3ad0780a169c5cc84bd4ee4357e

Alibaba Cloud Linux 2的内核在4.19.91-22.al7.x86_64及其之后的版本中合入了该优化项，*/proc/meminfo*文件内的统计信息 `Active(anon)` 和 `Inactive(anon)` 的数据将发生变化。

> **说明** 您可以在操作系统内运行uname -r命令获取内核版本信息。

变更详情

Alibaba Cloud Linux 2的内核在4.19.91-22.al7.x86_64版本之前（不包含该版本），应用程序申请的匿名页（anon page）默认被统计到*/proc/meminfo*文件的 `Active(anon)` 中，当内存不足时才会被统计到 `Inactive(anon)` 中。

当内核升级到4.19.91-22.al7.x86_64及其之后的版本时，应用程序申请的匿名页（anon page）默认被统计到*/proc/meminfo*文件的 `Inactive(anon)` 中，当被访问后才会切换到 `Active(anon)` 中。因此，如果您在使用*/proc/meminfo*文件内的 `Active(anon)` 和 `Inactive(anon)` 来统计匿名页状态的数据，需要对本次变化进行相应的调整。

变更影响及建议

由于统计匿名页状态的信息（即 `Active(anon)` 和 `Inactive(anon)` ）发生变化，因此相同的应用程序在本次变更前所查询到的 `Active(anon)` 和 `Inactive(anon)` 的数据，与变更后查询的到数据将不一致。

建议您根据所使用的Alibaba Cloud Linux 2操作系统中最新的匿名页状态的统计数据，对应用程序的配置进行相应的调整。

5.6.21. 增强容器资源可见性

Alibaba Cloud Linux 2从内核版本kernel-4.19.91-22.2.al7开始，在内核层面提供了容器资源视图功能的相关接口，实现对容器资源的可见性增强。本文将对该功能的接口进行说明，并提供示例场景供您参考。

背景信息

Alibaba Cloud Linux 2的容器资源视图功能接口默认状态下是未启动的，当您在启动该功能后，如果在容器中使用**top**、**free**等命令，让容器读取以下接口的数据时，将直接获取容器资源信息，而不是获取容器所在的宿主机（即ECS实例）资源信息。

- */proc/cpuinfo*
- */proc/meminfo*
- */sys/devices/system/cpu/online*

接口说明

接口	说明
/proc/sys/kernel/rich_container_enable	该接口控制容器资源视图功能是否开启。取值范围： • 0：关闭容器资源视图功能。 • 1：开启容器资源视图功能。 默认值：0
/proc/sys/kernel/rich_container_source	该接口控制cgroup接口的数据源。取值范围： • 0：使用指针current所在的cgroup接口作为数据源。 • 1：使用child reaper（即当前PID Namespace的1号进程）所在的cgroup作为数据源。 默认值：0

接口	说明
/proc/sys/kernel/rich_container_cpuinfo_source	该接口控制*/proc/cpuinfo*接口以及*/sys/devices/system/cpu/online*接口显示的CPU数量。取值范围： • 0：使用Kubernetes的Request和Limit数据的比值（`Request/Limit`），即`quota`与`period`的比值（`quota/period`）。 • 1：使用*cpuset.cpus*接口中的CPU数据源。 • 2：使用`cpu.shares`值除以`/proc/sys/kernel/rich_container_cpuinfo_sharesbase`值的向上取整后的数据（原始数据如果包含小数，则整数位加1后，只取整数作为最终数据，例如：原始数据为1.1，则最终数据为2）。最终数据最多不超过实际在线CPU的数量。 默认值：0
/proc/sys/kernel/rich_container_cpuinfo_sharesbase	当*/proc/sys/kernel/rich_container_cpuinfo_source*接口的取值为2时，需要使用该接口作为计算公式的一部分获取最终数据。取值范围：大于等于2的整数值。 默认值：1024

接口使用示例

本示例中，已在一台Linux实例中部署Docker，并创建了一个内存大小为1 GB的容器。

- 如果您未开启容器资源视图功能，即*/proc/sys/kernel/rich_container_enable*接口的值为0。当您在容器中运行**free -m**命令时，查看到的资源信息如下图所示，该信息为容器所在的宿主机（Linux实例）资源信息。

```
root@86ed7d[redacted]:/var/www# free -m
             total       used       free     shared    buffers     cached
Mem:          7609       1998       5610          1        102       1446
-/+ buffers/cache:        449       7159
Swap:            0          0          0
```

- 如果您在宿主机（Linux实例）中运行命令**echo 1 > /proc/sys/kernel/rich_container_enable**开启了容器资源视图功能，当您在容器中运行**free -m**命令时，查看到的资源信息如下图所示，该信息为容器资源信息。

```
root@86ed7d[redacted]:/var/www# free -m
             total       used       free     shared    buffers     cached
Mem:          1024          0       1023          0          0          0
-/+ buffers/cache:          0       1023
Swap:            0          0          0
```

特殊场景说明

一般情况下，开启容器资源视图功能后，使用相关接口的默认值即可满足常规需求，但您需要注意以下特殊场景的接口配置：

对于非共享PID Namespace的Pod，其中的每一个容器都是独立的PID Namespace，如果使用systemd启动某个特权容器，容器的进程号为1号，则采集监控数据的任务可能位于容器的某个子cgroup中，而不是根cgroup。

例如，当您通过SSH登录容器并运行**cat /proc/cpuinfo**命令后：

- 如果*/proc/sys/kernel/rich_container_source*取值为默认值0，则指针current实际是位于容器的sshd.service所创建的子cgroup中，此时查看的结果为错误数据。
- 如果您运行**echo 1 > /proc/sys/kernel/rich_container_source**命令，使用child reaper（即当前PID Namespace的1号进程）所在的cgroup作为数据源，即可查看到正确的数据。

5.6.22. SMC-R说明

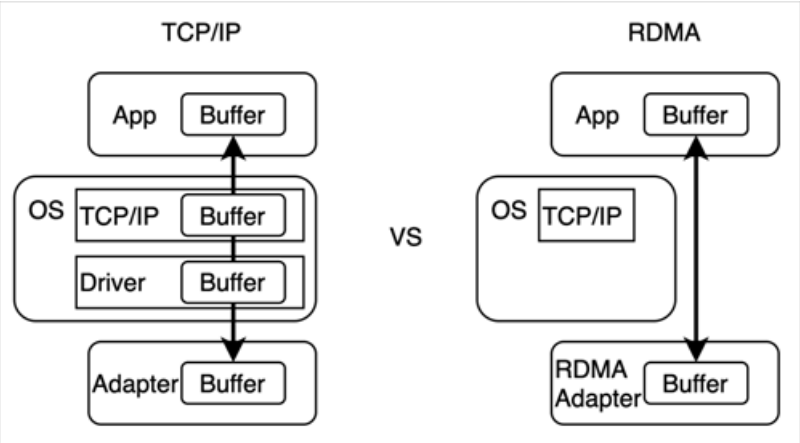
阿里云Alibaba Cloud Linux 3操作系统增加了对SMC-R的支持，基于阿里云弹性RDMA技术，实现对TCP应用透明无损的替换，为内存数据库、RPC、大文件传输等场景提供相比TCP更好的性能。本文将为您介绍SMC-R及其使用方法。

背景信息

SMC-R是基于RDMA的共享内存通信（Shared Memory Communications over RDMA）的英文缩写，其实现依赖于RDMA。在了解SMC-R之前，您需要先了解什么是RDMA以及阿里云提供的弹性RDMA服务：

RDMA是一种旁路内核的远程内存直接访问技术，被广泛应用于数据密集型和计算密集型场景中，是高性能计算、机器学习、数据中心、海量存储等领域的重要解决方案。RDMA支撑了阿里云ESSD云盘、PolarDB数据库等核心业务，并在双11等重大场景得到充分验证。

RDMA具有零拷贝、协议栈卸载的特点。RDMA将协议栈的实现下沉至RDMA网卡（RNIC），绕过内核直接访问远程内存中的数据。由于不经过操作系统内核协议栈，RDMA与传统TCP网络相比不仅节省了内核协议栈处理和数据拷贝所需的CPU资源，同时也提高了网络吞吐量、降低了网络通信时延。两者协议栈差异如下图所示：



过去，RDMA只能在一些数据中心网络中通过网卡和交换机紧密配合使用，部署复杂度高。如今，阿里云弹性RDMA将复杂的RDMA技术带到云上，使云服务器ECS的用户也能使用高性能的RDMA传输，无需关心底层复杂的网卡、交换机等物理网络环境配置，降低了使用RDMA的复杂程度。

然而，由于RDMA使用的IB verbs接口和常用的POSIX socket接口存在巨大的差异，普通的应用程序如果要用好RDMA，往往需要面临着大量的业务改造，高效的使用IB verbs接口仍存在较高的技术门槛。

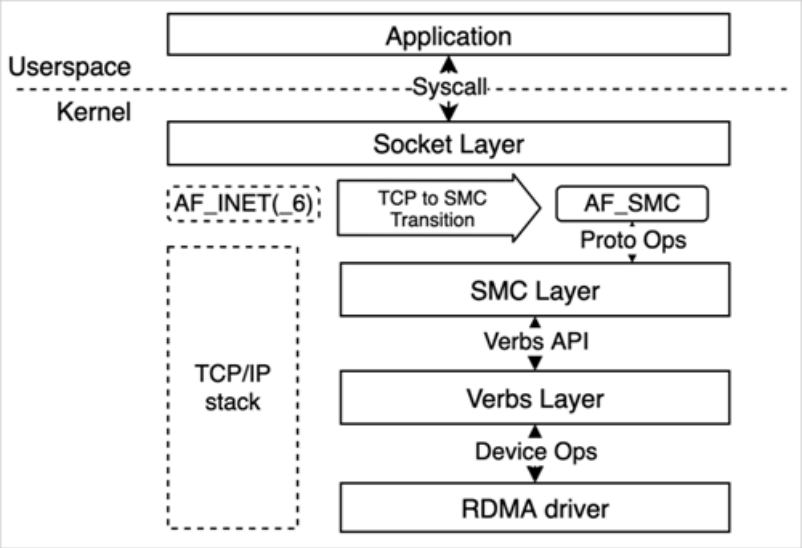
因此，为了充分挖掘弹性RDMA的潜力，为云上用户提供更好的网络性能，Alibaba Cloud Linux 3提供并优化了SMC-R，同时增加了对弹性RDMA的支持。SMC-R是一种对应用提供标准的socket接口，而底层采用RDMA进行通信的技术。其在高效使用RDMA技术的同时，保留对标准TCP应用的兼容，使更多的应用无需做任何修改便能享受RDMA带来的技术红利。

技术架构

SMC-R技术架构说明如下：

- 协议层级与透明替换

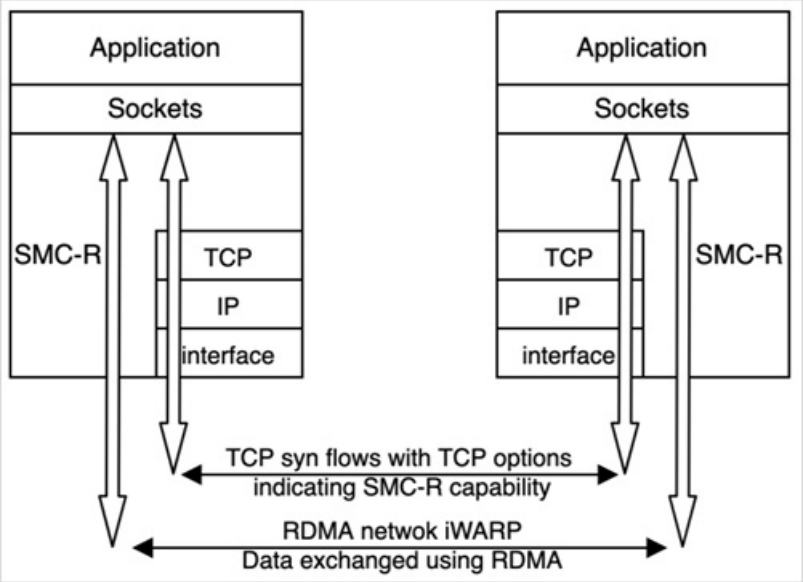
SMC-R是一套完全兼容socket的可靠、流式的传输协议。SMC-R工作于内核空间，处于socket层和内核IB verbs层之间，向上支持常见的socket接口，向下使用IB verbs内核态接口配合RDMA驱动传输数据。Alibaba Cloud Linux 3提供了控制socket层协议族替换的工具，实现net namespace维度或单个应用维度下的TCP至SMC-R透明替换能力，您无需修改任何网络应用即可完成从TCP到SMC-R的转换，享受RDMA带来的网络性能提升。技术架构图如下所示：



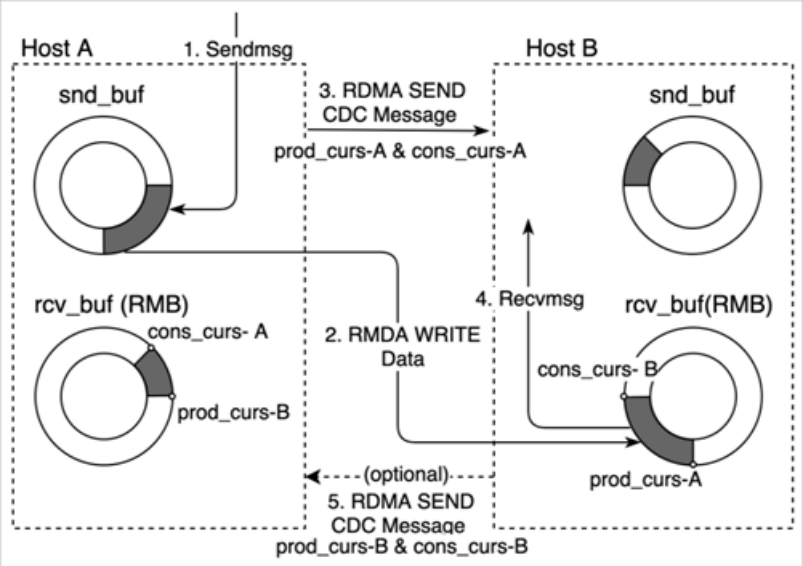
- 自动协商和安全回退
  SMC-R具备自动协商、动态回退TCP的能力。SMC-R建立RDMA链路时，首先在内核中与通信对端建立TCP连接，在握手过程中使用特殊的TCP选项表明自身支持SMC-R，并确认对端同样支持SMC-R。
  - 若协商过程中确认两端均使用SMC-R，则SMC-R为用户态网络应用申请所需RDMA资源，包括准备RDMA异步通信模型所需的QP与CQ、创建发送数据缓冲区、创建接收数据缓冲区并将其注册为可被远程节点直接访问的远程内存缓冲区RMB（Remote Memory Buffer），完成RDMA链路的初始化。SMC-R将访问RMB所需的访问密钥以及起始地址封装成远程访问令牌（RToken）告知远程节点，作为其访问RMB的重要验证信息。
  - 若协商过程中发现收发两端其一无法支持SMC-R时，将触发SMC-R回退机制，使用协商时建立的TCP连接完成数据传输，以保障网络的稳定和可靠。

> **说明** 需要注意的是，SMC-R仅支持连接协商期间回退至TCP协议栈，但不支持数据传输过程中的回退。

协商和数据传输流如下图所示：



- 环形内存和数据收发
  SMC-R实现高性能传输的关键在于高效的RDMA网络和环形共享内存结构。SMC-R使用RDMA WRITE单边操作的方式将网络应用传递至内核的数据直接高效地写入远程节点环形RMB中，并伴随着使用RDMA SEND/RECV双边操作的方式交互连接数据管理CDC（Connection Data Control）消息，用于更新、同步RMB中的数据游标（Cursor）。工作原理说明：
  针对一侧RMB，读者更新数据消费者游标（Consumer Cursor），标识即将读取的下一字节地址。为避免数据丢失，写者不会将数据写入超过消费者游标的RMB空间中。相似的，写者更新生产者游标（Producer Cursor），标识即将写入的下一字节地址，为确保数据的正确性，读者不会读取超过生产者游标的RMB空间中的内容。数据游标的更新与同步伴随着网络数据传输的始终，确保数据传输的安全与可靠。
  数据传输过程如下图所示：



核心优势

SMC-R的优势主要体现在以下几点：

- 高性能
  得益于RDMA将数据面功能下沉至RNIC并旁路内核直接访问对端环形接收缓冲区，SMC-R相较于传统TCP协议栈在合适的场景下可获得更低的时延、更高的吞吐量，以及更小的CPU负载。详细说明如下：
  - 更轻薄的协议栈。

- 使用RDMA进行通信，网络时延更低、CPU占用更少、吞吐量更高。
- 高效可靠的远程环形缓冲区直接访问。

- 透明替换
  SMC-R兼容POSIX socket接口，通过sysctl和用户态工具支持net namespace或单个应用维度下的TCP至SMC-R协议栈透明替换，在用户无修改的情况下完成新连接协议栈替换，无需额外的应用改造和开发成本。详细说明如下：
  - 兼容socket接口的RDMA RC传输，实现可靠的流式传输协议。
  - 自动协议协商和安全回退TCP机制。
  - net namespace和应用维度的协议栈无损透明替换。
  - 底层兼容弹性RDMA iWARP和RoCE网络。

应用场景

基于SMC-R的高性能、透明替换等优势，该技术的典型应用场景示例如下：

- 时延敏感的数据查询和处理
  Redis、memcached、PostgreSQL等高性能数据查询与处理的场景，对网络性能有极高的要求。SMC-R为应用提供无侵入式透明替换TCP的能力，无需应用二次开发和适配，即可为应用提供最高50%的QPS提升。
- 高吞吐的数据传输
  集群内的大规模数据交互与传输，往往需要占用大量的带宽和CPU资源。得益于SMC高效的通信模型，SMC-R在相同的吞吐性能下，CPU资源使用显著低于传统TCP，为应用节省更多的计算资源。

使用说明

Alibaba Cloud Linux 3提供丰富的SMC-R运维监控工具，向您提供完善的SMC-R状态监控和故障诊断功能。您可以通过下述步骤使用SMC-R：

1. 加载SMC-R模块。

   SMC-R默认编译为内核模块，您可在系统中手动加载smc与smc_diag内核模块。命令说明如下：

   i. 加载 `smc` 内核模块。

   ```
   modprobe smc
   ```

   ii. 加载 `smc_diag` 内核模块。

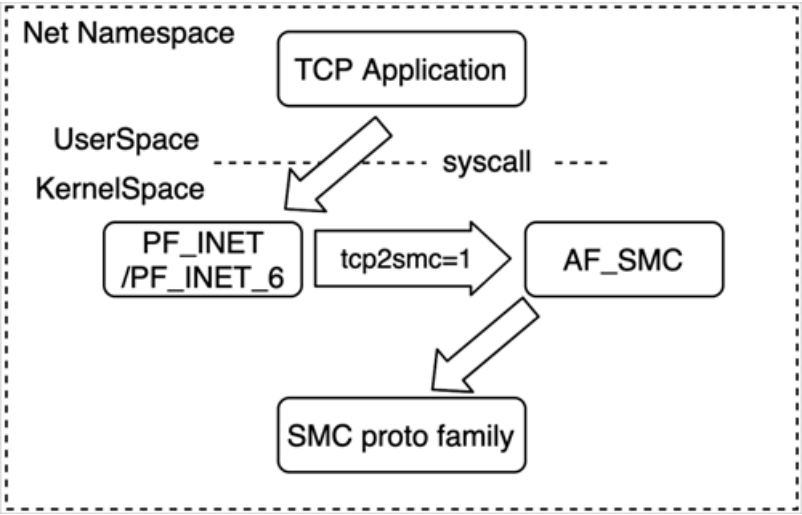
   ```
   modprobe smc_diag
   ```

2. 开启透明替换。

   Alibaba Cloud Linux 3支持两个维度的透明替换。具体说明如下：

   - net namespace维度

Alibaba Cloud Linux 3为您提供了将net namespace范围内所有新创建的TCP socket替换为SMC-R socket的功能。替换过程如下图所示：



在net namespace维度开启透明替换的操作说明如下：

a. 运行以下命令，打开net namespace范围全局替换。

```
sysctl net.smc.tcp2smc=1
```

默认情况下，`sysctl net.smc.tcp2smc=0`。当`sysctl net.smc.tcp2smc=1`时，应用新创建的socket的协议族将由`PF_INET/PF_INET6`转变为`AF_SMC`，即从TCP socket转变为SMC-R socket。

b. 运行应用。
若对端同样执行步骤1中所述操作，则两端将使用SMC-R传输数据，否则将回退至TCP协议完成数据传输。协商过程的详细说明，请参见技术架构的自动协商和安全回退。

c. 运行以下命令，关闭net namespace范围全局替换。

```
sysctl net.smc.tcp2smc=0
```

- 应用维度
Alibaba Cloud Linux 3还提供了应用维度的TCP替换为SMC-R功能。功能实现需要基于SMC-R的运维监控工具集`smc-tools`。

> **说明** `smc-tools`工具集的安装命令为yum install smc-tools -y。关于`smc-tools`工具集的更多信息，请参见下文的步骤3。

利用`smc-tools`工具集中的脚本`smc_run`运行应用程序时，`smc_run`将使用`LD_PRELOAD`环境变量把`smc-tools`工具集中的*libsmc-preload.so*定义为优先加载的动态库。*libsmc-preload.so*将尝试把应用程序新创建的TCP socket替换为SMC-R socket。`smc_run`命令的使用说明如下：

```
Usage: smc_run [ OPTIONS ] COMMAND
Run COMMAND using SMC for TCP sockets
```

例如，当您尝试使用SMC-R运行当前目录下的*testApp*应用程序时，需要运行以下命令：

```
smc_run ./testApp
```

与net namespace维度的透明替换类似，需要收发两端均使用 `smc_run` 将TCP透明替换至SMC-R，才能在两端间建立SMC-R连接，使用RDMA传输数据。

3. 使用SMC-R的运维监控工具，对SMC-R进行监控。

   `smc-tools` 工具集为您提供了多个维度的SMC-R跟踪诊断，主要包括：

   - **smcr**：提供SMC-R相关的linkgroup、device等信息。
   - **smcss**：提供活跃的SMC socket相关信息。

     i. 运行以下命令，安装SMC-R的运维监控工具集 `smc-tools` 。

     ```
     yum install smc-tools -y
     ```

     ii. 使用**smcr**。

     smcr用于显示SMC-R linkgroup、device等信息。
     命令说明如下：

     ```
     Usage: smcr  [ OPTIONS ] OBJECT {COMMAND | help}
     OBJECT : { linkgroup | device }
             linkgroup
                 Linkgroup(s) or link(s) used by SMC-R.
             device
                 One or more SMC-R devices.
     OPTIONS : {-v[ersion] | -d[etails] | -dd[etails]}
             -v, -version
                 Print the version of the smcr utility and exit.
             -d, -details
                 Print detailed information.
             -dd, -ddetails
                 Print more detailed information.
     ```

     使用示例：

     - 您可以运行以下命令，查看支持SMC-R的设备。

       ```
       smcr device
       ```

       返回结果示例：

       ```
       Net-Dev         IB-Dev    IB-P  IB-State  Type          Crit  #Links  PNET-ID
       eth0            erdma_01    1    ACTIVE  0x7ffd          No       0
       ```

     - 您可以运行以下命令，查看SMC-R linkgroup的信息。

       ```
       smcr linkgroup
       ```

       返回结果示例：

       ```
       LG-ID    LG-Role  LG-Type  VLAN  #Conns  PNET-ID
       00000100 CLNT     SINGLE      0       1
       ```

iii. 使用smcss。

smcss用于显示SMC-R相关socket的详细信息。
命令说明如下：

```
Usage: smcss [ OPTIONS ]
OPTIONS :
       (none)
              displays a list of connecting, closing, or connected SMC sockets with
basic information.
       -a, --all
              displays all types of SMC sockets: listening, opening, closing, and c
onnected.
       -l, --listening
              shows listening sockets only. These are omitted by default.
       -d, --debug
              displays additional debug information, such as shutdown state.
       -D, --smcd
              displays additional SMC-D specific information. Shows SMC-D sockets o
nly.
       -h, --help
              displays usage information.
       -R, --smcr
              displays additional SMC-R specific information. Shows SMC-R sockets o
nly.
       -v, --version
              displays program version.
       -W, --wide
              do not truncate IP addresses.
```

使用示例：
您可以运行以下命令，查看所有的SMC-R sockets的详细信息。

```
smcss -a -R -d
```

返回结果示例：

```
State          UID   Inode   Local Address           Peer Address            Intf M
ode Shutd Token    Sndbuf   Rcvbuf   Peerbuf  rxprod-Cursor rxcons-Cursor rxFlags t
xprod-Cursor txcons-Cursor txFlags txprep-Cursor txsent-Cursor txfin-Cursor  Role I
B-device       Port Linkid GID                                       Peer-GID
ACTIVE         00000 1105985880 192.168.XX.XX:49080    192.168.XX.XX:10003    0000
SMCR  <->  00000001 00020000 00040000 00040000 0001:00026256 0001:00026256 00:00
0001:00026264 0001:00026256 00:00   0003:00006264 0003:00006264 0003:00006264 CLNT
erdma_012211    01   01     0016:3e01:2211:0000:0000:0000:0000:0000  0016:3e01:43b4
:0000:0000:0000:0000:0000
```

5.6.23. 内核统一异常框架（UKFEF）

Alibaba Cloud Linux 3在内核版本5.10.60-9.al8.x86_64增加了UKFEF（Unified Kernel Fault Event Framework），用于统计可能导致风险的系统异常事件，并统一格式输出事件报告。本文主要介绍UKFEF所统计的事件、事件报告输出形式以及控制UKFEF的接口。

背景信息

操作系统在出现严重问题前，可能会输出一些特征或提示信息。在运维过程中，您可以利用这些信息进行故障预测和实施运维操作，但由于这些信息分散在系统中的不同模块，且输出格式各异。因此，您在收集系统异常事件时可能面临以下问题：

- 解析系统异常事件（例如异常事件的含义、可能造成的影响等）需要一定的专业知识作为基础。
- 不同格式的异常事件，对于自动化运维不友好，您需要在信息采集时做格式匹配，并需要做数据清洗。

基于以上问题，Alibaba Cloud Linux 3在操作系统内核层面提供了内核统一异常框架（UKFEF）。UKFEF针对各类可能导致风险的系统异常事件进行统计，并自动判断事件的严重程度，然后统一格式输出事件报告，报告包括了问题产生的场景以及建议的风险级别，从而简化运维过程中对系统异常的识别难度。同时，UKFEF将已知异常事件进行分级，并提供了历史内核版本不具备的系统风险报告。

UKFEF功能按照异常事件的类型、影响、统计等多个维度输出报告，便于您在运维时高效的对系统异常进行诊断。此外，事件报告通过多种形式输出，避免数据丢失。

事件说明

UKFEF划分的事件类型、事件级别，以及事件报告形式的说明如下：

事件相关信息	说明
事件类型	UKFEF统一收集以下操作系统内核常见事件： • soft lockup • RCU（Read-Copy Update） stall • hung task • global OOM（Out of Memory） • cgroup OOM（Out of Memory） • page allocation failure • list corruption • bad mm_struct • I/O error • EXT4-fs error • MCE（Machine Check Exception） • fatal signal • warning • panic

事件相关信息	说明
事件级别	UKFEF将异常事件分为三个级别： • Slight：不影响系统继续运行，但系统内部署的业务可能发生抖动，您可以继续观察事件变化。 • Normal：当前应用进程可能会出现异常。建议对当前应用采取措施，例如 `kill` 、重启或迁移。 • Fatal：可能会对系统产生致命影响。建议立即进行业务迁移。

事件相关信息	说明

事件报告	UKFEF将通过以下方式输出事件报告：
	● 通过内核日志输出单次事件的详细信息。信息内容示例如下：
	`class Fault event[module:type]:messages. At cpu cpuid, task pid(cmdline). Total fault: cnt`
	具体说明如下：
	○ *class*：对应异常事件的级别。
	○ *module*：表示异常事件所属的模块（sched、mem、io、fs、net、hardware以及由多个模块引起的异常会输出general）。
	○ *type*：对应异常事件的类型。
	○ *messages*：事件自身的自定义消息。
	○ *cpuid*：发生异常事件的CPU号。
	○ *pid(cmdline)*：异常事件对应进程的pid和cmdline。
	说明 如果pid为-1，则表示没有对应的进程。
	○ *cnt*：表示系统启动以来当前类型的异常事件出现的总和。
	● 通过*/proc/fault_events*文件输出各类异常事件的总和。文件输出内容示例如下：
	`Total fault events: 0`
	`Slight: 0`
	`Normal: 0`
	`Fatal: 0`
	`soft lockup: 0`
	`rcu stall: 0`
	`hung task: 0`
	`global oom: 0`
	`cgroup oom: 0`
	`page allocation failure: 0`
	`list corruption: 0`
	`bad mm_struct: 0`
	`io error: 0`
	`ext4 fs error: 0`
	`mce: 0`
	`fatal signal: 0`
	`warning: 0`
	`panic: 0`

控制UKFEF的接口说明

接口	说明
`/proc/sys/kernel/fault_event_enable`	该接口控制UKFEF的启用与关闭。取值范围： • 1：启用UKFEF。 • 0：关闭UKFEF。
`/proc/sys/kernel/fault_event_print`	该接口控制UKFEF是否输出事件报告。取值范围： • 1：输出。 • 0：不输出。
`/proc/sys/kernel/panic_on_fatal_event`	该接口控制出现Fatal事件时，是否触发操作系统的Panic机制。取值范围： • 1：触发。 • 0：不触发。

5.7. 操作系统迁移工具

5.7.1. CentOS 8迁移Alibaba Cloud Linux 3

CentOS官方已计划停止维护CentOS Linux项目，您可以通过Alibaba Cloud Linux提供的迁移工具将CentOS 8操作系统平滑迁移至Alibaba Cloud Linux 3操作系统。本文介绍如何使用操作系统迁移工具。

迁移限制

Alibaba Cloud Linux 3选用Linux kernel 5.10 LTS作为Alibaba Cloud Linux 3的内核，并选用GCC 10.2、binutils 2.35、glibc 2.32作为基础工具链。在软件包生态上与CentOS 8兼容。当您在使用本文介绍的操作系统迁移工具将CentOS 8迁移为Alibaba Cloud Linux 3时，工具会对待迁移的操作系统进行基础判断。因此您需要注意以下操作系统相关特性或软件的迁移限制：

特性或软件	支持情况	是否影响操作系统迁移流程	说明
图形化界面	不支持	是	Alibaba Cloud Linux 3不支持图形化界面，因此迁移工具不支持迁移已配置图形化界面的CentOS 8操作系统。
i686架构的软件包	不支持	是	Alibaba Cloud Linux 3不提供i686架构的软件包。如果您当前使用的CentOS 8系统内带有i686架构的软件包，则不支持使用迁移工具迁移操作系统。您需要先删除这些软件包，然后再进行迁移操作，以免迁移时系统发生异常。
epel-modular	不支持	否	CentOS 8中EPEL源所依赖的platform与Alibaba Cloud Linux 3不同。因此，您可以迁移操作系统，但需要注意迁移后无法安装基于epel-modular的软件包。
C/C++语言程序兼容性	不保证	否	Alibaba Cloud Linux 3选用GCC 10.2、binutils 2.35、glibc 2.32作为基础工具链，且系统自身的软件包已经做了兼容性处理。操作系统迁移后，建议您基于新的基础工具链重新对您的C/C++语言程序进行编译验证，避免出现兼容性问题。

特性或软件	支持情况	是否影响操作系统迁移流程	说明
内核模块兼容性	不支持	否	Alibaba Cloud Linux 3选用Linux kernel 5.10 LTS作为内核，在软件包生态上与CentOS 8兼容，但您需要注意，Alibaba Cloud Linux 3无法完全兼容CentOS 8的4.18内核。因此，依赖于内核接口编程的业务（例如内核OOT模块开发、硬件使能等业务场景），您需要在迁移前自行做好迁移评估，避免迁移后业务无法正常运行。
MySQL数据库	仅支持向同版本或更高版本的MySQL迁移	• 如果向同版本或更高版本的MySQL迁移则不影响 • 如果向低版本的MySQL迁移则影响	Alibaba Cloud Linux 3支持MySQL数据库，但您需要注意，由于MySQL不支持降低版本，当Alibaba Cloud Linux 3提供的MySQL版本低于待迁移的CentOS 8内的MySQL版本时，不支持使用迁移工具完成操作系统迁移。
操作系统热迁移	不支持	否	使用操作系统工具迁移操作系统时涉及软件包的重新安装，会引起系统内服务重启，进而造成业务中断。因此，您在迁移前需要做好数据备份（具体操作请参见快照概述）并隔离待迁移的操作系统环境，避免影响正常业务。

操作系统迁移工具在迁移过程中涉及软件包的下载与安装，会产生一定的资源消耗。因此，迁移前您需要确保实例内保留了以下可用的资源容量：

- 内存大小：300 MiB
- 云盘容量：
  - */usr*目录需要250 MiB
  - */var*目录需要1.5 GiB
  - */boot*目录需要50 MiB

> **说明** 如果您的实例对应的计算资源（vCPU与内存）、存储资源（系统盘与数据盘）较小，建议您停止实例内的业务再进行操作系统迁移，避免因资源不足而迁移失败。

操作步骤

1. 远程连接待迁移的CentOS 8实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 切换源地址。

   CentOS 8操作系统版本结束了生命周期（EOL），按照社区规则，CentOS 8的源地址*http://mirror.centos.org/centos/8/*内容已移除，您在阿里云上继续使用默认配置的CentOS 8的源会发生报错。如果您需要使用CentOS 8系统中的一些安装包，则需要手动切换源地址。具体操作，请参见CentOS 8 EOL如何切换源？。

3. 依次运行以下命令，安装迁移工具。

i. 下载迁移工具软件源。

```
wget http://mirrors.aliyun.com/alinux/migration/alinux-migration.repo -O /etc/yum.repos.d/alinux-migration.repo
```

ii. 安装迁移工具centos8toalinux3。

```
yum -y install centos8toalinux3
```

4. 运行以下命令，执行迁移工具。

> **说明** 迁移工具支持记录操作系统迁移前后的软件包的变化。如果您需要在迁移后查看记录，需要运行centos8toalinux3.py -V命令。如何查看迁移前后的记录文件，请参见常见问题。

```
centos8toalinux3.py
```

迁移结果说明：

- 如果出现如下图所示的提示信息，则表示您的CentOS 8操作系统配置了图形化界面，迁移工具不支持迁移操作，并自动结束了迁移操作。

```
[root@localhost noarch]# centos8toalinux3.py
Checking if the tool is executed by root user
Checking required packages
Checking if there is GUI installed.
It seems that your system install a GUI module, but still now we don't support a GUI transfer.
```

- 如果出现如下图所示的提示信息，则表示迁移操作完成。

```
Complete!
gpg-pubkey-8483c65d-5ccc5b19 CentOS (CentOS Official Signing Key) <security@centos.org>
remove centos gpg-pubkey
Removing yum cache
Sync successfully, update grub.cfg.
Generating grub configuration file ...
done
Switch complete. Alinux recommends rebooting this system.
```

5. 运行以下命令，查看迁移后的操作系统信息。

```
cat /etc/os-release
```

如下图所示，表示操作系统已成功迁移为Alibaba Cloud Linux 3。

```
[root@[illegible] ~]# cat /etc/os-release
NAME="Alibaba Cloud Linux"
VERSION="3 (Soaring Falcon)"
ID="alinux"
ID_LIKE="rhel fedora centos anolis"
VERSION_ID="3"
PLATFORM_ID="platform:al8"
PRETTY_NAME="Alibaba Cloud Linux 3 (Soaring Falcon)"
ANSI_COLOR="0;31"
HOME_URL="https://www.aliyun.com/"
```

6. 迁移后配置检查。

迁移完成后，需要检查当前系统中是否残留CentOS Vault源。如果系统中有残留CentOS Vault源，您需要删除，否则会出现Alibaba Cloud Linux 3和CentOS 8源共存的问题，一旦执行**yum update**命令可能会错误地安装CentOS包。

i. 运行以下命令，检查当前系统中是否残留CentOS Vault源。

```
yum repolist
```

如果出现类似如下返回信息中的 `CentOS-8.5.2111 - Base - mirrors.aliyun.com` 信息，表示系统中有残留CentOS repo文件。

```
# yum repolist
仓库 id                                                          仓库名称
AppStream                                                        CentOS-8.5
.2111 - AppStream - mirrors.aliyun.com
alinux3-module                                                   alinux3-mo
dule
alinux3-os                                                       alinux3-os
alinux3-plus                                                     alinux3-pl
us
alinux3-powertools                                               alinux3-po
wertools
alinux3-updates                                                  alinux3-up
dates
base                                                             CentOS-8.5
.2111 - Base - mirrors.aliyun.com
epel                                                             Extra Pack
ages for Enterprise Linux 8 - x86_64
extras                                                           CentOS-8.5
.2111 - Extras - mirrors.aliyun.com
```

ii. 运行以下命令，查找CentOS repo文件。

```
grep -rn "CentOS-8.5.2111" /etc/yum.repos.d/*.repo
```

查找结果如下所示。

```
# grep -rn "CentOS-8.5.2111" /etc/yum.repos.d/*.repo
/etc/yum.repos.d/Centos-vault-8.5.2111.repo:14:name=CentOS-8.5.2111 - Base - mirror
s.aliyun.com
/etc/yum.repos.d/Centos-vault-8.5.2111.repo:24:name=CentOS-8.5.2111 - Extras - mirr
ors.aliyun.com
/etc/yum.repos.d/Centos-vault-8.5.2111.repo:34:name=CentOS-8.5.2111 - Plus - mirror
s.aliyun.com
/etc/yum.repos.d/Centos-vault-8.5.2111.repo:43:name=CentOS-8.5.2111 - PowerTools -
mirrors.aliyun.com
/etc/yum.repos.d/Centos-vault-8.5.2111.repo:53:name=CentOS-8.5.2111 - AppStream - m
irrors.aliyun.com
```

iii. 运行以下命令，重命名找到的repo文件。

```
mv /etc/yum.repos.d/Centos-vault-8.5.2111.repo /etc/yum.repos.d/Centos-vault-8.5.21
11.repo.bak
```

7. 运行以下命令，重启ECS实例，使系统进入Alibaba Cloud Linux 3操作系统内核。

```
reboot
```

待ECS实例重启后，您可以运行**uname -r**命令查看Alibaba Cloud Linux 3内核版本信息。示例操作如下图所示：

```
[root@[redacted] ~]# uname -r
5.10.60-9.al8.x86_64
```

常见问题

- 如何确认操作系统迁移前后的变化？
  操作系统迁移工具支持记录迁移前后的软件包信息，如果您通过**centos8toalinux3.py -V**命令执行迁移操作，迁移完成后您可以通过记录文件对比迁移前后的变化。记录文件存放于*/var/tmp*目录下，该目录下不同命名的文件说明如下：
  - 迁移前软件包（RPM）的信息记录在下列文件：
    - `$(hostname)-rpms-list-before.log`
    - `$(hostname)-rpms-verified-before.log`
  - 迁移后软件包（RPM）的信息记录在下列文件：
    - `$(hostname)-rpms-list-after.log`
    - `$(hostname)-rpms-verified-after.log`
- 迁移过程中出现异常并导致迁移失败如何处理？
  迁移操作不可逆，如果迁移过程中出现异常，则无法再恢复到系统原始状态。因此建议您在迁移操作前为ECS实例创建快照备份数据，当迁移过程中出现异常，可通过快照回滚云盘。
  如果因软件包的依赖关系导致迁移失败（例如 `yum distro-sync` 执行后报错），则您需要保存报错信息并提交工单反馈。

5.7.2. CentOS 7迁移Alibaba Cloud Linux 2

CentOS官方已计划停止维护CentOS Linux项目，您可以通过Alibaba Cloud Linux提供的迁移工具将CentOS 7操作系统平滑迁移至Alibaba Cloud Linux 2操作系统。本文介绍如何使用操作系统迁移工具。

背景信息

在使用操作系统迁移工具前，您需要注意：

- Alibaba Cloud Linux 2使用4.19内核，CentOS 7使用3.10内核，两个版本的内核无法相互兼容，依赖于内核接口编程的业务，例如涉及内核OOT模块开发、硬件使能等，需提前做好评估，明确是否适合直接迁移，以免OS迁移后业务无法运行。
- 操作系统的迁移操作不可逆，其中涉及到系统内软件包的重新安装。因此您需要在迁移前为ECS实例创建快照备份数据。关于快照的更多信息，请参见快照概述。
- Alibaba Cloud Linux 2不支持图形化界面，因此迁移工具不支持迁移已配置图形化界面的CentOS 7操作系统。

操作步骤

1. 远程连接待迁移的CentOS 7实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 依次运行以下命令，安装迁移工具。

   i. 下载迁移工具软件源。

   ```
   wget http://mirrors.aliyun.com/alinux/migration/alinux-migration.repo -O /etc/yum.repos.d/alinux-migration.repo
   ```

   ii. 安装迁移工具centos7toalinux2。

   ```
   yum -y install centos7toalinux2
   ```

3. 运行以下命令，执行迁移工具。

> **说明** 迁移工具支持记录操作系统迁移前后的软件包的变化。如果您需要在迁移后查看记录，需要运行centos7toalinux2.py -V命令。如何查看迁移前后的记录文件，请参见常见问题。

```
centos7toalinux2.py
```

迁移结果说明：

- 如果出现如下图所示的提示信息，则表示您的CentOS 7操作系统配置了图形化界面，迁移工具不支持迁移操作，并自动结束了迁移操作。

```
[root@localhost ~]# centos7toalinux2.py
Checking if the tool is executed by root user
Checking required packages
Checking if there is GUI installed.
It seems that your system install a GUI module, but still now we don't support a GUI transfer.
```

- 如果出现如下图所示的提示信息，则表示迁移操作完成。

```
Sync successfully, update grub.cfg.
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-4.19.91-24.1.al7.x86_64
Found initrd image: /boot/initramfs-4.19.91-24.1.al7.x86_64.img
Found linux image: /boot/vmlinuz-3.10.0-1062.18.1.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-1062.18.1.el7.x86_64.img
Found linux image: /boot/vmlinuz-3.10.0-1062.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-1062.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-20200426154603174201708213343640
Found initrd image: /boot/initramfs-0-rescue-20200426154603174201708213343640.img
done
Switch complete. Alinux recommends rebooting this system.
```

4. 运行以下命令，查看迁移后的操作系统信息。

```
cat /etc/os-release
```

如下图所示，表示操作系统已成功迁移为Alibaba Cloud Linux 2。

```
[root@i[illegible] ~]# cat /etc/os-release
NAME="Alibaba Cloud Linux (Aliyun Linux)"
VERSION="2.1903 LTS (Hunting Beagle)"
ID="alinux"
ID_LIKE="rhel fedora centos anolis"
VERSION_ID="2.1903"
PRETTY_NAME="Alibaba Cloud Linux (Aliyun Linux) 2.1903 LTS (Hunting Beagle)"
ANSI_COLOR="0;31"
HOME_URL="https://www.aliyun.com/"
```

5. 运行以下命令，重启ECS实例，使系统进入Alibaba Cloud Linux 2操作系统内核。

```
reboot
```

待ECS重启完成，您可以运行**uname -r**命令查看Alibaba Cloud Linux 2内核版本信息。示例操作如下图所示：

```
[root@i[illegible] ~]# uname -r
4.19.91-24.1.al7.x86_64
```

常见问题

- 如何确认操作系统迁移前后的变化？

操作系统迁移工具支持记录迁移前后的软件包信息，如果您通过**centos7toalinux2.py -V**命令执行迁移操作，迁移完成后您可以通过记录文件对比迁移前后的变化。记录文件存放于*/var/tmp*目录下，该目录下不同命名的文件说明如下：

- 迁移前软件包（RPM）的信息记录在下列文件：
  - `$(hostname)-rpms-list-before.log`
  - `$(hostname)-rpms-verified-before.log`
- 迁移后软件包（RPM）的信息记录在下列文件：
  - `$(hostname)-rpms-list-after.log`
  - `$(hostname)-rpms-verified-after.log`

- 迁移过程中出现异常并导致迁移失败如何处理？
  迁移操作不可逆，如果迁移过程中出现异常，则无法再恢复到系统原始状态。因此建议您在迁移操作前为ECS实例创建快照备份数据，当迁移过程中出现异常，可通过快照回滚云盘。
  如果因软件包的依赖关系导致迁移失败（例如 `yum distro-sync` 执行后报错），则您需要保存报错信息并提交工单反馈。

5.8. 已知问题

本文介绍了Alibaba Cloud Linux镜像的已知问题、问题涉及范围以及解决方法。
Alibaba Cloud Linux 2已知问题：

- 开启内核选项CONFIG_PARAVIRT_SPINLOCK可能导致性能问题
- 内核特性透明大页THP开关置为always可能会导致系统不稳定或性能下降
- NFS v4.0版本中委托（Delegation）功能可能存在问题
- NFS v4.1/4.2版本中存在缺陷可能导致应用程序无法退出
- Meltdown/Spectre漏洞修复会影响系统性能

开启内核选项CONFIG_PARAVIRT_SPINLOCK可能导致性能问题

- 问题描述：开启内核选项CONFIG_PARAVIRT_SPINLOCK后，当ECS实例vCPU数量较多，且应用中有大量锁竞争操作时，应用性能会受到较大影响（例如， Nginx应用的短连接处理能力会因此大幅下降），您可能会在应用中观察到性能下降的问题。
- 修复方案：内核选项CONFIG_PARAVIRT_SPINLOCK在Alibaba Cloud Linux 2上默认处于关闭状态。如果您不确定如何处理内核问题，请勿开启CONFIG_PARAVIRT_SPINLOCK。

内核特性透明大页THP开关置为always可能会导致系统不稳定或性能下降

- 问题描述：在您的生产环境系统中，将透明大页THP（Transparent Huge Page）开关置为*always*，可能会引发系统不稳定和性能下降等问题。
- 修复方案：关于透明大页THP相关的性能调优方法，请参见Alibaba Cloud Linux 2系统中与透明大页THP相关的性能调优方法。

NFS v4.0版本中委托（Delegation）功能可能存在问题

- 问题描述：NFS委托（Delegation）功能在v4.0版本中可能存在问题。详情请参见NFS委托功能v4.0版本。
- 修复方案：使用NFS v4.0版本时，建议您不要开启Delegation功能。如需从服务器端关闭该功能，请参见社区文档。

NFS v4.1/4.2版本中存在缺陷可能导致应用程序无法退出

- 问题描述：在NFS的v4.1和v4.2版本中，如果您在程序中使用异步I/O（AIO）方式下发请求，且在所有I/O

返回之前关闭对应的文件描述符，有一定几率触发活锁，导致对应进程无法退出。

- 修复方案：该问题已在内核4.19.30-10.al7及以上版本中修复。由于该问题出现概率极低，您可根据实际需要决定是否升级内核修复该问题。如需修复，请在终端执行sudo yum update kernel -y命令，升级完成后重启系统即可。

> 注意
> - 升级内核版本可能会导致系统无法开机等风险，请谨慎操作。
> - 升级内核前，请确保您已创建快照或自定义镜像备份数据。具体操作，请参见创建一个云盘快照或使用实例创建自定义镜像。

Meltdown/Spectre漏洞修复会影响系统性能

- 问题描述：Alibaba Cloud Linux 2内核中，默认打开了针对处理器硬件高危安全漏洞Meltdown和Spectre的修复功能。由于此修复功能会影响系统性能，因此在常见的性能基准套件测试中，可能会观察到不同程度的性能下降现象。
- 修复方案：Meltdown和Spectre是英特尔芯片中发现的两个高危漏洞，攻击者可通过这两个漏洞来访问核心内存，从而窃取应用程序中的敏感信息，因此，建议您不要在系统中关闭此类高危漏洞的修复功能。但如果您对系统性能有极高要求，可以关闭该修复功能，具体操作请参见Alibaba Cloud Linux 2系统中如何关闭CPU漏洞修复。

5.9. Alibaba Cloud Linux知识库

本文提供Alibaba Cloud Linux镜像的故障排查与解决方案。

- Alibaba Cloud Linux 2
  - 如何解决Alibaba Cloud Linux 2中polkit内存泄漏问题？
  - Alibaba Cloud Linux 2系统中systemd服务异常问题说明
  - 如何避免因cgroup引起的应用性能抖动
  - 出现OOM Killer的原因与解决方案
  - 如何排查Linux slab_unreclaimable内存占用高的原因？
  - Linux内存碎片化的应对措施
  - Alibaba Cloud Linux 2实例修改网络服务的方法及影响说明
  - 如何在Alibaba Cloud Linux 2系统中配置Kdump
  - Alibaba Cloud Linux 2.1903镜像的ECS实例启动或重启后系统时间同步存在延迟
  - Alibaba Cloud Linux 2系统的经典网络ECS实例无法执行yum命令
  - Alibaba Cloud Linux 2系统的ECS实例运行低版本Docker镜像时报“段错误（segfault）”
  - Alibaba Cloud Linux 2系统的ECS实例无法查询和配置路由信息
  - ECS实例中的应用偶尔出现丢包现象并且内核日志（dmesg）存在“kernel: nf_conntrack: table full, dropping packet”的报错信息
  - Alibaba Cloud Linux 2系统的ECS实例创建大量进程后进程最终创建失败
  - Alibaba Cloud Linux 2系统中TCP拥塞控制算法BBR对网络性能的影响
  - Alibaba Cloud Linux 2系统的ECS实例中Ext4文件系统的Buffer I/O写性能不及预期
  - Alibaba Cloud Linux 2系统的ECS实例执行ss命令时返回的Send-Q字段值为0
  - Alibaba Cloud Linux 2系统中与透明大页THP相关的性能调优方法
  - Alibaba Cloud Linux 2系统的ECS实例挂载Overlayfs时共用挂载目录导致挂载失败

- Alibaba Cloud Linux 2快速启动版（qboot）系统的ECS实例系统盘自动扩容失败
- Alibaba Cloud Linux 2快速启动版（qboot）系统的ECS实例升级内核失败
- Alibaba Cloud Linux 2系统的ECS实例内核日志（dmesg）存在“integrity: Unable to open file”信息
- 如何在Alibaba Cloud Linux 2实例中通过“/etc/resolv.conf”文件自定义配置DNS
- 在Alibaba Cloud Linux 2实例中使用docker-ce、epel等第三方YUM源安装软件失败

- Alibaba Cloud Linux 3
  - Alibaba Cloud Linux 3系统空载下load大于1的解决方案
  - Alibaba Cloud Linux 3系统中使用docker-ce、epel等第三方DNF（YUM）源安装软件失败

5.10. Alibaba Cloud Linux FAQ

本文提供了Alibaba Cloud Linux镜像的常见问题与解决方案。

- Alibaba Cloud Linux 2和Alibaba Cloud Linux 3的差异有哪些？
- Alibaba Cloud Linux的多个镜像之间有何不同？
- 如何开始在阿里云上使用Alibaba Cloud Linux?
- 在阿里云ECS中运行Alibaba Cloud Linux是否有任何相关成本？
- Alibaba Cloud Linux支持哪些阿里云ECS实例类型？
- Alibaba Cloud Linux是否支持32位应用程序和库？
- Alibaba Cloud Linux是否支持图形化界面（GUI）？
- 是否可以在本地使用Alibaba Cloud Linux?
- 是否可以查看Alibaba Cloud Linux 2组件的源代码？
- Alibaba Cloud Linux 2是否与历史版本的Aliyun Linux向后兼容？
- Alibaba Cloud Linux 2上支持运行哪些第三方应用程序？
- 相比其他Linux操作系统，Alibaba Cloud Linux 2有哪些优势？
- Alibaba Cloud Linux 2怎样保证数据安全？
- Alibaba Cloud Linux 2是否支持数据加密？
- 怎样设置Alibaba Cloud Linux 2的有关权限？

Alibaba Cloud Linux 2和Alibaba Cloud Linux 3的差异有哪些？

Alibaba Cloud Linux 2即为原Aliyun Linux 2，与Alibaba Cloud Linux 3的差异主要体现在内核版本、编译器以及生命周期上。具体说明如下表所示。

差异点	Alibaba Cloud Linux 2	Alibaba Cloud Linux 3
内核版本	4.19	5.10
编译器	GCC 4.8.5	GCC 10.2
生命周期（EOL）	2024-03-31	2031-04-30

Alibaba Cloud Linux的多个镜像之间有何不同？

Alibaba Cloud Linux的镜像发布记录请参见Alibaba Cloud Linux 2镜像发布记录和Alibaba Cloud Linux 3镜像发布记录。Alibaba Cloud Linux包括的镜像之间的关系，请参见Alibaba Cloud Linux镜像。

如何开始在阿里云上使用Alibaba Cloud Linux?

阿里云为Alibaba Cloud Linux提供了公共镜像，您可以在创建ECS实例时，选择公共镜像下的Alibaba Cloud Linux镜像的版本。

在阿里云ECS中运行Alibaba Cloud Linux是否有任何相关成本？

没有。运行Alibaba Cloud Linux是免费的，您只需支付ECS实例运行的费用。

Alibaba Cloud Linux支持哪些阿里云ECS实例类型？

Alibaba Cloud Linux支持大部分阿里云ECS实例类型，包括弹性裸金属服务器。

> **说明** Alibaba Cloud Linux不支持使用Xen虚拟机平台的实例。

Alibaba Cloud Linux是否支持32位应用程序和库？

暂不支持。

Alibaba Cloud Linux是否支持图形化界面（GUI）？

Alibaba Cloud Linux 2和Alibaba Cloud Linux 3均不支持图形化界面。

是否可以在本地使用Alibaba Cloud Linux？

可以。Alibaba Cloud Linux提供了qcow2格式的本地镜像，目前只支持KVM虚拟机。具体操作，请参见在本地使用Alibaba Cloud Linux 2镜像或在本地使用Alibaba Cloud Linux 3镜像。

是否可以查看Alibaba Cloud Linux 2组件的源代码？

Alibaba Cloud Linux 2遵循开源协议。您可以通过yumdownloader工具或者在阿里云开源站点下载源代码包，也可以从Github站点下载Alibaba Cloud Linux 2内核源代码树，详情请参见Github。

Alibaba Cloud Linux 2是否与历史版本的Aliyun Linux向后兼容？

Alibaba Cloud Linux 2完全兼容Aliyun Linux 17.01。

> **说明** 如果您使用了自行编译的内核模块，可能需要在Alibaba Cloud Linux 2上重新编译才能正常使用。

Alibaba Cloud Linux 2上支持运行哪些第三方应用程序？

当前Alibaba Cloud Linux 2与CentOS 7.6.1810版本二进制兼容，因此所有可以运行在CentOS上的应用程序，均可在Alibaba Cloud Linux 2上流畅运行。

相比其他Linux操作系统，Alibaba Cloud Linux 2有哪些优势？

Alibaba Cloud Linux 2与CentOS 7.6.1810发行版保持二进制兼容，在此基础上提供差异化的操作系统功能。

与CentOS及RHEL相比，Alibaba Cloud Linux 2的优势体现在：

- 满足您的操作系统新特性诉求，更快的发布节奏，更新的Linux内核、用户态软件及工具包。
- 开箱即用，最简用户配置，最短时间服务就绪。
- 最大化用户性能收益，与云基础设施联动优化。
- 与RHEL相比没有运行时计费，与CentOS相比有商业支持。

Alibaba Cloud Linux 2怎样保证数据安全？

Alibaba Cloud Linux 2二进制兼容CentOS 7.6.1810/RHEL 7.6，遵从RHEL的安全规范。具体体现在以下几个方面：

- 使用业内标准的漏洞扫描及安全测试工具，定期做安全扫描。

- 定期评估CentOS 7的CVE补丁，修补OS安全漏洞。
- 与安全团队合作，支持阿里云现有的OS安全加固方案。
- 使用CentOS 7相同的机制，发布用户安全警告及补丁更新。

Alibaba Cloud Linux 2是否支持数据加密？

Alibaba Cloud Linux 2保留CentOS 7的数据加密工具包，并确保CentOS 7与KMS协同工作的加密方案可以在Alibaba Cloud Linux 2得到支持。

怎样设置Alibaba Cloud Linux 2的有关权限？

Alibaba Cloud Linux 2属于与CentOS 7同源的操作系统。CentOS 7的管理员可以无缝地使用完全一致的管理命令做相关的权限设置，Alibaba Cloud Linux 2的缺省权限设置与阿里云CentOS 7镜像完全一致。

6.自定义镜像

6.1. 自定义镜像概述

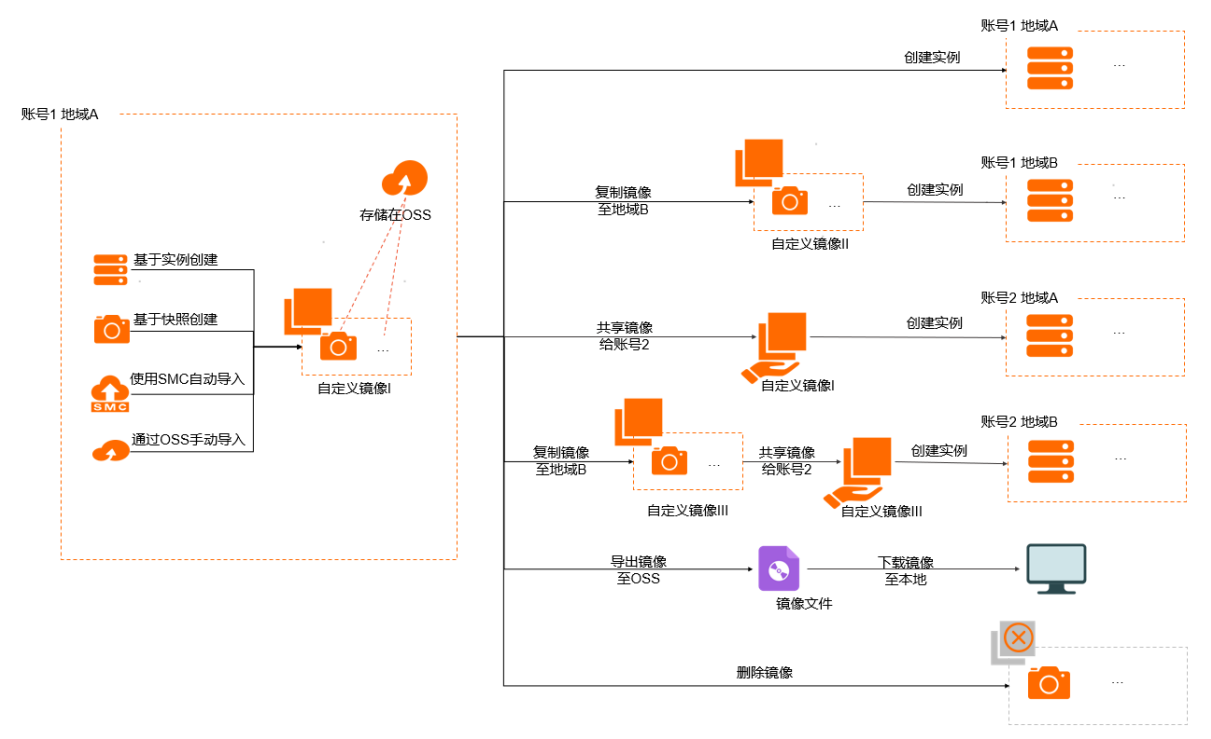
自定义镜像是您基于实例或快照创建的镜像，或者从本地导入的镜像，包含已部署的应用、数据等信息。使用自定义镜像可以快速创建更多相同配置的实例，无需每次创建实例时重复配置操作。

自定义镜像使用流程

当您成功创建或成功导入自定义镜像后，镜像的状态为**可用**。此时，您可以使用该镜像创建实例，可以将其共享给其他阿里云账号使用，或复制该镜像到其他地域使用，或导出该镜像到OSS存储空间（OSS Bucket）。不再需要该镜像时，您可以将其删除。

> **说明** 只有自定义镜像的创建者可以使用、共享、复制和删除该镜像。

自定义镜像的典型使用流程如下图所示。



相关操作

自定义镜像支持的相关功能操作如下表所示。

操作	说明	相关文档

操作	说明	相关文档
创建镜像	您可以通过已有实例或快照创建自定义镜像，以便快速复制系统环境，免除重复配置。您还可以使用镜像定义工具Packer创建自定义镜像。 如果您在创建自定义镜像时设置了镜像族系，自定义镜像可以被设置为弃用或者恢复可用。设置为弃用，可以实现镜像族系内可用的自定义镜像回滚；设置为恢复可用，可以恢复镜像族系的最新自定义镜像。	• 使用实例创建自定义镜像 • 使用快照创建自定义镜像 • 使用Packer创建自定义镜像 • 使用Packer创建并导入本地镜像 • 弃用镜像或恢复可用镜像
导入镜像	您可以从本地导入自定义镜像。	导入镜像流程
更新镜像	运维编排服务OOS为更新自定义镜像的场景提供了公共模版。您只需选择一个源镜像，输入更新镜像所需的云助手脚本等必要参数，就可以创建随机或定时的运维任务，一键更新自定义镜像。	更新自定义镜像
复制镜像	您需要在其他地域使用该镜像时，可以复制该镜像到目标地域。复制后的镜像独立存在，拥有唯一的镜像ID。	复制镜像
共享镜像	创建自定义镜像后，您可以将镜像共享给其他阿里云账号使用。该账号可以使用您共享的自定义镜像，快速创建运行同一镜像环境的ECS实例。	共享自定义镜像
导出镜像	创建自定义镜像后，您可以导出镜像到OSS存储空间（OSS Bucket），并下载到本地使用。	导出镜像
修改镜像信息	为了方便您管理自定义镜像，您可以根据需要修改自定义镜像的名称和描述。	修改自定义镜像信息
删除镜像	当您不再需要一个自定义镜像，可以将其删除。	删除自定义镜像

6.2. 创建自定义镜像

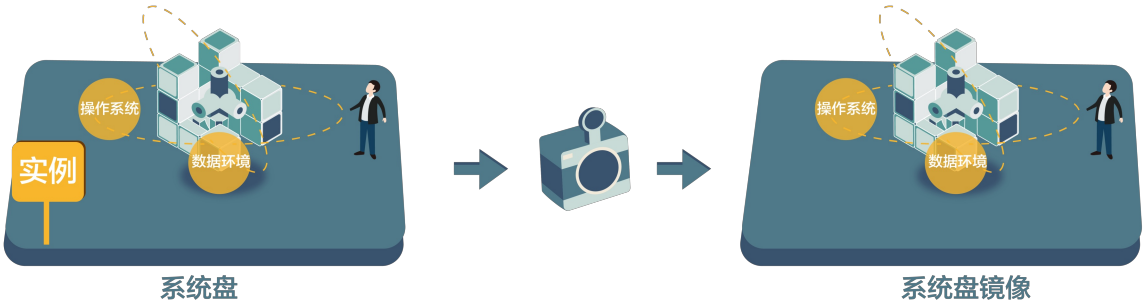
6.2.1. 使用快照创建自定义镜像

通过创建自定义镜像，您可以将一台ECS实例的操作系统、数据制作成环境副本，再通过自定义镜像创建多台ECS实例，快速复制系统环境。

前提条件

您已经创建了一份系统盘快照。具体步骤，请参见创建一个云盘快照。

背景信息



使用快照创建自定义镜像前，请仔细阅读下列注意事项：

- 用来创建自定义镜像的快照：
  - 必须包含一份系统盘快照创建自定义镜像。仅包含数据盘快照无法创建自定义镜像。
  - 加密快照和非加密快照均可用于创建自定义镜像。
  - 创建快照的源ECS实例到期或释放后，使用该快照创建的自定义镜像不受影响，使用该镜像创建的ECS实例也不受影响。
- 自定义镜像：
  - 通过本文步骤创建的自定义镜像不能跨地域使用。如需跨地域使用，请参见复制镜像。
  - 自定义镜像与ECS实例的计费方式相互独立。例如，使用包年包月ECS实例创建的自定义镜像，可用于创建按量付费ECS实例。
- 使用自定义镜像创建的ECS实例：
  - 支持升级vCPU、内存、带宽、云盘等。
  - 支持更换操作系统，更换后，原来的自定义镜像仍可继续使用。详情请参见更换系统盘（非公共镜像）。
  - 部分VPC网络Linux系统可能出现网络无法连通的异常情况，主要与*/etc/sysconfig/network*的配置相关。详情请参见使用自定义镜像创建VPC网络实例后网络出现异常。
- 数据安全建议：
  请提前删除快照中的敏感数据，避免数据安全隐患。

操作步骤

1. 登录ECS管理控制台。
2. 选择以下任意一种方法，找到需要创建自定义镜像的系统盘快照。
   - 通过实例页面：
     a. 在左侧导航栏，选择**实例与镜像 > 实例**。
     b. 在顶部菜单栏处，选择地域。
     c. 找到目标实例，单击实例ID，或在**操作**列，单击**管理**。

d. 单击**快照**页签。找到**云盘属性**为**系统盘**的目标快照。在**操作**列，单击**创建自定义镜像**。

- 通过快照页面：
  a. 在左侧导航栏，选择**存储与快照 > 快照**。
  b. 在顶部菜单栏处，选择地域。
  c. 选择一个**云盘属性**为**系统盘**的快照，单击**创建自定义镜像**。

3. 在弹出的**创建自定义镜像**对话框中，完成以下配置：

配置项	说明	相关文档
系统快照ID	必须是系统盘快照。	不涉及
名称与描述	输入镜像名称和描述信息。	不涉及
（可选）**镜像族系**	您可以在创建自定义镜像时选择镜像族系。设置了镜像族系功能的自定义镜像可以被设置为弃用或者恢复可用，来实现镜像的平滑更新与回滚。	镜像族系
（可选）**资源组**	选择相应的资源组，从用途、权限等角度管理创建的自定义镜像。	资源组
（可选）**添加数据盘快照**	选中**添加数据盘快照**，并单击**增加**后，选择数据盘快照ID。 ○ 如果不选择数据盘快照ID，则该数据盘会创建为空盘，默认容量为5GiB。 ○ 如果选择了数据盘快照ID，则云盘容量为快照的容量。	快照概述
标签	选择相应的标签。 ○ 可选：大多数场景为可选项。 ○ 必选：当您使用的RAM账号被赋予了强制绑定标签的相关RAM策略时，为必选项，否则会报错权限不足。	创建带特定标签的资源

4. 单击**创建**。

后续步骤

创建自定义镜像后，您可以：

- 使用自定义镜像创建实例
- 更换操作系统（非公共镜像）

相关文档

- CreateImage

6.2.2. 使用实例创建自定义镜像

创建实例后，您可以根据业务需要自定义实例（如安装软件、部署应用环境等），并为更新后的实例创建自定义镜像。使用该镜像创建的新实例，会包含您已配置的自定义项，省去您重复自定义实例的时间。

前提条件

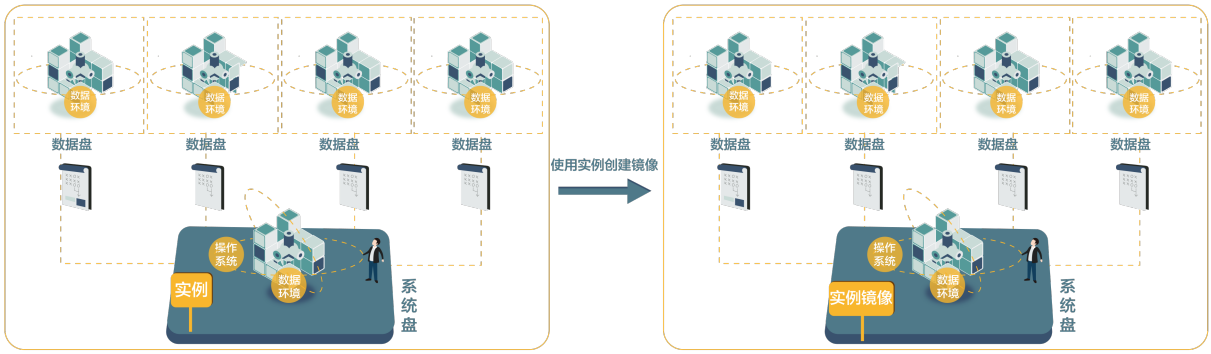
已将实例中的敏感数据删除，避免数据安全隐患。

Linux实例创建自定义镜像前，请做下列检查：

- 检查实例的网络配置。请根据您的Linux系统版本并参见CentOS示例进行操作。
- 检查系统盘使用剩余空间，确保系统盘没有被写满。

背景信息

创建自定义镜像的过程中，ECS会为实例的每块磁盘自动创建一个快照，这些快照组合起来构成一个自定义镜像，如下图所示。



创建自定义镜像前，请仔细阅读以下注意事项：

- 无需停止实例即可创建镜像。

  > **说明** 在实例运行时进行创建镜像的操作，可能导致部分实时数据未保存至镜像文件中。为保证数据完整性，建议您停止实例后再进行创建镜像的操作。如果您的实例不方便停止，也可以先创建快照一致性组，然后通过快照一致性组创建镜像。更多信息，请参见创建快照一致性组。

- 镜像创建过程中，不能改变实例的状态。例如，不要停止、启动或者重启实例，避免创建失败。
- 包年包月实例已到期时，无法直接为其创建镜像。您可以为实例的系统盘创建快照，再使用快照创建自定义镜像。
- 实例释放后，无法为其创建镜像。若您为实例保存了系统盘快照，可以通过该快照创建自定义镜像。
- 实例及其创建的镜像属于同一个地域。例如，实例地域为华东1，则其创建的镜像也在华东1地域。跨地域使用镜像，请参见复制镜像。

- 创建镜像所需时间，取决于实例磁盘的大小。
- 本地SSD型实例规格不支持创建包含系统盘和数据盘的镜像。更多信息，请参见本地SSD型实例规格族介绍。

使用Linux实例创建自定义镜像时，还需要注意以下情况：

- 不要在*/etc/fstab*文件中加载数据盘信息，否则使用该镜像创建的实例无法启动。
- 请勿随意升级内核或操作系统版本。
- 请勿调整系统盘分区。系统盘目前只支持单个根分区。
- 请勿修改关键系统文件，如*/sbin*、*/bin*、*/lib*目录等。
- 请勿修改默认登录用户名root。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标实例。在**操作**列中，单击**更多 > 云盘和镜像 > 创建自定义镜像**。
5. 在弹出的**创建自定义镜像**对话框中，完成以下配置：

配置项	说明	相关文档
名称与描述	输入镜像名称和描述信息。	不涉及
（可选）**镜像族系**	您可以在创建自定义镜像时选择镜像族系。设置了镜像族系功能的自定义镜像可以被设置为弃用或者恢复可用，来实现镜像的平滑更新与回滚。	镜像族系
（可选）**资源组**	选择相应的资源组，从用途、权限等角度管理创建的自定义镜像。	资源组
标签	选择相应的标签。 ○ 可选：大多数场景为可选项。 ○ 必选：当您使用的RAM账号被赋予了强制绑定标签的相关RAM策略时，为必选项，否则会报错权限不足。	创建带特定标签的资源

6. 单击**创建**。

> **说明** 所有磁盘的快照全部创建结束后，镜像才能使用。请耐心等待。

后续步骤

成功创建自定义镜像后，您可以：

- 使用自定义镜像创建实例
- 共享镜像给其他阿里云账号
- 导出镜像到OSS存储桶或本地

相关文档

- 使用快照创建自定义镜像

- 修改自定义镜像信息
- CreateImage

6.2.3. 使用Packer创建自定义镜像

Packer是一款轻量级的镜像定义工具，能够运行在常用的主流操作系统（如Windows、Linux和macOS）上。参见本文安装并使用Packer，轻松创建自定义镜像。

背景信息

本文描述以Linux系统的服务器为例，Windows系统的操作请参见Packer官方文档。

步骤一：安装Packer

1. 连接并登录到Linux服务器。

   登录ECS Linux实例服务器，请参见通过密码认证登录Linux实例。

2. 执行命令 `cd /usr/local/bin` 进入*/usr/local/bin*目录。

   > **说明** */usr/local/bin*目录为环境变量目录，您可以将Packer安装到该目录下或其他已添加到环境变量的目录下。

3. 执行命令 `wget https://releases.hashicorp.com/packer/1.1.1/packer_1.1.1_linux_amd64.zip` 获取Packer安装包。

   访问Packer下载页面，获取其他版本Packer安装包。

4. 执行命令 `unzip packer_1.1.1_linux_amd64.zip` 解压文件。

5. 执行命令 `packer -v` 验证Packer安装状态。

   - 若Linux服务器返回Packer版本号，表示您已正确安装Packer。
   - 若Linux服务器提示 `command not found` 表示Packer未正确安装。

步骤二：定义Packer模板

使用Packer创建自定义镜像时，需要创建一个JSON格式的模板文件。在该模板文件中，您需要指定创建自定义镜像的生成器和配置器。详情请参见Alicloud Image Builder（生成器）和Provisioners（配置器）。Packer具有多种配置器，可用于配置自定义镜像的内容生成方式，以下以常用的Shell配置器为例，定义Packer模板。

在Linux服务器中创建名为*alicloud*的JSON文件并粘贴以下内容。

```
{
     "variables": {
       "access_key": "{{env `ALICLOUD_ACCESS_KEY`}}",
       "secret_key": "{{env `ALICLOUD_SECRET_KEY`}}"
     },
     "builders": [{
       "type":"alicloud-ecs",
       "access_key":"{{user `access_key`}}",
       "secret_key":"{{user `secret_key`}}",
       "region":"cn-beijing",
       "image_name":"packer_basic",
       "source_image":"centos_7_02_64_20G_alibase_20170818.vhd",
       "ssh_username":"root",
       "instance_type":"ecs.n1.tiny",
       "internet_charge_type":"PayByTraffic",
       "io_optimized":"true"
     }],
     "provisioners": [{
       "type": "shell",
       "inline": [
         "sleep 30",
         "yum install redis.x86_64 -y"
       ]
     }]
   }
```

您需要自定义的参数值如下表所示。

参数	描述
access_key	您的AccessKey ID。更多详情，请参见获取AccessKey。 **说明** 由于AccessKey权限过大，为防止错误操作，建议您创建RAM用户，并使用RAM子账号创建AccessKey。具体步骤，请参见创建RAM用户和获取AccessKey。
secret_key	您的AccessKeySecret。更多详情，请参见获取AccessKey。
region	创建自定义镜像时使用临时资源的地域。
image_name	自定义镜像的名称。
source_image	基础镜像的名称，可以从阿里云公共镜像列表获得。
instance_type	创建自定义镜像时生成的临时实例的类型。
internet_charge_type	创建自定义镜像时临时实例的公网带宽付费类型。
provisioners	创建自定义镜像时使用的Packer配置器类型。详情请参见Packer配置器。

步骤三：使用Packer创建自定义镜像

指定Packer模板文件生成自定义镜像的操作步骤如下：

1. 运行命令 `export ALICLOUD_ACCESS_KEY=<您的AccessKey ID>` 导入您的AccessKey ID。
2. 运行命令 `export ALICLOUD_SECRET_KEY=<您的AccessKey Secret>` 导入您的AccessKey Secret。
3. 运行命令 `packer build alicloud.json` 创建自定义镜像。

示例运行结果如下，以下示例将创建含Redis的自定义镜像。

```
alicloud-ecs output will be in this color.
==> alicloud-ecs: Prevalidating alicloud image name...
alicloud-ecs: Found image ID: centos_7_02_64_20G_alibase_20170818.vhd
==> alicloud-ecs: Start creating temporary keypair: packer_59e44f40-c8d6-0ee3-7fd8-b1ba08ea
94b8
==> alicloud-ecs: Start creating alicloud vpc
----------------------------
==> alicloud-ecs: Provisioning with shell script: /var/folders/3q/w38xx_js6cl6k5mwkrqsnw7w0
000gn/T/packer-shell257466182
alicloud-ecs: Loaded plugins: fastestmirror
----------------------------
alicloud-ecs: Total                                             1.3 MB/s | 650 kB 00:00
alicloud-ecs: Running transaction check
----------------------------
==> alicloud-ecs: Deleting temporary keypair...
Build 'alicloud-ecs' finished.
==> Builds finished. The artifacts of successful builds are:
--> alicloud-ecs: Alicloud images were created:
cn-beijing: m-2ze12578be1oa4ovs6r9
```

后续步骤

使用自定义镜像创建实例

相关文档

- packer-provider
- Packer官方文档

6.2.4. 使用Packer创建并导入本地镜像

Packer是一款轻量级的镜像定义工具，能够运行在主流操作系统（如Windows、Linux和macOS）上。本文示范了如何为CentOS 6.9制作本地镜像并上传至阿里云平台。您可根据需要自定义Packer模板为其他操作系统制作镜像。

前提条件

- 已创建AccessKey。详细步骤，请参见获取AccessKey。

  > **说明** 由于AccessKey权限过大，为防止数据泄露，建议您先创建RAM用户，再使用RAM用户创建AccessKey。创建RAM用户的具体操作请参见创建RAM用户。

- 已开通OSS服务。详细步骤，请参见开通OSS服务。

背景信息

本文示例步骤使用了如下版本软件。操作时，请以您的实际软件版本为准。

- 服务器操作系统：Ubuntu 16.04
- 待制作镜像的操作系统：CentOS 6.9

使用示例

您可以参见以下使用示例基于CentOS 6.9系统创建本地镜像：

1. 运行 `egrep "(svm|vmx)" /proc/cpuinfo` 命令，查看您的源服务器或虚拟机是否支持KVM。
   返回如下信息时，表示支持KVM。

```
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm
constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmperf t
sc_known_freq pni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr
pdcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdran
d lahf_lm abm 3dnowprefetch epb intel_pt tpr_shadow vnmi flexpriority ept vpid fsgsbase
tsc_adjust bmi1 avx2 smep bmi2 erms invpcid mpx rdseed adx smap clflushopt xsaveopt xsa
vec xgetbv1 xsaves dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_epp
flags        : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
```

2. 若您的源服务器或者虚拟机支持KVM，依次运行以下命令安装KVM。

```
sudo apt-get install qemu-kvm qemu virt-manager virt-viewer  libvirt-bin bridge-uti
ls  #安装KVM及相关控件
```

```
sudo virt-manager  #开启virt-manager
```

   如果可以通过GUI创建虚拟机，表示您已经成功安装KVM。

3. 安装Packer。
   详细步骤，请参见安装Packer。
4. 依次运行以下命令定义Packer模板。

> **说明** 以下示例命令基于CentOS 6.9系统。如果您需要为其他操作系统制作镜像，请根据需要自定义Packer模板配置文件*centos.json*，详情请参见自定义Packer模板。

```
cd /usr/local  #切换所在目录
```

```
wget https://github.com/hashicorp/packer-plugin-alicloud/blob/main/builder/examples
/local/centos.json  #下载阿里云官方发行的centos.json配置文件
```

```
wget https://github.com/hashicorp/packer-plugin-alicloud/blob/main/builder/examples
/local/http/centos-6.8/ks.cfg  #下载阿里云官方发行的ks.cfg配置文件
```

```
mkdir -p http/centos-6.9  #创建目录
```

```
mv ks.cfg http/centos-6.9/  #移动文件ks.cfg到目录http/centos-6.9中
```

5. 依次运行以下命令创建并导入本地镜像。

```
export ALICLOUD_ACCESS_KEY=<您的AccessKeyID>      #导入您的AccessKeyID
```

```
export ALICLOUD_SECRET_KEY=<您的AccessKeySecret>  #导入您的AccessKeySecret
```

```
packer build centos.json                          #创建本地镜像并导入到阿里云平台
```

运行的示例结果如下：

```
qemu output will be in this color.
 ==> qemu: Downloading or copying ISO
     qemu: Downloading or copying: http://mirrors.aliyun.com/centos/6.9/isos/x86_64/Cen
tOS-6.9-x86_64-minimal.iso
 ..............................................
 ==> qemu: Running post-processor: alicloud-import
     qemu (alicloud-import): Deleting import source https://oss-cn-beijing.aliyuncs.com
/packer/centos_x86_64
 Build 'qemu' finished.
 ==> Builds finished. The artifacts of successful builds are:
 --> qemu: Alicloud images were created:
 cn-beijing: XXXXXXXX
```

6. 等待一段时间后，在对应地域的ECS控制台镜像详情页查看上传结果，如示例中的华北二。

自定义Packer模板

基于CentOS 6.9系统创建本地镜像的示例，请参见使用示例。如果您需要为其他操作系统创建本地镜像，可参见CentOS 6.9的JSON文件（如下所示），自定义Packer模板。

```
{"variables": {
        "box_basename": "centos-6.9",
        "build_timestamp": "{{isotime \"20060102150405\"}}",
        "cpus": "1",
        "disk_size": "4096",
        "git_revision": "__unknown_git_revision__",
        "headless": "",
        "http_proxy": "{{env `http_proxy`}}",
        "https_proxy": "{{env `https_proxy`}}",
        "iso_checksum_type": "md5",
        "iso_checksum": "af4axxxxxxxxxxxxxxxx192a2",
        "iso_name": "CentOS-6.9-x86_64-minimal.iso",
        "ks_path": "centos-6.9/ks.cfg",
        "memory": "512",
```

```
        "metadata": "floppy/dummy_metadata.json",
        "mirror": "http://mirrors.aliyun.com/centos",
        "mirror_directory": "6.9/isos/x86_64",
        "name": "centos-6.9",
        "no_proxy": "{{env `no_proxy`}}",
        "template": "centos-6.9-x86_64",
        "version": "2.1.TIMESTAMP"
      },
    "builders":[
        {
          "boot_command": [
            "<tab> text ks=http://{{ .HTTPIP }}:{{ .HTTPPort }}/{{user `ks_path`}}<enter><w
ait>"
          ],
          "boot_wait": "10s",
          "disk_size": "{{user `disk_size`}}",
          "headless": "{{ user `headless` }}",
          "http_directory": "http",
          "iso_checksum": "{{user `iso_checksum`}}",
          "iso_checksum_type": "{{user `iso_checksum_type`}}",
          "iso_url": "{{user `mirror`}}/{{user `mirror_directory`}}/{{user `iso_name`}}",
          "output_directory": "packer-{{user `template`}}-qemu",
          "shutdown_command": "echo 'vagrant'|sudo -S /sbin/halt -h -p",
          "ssh_password": "vagrant",
          "ssh_port": 22,
          "ssh_username": "root",
          "ssh_wait_timeout": "10000s",
          "type": "qemu",
          "vm_name": "{{ user `template` }}.raw",
          "net_device": "virtio-net",
          "disk_interface": "virtio",
          "format": "raw"
        }
      ],
    "provisioners": [{
          "type": "shell",
          "inline": [
                "sleep 30",
                "yum install cloud-util cloud-init -y"
              ]
        }],
      "post-processors":[
        {
          "type":"alicloud-import",
          "oss_bucket_name": "packer",
          "image_name": "packer_import",
          "image_os_type": "linux",
          "image_platform": "CentOS",
          "image_architecture": "x86_64",
          "image_system_size": "40",
          "region":"cn-beijing"
        }
      ]
}
```

使用示例中使用的生成器为QEMU Builder，该生成器用于创建虚拟机镜像。Packer生成器的必需参数说明，如下表所示。其余可选参数，请参见Packer QEMU Builder页面。

Packer生成器参数说明

必需参数	类型	描述
iso_checksum	string	操作系统的ISO文件的校验和。Packer在启动挂载了ISO的虚拟机之前检查该参数。至少指定iso_checksum或者iso_checksum_url参数；当您指定了参数iso_checksum时，参数iso_checksum_url的值被自动忽略。
iso_checksum_type	string	已指定的操作系统的ISO文件的校验和类型。取值范围： • none：忽略校验和过程。不推荐指定该值 • md5 • sha1 • sha256 • sha512
iso_checksum_url	string	一个包含了操作系统ISO文件校验和的文件链接（URL），样式为GNU或者BSD。您需要至少指定iso_checksum或者iso_checksum_url参数；当您指定了参数iso_checksum时，参数iso_checksum_url的值被自动忽略。
iso_url	string	一个指向ISO并包含安装镜像的URL。这个URL可以是一个HTTP链接，也可以是一个文件路径： • 如果是HTTP链接，Packer从HTTP链接下载文件并缓存运行。 • 如果是IMG或者QCOW2文件链接，QEMU直接使用文件创建自定义镜像。当您指定了文件路径时，请将参数disk_image置为*true*。
headless	boolean	Packer默认通过启动图形化虚拟机界面构建QEMU虚拟机。当您将headless置为*True*时，将启动一个没有控制台的虚拟机。

使用示例中使用的配置器中包含了Post-Processor模块，该模块实现自动化上传本地镜像到ECS云平台。Post-Processor模块的必需参数如下表所示。其余可选参数，请参见Packer Alicloud Import Post-Processor页面。

Packer配置器部分参数说明

必需参数	类型	描述
access_key	string	您的AccessKeyID。
secret_key	string	您的AccessKeySecret。
region	string	本地镜像上传的阿里云地域ID，如本示例中的 `cn-beijing` 。更多地域信息，请参见地域和可用区。

必需参数	类型	描述
image_name	string	您的本地镜像的名称。 • 由 [2, 128] 位英文或中文字符组成。 • 必须以大小写字母或中文字符开始。 • 可以包含数字、下划线（_）或者连字符（-）。 • 不能以http://或https://开头。
oss_bucket_name	string	您的OSS Bucket名称。若您指定了一个不存在的Bucket名称，Packer上传镜像时自动创建一个同名Bucket。
image_os_type	string	镜像类型，取值范围： • linux • windows
image_platform	string	镜像发行版本。例如，本示例中的CentOS。
image_architecture	string	镜像发行版本的架构平台，取值范围： • i386 • x86_64
format	string	镜像的格式，取值范围： • RAW • VHD

后续步骤

您可以使用上传至阿里云平台的自定义镜像创建ECS实例，请参见使用自定义镜像创建实例。

相关文档

相关文档

- Packer官方文档
- packer
- opstools
- packer-provider
- Anaconda Kickstart

6.2.5. 使用OOS创建自定义镜像

运维编排服务OOS为创建自定义镜像的场景提供了公共模版ACS-ECS-CreateAndCopyImage，支持一键完成发送远程命令、创建自定义镜像、复制镜像等操作。

背景信息

您可以在OOS控制台查看公共模板的信息，例如执行模板时的默认流程等。具体操作，请参见查看公共模板信息。

操作步骤

1. 进入运维任务设置页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**实例与镜像 > 镜像**。
   iii. 在顶部菜单栏左上角处，选择地域。
   iv. 在**创建镜像**区域，单击**运维编排创建**。
2. 在**创建或更新镜像**页面中，完成执行设置。
   i. 保持默认选中**从已有实例创建镜像**。
   ii. 完成通用设置。

      输入镜像名称和描述，并选择执行相关操作时权限的来源。
   iii. 完成镜像分发设置。

设置项	说明
需要复制的目标地域	在当前地域创建镜像后，自动将镜像复制到一个或多个地域。
镜像共享账号ID	创建镜像后，自动将镜像共享给一个或多个其他阿里云账号。

   iv. 选择实例。

      基于选择的实例创建自定义镜像。创建自定义镜像时，系统会为云盘自动生成快照，因此保有自定义镜像会产生快照费用。
   v. 输入远程命令。

      在创建自定义镜像前向实例发送的远程命令，具体效果由命令内容决定，例如您可以在实例上安装软件、记录运维任务执行时间等。
   vi. 设置高级选项。

设置项	说明
伸缩组配置ID	创建镜像后，自动使用该镜像更新指定伸缩组配置中的镜像参数。
标签	为本次任务绑定标签，方便后续筛选。
保存模板	将本次任务的设置保存为自定义模板，方便后续重复执行。

   vii. 单击**立即执行**。

执行结果

任务状态变为**运行中**，您可以单击执行ID查看输出参数、执行日志等信息。任务状态变为**成功**后即表示自定义镜像创建成功，并按设置完成了复制镜像等操作。

6.3. 导入镜像

6.3.1. 导入镜像流程

导入本地镜像文件适用于在云上部署业务的场景，您可以使用导入的自定义镜像创建ECS实例或更换系统盘。本文介绍导入镜像的操作流程。

Linux镜像导入流程

Linux镜像的导入流程如下：

1. 制作自定义镜像前，在源服务器上完成以下准备工作。
   i. 安装并使用镜像规范检测工具，自动检测Linux系统设置是否符合导入条件。更多详情，请参见使用工具检测镜像规范。
   ii. 安装cloud-init，使运行该镜像的实例能成功完成初始化配置。更多详情，请参见安装cloud-init。
   iii. 安装virtio驱动，使该镜像创建的ECS实例能够启动。更多详情，请参见安装virtio驱动。
2. 阅读导入镜像必读。
3. 转换镜像格式（RAW、VHD和qcow2格式镜像文件除外）。更多详情，请参见转换镜像格式。
4. 导入自定义镜像。
   若自定义镜像的操作系统不在阿里云所支持的平台列表中，并且不能安装cloud-init时，您可以在导入自定义镜像时选择Customized Linux（定制版镜像）。更多详情，请参见定制Linux自定义镜像。

Windows镜像导入流程

Windows镜像的导入流程如下：

1. 安装virtio驱动
2. 导入镜像必读
3. 转换镜像格式
4. 导入自定义镜像

6.3.2. 使用工具检测镜像规范

制作要导入的自定义镜像前，建议您使用镜像规范检测工具，自动检测Linux操作系统设置是否符合导入条件。工具主要检测导入的自定义镜像是否为有效镜像、自定义镜像是否可以创建出功能齐全的ECS实例等。本文通过操作示例、参数和输出项详细为您介绍如何使用镜像规范检测工具。

背景信息

ECS支持使用自定义镜像创建实例。该自定义镜像可以是基于您的线下服务器、虚拟机或者其他云平台的云主机创建的镜像，您需要先将镜像导入ECS，才可使用其创建实例。导入阿里云的自定义镜像需满足一定要求，详情请参见导入镜像必读。

为缩短镜像制作周期，我们推荐您使用ECS镜像规范检测工具（下文简称检测工具）。检测工具能基于Linux服务器环境自动检测各项配置指标、快速定位不合规配置、生成TXT和JSON格式检测报告并给出解决意见，省去您逐项检查系统的时间，方便您快速修复系统配置并制作出符合规范的镜像。

目前检测工具仅支持检测Linux类型镜像，包括Ubuntu、CentOS、Debian、RedHat、SLES（SUSE Linux Enterprise Server）、OpenSUSE、FreeBSD、CoreOS和其它Linux发行版本。

本文以CentOS 7.4 64位操作系统为例，介绍检测工具的操作步骤。

操作步骤

完成以下操作，使用检测工具：

1. 登录您的服务器、虚拟机或者其他云平台的云主机。
2. 运行以下命令下载检测工具到当前目录。

   ```
   wget http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach/73848/cn_zh/1557459863884/image_check
   ```

   您也可以单击此处下载检测工具。

3. 使用root权限运行检测工具，避免检测工具无法读取已设置访问权限的配置文件。

```
chmod +x image_check
sudo <检测工具所在路径>/image_check -p [目标路径]
```

本示例中，*<检测工具所在路径>*为当前目录，生成报告的目标路径为当前目录，因此运行检测工具的命令为：

```
sudo ./image_check
```

> **说明** 您可使用 `-p [目标路径]` 指定检测报告的生成路径，若不指定则报告默认输出在检测工具所在的路径。

4. 等待检测工具检测系统配置。

```
Begin check your system......
The report is generating.
----------------------------------------
The infomation you need to input when you import your image to Alibaba Cloud website:
Current system: CentOS
Architecture: x86_64
System disk size: 42 GB
----------------------------------------
Check driver                                                [  OK  ]
Check shadow file authority                                 [  OK  ]
Check security                                              [  OK  ]
Check qemu-ga                                               [  OK  ]
Check network                                               [  OK  ]
Check ssh                                                   [  OK  ]
Check firewall                                              [  OK  ]
Check filesystem                                            [  OK  ]
Check device id                                             [  OK  ]
Check root account                                          [  OK  ]
Check password                                              [  OK  ]
Check partition table                                       [  OK  ]
Check lib                                                   [  OK  ]
Check disk size                                             [  OK  ]
Check disk use rate                                         [  OK  ]
Check inode use rate                                        [  OK  ]
----------------------------------------
16 items are OK.
0 items are failed.
0 items are warning.
----------------------------------------
The report is generated: /root/image_check_report_2019-05-10_13-28-21.txt
Please read the report to check the details.
```

5. 查看检测报告。

检测工具运行结果中，会显示检测报告所在路径。本示例中，检测报告所在路径为*/root*。检测报告格式为 `image_check_report_日期_时间.txt` 或 `image_check_report.json` 。

检测项

为避免您制作的自定义镜像创建出功能不全的ECS实例，检测工具主要检查服务器中以下配置项。

检测项	不合规后果	合规建议
driver	无法正常启动ECS实例	安装虚拟化驱动，请参见安装virtio驱动
/etc/shadow	无法修改密码文件，进而无法根据自定义镜像创建ECS实例	不要使用 `chattr` 命令锁定*/etc/shadow*文件
SElinux	无法正常启动ECS实例	不要通过修改*/etc/selinux/config*开启SELinux
qemu-ga	ECS所需要的部分服务不可用，实例功能不全	卸载qemu-ga
network	ECS实例网络功能不稳定	关闭或删除Network Manager，并打开network服务
ssh	无法从控制台远程连接ECS实例	打开SSH服务，不要设置PermitRootLogin
firewall	系统无法自动配置您的ECS实例环境	关闭防火墙Iptables、Firewalld、IPFILTER（IPF）、IPFIREWALL（IPFW）或PacketFilter（PF）
file system	无法扩容磁盘	• 推荐使用xfs、ext3、ext4文件系统 • 容许使用ext2、ufs、udf文件系统 • ext4文件系统不要使用 `64 bit` 特性（feature） **说明** `64 bit` 是ext4文件系统的特性之一。您可使用**man ext4**命令查看其详细说明。
device id	无法正常启动ECS实例	清理*fstab*文件，去除文件中不需要的device id，保证使用的device id都在**blkid**命令的显示结果中
root	无法使用用户名和密码远程连接ECS 实例	保留root账号
passwd	ECS实例无法新增用户	保留passwd命令，或重新安装passwd
分区表	无法正常启动ECS实例	采用MBR分区
/lib	无法自动化配置ECS实例	*/lib*和*/lib64*的指向位置不能为绝对路径，修改链接文件*/lib*和*/lib64*的指向位置为相对路径
system disk	N/A	增加系统盘容量，系统盘空间最佳为40 GiB至500 GiB。并在导入镜像时根据镜像的虚拟文件大小而非使用容量配置系统盘容量
disk usage	无法为ECS实例安装必要的驱动或服务	保持足够的磁盘空间
inode usage	无法为ECS实例安装必要的驱动或服务	保持足够的inode资源

检测工具会根据检测项给出 `OK` 、 `FAILED` 或者 `WARNING` 检测结果。

- `OK` ：检测项均符合要求。
- `FAILED` ：检测项不符合要求，使用该自定义镜像创建的ECS实例无法正常启动。建议您修复报错项后再制作镜像，以提高实例启动效率。
- `WARNING` ：检测项不符合要求，使用该自定义镜像创建的ECS实例可以安全启动，但ECS无法通过有效途径干预您的实例配置。您可以选择立即修复，也可以暂时忽略问题直接制作镜像。

输出项

检测工具运行结束后，会在目标路径输出TXT和JSON两种格式的检测报告。

> **说明** 检测报告的目标路径可使用 `-p [目标路径]` 指定。若不指定，则默认生成到检测工具所在路径。

- TXT格式报告名称为 `image_check_report_日期_时间.txt` ，报告内容包括服务器配置信息以及检测结果。以CentOS 7.4 64位操作系统为例：

```
The information you need to input when you import your image to Alibaba Cloud Website:
  Current system is: CentOS      #服务器操作系统
  Architecture: x86_64           #系统架构
  System disk size: 42 GB        #服务器系统盘容量
  ----------------------------------------
   Check driver                  #检测项名称
   Pass: kvm drive is exist      #检测结果
   Alibaba Cloud supports kvm virtualization technology
   We strongly recommend installing kvm driver.
```

- JSON格式报告名称为 `image_check_report.json` ，报告内容包括服务器配置信息以及检测结果。以CentOS 7.4 64位操作系统为例：

```
"platform": "CentOS",       \\服务器操作系统
  "os_big_version": "7",      \\操作系统版本号（高位）
  "os_small_version": "4",    \\操作系统版本号（低位）
  "architecture": "x86_64",   \\系统架构
  "system_disk_size": "42",   \\服务器系统盘容量
  "version": "1.0.2",         \\检测工具版本
  "time": "2018-05-14_19-18-10", \\检测时间
  "check_items": [{
      "name": "driver",       \\检测项名称
      "result": "OK",         \\检测结果
      "error_code": "0",      \\错误码
      "description": "Pass: kvm driver exists.", \\描述
      "comment": "Alibaba Cloud supports kvm virtualization technology. We strongly recom
mend installing kvm driver."
  }]
}
```

后续步骤

查看导入镜像注意事项

6.3.3. 导入镜像必读

为保证自定义镜像的可用性和提高镜像的导入效率，请您在导入镜像前，仔细阅读本文中提及的导入阿里云ECS自定义镜像的限制条件。这些限制条件是镜像导入功能对导入的自定义镜像操作系统的约束。

Windows Server操作系统镜像

必读项	说明
系统限制	• 请确认文件系统的完整性。 • 请勿修改关键系统文件。 • 请检查系统盘的剩余空间，确保系统盘没有被写满。 • 请根据镜像的虚拟磁盘大小而非使用容量配置导入的系统盘大小，系统盘容量范围支持40 GiB~500 GiB。 • 关闭防火墙。 • 安全组放行RDP 3389端口。 • administrator账号的登录密码必须为8~30个字符，同时包含大小写英文字母、数字和特殊符号中的三类字符。特殊符号可以是 `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /` 。其中，不能以正斜线（/）为密码首字符。 • 以UEFI方式启动的系统，系统所在磁盘的启动分区（C盘）之后不能再存在其他分区，否则将导致实例启动失败或者磁盘扩容失败。

不支持项	• 不支持ISO镜像文件。请在线下环境通过VirtualBox等工具制作后，转换成RAW、VHD或qcow2等格式。
	• 不支持在镜像中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。
	• 不支持在Windows Server中安装社区版Virtio驱动。如已安装，请移除以下文件的只读属性。
	  ○ *C:\Windows\System32\drivers\netkvm.sys*
	  ○ *C:\Windows\System32\drivers\balloon.sys*
	  ○ *C:\Windows\System32\drivers\vioser.sys*
	  ○ *C:\Windows\System32\drivers\viostor.sys*
	  ○ *C:\Windows\System32\drivers\pvpanic.sys*

支持项	• 支持多分区系统盘。
	• 支持NTFS文件系统，支持MBR和GPT分区。
	• 支持RAW、qcow2和VHD格式镜像。其他格式必须转换镜像格式后再导入，具体操作，请参见转换镜像格式。
	• 支持导入包含以下操作系统版本的镜像：
	  ○ Microsoft Windows Server 2022
	  ○ Microsoft Windows Server 2019
	  ○ Microsoft Windows Server 2016
	  ○ Microsoft Windows Server 2012 R2
	  ○ Microsoft Windows Server 2012
	  ○ Microsoft Windows Server 2008 R2
	  ○ Microsoft Windows Server 2008
	  ○ Windows Server 2003 Service Pack 1（SP1）及以上版本

Linux操作系统镜像

必读项	说明

系统限制	• 请确认文件系统的完整性。
	• 请勿修改关键系统文件，如*/sbin*、*/bin*和*/lib**等目录。
	  ○ 请勿修改*/etc/issue**，否则ECS无法正常识别系统发行版，从而创建系统失败。
	  ○ 请勿修改*/boot/grub/menu.lst*，否则无法启动ECS实例。
	  ○ 请勿修改*/etc/fstab*，否则无法加载异常分区从而无法启动ECS实例。
	  ○ 请勿将*/etc/shadow*修改为只读，否则将导致无法修改密码文件，从而创建系统失败。
	  ○ 不建议修改*/etc/selinux/config*文件以开启SELinux，否则系统无法启动。如果必须开启，请参见开启或关闭SELinux。
	• 请检查系统盘的剩余空间，确保系统盘没有被写满。
	• 关闭防火墙。
	• 安全组放行SSH 22端口。
	• 开启DHCP（Dynamic Host Configuration Protocol）服务。
	• 安装Xen或者KVM虚拟化驱动。具体步骤，请参见安装virtio驱动。
	• 安装cloud-init，以保证能成功配置hostname、NTP源和yum源。具体操作，请参见安装cloud-init。
	• root账号的登录密码必须是8~30个字符，并且同时包含大小写字母、数字和特殊符号中的三类字符。特殊符号可以是 `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /` 。
	• 以UEFI方式启动的系统，系统所在磁盘的根分区之后不能再存在其他分区，否则将导致实例启动失败或者磁盘扩容失败。

不支持项	• 不支持ISO镜像文件。请在线下环境通过VirtualBox等工具制作后，转换成RAW、VHD或qcow2等格式。 • 不支持多个网络接口。 • 不支持IPv6地址。 • 不支持调整系统盘分区，只支持单个根分区。 • 不支持在镜像中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。 • 不支持通过LVM跨磁盘构建的系统盘分区（根分区），否则可能导致ECS实例启动异常。

必读项	说明
支持项	• 支持RAW、qcow2和VHD格式镜像。其他格式必须转换镜像格式后再导入，具体操作，请参见转换镜像格式。 • 支持xfs、ext3和ext4文件系统，支持MBR和GPT分区。 • 支持ext4文件系统，但不能包含特性 `64bit` ，并且特性 `project` 和 `quota` 不能成对出现。您可以运行以下命令查看ext4文件系统中包含的特性列表。 `tune2fs -l <ext4文件系统盘所在路径> | grep features` • 支持导入包含以下操作系统版本的镜像： ○ Alibaba Cloud Linux ○ Anolis ○ CentOS 5/6/7/8 ○ CentOS Stream ○ Debian 6/7/8/9/10 ○ FreeBSD ○ OpenSUSE 13/42/15 ○ RedHat ○ RHEL（Red Hat Enterprise Linux） ○ SUSE Linux 10/11/12/15 ○ Ubuntu 10/12/13/14/16/18/20 ○ CoreOS 681.2.0+ ○ AlmaLinux ○ Rocky Linux

补充说明：

如果您待导入的镜像对应的系统架构为arm64，或者对应的操作系统为CentOS Stream、Anolis、AlmaLinux或Rocky Linux时，您需要注意：

- 为了使导入后的镜像支持配置密码或者支持修改密钥对，镜像必须满足以下条件：
  - 操作系统的内核需要支持 `CONFIG_FW_CFG_SYSFS` 特性。Linux社区内核4.6版本之后默认支持该特性，CentOS的内核在3.10.0-826.el7版本之后默认支持该特性。您可以在该镜像对应的服务器内运行 `grep -nr CONFIG_FW_CFG_SYSFS /boot/config-$(uname -r)` 命令，如果回显结果中包含 `CONFIG_FW_CFG_SYSFS=y` 信息，则说明该镜像中的内核已支持 `CONFIG_FW_CFG_SYSFS` 特性。
  - 操作系统中已安装阿里云最新版本cloud-init。其中，19.1版本cloud-init必须在19.1.3版本及以上，部分低版本操作系统中的0.7.6a版本cloud-init必须在0.7.6a15版本及以上。具体操作，请参见安装cloud-init。
  - 操作系统需要支持SHA-512加密算法。
- 为了使导入后的镜像支持扩容云盘与扩容文件系统，镜像必须满足以下条件：
  - 操作系统的内核版本需要高于3.6版本。
  - 支持growpart命令。支持该命令需要安装 `cloud-utils-growpart` 包，不同操作系统安装方式有所不同。具体操作，请参见扩展分区和文件系统_Linux系统盘。

- 支持resize2fs命令。支持该命令需要安装 `e2fsprogs` 包，该包在操作系统中默认已安装，如果没有安装您需要自行安装（例如，CentOS 7操作系统内 `e2fsprogs` 包的安装命令为**yum install -y e2fsprogs**）。
- 操作系统中已安装阿里云最新版本cloud-init。其中，19.1版本cloud-init必须在19.1.3版本及以上，部分低版本操作系统中的0.7.6a版本cloud-init必须在0.7.6a15版本及以上。具体操作，请参见安装cloud-init。

非标准平台Linux镜像

为便于区分，如果您导入的Linux系统镜像不在ECS提供的公共镜像列表里，该操作系统平台镜像为非标准平台镜像。非标准平台镜像虽然来自标准操作系统平台，但该类镜像属于系统关键性配置文件、系统基础环境和应用方面没有遵守标准平台要求的镜像。您在导入镜像前后，需要自行在镜像对应的操作系统内进行相关配置，以保证镜像可用。导入非标准平台镜像时支持选择的镜像类型以及配置说明如下：

- Others Linux：ECS统一标识为其他系统类型。如果导入Others Linux平台镜像，ECS不会对所创建的实例做任何处理。完成实例创建后，请通过ECS管理控制台的远程连接功能连接实例，再自行配置IP、路由和密码等。如果您在制作镜像前开启了DHCP，ECS会自动为您配置网络。
- Customized Linux：定制版镜像。导入Customized Linux镜像前，请按照ECS标准系统配置方式配置实例的网络和密码等。更多信息，请参见定制Linux自定义镜像。

6.3.4. 安装cloud-init

为保证运行镜像的ECS实例能成功完成初始化配置，建议您在制作Linux类型自定义镜像时，在源服务器上安装cloud-init。本文介绍安装阿里云版cloud-init和社区版cloud-init的操作步骤。

背景信息

cloud-init是云平台为Linux操作系统的虚拟机做系统初始化配置的开源服务软件。阿里云、AWS、Azure和OpenStack等主流云平台均支持cloud-init。阿里云版cloud-init能在ECS实例启动阶段完成系统初始化配置，包括NTP、软件源、主机名和SSH密钥对等，同时执行实例自定义数据（User data）脚本。更多信息，请参见cloud-init官方文档。

阿里云所有公共镜像默认安装cloud-init。为保证使用自定义镜像创建的ECS实例能自动初始化系统配置，建议您在以下场景中为Linux服务器安装阿里云版cloud-init。

- 准备迁移上云的，但未安装cloud-init的Linux服务器。

> **说明** 不准备迁移上云的服务器需谨慎安装。

- 已安装cloud-init，但版本低于0.7.9的Linux服务器。
- 已在阿里云运行的，但未安装cloud-init的ECS实例。

版本说明

不同云平台及不同版本之间的cloud-init不完全兼容，请选择合适的版本并配置合适的数据源（datasource）。其中，阿里云cloud-init的最新版本为19.1.10，数据源为 `Aliyun` 。您可以在cloud-init官方网站自行下载其他版本的cloud-init。

> **注意** 安装后，cloud-init默认开机自启动，若您选择的版本不兼容或数据源配置不当，下次重启服务器时可能导致cloud-init运行异常、系统启动缓慢，甚至无法正常启动系统。因此，请选择较高版本，以及合适的数据源（如 `Aliyun` ）。

使用cloud-init时，您需要注意以下版本区别。

- 0.7.6a版本：初期的阿里云版本cloud-init，在Python环境上依赖于Python 2.7。部分低版本操作系统的公

共镜像仍旧保持该版本cloud-init。如果您所使用的镜像需要安装cloud-init 0.7.6a版本，请参见（可选）安装阿里云版cloud-init 0.7.6a15。

> **说明** 由于Python社区停止对Python 2.7的技术支持，建议您尽量使用高版本cloud-init，避免依赖库隐患。

- 低于社区0.7.9版本：初期的社区版cloud-init，不适用于初始化ECS实例，必须升级至较高版本。
- 18版本：高于18版本的cloud-init会自动完成网络的初始化配置，自动配置的网络为 `BOOTPROTO=dhcp DEVICE=eth0 ONBOOT=yes STARTMODE=auto TYPE=Ethernet USERCTL=no` 。如果您安装了cloud-init后有自定义网络配置的需求，请参见（可选）自定义网络配置。
- 19.1版本：阿里云公共镜像将逐步升级到cloud-init 19.1版本，在Python环境上依赖于Python 3.6。

检查cloud-init版本

1. 登录源服务器。
2. 运行以下命令检查是否已安装cloud-init。

   ```
   which cloud-init
   ```

   无路径输出信息表示未安装，您需要安装阿里云版cloud-init。
3. 运行以下命令检查cloud-init版本号。

   ```
   cloud-init --version
   ```

   如果返回版本低于社区0.7.9版本，您需要安装阿里云版cloud-init 19.1.10。
4. 完成服务器数据备份。

（推荐）安装阿里云版cloud-init 19.1.10

按以下步骤，下载数据源为 `Aliyun` 的19.1.10版本cloud-init。

1. 确保源服务器已安装Python PIP依赖库。

   以安装python3-pip依赖库为例，Linux部分发行版的安装命令如下。

   - CentOS/Red Hat Enterprise Linux：

     ```
     yum -y install python3-pip
     ```

   - Ubuntu/Debian：

     ```
     apt-get -y install python3-pip
     ```

   - OpenSUSE/SUSE：

     ```
     zypper -n install python3-pip
     ```

2. 运行以下命令下载阿里云版cloud-init。

   ```
   wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tgz
   ```

3. 运行以下命令解压cloud-init安装包到当前目录。

   ```
   tar -zxvf cloud-init-19.1.10.tgz
   ```

4. 进入*cloud-init*目录下，并安装依赖库。

```
cd ./cloud-init-19.1.10
pip3 install -r ./requirements.txt
```

5. 进入*cloud-init*的*tools*目录。

```
cd ./tools
```

6. 运行以下命令执行安装cloud-init的脚本*deploy.sh*。

```
bash ./deploy.sh <issue> <major_version>
```

*deploy.sh*脚本的参数说明和取值示例如下：

参数	说明	示例
<issue>	操作系统平台类型。取值范围：*centos*| *redhat*|*rhel*| *debian*| *ubuntu*| *opensuse*| *sles*。参数取值均大小写敏感，其中*sles*表示SUSE/SLES。	centos
<major_version>	操作系统平台主要版本号。 **说明** ubuntu 14不支持安装阿里云版cloud-init 19.1.10。	CentOS 7.6的主要版本号为*7*

例如，您当前的操作系统为CentOS 7，则需要运行的命令为 `bash ./deploy.sh centos 7` 。

7. 确认cloud-init是否安装成功。
若返回 `"description": "success"` ，表示安装成功。

```
{
"status_code": 0,
"description": "success"
}
```

不同Linux发行平台安装阿里云cloud-init的Shell脚本示例如下，供您参考。实际安装时，请根据您的操作系统适当调整脚本。

- CentOS 7/8

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools' >& /dev/null; then
  yum -y install python3-pip
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tgz
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/redhat-release | grep -Eo '[0-9]+\.?[0-9]+' | head -1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh centos "$issue_major"
```

- Red Hat Enterprise Linux 7/8

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools' >& /dev/null; then
  yum -y install python3-pip
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tg
z
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[0-9]+' | head
-1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh rhel "$issue_major"
```

- Ubuntu 16/18/20

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools' >& /dev/null; then
  apt-get install python36 python3-pip -y
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tg
z
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[0-9]+' | head
-1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh ubuntu "$issue_major"
```

- Debian 9/10

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools' >& /dev/null; then
  apt-get -y install python3-pip
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tg
z
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[0-9]+' | head
-1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh debian "$issue_major"
```

- SUSE 12/15

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools'>& /dev/null; then
  zypper -n install python3-pip
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud/etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tg
z
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[0-9]+' | head
-1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh sles "$issue_major"
```

- OpenSUSE 15

```
# 检查安装python3-pip
if ! python3 -c 'import setuptools'>& /dev/null; then
  zypper -n install python3-pip
fi
# 备份旧版cloud-init
test -d /etc/cloud && mv /etc/cloud/etc/cloud-old
# 下载并解压阿里云版cloud-init
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.10.tg
z
tar -zxvf ./cloud-init-19.1.10.tgz
# 安装cloud-init
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[0-9]+' | head
-1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh opensuse"$issue_major"
```

（可选）安装阿里云版cloud-init 0.7.6a15

部分低版本操作系统仍旧保持该版本cloud-init。例如，CentOS 6、Debian 9及SUSE Linux Enterprise Server 12等。

> **说明** 阿里云公共镜像CentOS 6、Debian 9及SUSE Linux Enterprise Server 12默认已安装 `cloud-init-0.7.6a15` 。如果您需要进行测试，请先运行命令**mv /etc/cloud/cloud.cfg /etc/cloud/cloud.cfg_bak**备份配置文件。

1. 运行以下命令，检查操作系统的版本为CentOS 6、Debian 9及SUSE Linux Enterprise Server 12。

```
cat /etc/issue
```

2. 运行以下命令，下载并解压阿里云版cloud-init 0.7.6a15。

```
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/cloud-init-0.7.6a15.tgz
tar -zxvf cloud-init-0.7.6a15.tgz
```

3. 进入*cloud-init*的*tools*目录。

```
cd cloud-init-0.7.6a15/tools/
```

4. 运行以下命令。安装cloud-init。

```
bash ./deploy.sh <issue> <major_version>
```

*deploy.sh*脚本的参数说明和取值示例如下：

参数	说明	示例
<issue>	操作系统平台类型。取值范围：*centos* | *debian* | *sles*。参数取值均大小写敏感，其中*sles*表示SUSE/SLES。	centos
<major_version>	操作系统平台主要版本号。	CentOS 6.5的主要版本号为*6*

例如，您当前的操作系统为CentOS 6，则需要运行的命令为 `bash ./deploy.sh centos 6` 。

（可选）安装社区版cloud-init

1. 确保源服务器已安装Git、Python和Python PIP依赖库。

   以安装Git、python3.6和python3-pip依赖库为例，Linux部分发行版的安装命令如下。

   - CentOS/Red Hat Enterprise Linux：

     ```
     yum -y install git python36 python3-pip
     ```

   - Ubuntu/Debian：

     ```
     apt-get -y install git python36 python3-pip
     ```

   - OpenSUSE/SUSE：

     ```
     zypper -n install git python36 python3-pip
     ```

2. 运行以下命令使用Git下载cloud-init源码包。

   ```
   git clone https://git.launchpad.net/cloud-init
   ```

3. 进入cloud-init目录。

   ```
   cd ./cloud-init
   ```

4. 运行以下命令安装所有依赖库。

   ```
   pip3 install -r ./requirements.txt
   ```

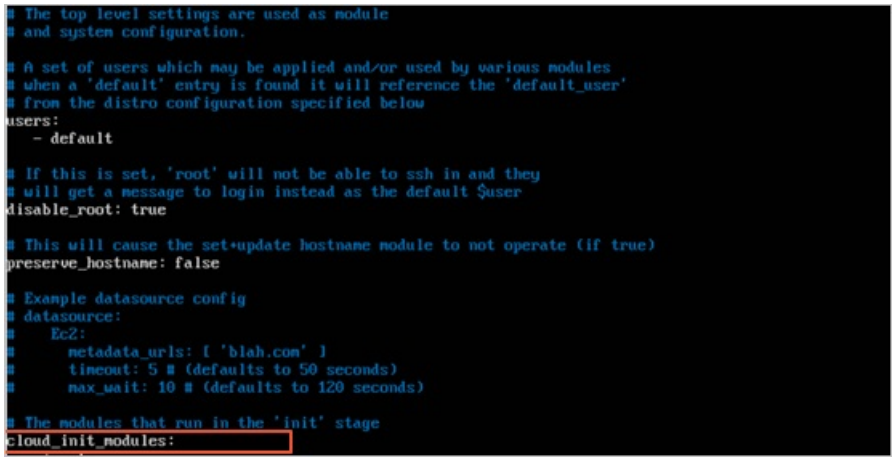
5. 运行以下命令安装cloud-init。

   ```
   python3 setup.py install
   ```

6. 修改配置文件*cloud.cfg*。

i. 打开配置文件。

```
vi /etc/cloud/cloud.cfg
```



ii. 将 `cloud_init_modules:` 之前的配置修改为以下内容。

```
# Example datasource config
# The top level settings are used as module
# and system configuration.
# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
   - default
user:
    name: root
    lock_passwd: False
# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the above $user
disable_root: false
# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false
syslog_fix_perms: root:root
datasource_list: [ AliYun ]
# Example datasource config
datasource:
    AliYun:
        support_xen: false
        timeout: 5 # (defaults to 50 seconds)        max_wait: 60 # (defaults to 12
0 seconds)
#      metadata_urls: [ 'blah.com' ]
# The modules that run in the 'init' stage
cloud_init_modules:
```

（可选）自定义网络配置

1. 安装cloud-init后，打开*/etc/cloud/cloud.cfg*文件。

```
vim /etc/cloud/cloud.cfg
```

2. 按进入编辑模式，在 `Example datasource config` 之前增加disabled配置。

```
network:
  config: disabled
```

说明 增加该配置之后，cloud-init不会管理*/etc/sysconfig/network-scripts/*下网络配置，需要您自行管理。

```
# and system configuration.

# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
   - default

user:
    name: root
    lock_passwd: False

# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the default $user
disable_root: false

# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false

manage_etc_hosts: localhost

network:
  config: disabled


datasource_list: [ AliYun ]

# Example datasource config
```

3. 编辑完成后，按*Esc*键退出编辑模式，然后输入 `:wq` 并回车，保存退出文件。

（可选）不修改主机名以及/etc/hosts配置文件

cloud-init的配置文件中，默认设置了不保留主机名。如果您不希望实例的主机名以及/etc/hosts配置文件被修改，可以参考以下操作修改cloud-init的配置文件。

1. 安装cloud-init后，打开*/etc/cloud/cloud.cfg*文件。

```
vim /etc/cloud/cloud.cfg
```

2. 按*i*进入编辑模式，将 `preserve_hostname: false` 修改为 `preserve_hostname: true` 。

```
# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: true

manage_etc_hosts: localhost
```

3. 编辑完成后，按*Esc*键退出编辑模式，然后输入 `:wq` 并回车，保存退出文件。
   当 `preserve_hostname: true` 时，cloud-init将不会自动修改主机名以及/etc/hosts配置文件。

故障排查

- 通过Python 3安装cloud-init时，缺少依赖库怎么处理？

不同镜像缺少的库可能不同，您都可以通过pip安装，之后再次安装cloud-init。

- cloud-init运行异常，提示报错信息，如何处理？
  如果系统默认软件包管理器（例如**yum**）和**pip**管理器分别安装过不同版本的依赖库，可能造成库版本冲突，导致cloud-init运行异常。建议您根据报错信息按需下载依赖库。

报错信息	原因	排错命令
`no setuptools module in python`	缺失模块python setuptools	以python3.6为例： ○ CentOS/Red Hat：`yum -y install python3-pip` ○ Ubuntu/Debian：`apt-get -y install python3-pip` ○ OpenSUSE/SUSE：`zypper -n install python3-pip`

`File "/root/cloud-init/cloudinit/log.py", line 19, in <module>`
`import six`
`ImportError: No module named six )`
	缺失依赖库six	`pip3 install six`

`File "/root/cloud-init/cloudinit/url_helper.py", line 20, in <module>`
`import oauthlib.oauth1 as oauth1`
`ImportError: No module named oauthlib.oauth1 )`
	缺失依赖库oauthlib	`pip3 install oauthlib`

报错时没有明确缺少的依赖库	未映射相关错误信息	根据cloud-init的*requirements.txt*文件里显示的库，运行以下命令安装所有依赖库： `pip3 install -r requirements.txt`

- 如何确定cloud-init已成功安装且版本正确？
  当您安装好cloud-init后，可以使用**cloud-init --version**命令查看cloud-init的版本信息，如果符合预期版本，则表示cloud-init已成功安装。例如，您安装的是阿里云版cloud-init 19.1.10。安装完成后，如果运行**cloud-init --version**命令的回显信息包含`19.1.10`，则表示cloud-init 19.1.10已成功安装。
- 实例中安装了新版本的Python 3导致了cloud-init执行异常，如何处理？
  如果您在实例中安装了新版本的Python 3（例如Python 3.9），并将新版本的Python 3设置为默认版本（即已为新版Python 3创建了软链接，例如，**ln -s /usr/bin/python3.9 /usr/bin/python3**），则会导致已安装的cloud-init执行异常。例如，运行**cloud-init --version**将会报错：

```
$cloud-init --version
Traceback (most recent call last):
  File "/usr/local/bin/cloud-init", line 33, in <module>
    sys.exit(load_entry_point('cloud-init==19.1.9', 'console_scripts', 'cloud-init')())
  File "/usr/local/bin/cloud-init", line 22, in importlib_load_entry_point
    for entry_point in distribution(dist_name).entry_points
  File "/usr/lib64/python3.9/importlib/metadata.py", line 524, in distribution
    return Distribution.from_name(distribution_name)
  File "/usr/lib64/python3.9/importlib/metadata.py", line 187, in from_name
    raise PackageNotFoundError(name)
importlib.metadata.PackageNotFoundError: cloud-init
```

您可以通过以下任一方式解决该问题：

- 方式一：使用新版的Python 3重新安装cloud-init。
- 方式二：修改cloud-init执行文件，将Python解释器对应的路径修改为历史版本的Python 3。以Python 3.6为例，修改cloud-init执行文件中解释器的操作如下：
  a. 运行以下命令，打开cloud-init文件。

     ```
     vim   /usr/local/bin/cloud-init
     ```

  b. 按*i*进入编辑模式，将文件开头 `#!` 后的内容修改为Python 3.6所在的路径。
     修改后，对应的 `#!` 行内容如下所示：

     ```
     #!/usr/bin/python3.6
     ```

  c. 按*Esc*键退出编辑模式，然后输入 `:wq` 并回车，保存退出文件。

- 安装cloud-init后，在创建实例时设置的实例元数据中的自定义数据（user-data）不执行或者执行失败，如何处理？
  i. 在实例内，运行以下命令，检查实例元数据中的user-data是否存在。

     ```
     curl http://100.100.100.200/latest/user-data
     ```

     检查结果说明：
     - 如果已设置了user-data，则会返回对应的user-data信息。您需要继续下一步进行问题排查。
     - 如果没有返回信息，则表示您没有设置user-data。

  ii. 通过多种方式，排查user-data不执行或执行失败的原因。
     - 检查user-data数据格式是否准确。
       user-data的数据由cloud-init执行，您需要确保数据格式准确无误。例如，user-data的首行必须以 `#!` 开头。更多信息，请参见使用实例自定义数据（Linux实例）。
     - 检查在创建实例时，是否选择了**仅加固模式**。
       如果选择了**仅加固模式**，将导致cloud-init组件初始化配置失败，影响实例的元数据、自定义数据等配置。更多信息，请参见查看实例元数据。
     - 通过cloud-init的日志文件*/var/log/cloud-init.log*，查看user-data执行结果，并根据报错信息排查问题。
       日志文件记录信息示例如下：

       ```
       util.py[DEBUG]: Running command ['/var/lib/cloud/instance/scripts/part-001'] with
       allowed return codes [0] (shell=False, capture=False)
       ```

- 查看user-data执行过程的标准输出以及标准错误输出。
  在Linux系统初始化工具systemd中，user-data由系统服务cloud-final.service执行，您可以运行以下命令查看user-data执行过程的标准输出以及标准错误输出，并根据输出内容排查问题。

  ```
  journalctl -u cloud-final.service
  ```

- 如果以上方式均无法定位user-data不执行或者执行失败的原因，建议您将user-data内容拷贝到本地主机进行调试，查看是否可以成功执行。

- 安装cloud-init后，但系统初始化配置和实例自定义数据（User data）脚本无法正常执行，如何处理？

  i. 运行以下命令，检查cloud-init的四个服务是否设置为开机自启动。

  ```
  systemctl is-enabled cloud-init-local.service
  systemctl is-enabled cloud-init.service
  systemctl is-enabled cloud-config.service
  systemctl is-enabled cloud-final.service
  ```

  如果出现报错信息或者 `disabled` 信息，表示cloud-init未设置开机自启动。

  ii. 运行以下命令，设置cloud-init开机自启动。

  ```
  systemctl enable cloud-init-local.service
  systemctl enable cloud-init.service
  systemctl enable cloud-config.service
  systemctl enable cloud-final.service
  ```

- 在创建实例时对系统盘进行扩容，但在实例内部发现根分区大小并没有自动扩容，如何处理？
  Linux实例分区自动扩容由cloud-init提供支持，需要确保系统安装growpart工具且*cloud.cfg*文件中配置正确。

  i. 运行以下命令，检查系统是否安装growpart工具。

  ```
  which growpart
  ```

  ii. （可选）如果没有安装，运行以下命令，安装growpart工具。

  - RHEL系列：

    ```
    yum -y install cloud-utils-growpart
    ```

  - Debian系列：

    ```
    apt -y install cloud-guest-utils
    ```

  iii. 运行以下命令，查看*/etc/cloud/cloud.cfg*文件中是否存在如下图中的内容。

  ```
  cat /etc/cloud/cloud.cfg
  ```

```
# The modules that run in the 'init' stage
cloud_init_modules:
 - migrator
 - source-address
 - pip-source
 - seed_random
 - bootcmd
 - write-files
 - [ growpart, once-per-instance ]
 - [ resizefs, once-per-instance ]
 - set_hostname
 - update_hostname
 - update_etc_hosts
 - rsyslog
 - users-groups
 - ssh
```

iv. （可选）如果不存在，添加该内容到*/etc/cloud/cloud.cfg*文件中。

后续步骤

- 对于准备迁移上云的Linux服务器：
  您可以使用迁云工具或导入自定义镜像的方式上云。具体操作，请参见使用迁云工具迁移或导入自定义镜像。
- 对于已在阿里云上运行Linux自定义镜像的ECS实例：
  您可以重启系统验证结果。如果系统自动配置了主机名、软件源和NTP等配置，则表示已成功安装cloud-init。例如，查看网络配置文件。

```
[root@iZbp1ios3psx4hoi******Z ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no
```

相关文档

- cloud-init官网 - 阿里云数据源说明文档

6.3.5. 安装virtio驱动

为避免部分服务器、虚拟机或者云主机的操作系统在导入自定义镜像后，创建的ECS实例无法启动，您需要在导入镜像前检查是否需要在源服务器中安装virtio驱动。

背景信息

根据您源服务器的操作系统，判断是否需要手动安装virtio驱动。

源服务器的操作系统	说明
• Windows Server 2008 • Windows Server 2012 • Windows Server 2016 • Windows Server Version ****（半年渠道） • Windows Server 2019及以上版本 • CentOS 6/7/8及以上版本 • Ubuntu 12/14/16/18/20及以上版本 • Debian 7/8/9/10及以上版本 • SUSE 11/12/15及以上版本	如果源服务器的操作系统如左侧所示，在导入自定义镜像时，阿里云将会自动处理virtio驱动。 默认已安装virtio驱动的系统，需要注意修复临时文件系统。具体操作，请参见步骤二：修复临时文件系统。
其他操作系统	如果源服务器的操作系统为其他Linux版本，请根据以下步骤安装virtio驱动： 1. 步骤一：检查服务器内核是否支持virtio驱动 2. 步骤二：修复临时文件系统 3. 步骤三：下载内核安装包 4. 步骤四：编译内核

步骤一：检查服务器内核是否支持virtio驱动

1. 运行以下命令，检查当前操作系统的内核是否支持virtio驱动。

```
grep -i virtio /boot/config-$(uname -r)
```

```
[root@[redacted] ~]# grep -i virtio /boot/config-$(uname -r)
CONFIG_VIRTIO_VSOCKETS=m
CONFIG_VIRTIO_VSOCKETS_COMMON=m
CONFIG_VIRTIO_BLK=m
CONFIG_SCSI_VIRTIO=m
CONFIG_VIRTIO_NET=m
CONFIG_VIRTIO_CONSOLE=m
CONFIG_HW_RANDOM_VIRTIO=m
CONFIG_DRM_VIRTIO_GPU=m
CONFIG_VIRTIO=m
# Virtio drivers
CONFIG_VIRTIO_PCI=m
CONFIG_VIRTIO_PCI_LEGACY=y
CONFIG_VIRTIO_BALLOON=m
CONFIG_VIRTIO_INPUT=m
# CONFIG_VIRTIO_MMIO is not set
```

请检查CONFIG_VIRTIO_BLK和CONFIG_VIRTIO_NET这两个参数。

检查结果	说明
没有这两个参数	表示该操作系统没有安装virtio相关驱动，暂时不能直接导入阿里云云平台。您需要为您的服务器编译安装virtio驱动。具体操作，请参见步骤三：下载内核安装包和步骤四：编译内核。

检查结果	说明
参数取值为m	请执行下一步确认virtio驱动是否包含在临时文件系统initramfs或者initrd中。
参数取值为y	表示包含了virtio驱动，您可以直接导入自定义的镜像到阿里云。具体操作，请参见导入镜像必读和导入自定义镜像。

2. 运行以下命令，确认virtio驱动是否包含在临时文件系统initramfs或者initrd中。

```
lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
```

```
[root@ ~]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
Arguments: -f --add-drivers ' xen-blkfront xen-blkfront virtio_blk virtio_blk virtio_pci virtio_pci virtio_console virtio_console'
-rw-r--r--   1 root     root         7628 Sep 13 07:14 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/block/virtio_blk.ko.xz
-rw-r--r--   1 root     root        12820 Sep 13 07:15 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/char/virtio_console.ko.xz
-rw-r--r--   1 root     root         7980 Sep 13 07:16 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/scsi/virtio_scsi.ko.xz
drwxr-xr-x   2 root     root            0 Oct 24 14:09 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/virtio
-rw-r--r--   1 root     root         4340 Sep 13 07:16 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/virtio/virtio.ko.xz
-rw-r--r--   1 root     root         9480 Sep 13 07:16 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/virtio/virtio_pci.ko.xz
-rw-r--r--   1 root     root         8136 Sep 13 07:16 usr/lib/modules/3.10.0-693.2.2.el7.x86_64/kernel/drivers/virtio/virtio_ring.ko.xz
[root@ ~]#
```

确认结果说明：

- 如上图所示，表示initramfs已经包含了virtio_blk驱动，以及其所依赖的virtio.ko、virtio_pci.ko和virtio_ring.ko，您可以直接导入自定义的镜像到阿里云。更多信息，请参见导入镜像必读和导入自定义镜像。
- 如果临时文件系统initramfs没有包含virtio驱动，则需要修复临时文件系统。具体操作，请参见步骤二：修复临时文件系统。

步骤二：修复临时文件系统

通过检查，发现源服务器内核支持virtio驱动，但是临时文件系统initramfs或者initrd中没有包含virtio驱动时，需要修复临时文件系统。本章节以CentOS、RedHat、Debian和Ubuntu操作系统为例。

- CentOS/RedHat 8

```
mkinitrd -f --allow-missing \
            --with=virtio_blk --preload=virtio_blk \
            --with=virtio_net --preload=virtio_net \
            --with=virtio_console --preload=virtio_console \
            /boot/initramfs-$(uname -r).img $(uname -r)
```

- CentOS/RedHat 6/7

```
mkinitrd -f --allow-missing \
            --with=xen-blkfront --preload=xen-blkfront \
            --with=virtio_blk --preload=virtio_blk \
            --with=virtio_pci --preload=virtio_pci \
            --with=virtio_console --preload=virtio_console \
            /boot/initramfs-$(uname -r).img $(uname -r)
```

- CentOS/RedHat 5

```
mkinitrd -f --allow-missing \
            --with=xen-vbd  --preload=xen-vbd \
            --with=xen-platform-pci --preload=xen-platform-pci \
            --with=virtio_blk --preload=virtio_blk \
            --with=virtio_pci --preload=virtio_pci \
            --with=virtio_console --preload=virtio_console \
            /boot/initrd-$(uname -r).img $(uname -r)
```

- Debian/Ubuntu

```
echo -e 'xen-blkfront\nvirtio_blk\nvirtio_pci\nvirtio_console' >> \
/etc/initramfs-tools/modules
mkinitramfs -o /boot/initrd.img-$(uname -r)
```

步骤三：下载内核安装包

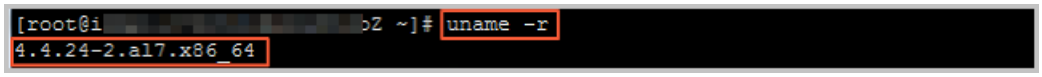
> **说明** 本章节以内核版本*linux-4.4.24.tar.gz*为例，您需要将内核版本修改为实际操作系统内核对应的版本。

1. 运行以下命令，安装编译内核的必要组件。

```
yum install -y ncurses-devel gcc make wget
```

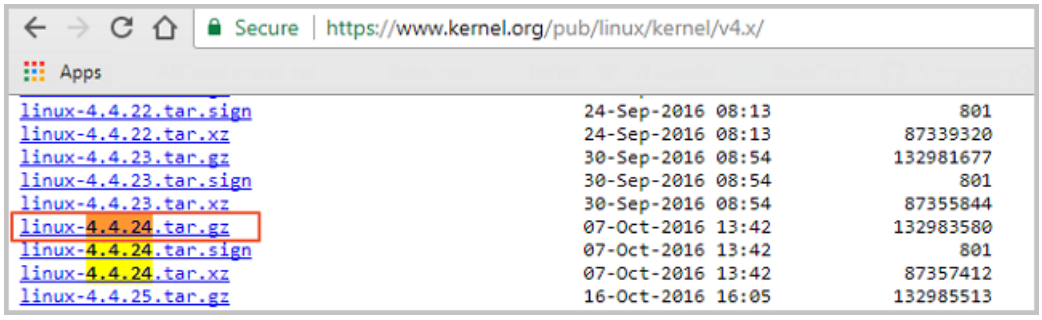
2. 运行以下命令，查询当前系统使用的内核版本，如示例中的4.4.24-2.a17.x86_64。

```
uname -r
```



3. 前往Linux内核列表页面查看对应的内核版本源码的下载地址。

   如下图示例中的4.4.24开头的*linux-4.4.24.tar.gz*的下载地址为 `https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz` 。



4. 运行以下命令，切换目录。

```
cd /usr/src/
```

5. 运行以下命令，下载安装包。

```
wget https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz
```

6. 运行以下命令，解压安装包。

```
tar -xzf linux-4.4.24.tar.gz
```

7. 运行以下命令，建立软链接。

```
ln -s linux-4.4.24 linux
```

8. 运行以下命令，切换目录。

```
cd /usr/src/linux
```

步骤四：编译内核

1. 依次运行以下命令，编译内核。

```
make mrproper
symvers_path=$(find /usr/src/ -name "Module.symvers")
test -f $symvers_path && cp $symvers_path .
cp /boot/config-$(uname -r) ./.config
make menuconfig
```

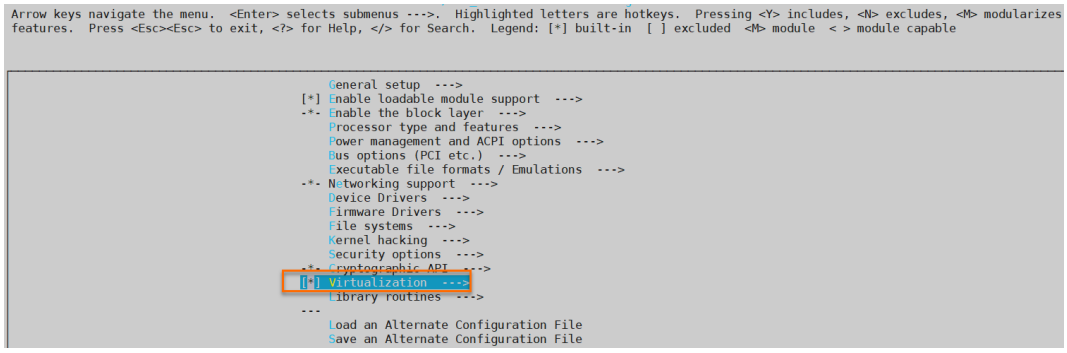
> **说明** 如果运行make menuconfig后报错，您可以根据报错提示进行修复。例如缺少ncurses-devel、bison、flex组件时，需要依次运行以下命令，安装相关组件。
>
> ```
> yum install ncurses-devel
> yum install bison
> yum install flex
> ```

2. 出现以下界面时，开始打开virtio相关配置：

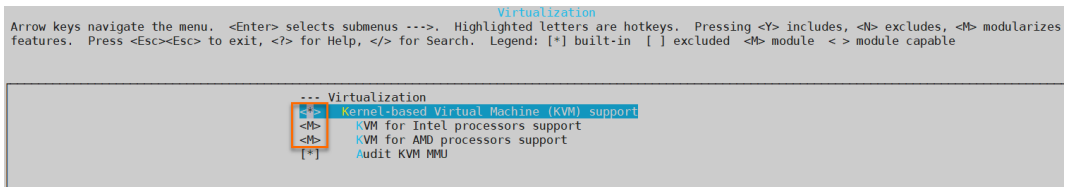
> **说明** 选*配置表示编译到内核，选*m*配置表示编译为模块。

i. 配置Virtualization项。

a. 使用空格键选择**Virtualization**项，并按*Enter*键进入详细列表。



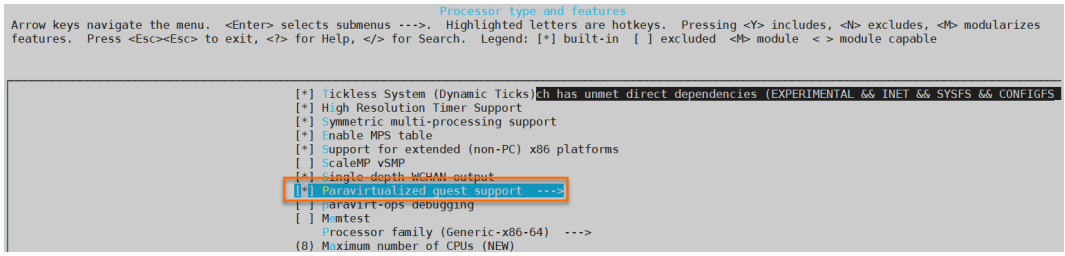
b. 确认是否选择了KVM（Kernel-based Virtual Machine）项。



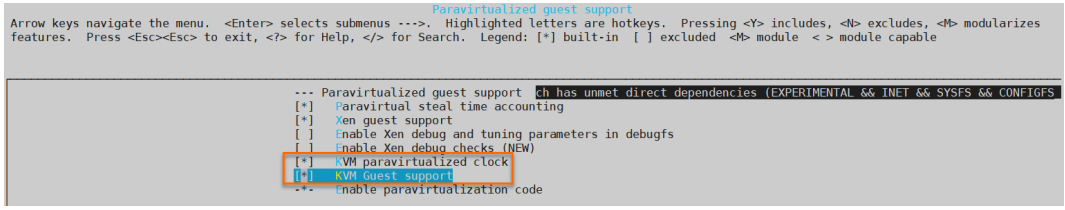
ii. 配置Processor type and features项。

a. 返回到主界面，通过上下键选择**Processor type and features**项，并按*Enter*键进入详细列表。

b. 使用空格键选择**Paravirtualized guest support**项，并按*Enter*键进入详细列表。



c. 确认是否选择了**KVM paravirtualized clock**和**KVM Guest support**项。



iii. 配置Device Drivers项。

a. 返回到主界面，通过上下键选择**Device Drivers**项，并按*Enter*键进入详细列表。

b. 使用空格键选择**Block devices**项，并按*Enter*键进入详细列表。

c. 确认是否选择了**Virtio block driver**项。

```
                                                    Block devices
Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).  Highlighted letters are hotkeys.  Pressing <Y> includes, <N>
excludes, <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in  [ ] excluded  <M> module  < > module
capable

                                        ↑(-)
                                <M>   Normal floppy disk support
                                < >   Parallel port IDE device support
                                <M>   Block Device Driver for Micron PCIe SSDs
                                <M>   Compressed RAM block device support
                                [ ]     Enable LZ4 algorithm support (NEW)
                                < >   Compaq Smart Array 5xxx support
                                < >   Mylex DAC960/DAC1100 PCI RAID Controller support
                                < >   Micro Memory MM5415 Battery Backed RAM support
                                <M>   Loopback device support
                                (0)     Number of loop devices to pre-create at init time
                                < >     Cryptoloop Support
                                < >   DRBD Distributed Replicated Block Device support
                                < >   Network block device support
                                < >   STEC S1120 Block Driver (NEW)
                                <M>   OSD object-as-blkdev support
                                <M>   Promise SATA SX8 support
                                <M>   RAM block device support
                                (16)    Default number of RAM disks
                                (16384) Default RAM disk size (kbytes)
                                [ ]     Support Direct Access (DAX) to RAM block devices (NEW)
                                <M>   Packet writing on CD/DVD media
                                (8)     Free buffers for data gathering
                                [ ]     Enable write caching
                                <M>   ATA over Ethernet support
                                <M>   Xen virtual block device support
                                < >   Xen block-device backend driver (NEW)
                                <M>   Virtio block driver
                                [ ]   Very old hard disk (MFM/RLL/IDE) driver
                                <M>   Rados block device (RBD)
                                ↓(+)
```

d. 回到上一级**Device Drivers**详细列表，通过上下键选择**Network device support**项，并按*Enter*键进入详细列表。

e. 确认是否选择了**Virtio network driver**项。

```
                                                    Network device support
Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).  Highlighted letters are hotkeys.
excludes, <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in  [ ]
capable

                                --- Network device support
                                [*]   Network core driver support
                                <M>     Bonding driver support
                                <M>     Dummy net driver support
                                < >     EQL (serial line load balancing) support
                                [*]     Fibre Channel driver support
                                <M>     Intermediate Functional Block support
                                <M>     Ethernet team driver support  --->
                                <M>     MAC-VLAN support
                                <M>       MAC-VLAN based tap driver
                                < >     IP-VLAN support (NEW)
                                <M>     Virtual eXtensible Local Area Network (VXLAN)
                                <M>     Generic Network Virtualization Encapsulation
                                <M>     Network console logging support
                                [*]       Dynamic reconfiguration of logging targets
                                <M>     Virtual Ethernet over NTB Transport
                                <M>     Universal TUN/TAP device driver support
                                [ ]     Support for cross-endian vnet headers on little-endian kernels
                                <M>     Virtual ethernet pair device
                                <M>     Virtio network driver
                                <M>     Virtual netlink monitoring device
                                < >   ARCnet support  ----
                                [ ]   ATM drivers  ----
                                      *** CAIF transport drivers ***
```

iv. 按*Esc*键退出内核配置界面，并根据弹窗提示选择**Yes**保存*.config*文件。

v. 检查virtio相关配置是否已经正确配置。

具体操作，请参见步骤一：检查服务器内核是否支持virtio驱动。

vi. （可选）如果检查后发现暂未设置virtio相关配置，依次运行以下命令自动触发编辑*.config*文件。

```
make oldconfig
make prepare
make scripts
make
make install
```

vii. 运行以下命令，查看virtio驱动的安装情况。

```
find /lib/modules/"$(uname -r)"/ -name "virtio*" | grep -E "virtio*"
grep -E "virtio*" < /lib/modules/"$(uname -r)"/modules.builtin
```

如果任一命令输出virtio_blk、virtio_pci、virtio_console等文件列表，表明您已经正确安装了virtio驱动。

后续步骤

检查virtio驱动后，您可以执行以下操作：

- 迁移服务器
- 导入自定义镜像

6.3.6. 定制Linux自定义镜像

当镜像的操作系统不在阿里云所支持的平台列表中，并且不能安装cloud-init时，您可以在导入自定义镜像时选择Customized Linux（定制版镜像）。阿里云将定制版Linux镜像当作无法识别的操作系统，您需要在导入镜像前，根据本文描述在镜像中添加解析脚本，便于初次启动时自动化配置实例。

限制要求

Customized Linux镜像具有如下限制条件：

- 第一个分区必须可以被写入。
- 第一个分区的文件类型只能是FAT32、EXT2、EXT3、EXT4或UFS。
- 虚拟文件的大小必须大于5GiB。

Customized Linux镜像具有如下安全要求：

- 不能存在可被远程利用的高危漏洞。
- 使用控制台的管理终端（VNC）登录实例时，如果存在初始默认密码，您必须在首次登录时修改，修改密码之前不允许进入实例做任何操作。详情请参见通过密码认证登录Linux实例。
- 不支持默认SSH密钥对，初始SSH密钥对必须由阿里云生成。

配置方法

制作并导入Customized Linux自定义镜像前，您需要进行如下配置。

1. 在镜像的第一个分区的根目录下新建目录*aliyun_custom_image*。
   使用该Customized Linux镜像所创建的实例初次启动时，阿里云会在*aliyun_custom_image*目录的*os.conf*文件中写入实例相关配置信息。如果不存在*os.conf*文件，则系统自动创建。
2. 在镜像中创建一份解析脚本，用以解析*os.conf*文件的系统配置。
   编写脚本，请参见解析脚本注意事项和解析脚本示例。

os.conf文件示例

- 经典网络类型实例*os.conf*文件示例。

```
hostname=<yourHostName>
password=<yourPassword>
eth0_ip_addr=10.0.0.2
eth0_mac_addr=00:xx:xx:xx:xx:23
eth0_netmask=255.255.255.0
eth0_gateway=10.0.0.1
eth0_route="10.0.0.0/8 10.0.0.1;172.16.0.0/12 10.0.0.1"
eth1_ip_addr=42.0.0.2
eth1_mac_addr=00:xx:xx:xx:xx:24
eth1_netmask=255.255.255.0
eth1_gateway=42.0.0.1
eth1_route="0.0.0.0/0 42.0.0.1"
dns_nameserver="7.7.7.7 8.8.8.8"
```

示例中各参数说明如下表所示。

参数名称	参数说明
hostname	主机名参数
password	密码参数，Base64编码的字符串
eth0_ip_addr	eth0网卡IP地址
eth0_mac_addr	eth0网卡MAC地址
eth0_netmask	eth0网卡掩码
eth0_gateway	eth0网卡默认网关
eth0_route	eth0内网路由列表，默认用半角分号分隔
eth1_ip_addr	eth1网卡IP地址
eth1_mac_addr	eth1网卡MAC地址
eth1_netmask	eth1网卡掩码
eth1_gateway	eth1网卡默认网关
eth1_route	eth1公网路由列表，默认用半角分号分隔
dns_nameserver	DNS地址列表，默认用空格分隔

- 专有网络VPC类型实例*os.conf*文件示例。

```
hostname=<yourHostName>
password=<yourPassword>
eth0_ip_addr=10.0.0.2
eth0_mac_addr=00:xx:xx:xx:xx:23
eth0_netmask=255.255.255.0
eth0_gateway=10.0.0.1
eth0_route="0.0.0.0/0 10.0.0.1"
dns_nameserver="7.7.7.7 8.8.8.8"
```

示例中各参数说明如下表所示。

参数名称	参数说明
hostname	主机名参数
password	密码参数，Base64编码的字符串
eth0_ip_addr	eth0网卡IP地址
eth0_mac_addr	eth0网卡MAC地址
eth0_netmask	eth0网卡掩码
eth0_gateway	eth0网卡默认网关
eth0_route	eth0内网路由列表，默认用半角分号分隔
dns_nameserver	DNS地址列表，默认用空格分隔

解析脚本注意事项

实例初次启动时，正常情况下阿里云自动将配置项的相关信息写入第一个分区的根目录下*aliyun_custom_image*目录的*os.conf*文件中。配置Customized Linux镜像必须要在镜像中创建预定义解析脚本，用以从*os.conf*文件中读取实例配置信息并完成实例配置。

解析脚本需要满足的条件，如下表所示。

需满足的条件	配置说明
开机启动	解析脚本需要设置成开机自启动，例如，将解析脚本存放在*/etc/init.d/*目录下。
配置项取值规则	如os.conf 文件示例的配置项所述，VPC与经典网络类型实例的配置项数量和部分配置项的取值规则均有所不同。
配置文件读取路径	Customized Linux镜像在创建I/O优化实例或非I/O优化实例时，为第一个分区所分配的设备名默认不一样。所以在解析脚本中建议使用 `uuid` 或 `label` 识别第一个分区的设备。用户密码为Base64编码的字符串，设置密码时需要做相关处理。
判断VPC或经典网络	解析脚本判断该网络类型时，可以查看是否存在eth1_route或其他eth1相关的配置项。判断出当前实例的网络类型后再有针对性地解析和处理。 • VPC类型实例在*os.conf*文件的eth0_route参数中配置默认公网路由。 • 经典网络类型实例在*os.conf*文件的eth1_route参数中配置默认公网路由，内网路由配置在eth0_route中。
配置优化	*os.conf*文件中的配置在实例的整个生命周期中执行一次即可，解析脚本执行成功后建议删除*os.conf*文件。同时解析脚本如果没有读取到*os.conf*文件配置，则不执行文件中的配置。
自定义镜像处理	根据Customized Linux镜像创建的实例再制作自定义镜像时，镜像中也会包含这个开机启动脚本。阿里云会在实例第一次启动时写入*os.conf*配置，解析脚本在检测到该配置时即可执行相关配置。

需满足的条件	配置说明
修改相关配置时的处理	当实例的配置信息通过阿里云的控制台或API发生变更时，阿里云将相关信息写入到*os.conf*文件中，解析脚本将被再次执行从而下发这些更改。

解析脚本示例

解析脚本以CentOS操作系统为例，仅供您参考。实际操作时，请根据操作系统类型调整脚本内容。使用脚本前，务必在镜像中调试脚本，并保证调试通过。

```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          os-conf
# Required-Start:    $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: The initial os-conf job, config the system.
### END INIT INFO
first_partition_dir='/boot/'
os_conf_dir=${first_partition_dir}/aliyun_custom_image
os_conf_file=${os_conf_dir}/os.conf
load_os_conf() {
    if [[ -f $os_conf_file ]]; then
        . $os_conf_file
        return 0
    else
        return 1
    fi
}
cleanup() {
    # ensure $os_conf_file is deleted, to avoid repeating config system
    rm $os_conf_file >& /dev/null
    # ensure $os_conf_dir exists
    mkdir -p $os_conf_dir
}
config_password() {
    if [[ -n $password ]]; then
        password=$(echo $password | base64 -d)
        if [[ $? == 0 && -n $password ]]; then
            echo "root:$password" | chpasswd
        fi
    fi
}
config_hostname() {
    if [[ -n $hostname ]]; then
        sed -i "s/^HOSTNAME=.*/HOSTNAME=$hostname/" /etc/sysconfig/network
        hostname $hostname
    fi
}
config_dns() {
    if [[ -n $dns_nameserver ]]; then
        dns_conf=/etc/resolv.conf
```

```
        sed -i '/^nameserver.*/d' $dns_conf
        for i in $dns_nameserver; do
            echo "nameserver $i" >> $dns_conf
        done
    fi
}
is_classic_network() {
    # vpc: eth0
    # classic: eth0 eth1
    grep -q 'eth1' $os_conf_file
}
config_network() {
    /etc/init.d/network stop
    config_interface eth0 ${eth0_ip_addr} ${eth0_netmask} ${eth0_mac_addr}
    config_route eth0 "${eth0_route}"
    if is_classic_network ; then
        config_interface eth1 ${eth1_ip_addr} ${eth1_netmask} ${eth1_mac_addr}
        config_route eth1 "${eth1_route}"
    fi
    /etc/init.d/network start
}
config_interface() {
    local interface=$1
    local ip=$2
    local netmask=$3
    local mac=$4
    interface_cfg="/etc/sysconfig/network-scripts/ifcfg-${interface}"
    cat << EOF > $interface_cfg
DEVICE=$interface
IPADDR=$ip
NETMASK=$netmask
HWADDR=$mac
ONBOOT=yes
BOOTPROTO=static
EOF
}
config_default_gateway() {
    local gateway=$1
    sed -i "s/^GATEWAY=.*/GATEWAY=$gateway/" /etc/sysconfig/network
}
config_route() {
    local interface=$1
    local route="$2"
    route_conf=/etc/sysconfig/network-scripts/route-${interface}
    > $route_conf
    echo $route | sed 's/;/\n/' | \
        while read line; do
            dst=$(echo $line | awk '{print $1}')
            gw=$(echo $line | awk '{print $2}')
            if ! grep -q "$dst" $route_conf 2> /dev/null; then
                echo "$dst via $gw dev $interface" >> $route_conf
            fi
            if [[ "$dst" == "0.0.0.0/0" ]]; then
                config_default_gateway $gw
            fi
```

```
            fi
        done
}
################## sysvinit service portal ####################
start() {
    if load_os_conf ; then
        config_password
        config_network
        config_hostname
        config_dns
        cleanup
        return 0
    else
        echo "not load $os_conf_file"
        return 0
    fi
}
RETVAL=0
case "$1" in
    start)
        start
        RETVAL=$?
    ;;
    *)
        echo "Usage: $0 {start}"
        RETVAL=3
    ;;
esac
exit $RETVAL
```

6.3.7. 转换镜像格式

ECS只支持导入RAW、VHD和qcow2格式的镜像文件。其他镜像文件，需要转换格式后再导入。本文介绍如何利用qemu-img工具将其它格式的镜像文件转换成VHD或RAW格式。

背景信息

qemu-img支持以下镜像格式的转换：

- RAW、qcow2、qcow1、VMDK、VDI、VHD（vpc）、VHDX或QED格式的镜像转换成VHD格式
- RAW和VHD格式的互相转换

> **说明** qemu-img不支持转换iso镜像为VHD或RAW格式。如需转换，可以先将iso镜像安装到VHD或RAW介质，再制作相应格式的镜像。

本地为Windows操作系统

按以下步骤安装qemu-img并转换镜像文件格式：

1. 下载qemu-img并完成安装。

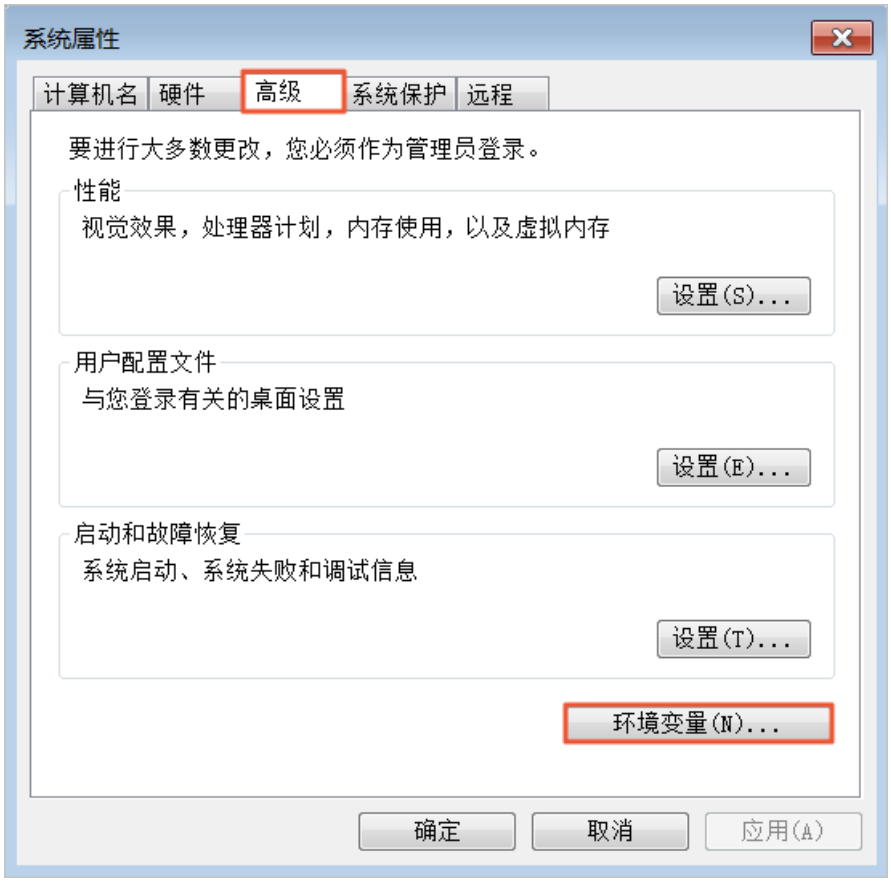
   本示例安装路径为*C:\Program Files\qemu*。下载地址：下载qemu-img。

2. 为qemu-img配置环境变量。

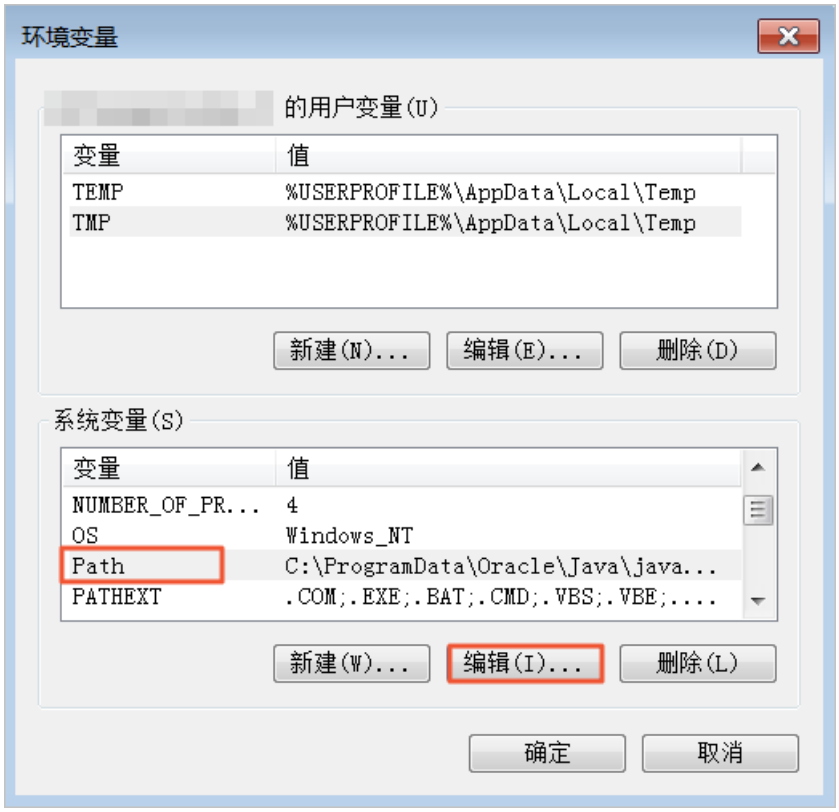
   i. 选择**开始 > 计算机**，右键单击**属性**。

ii. 在左侧导航栏里，单击**高级系统设置**。

iii. 在**系统属性**对话框里，单击**高级**页签，并单击**环境变量**。

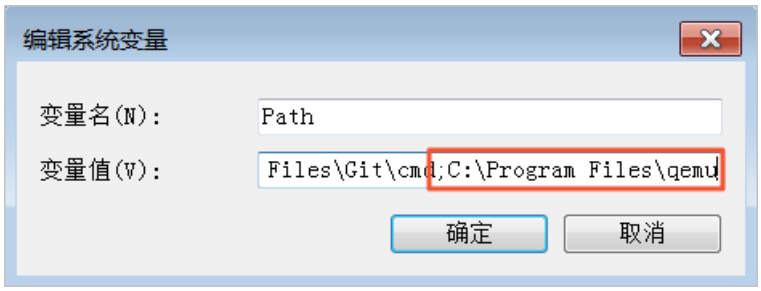


iv. 在**环境变量**对话框里，在**系统变量**部分找到**Path**，并单击**编辑**。如果**Path**变量不存在，单击**新建**。

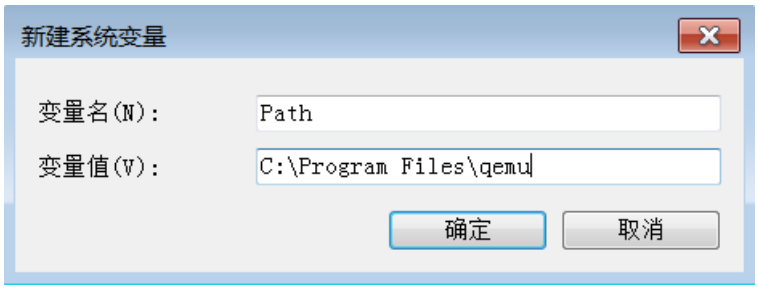


v. 添加系统变量值。

- 如果是**编辑系统变量**，在**变量值**里，添加*C:\Program Files\qemu*，不同的变量值之间以半角分号（;）分隔。



- 如果是**新建系统变量**，在**变量名**处输入*Path*，在**变量值**处输入*C:\Program Files\qemu*。



3. 测试是否成功配置环境变量。

   i. 打开Windows命令行工具。

   ii. 运行 `qemu-img --help` 命令。

如果命令返回值显示正常，即表示已配置环境变量。

4. 在**命令提示符**对话框里，使用**cd [源镜像文件所在的目录]**切换文件目录，例如 `cd D:\ConvertImage` 。
5. 运行 `qemu-img convert -f qcow2 -O raw centos.qcow2 centos.raw` 命令转换镜像文件格式，其中：
   - -f的参数值为源镜像文件的格式。
   - -O（必须是大写）的参数值为目标镜像格式、源镜像文件名称和目标文件名称。

转换完成后，目标文件会出现在源镜像文件所在的目录下。

本地为Linux操作系统

按以下步骤安装qemu-img并转换镜像文件格式：

1. 安装qemu-img。

   示例如下：
   - 如果本地为Ubuntu操作系统，运行 `apt-get install qemu-utils` 。
     如果在Ubuntu上安装qemu-utils时，出现 `Unable to locate package qemu-utils` 错误，请运行以下命令安装qemu-img工具：

     ```
     apt-get update #更新包列表
     apt-get install qemu-utils #安装qemu-img工具
     ```

   - 如果本地为CentOS操作系统，运行 `yum install qemu-img` 。
     如果在安装qemu-img时报错，且没有明确提示缺少哪些依赖库，您可以根据cloud-init的requirements.txt文件里显示的库，并运行 `pip install -r requirements.txt` 安装所有依赖库。
2. 运行 `qemu-img convert -f qcow2 -O raw centos.qcow2 centos.raw` 命令转换镜像文件格式，其中：
   - -f的参数值为源镜像文件的格式。
   - -O（必须是大写）的参数值为目标镜像格式、源镜像文件名称和目标文件名称。

转换完成后，目标文件会出现在源镜像文件所在的目录下。

后续步骤

导入自定义镜像

6.3.8. 导入自定义镜像

在云上部署业务时，您可以手动导入服务器的镜像文件，也可以由阿里云自动为您的服务器生成ECS镜像。本文介绍这两种方法的应用场景和操作步骤。

前提条件

手动导入镜像前，请您确认已完成以下操作：

- 了解镜像限制和要求。更多信息，请参见导入镜像必读、定制Linux自定义镜像和转换镜像格式。
- 已开通OSS服务。具体操作，请参见开通OSS服务。
- 如果您使用的是RAM用户，应预先联系阿里云账号授权AliyunECSImageImportDefaultRole角色策略获得操作许可。

背景信息

导入自定义镜像的应用场景如下：

功能	应用场景	操作步骤
自动导入	将一台或多台服务器（包括IDC服务器、虚拟机、其他云平台的云主机或其他类型的服务器）迁移至阿里云。	自动导入
手动导入	阿里云没有可用的操作系统类型供您选择。例如： • 服务器的操作系统类型在阿里云不存在。 • 服务器操作系统版本在阿里云已下线。 • 服务器的操作系统为线下定制系统。 手动导入自定义镜像功能，支持设置不同的许可证类型激活源操作系统，以降低您在云上使用镜像的费用。许可证类型的更多信息，请参见导入镜像参数说明表。	手动导入

自动导入

请您完成以下操作，由服务器迁移中心SMC为您的源服务器生成ECS镜像。

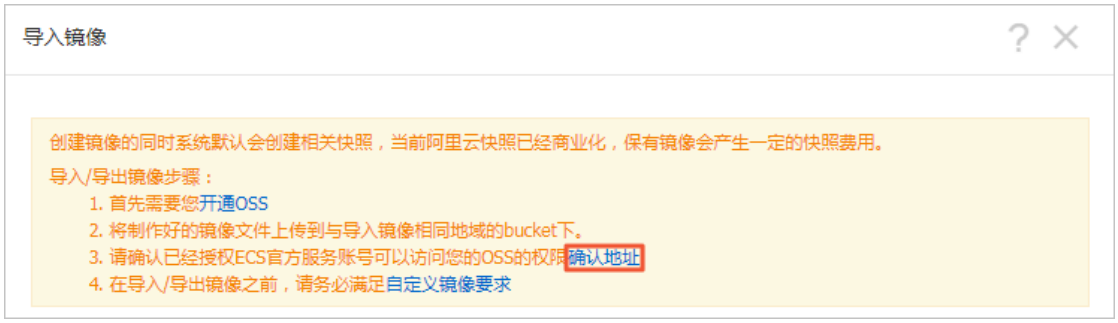
1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像**页面右上角，单击**SMC在线迁移**。
   页面跳转至服务器迁移中心SMC控制台。
5. 完成SMC所需操作。
   具体操作，请参见迁移流程。迁移完成后，SMC会为您的服务器生成一份自定义镜像。镜像名称以 `IMAGE_FROM_SMC` 开头。

手动导入

请您完成以下操作，将服务器的本地镜像文件导入阿里云ECS。

1. 使用OSS的第三方工具客户端或API上传制作好的自定义镜像。

   关于如何上传大于5 GiB文件的具体操作，请参见分片上传和断点续传上传。
2. 登录ECS管理控制台。
3. 在左侧导航栏，选择**实例与镜像 > 镜像**。
4. 在顶部菜单栏左上角处，选择地域。
5. 授权ECS服务访问您的OSS资源。
   i. 在**镜像**页面右上角，单击**导入镜像**。
   ii. 在**导入镜像**对话框里，单击提示信息第3步中的**确认地址**。



iii. 在**云资源访问授权**页面，查看到 `AliyunECSImageImportDefaultRole` 和 `AliyunECSExportDefaultRole` ，单击**同意授权**。

6. 导入自定义镜像。
   i. 在**镜像**页面右上角，再次单击**导入镜像**。
   ii. 在**导入镜像**对话框里，完成以下设置。

参数	是否必填	说明
镜像所在地域	是	由系统自动设置为当前地域。如需更换地域，请在顶部菜单栏选择新的地域，并重新打开**导入镜像**对话框。
OSS Object地址	是	填写从OSS控制台获取的镜像文件Object地址。更多信息，请参见分享文件。您需要注意： ■ 必须在同一个阿里云账号下完成获取OSS Object地址以及导入镜像的操作。 ■ OSS Object地址必须是您通过分享文件操作生成的公网URL。由OSS提供的内网地址不支持在导入镜像时使用，否则会导入失败并报错。关于什么是OSS内网地址，请参见获取OSS内网地址。
镜像名称	是	镜像文件导入后显示的名称。长度为2~128个字符，以大小写字母或中文开头，可包含数字、英文句号（.）、下划线（_）、半角冒号（:）和短划线（-）。
操作系统/平台	是	■ 操作系统： 选择待导入镜像的操作系统类型。取值范围：**Windows|Linux**。 待导入镜像的操作系统为非标准平台时，应选择**Linux**。 ■ 平台： 列表的值取决于操作系统的值。选择适用于待导入镜像的系统平台。 ■ Windows：支持Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016和Windows Server 2019。 ■ Linux：支持CentOS、SUSE、OpenSUSE、Ubuntu、Debian、FreeBSD、CoreOS、Aliyun、Anolis、RedHat、Customized Linux和Others Linux（请提交工单确认是否支持）。 ■ 如果您的镜像的操作系统是根据Linux内核定制开发的，请提交工单联系我们。
系统架构	是	64位操作系统选择**x86_64**；32位操作系统选择**i386**；ARM64位操作系统选择**arm64**。
镜像检测	否	镜像检测功能主要检测导入的自定义镜像是否为有效镜像、自定义镜像是否可以创建出功能齐全的ECS实例等。 选中**导入后执行检测**时，镜像检测功能会在该镜像导入后立即执行。检测完成后，您可以在自定义镜像列表**状态**列单击**详情**，查看镜像检测结果，并可针对检测结果中的修复建议进行修复。检测项范围及修复建议，请参见自定义镜像检测项说明。

参数	是否必填	说明
系统盘大小（GiB）	否	系统盘大小范围为5 GiB~500 GiB，且不能小于镜像文件的大小。
镜像格式	否	支持**自动检测**，或选择**RAW**、**QCOW2**、**VHD**、**VDI**等格式。 ■ 如果您不清楚镜像格式，可选择自动检测，系统将自动设置镜像格式。 ■ 如果您自行选择镜像格式，推荐使用传输内容更小的QCOW2或者VHD格式。 **说明** 不支持ISO镜像文件，需先转换成RAW、VHD或QCOW2格式再导入。您也可以使用Packer创建并导入本地镜像，具体操作，请参见使用Packer创建并导入本地镜像和Packer的DevOps配置。

许可证类型	否	镜像导入之后，激活源操作系统要使用的许可证类型。取值范围：
		■ **自带许可**：源操作系统自带的许可证。采用自带许可时，需确保您的许可证密钥能够在阿里云使用。
		关于Red Hat云接入和Windows许可证的详细信息，请参见Red Hat云接入概述和微软许可证与软件保障。
		■ **阿里云**：根据您设置的系统平台值，采用阿里云官方渠道许可证。
		■ **自动**（默认值）：由阿里云自动检测源操作系统并分配许可证。自动模式下，系统会自动搜索您设置的系统平台是否有阿里云官方渠道许可证，并做如下处理：
		  ■ 如果有阿里云官方许可证，则分配给导入的镜像。
		  ■ 如果没有该类许可，则切换成**自带许可**方式。

描述	否	填写镜像描述信息，便于后续管理。
添加数据盘镜像	否	同时导入包含数据盘的自定义镜像，支持的数据盘容量范围为5 GiB~1000 GiB。
资源组	否	您可以设置资源组，对镜像进行分级管理。
标签	否	您可以设置标签，将镜像归类，便于搜索与批量操作。

iii. 信息确认无误后，单击**确定**。系统会创建一个导入自定义镜像的任务。

7. （可选）在目标地域的镜像列表中查看导入进度。在任务完成前，您都可以通过任务管理找到该导入的自定义镜像，取消导入镜像任务。

   导入自定义镜像所需时间，取决于镜像文件的大小和当前导入任务的并发数，需要您耐心等待。

导入自定义镜像时，系统会自动生成一份快照，您可以在**快照列表**里看到快照信息。导入镜像任务未完成前，快照的状态会显示为**失败**。任务完成后，快照的状态自动更新为**成功**，镜像的状态自动更新为**可用**。快照的容量为导入的自定义镜像文件大小，与导入自定义镜像时设置的系统盘大小无关。目前快照容量已经收费，更多信息，请参见快照计费。

后续步骤

使用自定义镜像创建实例

相关文档

相关文档

- ImportImage
- 使用Packer创建并导入本地镜像
- 更换操作系统
- 镜像FAQ
- 什么是服务器迁移中心
- Red Hat云接入概述
- 微软许可证与软件保障

6.4. 更新自定义镜像

运维编排服务OOS为更新自定义镜像的场景提供了公共模版。您只需选择一个源镜像，输入更新镜像所需的云助手脚本等必要参数，就可以创建立即执行或定时执行的运维任务，一键更新自定义镜像。

前提条件

更新自定义镜像会自动创建临时资源并采用按量付费计费方式。开通按量付费ECS资源时，您的阿里云账户余额（即现金余额）和代金券的总值不得小于100.00元人民币。

背景信息

在更新自定义镜像的完整流程中，运维编排服务OOS的ACS-ECS-UpdateImage公共模板按顺序执行以下任务，并生成新的自定义镜像：

1. 检查新自定义镜像的名称是否已存在，以及是否符合规则。
2. 根据您配置的实例规格、源镜像ID、安全组ID等参数创建并运行一台临时ECS实例。
3. 检查临时ECS实例是否安装了云助手客户端，若缺失则安装云助手客户端。
4. 在临时ECS实例上，通过云助手执行脚本更新实例系统环境。

> **说明** 运维编排服务OOS通过调用云助手API执行Shell、Bat或者PowerShell等脚本，更新ECS实例的系统应用环境。更多详情，请参见云助手概述。

5. 停止临时ECS实例。
6. 根据临时ECS实例创建自定义镜像。
7. 释放临时ECS实例。

操作步骤

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

4. 在**镜像**页面，选择**自定义镜像**页签。
5. 找到目标镜像，在**操作**栏单击 ⋮ 图标，然后单击**更新镜像**。
6. 跳转至OOS管理控制台后，完成以下配置：
   i. 完成通用设置，包括输入新镜像名称和描述，并指定执行所使用到的权限来源。
   ii. （可选）完成镜像分发设置。您可以根据需要设置是否复制或共享该镜像。
   iii. 选择镜像。如果您在前一步操作已选择了目标镜像，此时将自动选中，请确认已选的镜像是否为需要操作的镜像。
   iv. 配置中转实例，设置用于创建临时ECS实例的专有网络、交换机、安全组和实例类型。
   v. （可选）发送远程命令。您可以根据需要选择命令类型并输入命令内容，该命令内容将在临时创建的ECS实例中执行。
   vi. （可选）完成高级选项配置。您可以根据需要设置伸缩组配置，添加标签或将当前配置保存为模板。
7. 单击**立即执行**，并在弹出的对话框中确认提示信息。
8. 在**创建或更新镜像**页面，您可以查看任务运行情况。

执行结果

若成功创建运维任务，且执行状态处于**运行中**，则表示更新镜像正在进行中。当执行状态转换为**成功**时，则表示镜像更新成功，您可以在基本详情的输出参数中查看新镜像ID。

> **说明** 如需了解更新镜像的详细过程，您可单击该执行的**详情**后，单击**日志**页签了解运维任务的实时进度和状态。

相关文档

相关文档

- 什么是运维编排服务
- 使用运维编排创建和更新自定义镜像
-

6.5. 复制镜像

复制镜像适用于跨地域部署ECS实例、跨地域备份数据。复制镜像后，您会在目标地域获得同样配置不同ID的镜像。

背景信息

复制镜像能解决以下业务需求：

业务需求	操作步骤	相关API
跨地域、同账号复制ECS实例	1. 使用实例创建自定义镜像 2. 复制镜像到目标地域（即本文操作）	1. CreateImage 2. CopyImage
跨地域、跨账号复制ECS实例	1. 使用实例创建自定义镜像 2. 复制镜像到目标地域（即本文操作） 3. 共享镜像	1. CreateImage 2. CopyImage 3. ModifyImageSharePermission
同地域、跨账号复制ECS实例	无需复制镜像。更多信息，请参见共享镜像	ModifyImageSharePermission
变更某一自定义镜像的加密状态、加密系统盘或者加密操作系统数据	同地域复制镜像时，选择加密选项 说明 • 在同地域复制自定义镜像时，仅支持加密复制。 • 复制加密镜像的过程中不支持取消复制。	CopyImage

复制镜像前，请仔细阅读以下注意事项：

- 可能产生的费用包括：
  - 复制的快照会占用快照容量。更多信息，请参见计费概述。

    说明 复制镜像时，会在目标地域生成对应的快照，随后在目标地域根据快照生成自定义镜像。这些生成的快照的保留时间均为永久，与源镜像的快照的保留时间无关。

  - 不同地域间的数据传输流量费。目前，未对这部分流量收费，具体收费时间以阿里云公告为准。
- 所需时间取决于镜像文件大小、网络传输速度、并发任务的排队数量。

  说明 如果您需要复制大容量镜像（例如大于2 TiB的镜像），可以先通过复制快照功能将快照复制到目标地域，再在目标地域使用快照创建镜像。具体操作，请参见复制快照和使用快照创建自定义镜像。

- 新镜像会丢失源镜像设置过的角色授权、服务授权、实例自定义数据等功能配置。

操作步骤

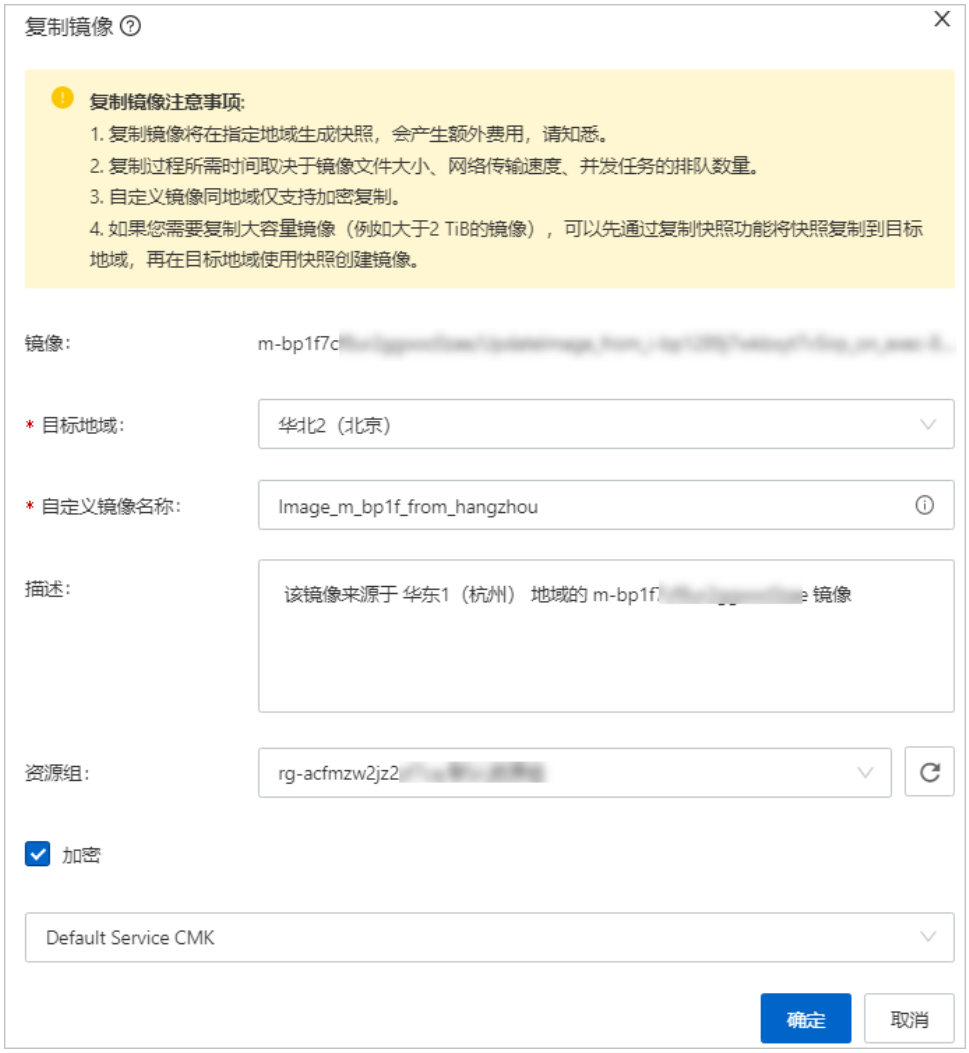
1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。

4. 在**镜像**页面，选择**自定义镜像**页签。
5. 选择需要复制的镜像，在**操作**列中，单击**复制镜像**。
6. 在**复制镜像**对话框中，完成以下配置。
   i. 确认选中的自定义镜像的ID。
   ii. 在**目标地域**的下拉列表中，选择一个地域，可以是同地域也可以跨地域。
   iii. 填写镜像在目标地域显示的**自定义镜像名称**，例如Image_m_bp1f_from_hangzhou。
   iv. （可选）填写镜像在目标地域显示的**描述**。
   v. （可选）选择资源组。
   vi. （可选）选中**加密**，在下拉列表中选择密钥Default Service CMK。

   Default Service CMK表示使用密钥管理服务KMS创建的默认密钥。

   > **说明** 在同地域复制自定义镜像时，仅支持加密复制，即您需要选中**加密**属性并选择加密密钥。

   vii. 单击**确定**。



7. 查看结果以及管理任务。

i. 在顶部菜单栏左上角处，切换到目标地域，查看自定义镜像的复制进度。
当进度显示为100%，镜像状态变为**可用**时，说明任务完成。目标地域生成一个新镜像，该镜像具有唯一的镜像ID。

ii. （可选）如果**进度**不是100%，**状态**为**创建中**时，您可以随时单击**取消复制**。

> **说明** 复制加密镜像的过程中不支持取消复制。

后续步骤

您可以使用复制的镜像创建实例或更换系统盘：

- 使用自定义镜像创建实例
- 更换操作系统（非公共镜像）

相关文档

- CopyImage
- CancelCopyImage
- 复制快照

6.6. 共享或取消共享镜像

共享镜像可用于跨账号部署ECS实例。创建自定义镜像后，您可以将镜像共享给其他阿里云账号使用。该账号可以使用您共享的自定义镜像，快速创建运行同一镜像环境的ECS实例。不再需要共享镜像给其他账号时，您可以取消共享镜像。

前提条件

共享镜像之前，请确认自定义镜像已清除敏感数据和文件。

背景信息

共享镜像不会占用被共享者的镜像额度，阿里云也不会向被共享者收取镜像共享费用。

被共享者使用您共享的镜像创建ECS实例，不会向您收取实例产生的费用，只会向被共享者收取该费用。共享镜像的计费详情，请参见费用详情。

被共享者只能使用共享镜像，无法删除镜像。如需删除共享镜像，您需要先取消共享后再删除。更多详情，请参见删除自定义镜像。

共享镜像前，请仔细阅读以下注意事项：

- 您只能共享自己的自定义镜像，其他用户共享给您的镜像无法再次共享。
- 每份自定义镜像最多可以共享给50个用户。
- 支持中国站、国际站和日本站账号之间共享镜像，但是基于镜像市场镜像创建的自定义镜像除外。
- 不支持跨地域共享镜像。如果您需要跨地域共享镜像，请先复制镜像到目标地域后再共享。更多详情，请参见复制镜像。
- ECS无法保证共享镜像的完整性和安全性，使用共享镜像时请确认镜像来自于可信任的共享者或共享账号，并需要自行承担风险。
- 加密自定义镜像在被共享之前，您需要通过阿里云访问控制进行相关授权。具体操作，请参见如何共享加

密自定义镜像？。

> **说明** 如果ECS实例挂载的云盘开启了加密功能，则通过该ECS实例所创建的自定义镜像为加密自定义镜像。关于加密功能的相关说明，请参见加密概述。

共享镜像

完成以下操作，将您的自定义镜像共享给其他阿里云账号。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义镜像**页签，选中待共享的自定义镜像。在**操作**栏，单击**共享镜像**。
5. 在**共享镜像**对话框中，输入待共享用户的账号ID并选中提示信息，然后单击**共享镜像**。

   仅支持共享给阿里云账号，不支持共享给RAM用户。阿里云账号ID的获取方式为：将鼠标移至控制台右上角的用户头像，在弹出的用户信息框中，如果标识了账号为**主账号**，则显示的账号ID即为阿里云账号ID。

   您成功共享镜像后，被共享者可以在ECS管理控制台同一地域中，选择**实例与镜像 > 镜像**页面，单击**共享镜像**页签，查看到共享镜像，并且被共享者可以进行以下操作：

   - 使用您共享的镜像创建一台或多台实例。
     创建实例时，在镜像区域，选择共享镜像即可。具体操作，请参见使用向导创建实例。
   - 使用您共享的镜像为实例更换系统盘。
     具体操作，请参见更换操作系统（非公共镜像）。

取消共享镜像

完成以下操作，取消共享您的自定义镜像给其他阿里云账号。

> **注意** 取消共享后：
> - 被共享者无法通过ECS管理控制台或ECS API查询到该镜像。
> - 被共享者无法使用该镜像创建实例和更换系统盘。
> - 被共享者使用共享镜像创建的实例无法重新初始化云盘。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义镜像**页签，选中待共享的自定义镜像。在**操作**栏，单击**共享镜像**。
5. 在**共享镜像**对话框中，找到待取消共享镜像的账号ID后，单击对应的**取消共享**。

相关文档

- ModifyImageSharePermission
- DescribeImageSharePermission

6.7. 导出镜像

创建自定义镜像后，您可以导出镜像到OSS存储空间（OSS Bucket），并下载到本地使用。本文介绍导出自定义镜像的操作步骤及相关注意事项。

前提条件

- 自定义镜像所在地域中已有可用的OSS Bucket。
  若尚未创建OSS Bucket，请先创建存储空间。

  > **说明** 导出自定义镜像会产生一定的OSS存储和下载的流量费用。计费详情，请参见计费概述。

- 待导出的自定义镜像满足以下限制条件：

- 不是基于镜像市场镜像创建的自定义镜像。
- 不能包含Windows Server系列操作系统。
- 不能包含四块以上数据盘快照，单块数据盘容量最大不能超过500GiB。

> **说明** 如果单块数据盘的容量超过500 GiB，请先将该盘中的数据分散转移到多个小于500 GiB的数据盘中，再使用小于500 GiB的数据盘创建和导出自定义镜像。

背景信息

导出自定义镜像的注意事项如下：

- 导出镜像所需时间取决于自定义镜像文件的大小和当前导出任务的并发数，需要您耐心等待。
- 导出的自定义镜像包含数据盘快照时，您的OSS Bucket中会出现多个文件。
  文件名带有*system*的表示系统盘快照，文件名带有*data*的表示数据盘快照。数据盘快照会有与数据盘对应的标识，即数据盘的挂载点，如xvdb或者xvdc。
- 使用导出的全镜像创建相同配置的Linux系统时，您需要确认*/etc/fstab*中记录的文件设备是否与导出的数据盘快照信息互相对应。
- 如果创建自定义镜像时云盘内无数据，那么导出镜像后解压缩也无数据。
- 导出后的镜像不能保证在其他平台正常启动，但您可以挂载镜像中的磁盘获取数据。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 授权ECS服务访问OSS的权限。
   i. 找到要导出的目标镜像，在**操作**栏，单击⋮图标，然后单击**导出镜像**。
   ii. 在**导出镜像**对话框，单击提示信息里的**确认地址**。

   iii. 在**云资源访问授权**对话框，单击**同意授权**授权ECS服务访问您的OSS资源。
5. 在左侧导航栏，选择**实例与镜像 > 镜像**。
6. 在**自定义镜像列表**页签，找到目标镜像，在**操作**列，再次单击**更多 > 导出镜像**。
7. 在**导出镜像**对话框，配置如下参数。
   - 选择镜像导出的格式，支持RAW、VHD、QCOW2、VDI和VMDK。

     > **说明** 选择镜像导出格式功能在部分地域可用，更多地域正在逐步开放中。

   - 选择一个与自定义镜像所属地域相同的OSS Bucket。

- 为自定义镜像的Object名称设置一个前缀。例如，将Demo设为前缀，则导出自定义镜像文件后，在OSS Bucket中的名称即为*Demo-[系统自动生成的文件名]*。

8. 单击**确定**，开始导出自定义镜像。

   在任务完成前，您都可以通过任务管理，在相应地域下找到导出自定义镜像的任务，取消导出自定义镜像。

后续步骤

下载自定义镜像。具体操作步骤，请参见下载自定义镜像文件。

> **说明** 如果您选择RAW作为镜像格式，导出后镜像文件扩展名默认为*.raw.tar.gz*，解压后扩展名为*.raw*。如果您的本地计算机为Mac OS X系统，推荐您使用gnu-tar解压工具。

相关文档

- ExportImage
- CancelTask

6.8. 修改自定义镜像信息

为了方便您管理自定义镜像，您可以根据需要修改自定义镜像的名称和描述。

前提条件

您已成功创建自定义镜像或已提交自定义镜像创建请求。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像** > **镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像**页面，单击**自定义镜像**页签，找到待修改的自定义镜像，修改名称和描述。
   - 修改名称
     a. 鼠标移动到待修改的镜像名称上，单击出现的图标。
     b. 在**镜像名称**文本框中填写新的镜像名称，单击**确定**。
   - 修改描述
     a. 在**操作**栏，单击图标，然后单击**编辑描述**。
     b. 在**编辑描述**对话框中，输入新的镜像描述，单击**确定**。

相关文档

- ModifyImageAttribute

6.9. 编辑自定义镜像标签

标签用于标识具有相同特征的资源，例如所属组织相同或用途相同的自定义镜像，您可以基于标签方便地检索和管理资源。本文介绍如何编辑已有自定义镜像的标签。

背景信息

标签的使用说明、支持资源、使用限制等信息，请参见标签概述和标签使用限制。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义镜像**页签，找到目标自定义镜像，在**标签**列将鼠标悬浮至 图标。
   - 如果自定义镜像尚未绑定标签，单击**添加**。
   - 如果自定义镜像已经绑定了标签，单击**编辑**。
5. 在**编辑标签绑定**对话框，选择已有标签或新建标签，然后单击**确定**。

后续步骤

绑定标签后，您可以基于标签筛选自定义镜像并完成各种管理动作，例如复制一类镜像、更新一类镜像等。

6.10. 删除自定义镜像

如果您不再需要某个自定义镜像，可以将其删除。

背景信息

删除自定义镜像前，请注意以下事项。

- 删除自定义镜像后，不能再使用该镜像创建实例。
- 删除自定义镜像后，已使用该镜像创建的实例：
  - 仍可正常使用，并会继续产生费用。
  - 将无法重新初始化系统盘。
- 删除共享镜像前，需预先解除该镜像的全部共享关系。删除共享镜像后：
  - 被共享者无法通过ECS管理控制台或ECS API查询到该镜像。
  - 被共享者无法使用该镜像创建实例和更换系统盘。
  - 被共享者使用共享镜像创建的实例无法重新初始化系统盘。
- 删除复制镜像的源镜像，对复制后的镜像没有影响。同样，删除复制后的自定义镜像，不影响源镜像。
- 删除自定义镜像，不会删除镜像中包含的快照，如不想保留快照，可同时在快照列表中删除对应快照。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义镜像**页面，选中一个或者多个需删除的**自定义镜像**，单击页面底部的**删除镜像**。
5. 在弹出的对话框中，勾选**确定要强制删除**。
6. 单击**确定**。

相关文档

- DeleteImage

6.11. 自定义镜像检测项说明

镜像检测功能主要检测导入的自定义镜像是否为有效镜像、自定义镜像是否可以创建出功能齐全的ECS实例等。自定义镜像检测功能会在镜像导入后立即执行。检测完成后，您可以在镜像控制台查看镜像检测结果，并可针对检测结果中的修复建议进行修复。

自定义镜像检测项说明及修复建议如下表所示。

检测项	检测说明	修复建议
GUESTOS.Platform	系统平台，包括Linux、Windows等。	无
GUESTOS.OSVersion	系统版本。	无
GUESTOS.Architecture	系统架构。	无
GUESTOS.RtcTimeMode	镜像硬件时钟时区RTC (Real Time Clock)，包括UTC和local。建议设置为标准的UTC模式。	如何设置硬件时钟的时间标准为UTC，请参见Linux时间和时区说明。
GUESTOS.BootMode	镜像启动模式，包括LEGACY和UEFI。	无
GUESTOS.KernelVersion	内核版本。	无
GUESTOS.Virtio	镜像中virtio驱动是否安装。ECS实例运行依赖相关虚拟化设备驱动，未安装该驱动会导致实例启动异常。	如何为镜像安装virtio 驱动，请参见安装virtio驱动。
GUESTOS.Nvme	镜像中NVMe驱动是否安装。部分ECS规格，例如ecs.g7se使用基于NVMe协议挂载的云盘，镜像中需要安装有相关驱动。	如何为镜像安装nvme驱动，请参见Linux自定义镜像如何适配NVMe系统盘？。
GUESTOS.Fstab	镜像中*/etc/fstab*文件配置了系统磁盘设备挂载信息，错误的配置会导致系统启动异常，例如配置的挂载设备信息不存在、设备UUID错误等。	如何配置正确的*/etc/fstab*，请参见如何在fstab文件中配置文件磁盘标识方式为UUID。
GUESTOS.Grub	镜像中grub引导文件是否正常。例如device设备配置异常、相关设备不存在、UUID错误等，会导致系统启动异常。	如何为镜像生成正确地配置grub文件，请参见如何修改Linux镜像Grub文件中的文件磁盘标识符为UUID。
GUESTOS.Dhcp	镜像中网络配置文件是否设置网络设置使用DHCP模式，如果镜像中设置为静态模式，会导致实例启动后网络配置异常。	如何设置镜像网络配置模式为DHCP，请参见如何在Linux镜像中配置网络为DHCP。
GUESTOS.Selinux	镜像是否关闭SELinux。云上镜像不建议开启SELinux，有可能会导致系统启动异常。	如何关闭SELinux，请参见开启或关闭SELinux。

检测项	检测说明	修复建议
GUEST OS.OnlineResizeFS	镜像是否支持根分区自动扩容。镜像中安装有cloud-init、growpart命令等，使用镜像创建实例后，根分区会自动扩容。例如您的镜像空间大小是20 GB，创建实例时系统盘大小为100 GB，则实例创建后，根分区会自动扩容至100 GB。	如何配置镜像支持自动扩容，请参见安装cloud-init。
GUEST OS.SystemImage	镜像是否是有效的系统盘镜像，请不要导入ISO镜像、空镜像等无效镜像。	无
GUEST OS.CloudAssistant	镜像是否安装云助手。云助手是为ECS打造的原生自动化运维工具，通过免密码、免登录、无需使用跳板机的形式，在ECS实例上实现批量运维、执行命令（Shell、PowerShell和Bat等）和发送文件等操作。建议您在镜像中安装云助手，帮助您高效运维ECS。	如何安装云助手，请参见安装云助手客户端。
GUEST OS.CloudInit	镜像中是否安装cloud-init。cloud-init是标准的云服务器初始化配置服务，为实例配置hostname、密钥、根分区扩容等。	如何为镜像安装cloud-init，请参见安装cloud-init。
GUEST OS.SecurityCenterAgent	镜像是否安装云安全中心Agent。云安全中心作为一个实时识别、分析和预警安全威胁的统一安全管理系统，为您提供安全态势总览、防勒索、防病毒、防篡改、合规检查等安全能力，全方位检测和防护您的服务器和Web应用安全。	如何为镜像安装云安全中心Agent，请参见安装Agent。

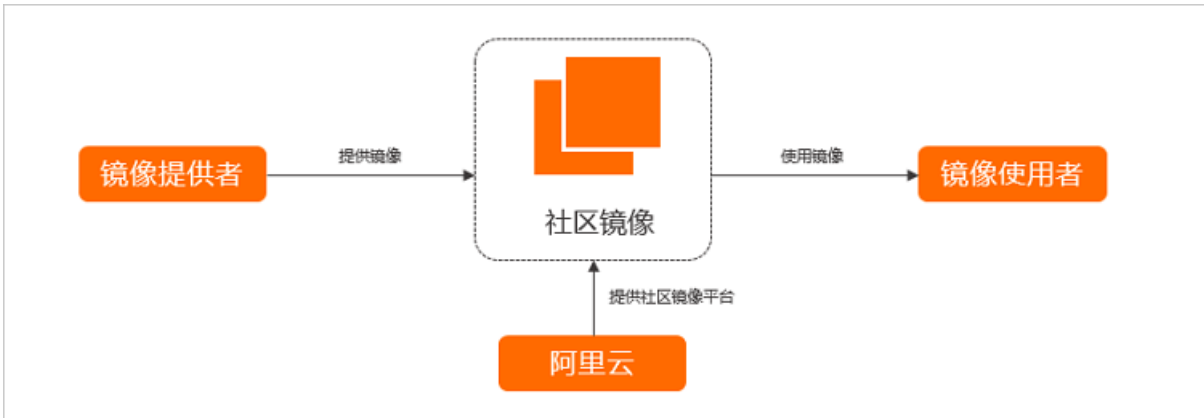
7.社区镜像

7.1. 社区镜像概述

社区镜像是一种完全公开的镜像。您可以将制作好的自定义镜像发布为社区镜像供他人使用，也可以获取并使用他人发布的社区镜像。

简介

社区镜像由以下三方共同参与：



其中：

- 阿里云：仅提供平台支撑，社区镜像由镜像提供者发布并负责。
- 镜像提供者：制作自定义镜像并发布为社区镜像，供他人使用。
- 镜像使用者：通过社区镜像可以获取更丰富的镜像种类。

相关操作

社区镜像支持的操作说明如下：

操作	说明	相关文档
发布社区镜像	您可以将可用状态的自定义镜像发布为社区镜像。	发布社区镜像
查找社区镜像	您可以通过社区镜像的名称、ID或OwnerId查找指定的社区镜像，进而使用该镜像来创建ECS实例。	查找社区镜像
使用社区镜像	您可以使用社区镜像快速部署与业务需求匹配的操作系统、应用程序和数据的ECS实例。	使用社区镜像
下架社区镜像	当您需要更新已发布的社区镜像版本或者不再维护社区镜像时，可以将当前已发布的社区镜像下架。	下架社区镜像

7.2. 发布社区镜像

您可以将可用状态的自定义镜像发布为社区镜像。本文介绍如何通过控制台发布社区镜像。

前提条件

- 社区镜像的所有者需要为对应镜像的质量与迭代负责，阿里云仅提供平台支撑。因此，在发布前请确保您

已充分了解*Product terms*、*Term of use*以及*Membership agreement*。

- 已检查并确认待发布的社区镜像名称与描述无敏感词、镜像内无木马病毒与漏洞、无弱口令。

背景信息

在您发布社区镜像前，请先了解以下注意事项：

- 社区镜像正在邀测中，如需使用请提交工单。
- 加密镜像不允许发布为社区镜像。
- 您必须签署*Product terms*、*Term of use*以及*Membership agreement*，否则不允许发布社区镜像。
- 社区镜像完全公开，在镜像所属地域下，其他所有的阿里云账号均可使用。
- 社区镜像不支持共享、导出与复制。

操作步骤

1. 进入镜像功能页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**实例与镜像 > 镜像**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 在**自定义镜像**页签，找到待发布为社区镜像的可用自定义镜像，然后在**操作**列，鼠标悬浮至⋮图标并单击**发布为社区镜像**。
3. 在**发布为社区镜像**对话框，完成社区镜像的发布。
   - 如果您之前未签署*社区镜像协议*，需要先选中**您已签署并同意以下协议**前的复选框，然后单击**发布**。

     > **注意** 请您仔细阅读*Product terms*、*Term of use*以及*Membership agreement*的内容，确认后签署协议。

   - 如果您之前已签署了协议，单击**确认**。

   发布成功后，您可以在**镜像**页面，单击**社区镜像**页签，查看已发布的社区镜像信息。

7.3. 查找社区镜像

您可以通过社区镜像的名称、ID或OwnerId查找指定的社区镜像，进而使用该镜像来创建ECS实例。本文介绍如何通过控制台查找社区镜像。

背景信息

社区镜像正在邀测中，如需使用请提交工单。

操作步骤

1. 进入镜像功能页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**实例与镜像 > 镜像**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 单击**社区镜像**页签。

   在**社区镜像**页签内，可以直接查看当前地域下的全部社区镜像。

3. 在搜索栏区域，查询指定的社区镜像信息。

   具体操作如下所示：

   i. 在①区域，选择搜索类型。支持的类型如下所示：
      - 镜像名称
      - 镜像ID
      - 社区镜像OwnerId
   ii. 在②区域，输入与搜索类型匹配的搜索值。
   iii. 在③区域，单击进行查询。

   例如，搜索镜像ID时，输入 `m-bp10pa9j0rio19ky****` 。查询结果如下所示：

后续步骤

您可以通过社区镜像创建ECS实例。更多信息，请参见使用社区镜像。

7.4. 使用社区镜像

您可以使用社区镜像快速部署与业务需求匹配的操作系统、应用程序和数据的ECS实例。本文介绍如何通过社区镜像创建ECS实例。

背景信息

如果您使用的社区镜像下架，则使用该社区镜像创建的ECS实例将无法重新初始化云盘。

操作步骤

1. 进入镜像功能页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**实例与镜像 > 镜像**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 单击**社区镜像**页签，查找您需要的社区镜像。

   具体的查找方式，请参见查找社区镜像。
3. 在查找到的社区镜像的**操作**列，单击**创建实例**。

4. 在云服务器ECS售卖页，完成ECS实例的创建。

   配置项说明：

   - 系统已默认指定了地域与社区镜像。
     如果您已知其它社区镜像的ID以及所属地域，也可以手动配置地域与镜像的信息。
   - 请根据业务需要，配置其他信息。具体操作，请参见使用向导创建实例。

7.5. 下架社区镜像

当您需要更新已发布的社区镜像版本或者不再维护社区镜像时，可以将当前已发布的社区镜像下架。本文介绍如何通过控制台下架社区镜像。

背景信息

下架社区镜像前，请您了解以下注意事项：

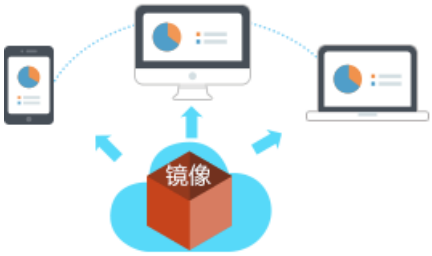
- 社区镜像正在邀测中，如需使用请提交工单。
- 已发布的社区镜像一旦下架，将不再对其他所有的阿里云账号公开。如果镜像已共享至其它阿里云账号，共享关系会继续保持。
- 当社区镜像下架后，已使用社区镜像创建的ECS实例将无法重新初始化云盘。

操作步骤

1. 进入镜像功能页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**实例与镜像 > 镜像**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 在**自定义镜像**页签，找到已发布为社区镜像的自定义镜像，然后在**操作**列，鼠标悬浮至⋮图标并单击**下架社区镜像**。
3. 在**下架社区镜像**对话框，确认镜像信息，然后单击**确定**。
   下架成功后，在**镜像**页面，系统将提示**镜像已从社区镜像下架**。

8.镜像市场

您可以购买镜像市场的镜像创建实例，快速获得预装的ECS实例的运行环境或软件应用，满足建站、应用开发、可视化管理等个性化需求，让ECS即开即用，省时方便。



阿里云镜像市场是指阿里云建立的、由镜像服务商ISV（Independent Software Vendor）向用户提供镜像及相关服务的网络平台。镜像市场的镜像在操作系统中整合了具体的软件环境和功能，如PHP运行环境及配套的管理软件等，供有相关需求的用户开通实例时选用。更多详情，请参见了解镜像市场。

使用镜像市场的镜像创建实例

您可以通过以下两种方式，使用镜像市场的镜像创建实例。具体操作，请参见创建ECS实例。

- 方式一：创建实例时，选择镜像市场的镜像。

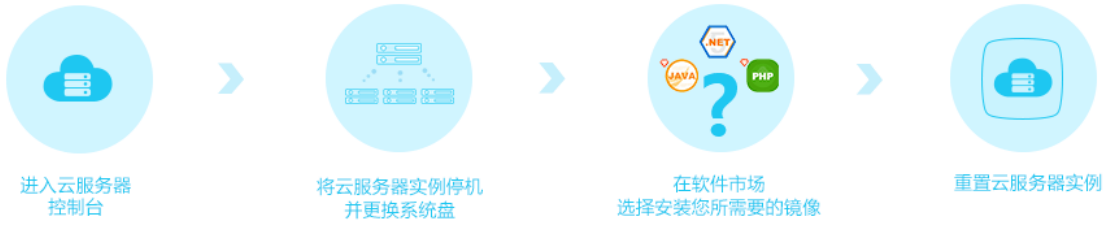
- 方式二：前往云市场购买镜像后创建实例。

> **说明** 使用镜像市场的镜像创建实例后，如果出现许可证失效等问题，您可以联系镜像提供服务商获得技术支持。

使用镜像市场的镜像更换操作系统

若您已购买了ECS实例，需要将实例的镜像更换为镜像市场的镜像，您可以更换系统盘。

更换系统盘时，在**更换系统盘**页面的**镜像类型**处选择**镜像市场**，并在**镜像市场**页面中选择您所需的镜像。具体步骤，请参见更换系统盘（非公共镜像）。



9.镜像族系

9.1. 镜像族系概述

阿里云提供了镜像族系（ImageFamily）功能，帮助您实现镜像平滑更新与回滚。您可以将更新的镜像设置镜像族系，通过镜像族系创建ECS实例时不再需要获取更新后的镜像ID，系统会自动选取镜像族系内可用的最新自定义镜像。您也可以通过弃用镜像族系内可用的最新自定义镜像，实现镜像回滚。

功能特性

- 当您通过RunInstances或CreateInstance接口创建ECS实例时，无需设置镜像ID参数 `ImageId` ，只需要设置镜像族系参数 `ImageFamily` ，系统会自动使用镜像族系中可用的最新自定义镜像创建ECS实例。
- 如果您想回滚镜像族系内的镜像，只需要将镜像族系内可用的最新自定义镜像设置为弃用或直接删除，然后通过镜像族系创建ECS实例即可实现镜像回滚。
- 镜像族系中弃用状态的镜像可以通过控制台或调用API ModifyImageAttribute恢复可用状态。

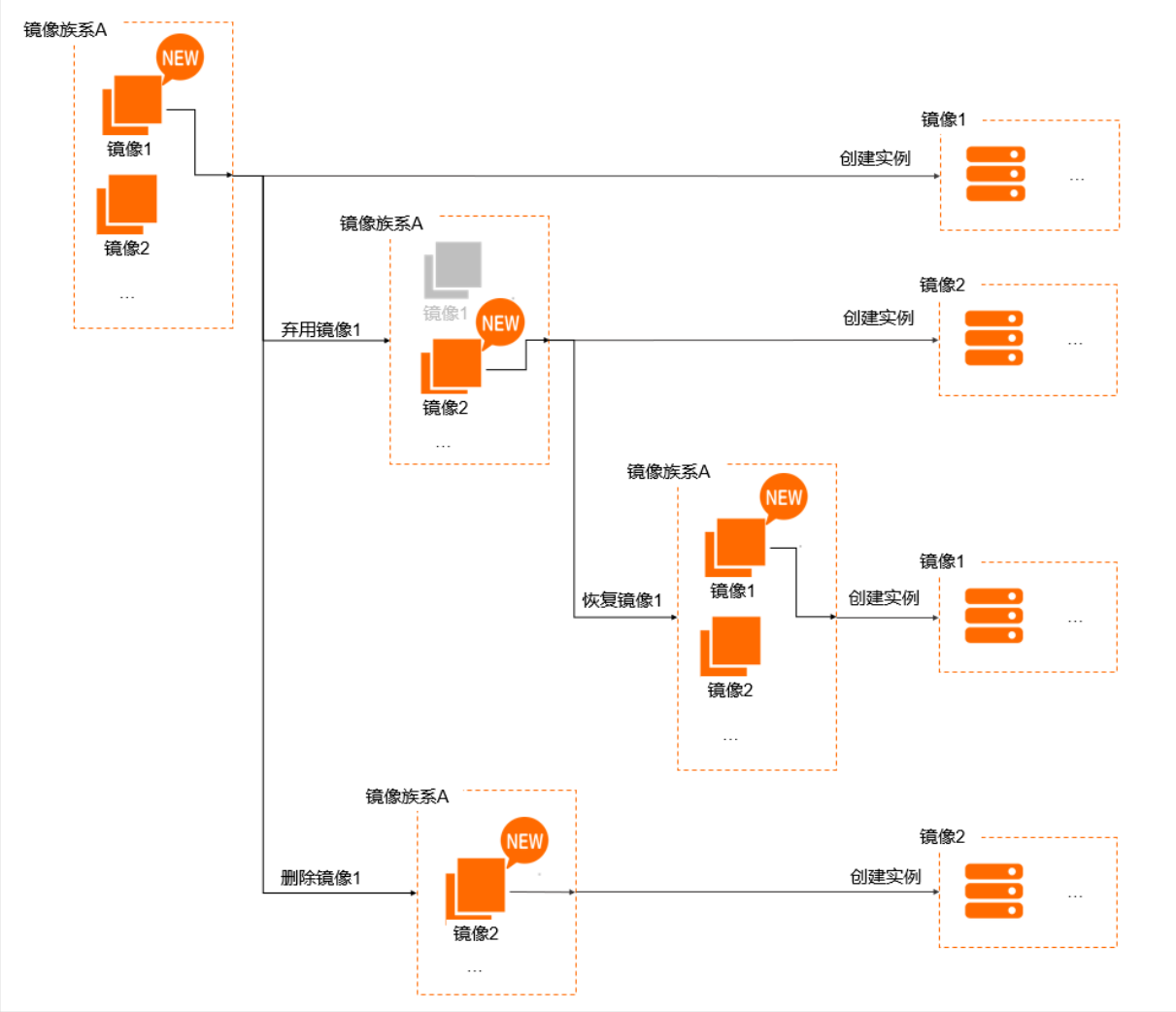
使用限制

- 只有自定义镜像能够设置镜像族系。
- 自定义镜像一旦设置镜像族系，支持修改但不支持删除镜像族系。
- 同一账号相同地域下，镜像族系名称唯一；不同地域下，允许存在相同的镜像族系名称。
- 同一个镜像族系内镜像数量不能超过100个。
- 同一个地域下，存在镜像的镜像族系数量不能超过100个。
- 如果自定义镜像已经共享给其它用户，需要先取消共享才可以修改为弃用状态。
- 弃用状态的自定义镜像可以进行创建实例、更换系统盘操作，但是不允许进行复制镜像或共享镜像。

使用说明

- 在使用镜像族系功能之前，需要先通过控制台或API为镜像设置镜像族系，具体操作请参见设置镜像族系。
- 只能通过API设置镜像族系创建ECS实例，系统会自动选择镜像族系内可用的最新自定义镜像，具体操作请参见通过镜像族系创建ECS实例。
- 镜像族系中的镜像可以弃用与恢复可用，弃用镜像能够实现镜像回滚，详情请参见弃用镜像或恢复可用镜像。
- 您可以调用API DescribeImageFromFamily查询指定镜像族系内最新的镜像，详情请参见DescribeImageFromFamily。

镜像族系的典型使用流程如下图所示。



相关文档

- RunInstances
- CreateInstance
- CreateImage
- DescribeImages
- ModifyImageAttribute

9.2. 设置镜像族系

本文分别介绍如何通过ECS控制台或调用API设置镜像族系。

前提条件

您已经创建ECS实例或已经创建了系统盘快照，具体操作请参见创建方式导航或创建一个云盘快照。

背景信息

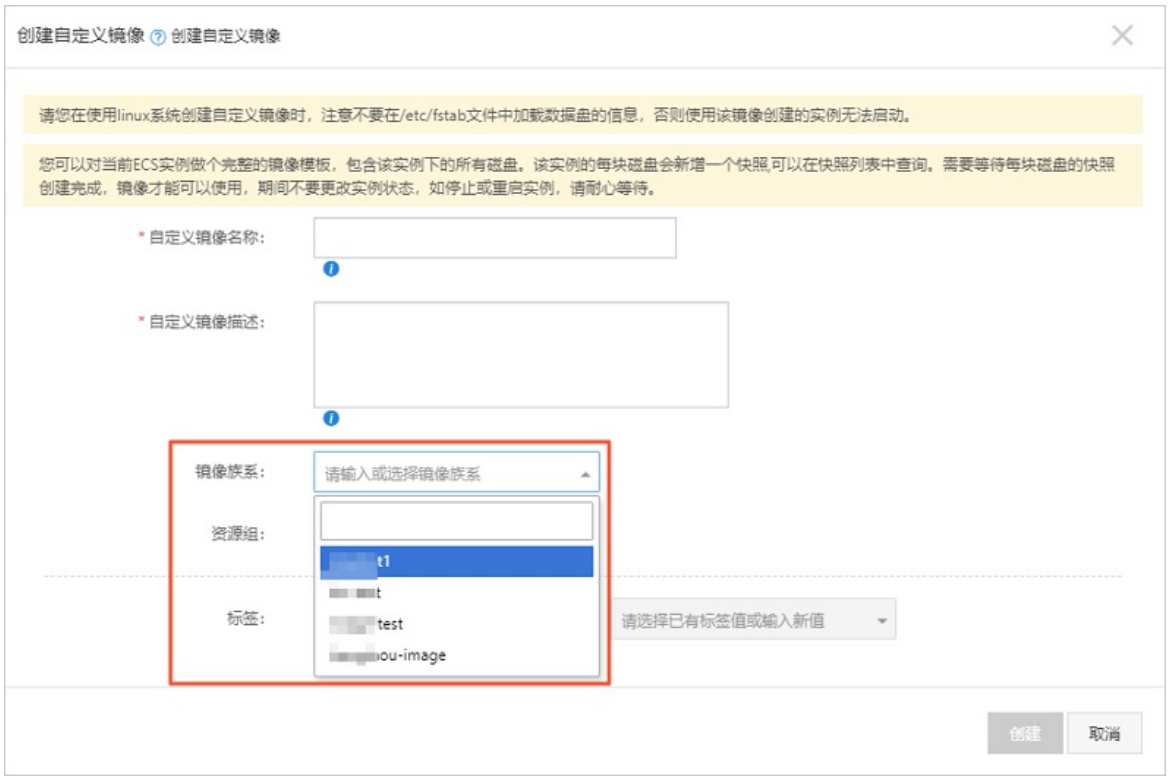
镜像族系不能单独创建，需要在创建自定义镜像时设置镜像族系。如果设置的镜像族系不存在，将会自动生成镜像族系。如果设置的镜像族系已存在，则自定义镜像将选择该镜像族系。

通过控制台设置镜像族系

1. 登录ECS管理控制台。
2. 在顶部菜单栏左上角处，选择地域。
3. 通过以下任意一种方式创建自定义镜像。
   - 在左侧导航栏中，单击**实例与镜像 > 实例**，通过实例创建自定义镜像，具体操作，请参见使用实例创建自定义镜像。
   - 在左侧导航栏中，单击**存储与快照 > 快照**，通过快照创建自定义镜像，具体操作，请参见使用快照创建自定义镜像。

   在创建自定义镜像过程中，需要在**创建自定义镜像**对话框内，为自定义镜像设置**镜像族系**。
   您可以输入自定义名称创建新的镜像族系，也可以选择已有的镜像族系。

   > **说明** 镜像族系的名称长度为2~128个英文或中文字符。必须以大小字母或中文开头，不能以http://、https://、acs:和aliyun开头。可以包含数字、半角冒号（:）、下划线（_）或者连字符（-）。



4. 在左侧导航栏中，单击**实例与镜像 > 镜像**，查看创建的自定义镜像以及对应的镜像族系信息。

   在**镜像族系**区域，搜索镜像族系或单击相应的镜像族系名称，查找对应的镜像信息。

通过API设置镜像族系

本节将调用CreateImage在创建自定义镜像时设置镜像族系，接口详情请参见CreateImage。

1. 登录OpenAPI开发者门户。
2. 查找并调用CreateImage接口创建自定义镜像并设置镜像族系。

   在本示例中，通过实例创建自定义镜像，设置名为 `hangzhou-image` 的镜像族系。API的请求参数说明如下：

   - RegionId：选择地域。例如， `cn-hangzhou` ，即华东1（杭州）。
   - InstanceId：实例ID。例如， `i-bp117mtgmllecpwl****` 。
   - ImageFamily：镜像族系名称。本示例中使用 `hangzhou-image` 。

   创建成功后得到自定义镜像ID。

```
{
    "RequestId": "46BC46F8-922C-4419-8B5D-E713F663E00A",
    "ImageId": "m-bp1h[redacted]"
}
```

3. 查找并调用DescribeImages接口查询上一步创建的镜像所属镜像族系。接口详情请参见DescribeImages。

   通过镜像ID查询，API的请求参数说明如下：

   - RegionId：选择与上一步相同的地域。
   - ImageId：镜像ID，输入上一步中创建好的自定义镜像ID。

   返回值的部分结果示例如下，镜像族系参数 `ImageFamily` 值为 `hangzhou-image` 。

```
},
"Status": "Available",
"Progress": "100%",
"Usage": "none",
"Architecture": "x86_64",
"ProductCode": "",
"IsCopied": false,
"ImageFamily": "hangzhou-image",
"IsSupportIoOptimized": true,
"IsSupportCloudinit": true,
"ImageName": "m-bp1h46wfpj[redacted]",
"DiskDeviceMappings": {
    "DiskDeviceMapping": [
        {
            "SnapshotId": "s-bp1h4[redacted]",
            "Type": "system",
            "Progress": "",
```

后续步骤

当您需要修改镜像的镜像族系时，可以通过调用API ModifyImageAttribute实现，详情请参见ModifyImageAttribute。

相关文档

- DescribeImageFromFamily

9.3. 通过镜像族系创建ECS实例

本文介绍如何通过镜像族系创建ECS实例。目前只支持通过调用RunInstances或CreateInstance接口设置镜像族系参数来创建ECS实例。

前提条件

已经创建一个或多个可用的自定义镜像并设置了相同的镜像族系，具体操作，请参见设置镜像族系。本示例中镜像族系为 `image-test` 。

背景信息

通过镜像族系创建ECS实例时，系统会自动选取镜像族系内可用的最新自定义镜像。最新自定义镜像的判断依据为镜像族系内可用自定义镜像的创建时间，创建时间最晚的自定义镜像为最新自定义镜像。例如，您的镜像族系内有两个可用的自定义镜像。一个是2020年01月01日创建的，另一个是2020年01月03日创建的，那么通过该镜像族系创建ECS实例时，系统将默认选择2020年01月03日创建的自定义镜像。

创建ECS实例的接口详情请参见RunInstances或CreateInstance。本文以RunInstances接口为例创建ECS实例。

使用API RunInstances创建ECS实例

1. 登录OpenAPI开发者门户。
2. 查找并调用RunInstances接口创建一台ECS实例。

   本示例中，通过镜像族系 `image-test` 创建ECS示例，API的请求参数说明如下：

   - RegionId：选择地域。例如， `cn-hangzhou` ，即华东1（杭州）。
   - InstanceType：实例规格。例如， `ecs.g6.large` 。
   - ImageFamily：镜像族系。本示例使用 `image-test` 。
   - SecurityGroupId：安全组ID。例如， `sg-bp1i4c0xgqxadew2****` 。
   - VSwitchId：交换机ID。例如， `vsw-bp1ddbrxdlrcbim46****` 。

   调用结果示例如下，得到创建的实例ID。

```
{
    "RequestId": "409D4604-84D0-4F16-B99E-809E2E72****",
    "InstanceIdSets": {
        "InstanceIdSet": [
            "i-bp1env7nl3mijm2t****"
        ]
    }
}
```

通过调用API验证镜像信息

1. 登录OpenAPI开发者门户。
2. 查找并调用DescribeImageFromFamily接口查询指定镜像族系内最新的镜像。

   本示例中，查询镜像族系 `image-test` 内最新的镜像，API的请求参数说明如下：

   - RegionId：选择镜像族系同一地域。
   - ImageFamily：镜像族系。本示例中使用 `image-test` 。

   返回值部分示例如下，得到最新可用自定义镜像的ID。

```
},
"ImageVersion": "",
"OSType": "linux",
"ImageId": "m-bp1[redacted]",
"CreationTime": "2020-03-17T06:19:19Z",
```

3. 查找并调用DescribeInstances接口查询实例的镜像信息。

   通过已创建的实例ID查询对应的镜像ID，判断是否为镜像族系中最新可用自定义镜像的ID。API的请求参数说明如下：

   - RegionId：选择ECS实例所在的地域。
   - InstanceIds：实例ID。格式为 `["i-bp1env7nl3mijm2t****"]` 。

   返回值的部分结果示例如下，对比实例的镜像ID与镜像族系中最新可用自定义镜像的ID一致。

```
"OSName": "CentOS  8.0 64位",
"InstanceNetworkType": "vpc",
"InnerIpAddress": {
    "IpAddress": []
},
"ExpiredTime": "2099-12-31T15:59Z",
"ImageId": "m-bp1[redacted]",
"EipAddress": {
    "AllocationId": "",
    "IpAddress": "",
    "InternetChargeType": ""
```

相关文档

- DescribeInstances
- DescribeImageFromFamily

9.4. 弃用镜像或恢复可用镜像

自定义镜像可以被设置为弃用，也可以恢复可用。通过将镜像状态设置为弃用，可以实现镜像族系内可用的自定义镜像回滚；通过将自定义镜像恢复可用，可以恢复镜像族系的最新自定义镜像。

前提条件

您已经创建两个自定义镜像，并设置在同一个镜像族系内，详情请参见设置镜像族系。本示例中镜像族系为 `image-test` ，包含两个镜像 `image1` 和 `image2` ，其中 `image2` 为可用的最新自定义镜像。

背景信息

无论自定义镜像是否设置了镜像族系，镜像的状态都可以改变。可用状态的镜像可以设置为弃用，而弃用状态的镜像也可以恢复可用。状态不同的镜像所能执行的操作也不同，具体请参见：

- 已经共享的自定义镜像，需要先取消共享才能将状态修改为弃用。
- 弃用状态的自定义镜像，可以直接创建实例或更换系统盘，但不能共享镜像或复制镜像。
- 通过将镜像族系中最新可用的自定义镜像状态设置为弃用，可以实现镜像回滚。在使用该镜像族系创建ECS实例时，将不会使用弃用状态的最新自定义镜像，而是使用除去该自定义镜像之外的最新可用自定义镜像。

> **注意** 如果您需要回滚镜像族系中的自定义镜像，可以将最新可用的自定义镜像设置为弃用状态，但如果该镜像为镜像族系中唯一一个可用状态的自定义镜像，则弃用镜像以后该镜像族系将无可用状态自定义镜像用来创建实例，因此请谨慎操作。

- 如果您需要使用镜像族系中已弃用的最新自定义镜像，将该自定义镜像恢复可用，即可作为最新可用的自定义镜像使用。

弃用镜像族系内的镜像实现镜像回滚

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 弃用镜像族系 `image-test` 中的最新版本镜像 `image2` 。
   i. 在**自定义镜像**页签的**镜像族系**区域中，通过搜索栏精确搜索 `image-test` 。
   ii. 在镜像 `image2` 的操作列，单击 ⋮ 图标，并单击**弃用镜像**。
   iii. 查看镜像 `image2` 的状态栏，显示为**弃用**。
5. 登录OpenAPI开发者门户。
6. 查找并调用DescribeImageFromFamily接口查询指定镜像族系内最新的镜像。

   本示例中，查询镜像族系 `image-test` 内最新的镜像，API的请求参数说明如下：
   - RegionId：镜像族系所在地域。
   - ImageFamily：镜像族系名称。本示例中使用 `image-test` 。

   返回值部分结果示例如下，得到可用的最新镜像名称为 `image1` ，说明实现了镜像族系内镜像回滚。

```
"OSName": "CentOS  7.2 64位",
"IsSupportIoOptimized": true,
"IsSupportCloudinit": true,
"ImageName": "image1",
"DiskDeviceMappings": {
    "DiskDeviceMapping": [
```

恢复镜像族系内的镜像

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 镜像**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义镜像**页签的**镜像族系**区域中，通过搜索栏精确搜索 `image-test` 。
5. 在弃用状态的镜像 `image2` 的操作列，单击 ⋮ 图标，并单击**恢复可用**。
6. 查看镜像 `image2` 的状态栏，显示为**可用**。

   此时镜像 `image2` 已恢复为可用的最新版本的镜像。您可以调用DescribeImageFromFamily接口查询定镜像族系内最新可用的自定义镜像。
7. 查找并调用DescribeImageFromFamily接口查询指定镜像族系内最新的镜像。

   本示例中，查询镜像族系 `image-test` 内最新的镜像，API的请求参数说明如下：

- RegionId：镜像族系所在地域。
- ImageFamily：镜像族系名称。本示例中使用 `image-test` 。

返回值部分结果示例如下，得到可用的最新镜像名称为 `image2` 。


```
"OSName": "CentOS  8.0 64位",
"IsSupportIoOptimized": true,
"IsSupportCloudinit": true,
"ImageName": "image2",
"DiskDeviceMappings": {
    "DiskDeviceMapping": [
```


相关文档

- ModifyImageAttribute
- DescribeImageFromFamily

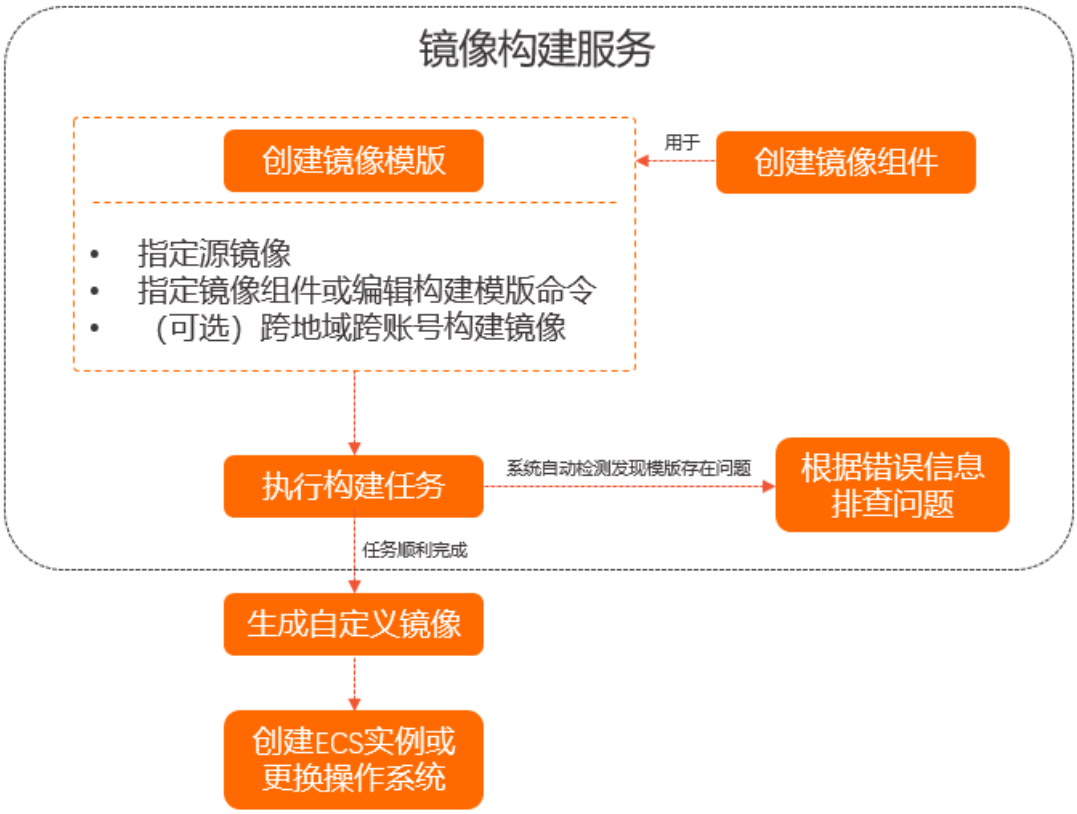
10.镜像构建服务（ImageBuilder）

10.1. 镜像构建服务（ImageBuilder）概述

镜像构建服务（Image Builder）是云服务器ECS为您提供的一站式镜像定制服务，并支持跨地域跨账号定制镜像。

简介

镜像构建服务的主要功能是镜像模版，您可以通过镜像模版完成镜像的定制、分发、共享等操作。业务流程的介绍如下所示。



1. （可选）创建镜像组件。
   镜像组件的内容由一条或多条构建模版命令组成。您可以通过复用镜像组件，快速完成镜像模版内容的定制。其中，构建模版命令是镜像构建服务提供的规范、透明的镜像定制方式。兼容Dockerfile的部分命令，更多信息，请参见镜像构建服务（ImageBuilder）指令集以及镜像构建服务（ImageBuilder）组件。
2. 创建镜像模版。
   镜像模版是镜像构建服务的主要功能，通过指定源镜像、镜像组件或构建模版命令实现对镜像内容的定制。同时支持将定制的镜像生成在指定的地域或共享至指定的阿里云账号。具体操作，请参见创建镜像模版。
3. 执行镜像构建任务。
   当您手动执行镜像模版时会生成一个构建任务，任务执行过程中会自动检测镜像模版中各配置项是否存在异常。具体操作，请参见查看与执行镜像模版。
4. 查看定制化的自定义镜像。

您可以根据业务需要，通过定制化的自定义镜像创建ECS实例或更换实例的操作系统。

计费

镜像构建服务本身不收费。通过镜像模版构建镜像时，系统会自动创建一台临时的ECS实例用于构建镜像，临时的ECS实例为按量计费实例，将收取一定的费用。更多信息，请参见按量付费。

> **说明** 临时ECS实例的各配置项默认保持系统定义的值，例如，实例规格默认按vCPU和内存最小的原则进行选择。您也可以根据业务需求手动设置临时ECS实例的各配置项。

应用场景

场景	说明
自定义镜像定制	您可以通过镜像模版，以公共镜像或已有的自定义镜像为基础，定制您需要的自定义镜像。
服务器应用运维	当您的服务器应用需要更新版本时，可以通过镜像模版实现。您只需要在镜像模版中设置源服务器的镜像信息，然后使用构建模版命令完成服务器内应用的更新即可。 您可以将每次更新应用创建的镜像模版作为一个应用版本，当您业务需要时，可以通过不同版本的镜像模版快速完成应用的更新或回滚。
镜像管理	当您的业务需要在多地域、多阿里云账号下，同步完成镜像的定制或版本迭代时，您可以通过镜像模版在完成镜像内容定制的同时，指定该镜像需要分发的地域或共享的阿里云账号。系统将帮助您在指定的地域下生成对应的镜像或将对应的镜像共享至指定的阿里云账号。

镜像构建服务典型应用场景的操作示例，请参见镜像构建服务（ImageBuilder）最佳实践。

优势

- 高效
  - 镜像构建服务兼容Dockerfile的一部分命令，便于您快速构建镜像。如果您熟悉Dockerfile命令，可以直接使用Dockerfile编辑命令，然后通过控制台导入Dockerfile模版。
  - 一站式的服务，为您节省了创建ECS实例、登录ECS实例完成运维操作，以及镜像的创建、更新、复制、共享所需的手动操作时间。
- 安全
  执行构建任务时，系统会自动帮助您检查镜像模版的各配置项是否存在异常。例如，检查中转实例的相关资源配额是否充足、构建模版命令是否正确执行等。

10.2. 镜像构建服务（ImageBuilder）指令集

本文介绍镜像构建服务支持的Dockerfile命令。

镜像构建服务所支持的命令兼容Dockerfile的一部分命令。如果您熟悉Dockerfile命令，即可快速上手使用镜像构建服务；如果您不熟悉Dockerfile命令，您可以通过本文了解镜像构建服务支持的命令。关于Dockerfile命令的详细说明，例如 `CMD` 与 `ENTRYPOINT` 命令的区别，请参见Dockerfile reference。

镜像构建服务支持的命令如下表所示。

命令	命令格式或示例	说明
FROM	• `FROM IMAGE:<镜像ID>` • `FROM IMAGE_FAMILY:<镜像族系名称>`	指定源镜像的命令。镜像组件中，不支持使用该命令；镜像模版中，当您配置源镜像后，系统会自动生成对应的 `FROM` 命令。 **说明** 在镜像模版中，如果您手动设置了 `FROM` 命令，那么配置源镜像后系统自动生成的 `FROM` 命令会被覆盖掉。
COMPONENT	`COMPONENT ic-bp18hy47cqavewsb****`	指定镜像组件，支持指定系统组件或您创建的自定义组件。该命令仅适用于镜像模版，当您创建镜像模版时，可以使用该命令，以一个或多个镜像组件拼装的方式快速完成镜像模版的定义。
RESTART	`RESTART`	重启服务器的命令，该命令后不允许添加任何内容。
RUN	`RUN echo hello;\` `echo world;`	镜像构建的命令。同一个命令允许设置多行，换行需要在前一行的末尾添加换行符（\）。
ENV	• `ENV key value` • `ENV key1="value1" key2="value2"`	系统变量配置的命令。命令以键值对的形式。 **说明** 使用 `ENV key1="value1" key2="value2"` 命令格式时，不能缺失双引号。
WORKDIR	• `WORKDIR /<path>` • `WORKDIR <path1>/<path2>`	设置工作目录的命令。
COPY	• `COPY {网络文件地址} 本地目录` • `COPY 本地文件路径 本地目录`	复制文件的命令。
USER	`USER <username>`	设置执行命令的用户的命令。 **说明** 变量 `<username>` 必须是系统中已存在的用户，否则执行命令将会报错。

命令	命令格式或示例	说明
LABEL	`LABEL user="username"\ date="2020-11-11" key="value"`	定义模版元信息的命令。同一个命令允许设置多行，换行需要在前一行的末尾添加换行符（\）。
CMD	• `CMD ["executable","param1","param2"]` • `CMD command param1 param2`	开机自启动的命令。
ENTRYPOINT	• `ENTRYPOINT ["executable","param1","param2"]` • `CMD command param1 param2`	开机自启动的命令。

10.3. 使用镜像构建服务（ImageBuilder）

10.3.1. 镜像构建服务（ImageBuilder）组件

镜像组件用于存储您在构建镜像时，常用的应用、配置、测试等命令，当您创建镜像模版时，可以在控制台选中指定的镜像组件，通过一个或多个镜像组件拼装的方式快速完成镜像模版的定义。本文介绍如何通过ECS控制台创建镜像组件。

背景信息

- 在操作前，您需要先阅读以下注意事项：
  - 仅支持创建您自定义的镜像组件。
  - 仅支持Linux操作系统的镜像。
  - 仅支持设置为镜像构建组件类型（Build）。
  - 命令内容大小不能超过16 KB，命令设置的上限为127个。
- 镜像组件的**构建模版**支持的命令详情，请参见镜像构建服务（ImageBuilder）指令集。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性** > **镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面，单击**镜像组件**页签。

   如果您第一次访问镜像构建服务，将进入**镜像构建服务**欢迎页，您需要先单击**镜像构建管理**进入**镜像构建管理**页面。
5. 单击**创建镜像组件**。

镜像组件配置项说明如下：

> **说明** 您可以通过Dockerfile导入模版，命令设置完成后可以预览模版。

- 设置镜像组件的**名称**与**描述**。
- 设置**系统类型**，目前仅支持Linux系统。
- 设置**组件类型**，目前仅支持镜像构建组件（Build）。
- 设置**标签**，便于统一管理资源。更多信息，请参见标签概述。
- 设置**构建模版**的**命令**与**内容**。

6. 完成配置后单击**创建**。
   创建成功后，您可以在**镜像组件**页签中查看镜像组件列表。镜像组件可用于创建镜像模版。具体操作，请参见创建镜像模版。

10.3.2. 创建镜像模版

您可以通过镜像模版定制镜像内容，并支持跨地域跨账号构建镜像。本文介绍如何通过ECS控制台创建镜像模版。

背景信息

- 在操作前，您需要先阅读以下注意事项：
  - 仅支持创建您自定义的镜像模版。
  - 仅支持设置Linux系统的公共镜像、自定义镜像、共享镜像或者镜像族系。
  - 通过镜像模版构建镜像时，需要创建中转实例辅助构建镜像，中转实例为按量计费的ECS实例，将收取一定的费用。更多信息，请参见按量付费。
  - 命令内容大小不能超过16 KB，命令设置的上限为127个。
- 镜像模版的**构建模版**支持的命令详情，请参见镜像构建服务（ImageBuilder）指令集。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性** > **镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面，单击**创建镜像模版**。
   如果您第一次访问镜像构建服务，将进入**镜像构建服务**欢迎页，此时请您单击**创建镜像模版**。
5. 完成镜像模版的配置项，然后单击**创建**。
   镜像模版的配置项说明如下各表所示。
   - **基本配置**区域

配置项	说明
构建模版名称	必填。镜像模版的名称。
描述	镜像模版的描述。
标签	镜像模版的标签，用于统一管理资源。更多信息，请参见标签概述。

   - **配置源镜像**区域

配置项	说明
通过Dockerfile导入模版	您可以直接通过Dockerfile导入已编辑好的模版内容，该内容会覆盖您通过ECS控制台已配置的**源镜像类型**、**镜像**和**构建模版**信息，请谨慎操作。
源镜像类型	支持设置**镜像**或**镜像族系**。
镜像或**镜像族**	必填。配置项根据**源镜像类型**的设置有所不同。 **说明** 目前仅支持选择Linux系统的镜像。 ■ **源镜像类型**为**镜像**时，第一个下拉列表支持选择**自定义镜像**、**公共镜像**、**共享镜像**。第二个下拉列表选择对应的镜像ID或镜像版本。 ■ **源镜像类型**为**镜像族系**时，需要选择指定的**镜像族**。
构建模版	需要设置**命令**与**内容**。支持的命令请参见背景信息。设置完成后可以单击**预览模版**查看模版内容。 **说明** **命令**支持选择**自定义组件**或**系统组件**，对应的**内容**为组件ID。

- **配置中转实例**区域

配置项	说明
虚拟交换机	需要配置当前地域下可使用的交换机。如果不配置系统将默认创建临时的VPC和交换机，请确保您地域下的资源配额充足。
实例规格	设置中转实例的实例规格。不设置值时，默认按vCPU和内存最小的原则，自动设置实例规格，并受实例规格的库存影响。例如，默认选择ecs.g6.large实例规格，如果库存不足，将选择ecs.g6.xlarge实例规格。
系统盘大小	中转实例的系统盘大小。取值范围为20~500 GiB，默认值40 GiB。
公网带宽/M	公网带宽默认值为0，即不具备公网访问能力。当您的镜像构建内容中存在需要访问公网的命令（例如下载命令）时，您必须设置一定值的公网带宽。否则镜像构建任务会失败。
镜像构建失败是否销毁中转实例	您可以根据需求选择是否保留中转实例。 **说明** 如果您选择保留中转实例，实例将持续计费。当您不再需要中转实例时，请及时手动释放。具体操作，请参见释放实例。

- **配置镜像分发**区域

配置项	说明
目标镜像名称	目标镜像名称前缀。最终完整的镜像名称由系统自动拼接名称前缀与构建任务ID（ExecutionId），格式为 `自定义名称前缀_构建任务ID` 。
当前地域	系统展示ECS控制台当前所在地域。
默认分发地域	如果需要将构建的镜像复制到多个地域，您可以设置分发地域，构建的镜像将会分发至指定地域。分发地域数量限制为0~20个。可以不设置分发地域。
共享UID	如果需要将构建的镜像共享至其他阿里云账号，你可以设置共享UID，构建的镜像将会共享至同地域下指定的阿里云账号。共享UID数量限制为0~20个。可以不设置共享UID。
创建后立即执行	您可以根据需求选择是否立即执行构建镜像任务。如果不立即执行，您可以手动执行任务，具体操作，请参见执行构建任务。

创建成功后，您可以在**镜像构建管理**页面查看已创建的镜像模版。

10.3.3. 查看与执行镜像模版

创建镜像模版后，您可以查看模版的详细信息。同时在详细信息页面，您也可以手动执行镜像构建任务。本文介绍如何查看模版的详细信息，以及如何手动执行镜像构建任务。

查看镜像模版

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面的**镜像模版**页签，找到需要查看的镜像模版，然后单击**模版名称**列的镜像模版ID。

   在**镜像模版详情**页面，您可以进行以下操作：
   - 查看镜像模版的**基本信息**。
   - 在**构建历史**页签，您可以查看构建任务的历史执行详情或者执行构建任务。
   - 在**查看模版**页签，查看镜像模版的内容。

执行构建任务

同一个镜像模版，同一时间只能执行一个构建镜像任务。取消构建镜像任务可同时执行多次，并且取消构建镜像任务和构建镜像任务之间互不干扰。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面的**镜像模版**页签，找到需要执行构建任务的镜像模版，然后单击**模版名称**列的镜像模版ID。
5. 在**构建历史**页签，单击**执行**。

   如果您希望取消执行中的镜像构建任务，可以单击**取消**。

构建镜像任务执行成功后，构建任务的状态会变更为通过的状态，并且生成对应的镜像ID。

> **说明** 如果状态异常，您可以查看**执行结果**的详细信息，定位并排查问题。

10.3.4. 删除镜像组件

镜像组件的内容暂不支持修改，当您创建的镜像组件存在异常时，您可以删除组件然后重新创建。此外，当您的业务需求不再需要某一镜像组件支持时，您可以直接删除该组件。本文介绍如何通过ECS控制台删除镜像组件。

背景信息

在操作前，您需要阅读以下注意事项：

- 目前仅支持删除您已创建的自定义镜像组件。
- 镜像组件被删除后，不会影响已使用该组件内容的镜像模版。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面，单击**镜像组件**页签。
5. 找到需要删除的镜像组件，在**操作**列，单击**删除**。
6. 确认要删除的镜像组件名称与ID，然后单击**确定**。

10.3.5. 删除镜像模版

镜像模版的内容暂不支持修改，当您创建的镜像模版存在异常时，您可以删除模版然后重新创建。此外，当您的业务需求不再需要某一镜像模版时，您可以直接删除该模版。本文介绍如何通过ECS控制台删除镜像模版。

前提条件

确保构建任务的状态为成功、失败或取消。如果存在运行状态的构建任务，则不允许直接删除模版。查看构建任务状态的具体操作，请参见查看镜像模版。

背景信息

镜像模版被删除后，不影响通过该模版已创建的自定义镜像的状态。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**镜像构建管理**页面，找到需要删除的镜像模版，然后在**操作**列，单击**删除**。

10.4. 镜像构建服务（ImageBuilder）最佳实践

本教程通过镜像构建服务构建Nginx开发环境的自定义镜像，并通过该镜像创建实例进行环境测试。

背景信息

镜像构建服务是阿里云提供的一站式镜像定制、构建、维护、验证、共享、分发服务。您可以使用镜像构建服务快速定制自定义镜像、快速完成镜像内应用的更新与回滚等场景。更多信息，请参见镜像构建服务（ImageBuilder）概述。

本教程中示例的资源配置说明如下所示。

- 地域：华北2（北京）
- 公共镜像：CentOS 8.2 64位
- 镜像模版构建内容：Nginx开发环境

通过以上资源配置完成镜像构建，然后使用已创建的自定义镜像创建实例，测试环境是否正常。

步骤一：创建并执行镜像模版

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
3. 在顶部菜单栏处，选择地域。
4. 在**镜像构建管理**页面，单击**创建镜像模版**。

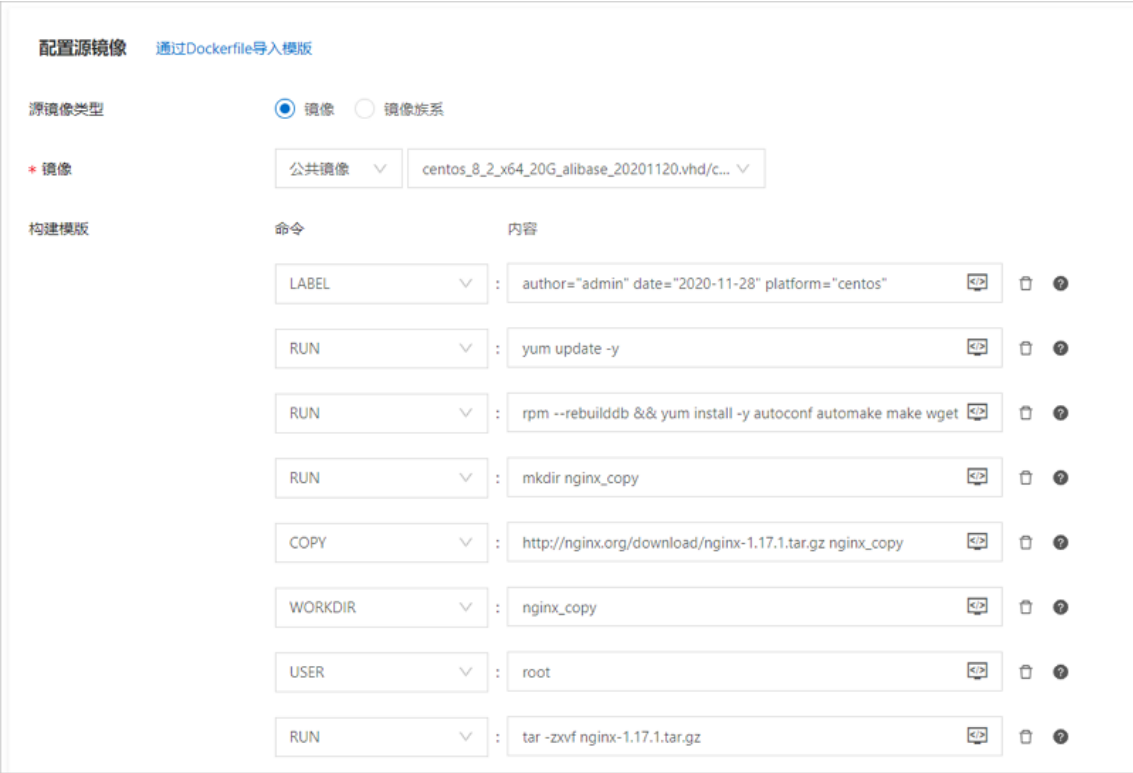
   如果您第一次访问镜像构建服务，将进入**镜像构建服务**欢迎页，此时请您单击**创建镜像模版**。
5. 配置镜像模版，完成后单击**创建**。

   本教程中，主要说明**配置源镜像**的示例配置。关于镜像模版的其它具体操作说明，请参见创建镜像模版。

   - **基本信息**：设置**构建模板名称**、**描述**及**标签**。
   - **配置源镜像**：单击**通过Dockerfile导入模版**，导入以下模版内容并单击**解析**。
     本教程中，示例模版内容如下所示。

```
FROM IMAGE:centos_8_2_x64_20G_alibase_20201120.vhd
LABEL author="admin" date="2020-11-28" platform="centos"
RUN yum update -y
RUN rpm --rebuilddb && yum install -y autoconf automake make wget net-tools zlib zlib
-devel make gcc openssl-devel pcre pcre-devel tar
RUN mkdir nginx_copy
COPY http://nginx.org/download/nginx-1.17.1.tar.gz nginx_copy
WORKDIR nginx_copy
USER root
RUN tar -zxvf nginx-1.17.1.tar.gz
ENV nginxversion nginx-1.17.1
WORKDIR $nginxversion
RUN ./configure --prefix=/usr/local/nginx && make && make install
WORKDIR /usr/local/nginx
ENTRYPOINT ["sbin/nginx","-c"]
CMD conf/nginx.conf
```

如下图所示。解析后，**镜像**和**构建模版**将自动完成配置。



- **配置中转实例**：根据您对构建镜像的需要，设置中转实例的规格、存储大小、公网带宽等资源。

  > **说明** 公网带宽默认值为0，即不具备公网访问能力。当您的镜像构建内容中存在需要访问公网的命令（例如下载命令）时，您必须设置一定值的公网带宽，否则将导致镜像构建任务失败。

- **配置镜像分发**：根据您的业务需求，可以将构建的镜像分发至指定地域或共享至指定阿里云账号。本教程中示例配置如下所示。
  - **目标镜像名称**：目标镜像名称前缀，最终生成的镜像名称会自动拼接执行任务返回的构建任务ID。本示例名称前缀设置为 `test-image` 。
  - **当前地域**：**默认分发 华北2（北京）**。
  - **默认分发地域**：华东1（杭州）。
  - **共享UID**：指定共享的阿里云账号。
  - **创建后立即执行**：选择**否**。

6. 在**镜像模版**页签，找到已创建的镜像模版，单击**模版名称**列的模版ID进入**镜像模版详情**页面。
7. 在**构建历史**页签，单击**执行**。

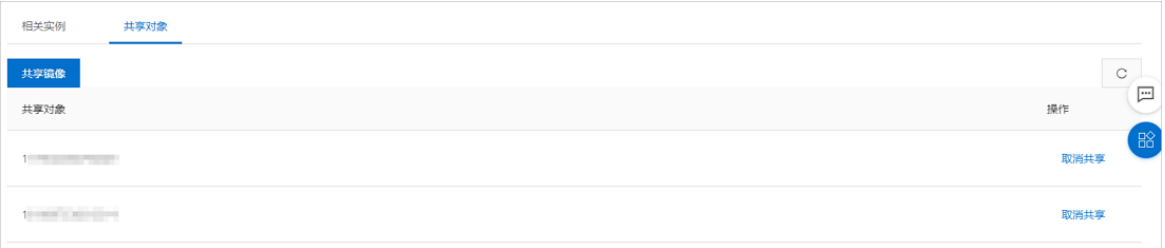
   构建镜像任务执行成功后，构建任务的状态会变更为图标 状态 状态，并且生成对应的镜像ID。

   > **说明** 如果状态异常，您可以查看**执行结果**的详细信息，定位并排查问题。

步骤二：查看构建成功的镜像

1. 在**镜像模版详情**页面的**构建历史**页签，单击镜像ID进入自定义镜像的详情页。

2. 单击**共享对象**查看已共享的阿里云账号。



3. 查看镜像分发的情况。
   i. 在左侧导航栏，单击**实例与镜像 > 镜像**。
   ii. 在顶部菜单栏处，选择镜像分发的地域。
   本示例中选择**华东1（杭州）**。
   iii. 在**自定义镜像**页签的**镜像名称**下拉列表后，通过搜索栏搜索分发的镜像名称。
   本示例中通过目标镜像名称前缀 `test-image` 搜索，查询到已分发的镜像表示分发成功。

   > **说明** 分发的镜像名称由 `自定义名称前缀_构建任务ID` 构成，因此您也可以通过构建任务ID进行搜索。

步骤三：创建实例并测试Nginx环境

1. 在左侧导航栏，选择**部署与弹性 > 镜像构建**。
2. 在顶部菜单栏处，选择镜像模版所在的地域。
   本示例中镜像构建的地域为**华北2（北京）**。
3. 在**镜像模版**页签，找到已创建的镜像模版，单击模版ID进入**镜像模版详情**页面。
4. 在**构建历史**页签，单击镜像ID进入自定义镜像的详情页。
5. 单击**创建实例**，然后完成实例的创建。
   请根据您的业务需求创建ECS实例，创建时请注意以下配置项，具体操作，请参见使用自定义镜像创建实例。
   - 需要分配公网IPv4地址。
   - 安全组入方向规则需要开放80端口。
6. 获取实例的公网IP。
   i. 实例创建完成后，返回**实例列表**页面。
   ii. 找到已创建的ECS实例，在**IP地址**列，复制公网IP地址。
7. 在本地环境打开浏览器，然后在地址栏输入 `ECS实例的公网IP` 进行访问。
   查看到如下图所示的页面，表示Nginx开发环境正常。

Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.

11.更换操作系统

您可以更换操作系统，例如把Linux系统更换成Windows系统，或把Ubuntu更换为CentOS。非中国内地的地域暂不支持Linux和Windows系统的互换，仅支持Linux和Linux、Windows和Windows同类型系统的更换。

更换操作系统是通过更换实例的系统盘实现的。

- 将系统盘的镜像更换为非公共镜像，请参见更换操作系统（非公共镜像）。
- 将系统盘的镜像更换为公共镜像，请参见更换操作系统（公共镜像）。

如果需要保留系统盘数据，减少业务中断时长，您可以通过服务器迁移中心SMC（Server Migration Center）迁移操作系统。SMC迁移目前仅支持以下场景：

- CentOS 7操作系统迁移为Alibaba Cloud Linux 2/Anolis OS 7操作系统。
- CentOS 8操作系统迁移为Alibaba Cloud Linux 3/Anolis OS 8操作系统。

具体操作，请参见迁移操作系统。

12.操作系统停止支持计划

由于产品生命周期、第三方支持、开源计划演进等原因，部分服务会在上线一段时间后停止技术支持。了解服务或软件的技术支持计划有助于您及时更新至稳定的软件版本。使用云服务器ECS时，您需要关注镜像运行的操作系统在官方平台公布的生命周期计划。

> **说明** 如果操作系统版本结束了生命周期（EOL），阿里云会同时停止对使用相应操作系统版本的ECS实例提供技术支持服务。
>
> - Alibaba Cloud Linux 2是阿里云官方操作系统。在EOL前，阿里云会为使用过程中遇到的问题提供技术支持。
> - 其他第三方操作系统，请联系操作系统原厂或者开源社区获得技术支持。同时，阿里云将对问题的调查提供相应的技术协助。如果第三方停止了对操作系统的支持或维护，阿里云的技术协助也相应停止。

Alibaba Cloud Linux EOL计划

版本	停止支持日期
Alibaba Cloud Linux 3	2031-04-30
Alibaba Cloud Linux 2	2024-03-31

第三方操作系统EOL计划

部分操作系统版本的EOL计划表如下所示：

- Anolis OS

版本	停止支持日期
Anolis OS 8	2031-06-30
Anolis OS 7	2024-06-30

- CentOS

版本	停止全面更新日期	停止维护更新日期
CentOS Stream 8	2024-05-31	2024-05-31
CentOS 8	2021-12-31	2021-12-31
CentOS 7	2020-08-06	2024-06-30
CentOS 6	2017-05-10	2020-11-30
CentOS 5	2007-04-12	2017-03-31

> **说明** CentOS Linux停止维护后的应对措施，请参见CentOS Linux停止维护后如何应对？。

- Debian

版本	代号	发布日期	停止支持日期	EOL LTS	EOL ELTS
Debian 13	Trixie	暂无明确时间	暂无明确时间	暂无明确时间	暂无明确时间
Debian 12	Bookworm	暂无明确时间	暂无明确时间	暂无明确时间	暂无明确时间
Debian 11	Bullseye	2021-08-14	2024-07	2026-06	暂无明确时间
Debian 10	Buster	2019-07-06	2022-07	2024-06	暂无明确时间
Debian 9	Stretch	2017-06-17	2020-07-06	2022-06-30	暂无明确时间
Debian 8	Jessie	2015-04-25	2018-06-17	2020-06-30	2022-06-30
Debian 7	Wheezy	2013-05-04	2016-04-25	2018-05-31	2020-06-30
Debian 6.0	Squeeze	2011-02-06	2014-05-31	2016-02-29	暂无明确时间
Debian 5.0	Lenny	2009-02-14	2012-02-06	暂无明确时间	暂无明确时间

- Ubuntu

版本	停止支持日期
Ubuntu 22.04 LTS	2027-04
Ubuntu 20.04 LTS	2030-04
Ubuntu 18.04 LTS	2028-04
Ubuntu 16.04 LTS	2026-04 **说明** Ubuntu 16.04在停止维护后可继续获取安全更新。具体操作，请参见Ubuntu 16.04 LTS停止支持维护后如何继续安全更新？。
Ubuntu 14.04 LTS	2024-04

- Red Hat

版本	发布日期	完全支持停止日期①	1阶段维护停止日期②	2阶段维护停止日期③	延长生命周期停止日期④	最终次发行版本
Red Hat 4	2005-02-14	2009-03-31	2011-02-16	2012-02-29	2017-03-31	Red Hat 4.9
Red Hat 5	2007-03-15	2013-01-08	2014-01-31	2017-03-31	2020-11-30	Red Hat 5.11

版本	发布日期	完全支持停止日期①	1阶段维护停止日期②	2阶段维护停止日期③	延长生命周期停止日期④	最终次发行版本
Red Hat 6	2010-11-10	2016-05-10	2017-05-10	2020-11-30	2024-06-30	Red Hat 6.10
Red Hat 7	2014-06-10	2019-08-06	2020-08-06	2024-06-30	不涉及	Red Hat 7.9
Red Hat 7（ARM）	2017-11-13	2020-11-30	不涉及	不涉及	不涉及	Red Hat 7.9
Red Hat 7（POWER9）	2017-11-13	2020-11-30	不涉及	不涉及	不涉及	Red Hat 7.9
Red Hat 7（System z (Structure A)）	2018-04-10	2020-11-30	不涉及	不涉及	不涉及	Red Hat 7.9
Red Hat 8	2019-05	2024-05	不涉及	2029-05	暂无明确时间	Red Hat 8.8

说明：

- ①：在完全支持阶段，Red Hat会为次发行版本提供更新的安装镜像。
- ②：在维护支持1阶段，Red Hat通常会在次发行版本中自由裁量提供不需要大量软件更改的硬件启用（Hardware Enablement）。在这个阶段不会提供新的软件功能。只有因安装程序（installer）变化而需要时，Red Hat才会在维护支持1阶段自由裁量为次发行版本提供更新的安装镜像。
- ③：在维护支持阶段（Red Hat 8）及维护支持 2 阶段（Red Hat 6和Red Hat 7），一般不会发布新的功能及新的硬件启用。在这个阶段可能会提供带有更新安装镜像的次发行版本。
- ④：对于处于延长生周阶段的产品，Red Hat会提供有限的技术支持。 在此阶段，不会提供程序漏洞修复、安全修复、硬件启用或根本原因分析，同时只对现有安装提供支持。

更多信息，请参见Red Hat。

- FreeBSD

版本	发布日期	停止维护更新日期
FreeBSD 13.0	2021-04-13	FreeBSD 13.1发布后3个月
FreeBSD 12.3	2021-12-07	FreeBSD 12.4发布后3个月
FreeBSD 12.2	2020-10-27	2022-03-31
FreeBSD 12.1	2019-11-04	2021-01-31
FreeBSD 12.0	2018-12-11	2020-02-04
FreeBSD 11.4	2020-06-16	2021-09-30

版本	发布日期	停止维护更新日期
FreeBSD 11.3	2019-07-09	2020-09-30
FreeBSD 11.2	2018-06-28	2019-10-31
FreeBSD 11.1	2017-07-26	2018-09-30
FreeBSD 11.0	2016-10-10	2017-11-30

- OpenSUSE

版本	停止维护更新日期
OpenSUSE 15.3	2022-11-30
OpenSUSE 15.2	2022-01-04
OpenSUSE 15.1	2021-02-02
OpenSUSE 15.0	2019-12-03
OpenSUSE 42.3	2019-07-01
OpenSUSE 42.2	2018-01-26
OpenSUSE 42.1	2017-05-17

- SUSE Linux

版本	发布日期	一般支持日期	拓展支持日期
SUSE Linux Enterprise Server 12	2014-10-27	2016-06-30	2019-07-01
SUSE Linux Enterprise Server 12 SP1	2015-12-15	2017-05-31	2020-05-31
SUSE Linux Enterprise Server 12 SP2	2016-11-08	2018-03-31	2021-03-31
SUSE Linux Enterprise Server 12 SP3	2017-09-07	2019-06-30	2022-06-30
SUSE Linux Enterprise Server 12 SP4	2018-12-12	2020-06-30	2023-06-30
SUSE Linux Enterprise Server 12 SP5	2019-12-09	2024-10-31	2027-10-31
SUSE Linux Enterprise Server 15	2018-07-16	2019-12-31	2022-12-31

版本	发布日期	一般支持日期	拓展支持日期
SUSE Linux Enterprise Server 15 SP1	2019-06-24	2021-01-31	2024-06-31
SUSE Linux Enterprise Server 15 SP2	2020-07-21	2021-12-31	2024-12-31
SUSE Linux Enterprise Server 15 SP3	2021-06-22	SUSE Linux Enterprise Server 15 SP4发布后6个月	暂无明确时间

- Fedora

版本	停止维护更新日期
Fedora 36	2023-05-16
Fedora 35	2022-11-15
Fedora 34	2022-05-17
Fedora 33	2021-11-30
Fedora 32	2021-05-25
Fedora 31	2020-11-24
Fedora 30	2020-05-26
Fedora 29	2019-11-26
Fedora 28	2019-05-28
Fedora 27	2018-11-30

- Rocky Linux

版本	发布日期	停止维护更新日期
Rocky Linux 8.5	2021-11-14	2031-11-14

- AlmaLinux

版本	发布日期	停止维护更新日期
AlmaLinux 8.5	2021-11	2031-11

- Fedora CoreOS
  暂无明确时间。
- Windows Server

版本	停止全面更新日期	停止维护更新日期
Windows Server 2022	2026-10-13	2031-10-14
Windows Server 2019数据中心版	2024-01-09	2029-01-09
Windows Server 2016数据中心版	2022-01-11	2027-01-12
Windows Server 2012数据中心版	2018-10-09	2023-10-10
Windows Server 2012 R2数据中心版	2018-10-19	2023-10-10
Windows Server 2008	已停止	已停止
Windows Server 2003	已停止	已停止

有关第三方操作系统版本的详细EOL计划，请访问相应官网查看。

- Anolis OS
- CentOS
- Debian
- Ubuntu
- Red Hat
- FreeBSD
- OpenSUSE
- SUSE Linux
- Fedora
- Rocky Linux
- AlmaLinux
- Fedora CoreOS
- CoreOS
- Microsoft Windows Server

13.常见问题

13.1. 镜像FAQ

本文介绍云服务器ECS镜像相关的常见问题及解决方案。

- 一般性FAQ
  - ECS实例选择了镜像后能更换吗？
  - ECS系统盘是否支持KMS加密，通过Terraform或Packer如何使用？
  - 快照和镜像有什么不同？有什么关系？
  - RHEL（Red Hat Enterprise Linux）镜像支持哪些实例规格族？
  - 阿里云提供的RHEL（Red Hat Enterprise Linux）镜像是否包括Red Hat官方订阅？
  - 使用Red Hat Enterprise Linux操作系统过程中遇到问题，如何获取技术支持？
  - Windows系统不同版本的内存限制有何不同？
  - SLES for SAP常见问题
- 自定义镜像FAQ
  - 数据盘的快照是否可以创建自定义镜像？
  - 如何查看数据盘？
  - 如何卸载（umount）和删除disktable里的数据？
  - 如何确认已经卸载数据盘，并可以新建自定义镜像？
  - 实例释放后，自定义镜像是否还存在？
  - 用于创建自定义镜像的实例到期或释放数据后，创建的自定义镜像是否受影响？使用自定义镜像开通的实例是否受影响？
  - 使用自定义镜像创建的实例是否可以更换操作系统？更换系统后原来的自定义镜像是否还可以使用？
  - 更换系统盘时另选操作系统，是否可以使用自定义镜像？
  - 已创建的自定义镜像，是否可以用于更换另一台云服务器ECS的系统盘数据？
  - 是否可以升级自定义镜像开通的云服务器ECS的CPU、内存、带宽、硬盘等？
  - 是否可以跨地域使用自定义镜像？
  - 包年包月实例的自定义镜像，是否可以用于创建按量付费的云服务器ECS？
  - 使用自定义镜像创建的实例，系统盘自动扩容失败的原因是什么？怎么办？
  - 创建自定义镜像、ECS实例时为何需要注释挂载项？
  - 如何配置并使用Docker私有镜像库？
  - 如何克隆ECS服务器？
  - 有些自定义镜像不支持创建I/O优化的实例，我该如何操作？
  - 在哪里查看导入镜像的进度？导入镜像需要多少时间？
  - 在哪里查看镜像创建进度？创建镜像需要多少时间？
- 复制镜像FAQ
  - 什么情况下需要复制镜像？
  - 可以复制哪些镜像？
  - 当前有哪些支持复制镜像功能的地域？
  - 复制一个镜像大概需要多久？

- 复制镜像怎么收费的？
- 在复制镜像过程中，源镜像和目标镜像有什么限制？
- 怎么复制我的云账号的镜像资源到其他阿里云账号的其他地域？
- 能否跨地域复制来源于镜像市场镜像的自定义镜像？
- 中国内地以外的地域迁移数据到中国内地地域有什么方法？

- 共享镜像FAQ
  - 我最多可以获得多少个共享镜像？
  - 每个镜像最多可以共享给多少个用户？
  - 我有多个站点的账号，能否互相共享镜像？
  - 使用共享镜像是否占用我的镜像名额？
  - 使用共享镜像创建实例的时候存不存在地域限制？
  - 使用共享镜像创建实例存在什么样的风险？
  - 我把自定义镜像共享给其他账号，存在什么风险？
  - 我能把别人共享给我的镜像再共享给其他人吗？
  - 我把镜像共享给他人，还能使用该镜像创建实例吗？
  - 华北地域服务器A制作的镜像能共享给华东地域的服务器B吗？
- 导入镜像FAQ
  - 导入自定义镜像时，是否支持自带许可证BYOL?
  - 导入自定义镜像支持哪些许可证类型？
  - 导入的自带许可BYOL镜像如何计费？
  - 自带许可证、订阅到期后，如何通过阿里云做认证和订阅？
- 导出镜像FAQ
  - 我想将镜像导出到本地进行测试，具体怎么操作？
  - 导出后的镜像是否支持在其他平台启动？
- 删除镜像FAQ
  - 如果使用自定义镜像创建了ECS实例，我可以删除这个镜像吗？
  - 我曾把自己账号中的某个自定义镜像共享给其他账号，现在我可以删除这个镜像吗？
  - 我把某个自定义镜像（M）的共享账号（A）给删除了，会有什么影响？
  - 删除镜像的时候提示“指定的镜像ID还存在保有实例，不能删除该镜像”，为什么？
- 更换镜像（操作系统）FAQ
  - 更换系统盘时，选择的镜像中包含数据盘的话，能通过更换系统盘实现更换镜像吗？
  - 我目前有一台ECS服务器，想用现有的镜像来更换这台ECS的操作系统，怎么操作？
  - 账号A的服务器制作镜像后，能给账号B更换系统盘用吗？
- 镜像费用FAQ
  - 为什么创建实例时自定义镜像的配置费用高于公共镜像？
- 镜像商业化FAQ
  - 镜像市场的镜像有哪些功能？
  - 镜像市场的镜像能带来哪些便利？

- 目前镜像市场的镜像支持哪些服务器环境和应用场景？
- 镜像市场的镜像是否安全？
- 镜像市场的镜像安装使用过程中出问题了怎么办？
- 如何购买镜像市场镜像？
- 按次购买的镜像的使用期限是多久？
- Red Hat和SUSE镜像支持退款吗？
- 镜像市场的镜像支持退款吗？
- 镜像市场商业化后，还有免费的镜像市场镜像吗？
- 在杭州买了一个镜像市场的镜像，能否在北京创建ECS实例或者更换系统盘？
- ECS实例使用镜像市场的镜像，升级和续费ECS实例，需要为镜像继续付费吗？
- ECS实例使用镜像市场的镜像，实例释放后，继续购买ECS实例还可以免费使用该镜像吗？
- 使用镜像市场镜像创建ECS实例，该实例创建一个自定义镜像，使用该自定义镜像创建ECS实例需要为该镜像付费吗？
- 来源于镜像市场的镜像复制到其他地域创建ECS实例，是否需要为该镜像付费？
- 如果把来源于镜像市场的自定义镜像共享给其他账号（B）创建ECS实例，账号B是否需要为该镜像付费？
- 如果使用镜像市场的镜像或者来源于镜像市场的镜像进行更换系统盘，需要付费吗？
- ECS实例正在使用镜像市场的镜像，更换系统盘需要收费吗？
- 怎么调用ECS API，使用镜像市场镜像或者来源镜像市场的自定义镜像或者共享镜像，创建ECS实例和更换系统盘？
- 如果没有购买镜像市场的镜像或者来源于镜像市场的镜像，在调用ECS API使用该镜像创建ECS实例和更换系统盘，会报错吗？
- 我的ESS是自动创建机器的，并且量是不固定，设置最小值为10台，最大值为100台，那么使用镜像市场的镜像如何保证我的需求实例能正常弹出来？
- 镜像市场的镜像是否支持批量购买？
- 如果之前使用的镜像市场的镜像，已不存在该商品（如：jxsc000010、jxsc000019），怎能保证已经设置的弹性伸缩组的机器能正常弹出？
- 1个product code能否支持不同region的镜像？
- 我买了100 product code同样值的镜像，是否可以支持在所有的地域可用？
- 勾选“I/O优化实例”选项导致购买ECS实例时无法选择镜像市场的镜像，为什么？怎么解决？

- 镜像市场包年包月镜像FAQ
  - 什么是镜像市场的包年包月和按周付费镜像？
  - 包年包月镜像能与哪种ECS实例搭配使用？
  - 怎么购买包年包月镜像？可以单独购买吗？
  - 包年包月镜像怎么付费？
  - 包年包月镜像到期了就不能用了吗？怎么继续使用？
  - 购买包年包月镜像后，如果我不想再使用这个镜像，能要求退款吗？
  - 退款时，费用怎么结算？
  - 包年包月镜像能转换为按量付费镜像吗？
  - 包年包月镜像与其它镜像之间能互换吗？更换后费用怎么计算？
  - 在哪里查看并管理我购买的包年包月镜像？

- 使用包年包月镜像制作的自定义镜像会收费吗？包年包月镜像过期对于自定义镜像有什么影响？

- ECS实例与操作系统镜像FAQ
  - CentOS 8 EOL（停止支持）之后相关的公共镜像会下架吗？
  - CentOS 8 EOL（停止支持）之后对我的ECS实例有什么影响？
  - AMD EPYCTM MILAN处理器的实例规格族不支持哪些操作系统？
  - 基于弹性裸金属实例规格的ECS实例，系统生成crash dump文件失败如何解决？
  - Linux操作系统内核回写时出现softlockup异常如何解决？
  - 在ECS实例内删除cgroup出现softlockup异常如何解决？
  - ECS实例宕机相关解决方案
  - 为什么我无法使用ssh-rsa签名算法的SSH密钥对远程连接Fedora 33 64位系统的实例？
  - FreeBSD系统如何打补丁编译内核？
  - 为什么Ubuntu某些版本的ECS实例中启动安骑士进程后系统负载较高？
  - 为什么有的ECS实例无法选择Windows操作系统？
  - 阿里云是否支持Windows Server 2008和Windows Server 2008 R2操作系统？
  - 实例的操作系统为Windows Server，现在提示Windows副本不是正版怎么办？
  - ECS实例使用操作系统需要付费吗？
  - 我能自己安装或者升级操作系统吗？
  - 操作系统是否有图形界面？
  - 如何选择操作系统？
  - 公共镜像自带FTP上传吗？
  - 阿里云支持哪些SUSE版本？
  - SUSE操作系统提供哪些服务支持？
  - ECS实例到期释放后，如果这个实例之前手动制作了镜像快照，能不能找回之前实例的数据？
  - 我先有一台ECS实例，想再买一台ECS实例并使用现有这台ECS实例的镜像部署，应该如何操作？
  - 我已经购买了新的ECS实例，如何把我的共享镜像恢复到这台新购ECS服务器上？
  - 我在阿里云有多个账号，想把账号A的一台ECS实例转移到账号B，或者用账号A购买一台ECS实例，把实例运行环境、应用迁移到账号B。怎么操作？
  - ECS实例之间如何迁移？
  - 两个不同专有网络下的ECS实例能否实现网络互通？
  - 如何处理CentOS DNS解析超时？
  - 为什么ECS默认没有启用虚拟内存或Swap说明？
  - 如何在公共镜像中开启kdump？
  - RHEL（Red Hat Enterprise Linux）镜像中如何获取dump文件？
  - 如何在RedHat 8.1系统的ECS实例中开启kdump？
  - 如何解决RedHat 8.1/8.2镜像在弹性裸金属服务器实例规格族的ECS实例下启动慢的问题？
  - vSwitch中实例数量过多导致CentOS实例夯机或异常重启，怎么办？
  - 如何检查与修复CentOS 7实例和Windows实例IP地址缺失问题？
  - 历史Linux镜像问题修复方案有哪些？
  - ECS实例启动时报错“UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.”，怎么办？
  - 如何从RHEL 7升级到RHEL 8（Red Hat Enterprise Linux 8）？

- 如何设置Linux系统的ECS实例的静态IP地址？
- CentOS/RedHat 7.x升级Systemd重启进入救援模式如何处理？
- 如何在Linux实例中自定义配置DNS？
- 在部署业务时如何让程序区分不同的ECS实例？
- 为什么使用Fedora CoreOS镜像创建部分实例后，CPU信息只有实例规格的一半？
- Linux操作系统配置IPv6地址后，安装了NTP服务的服务器时间无法同步，如何处理？

ECS实例选择了镜像后能更换吗？

可以更换。在ECS控制台，选择更换系统盘，即可选择所需的镜像进行更换。请注意，更换镜像会导致系统盘数据丢失，请在确认更换前做好数据备份。详情请参见更换操作系统。

ECS系统盘是否支持KMS加密，通过Terraform或Packer如何使用？

- ECS系统盘支持KMS的默认key加密以及BYOK加密。更多详情，请参见加密概述。
- Packer加密功能即将支持。
- Terraform中通过参数encrypted指定，详情请参见alicloud_disks。

快照和镜像有什么不同？有什么关系？

快照和镜像的不同如下：

- 镜像可直接用来创建ECS实例，而快照不可以。
- 快照可以是ECS实例系统盘或数据盘的数据备份，而镜像一定包含ECS实例系统盘的数据。
- 快照只能用于当前ECS实例磁盘的数据恢复，而镜像可用于当前ECS实例及其他实例更换系统盘或创建新的ECS实例。
- 应用场景不同。这里列举快照和自定义镜像的一些应用场景。
  快照适用场景：
  - 定期数据备份，按照设定的周期，每日、每周或每月自动执行快照策略对数据进行备份。
  - 临时数据备份，例如：
    - 系统更新、应用发布等系统临时变更，为防止操作错误，在执行变更前手工创建快照对系统进行备份。
    - 系统盘扩容前，创建快照备份数据。
    - 磁盘数据迁移，为磁盘创建快照，将磁盘作为另一块磁盘的基础数据。

  自定义镜像适用场景：
  - 备份短期内不会更改的系统，如已经完成发布或更新的应用系统。
  - 使用已经完成安装和配置的系统为模板，创建新的ECS实例，如批量部署应用。
  - 系统及数据迁移，如将经典网络的ECS实例迁移到VPC下。
  - 跨可用区和地域还原系统。

快照和镜像的关系如下：

- 使用实例创建自定义镜像时，ECS会为实例的每块云盘创建快照，即自定义镜像包含ECS实例所有磁盘的快照。具体步骤，请参见使用实例创建自定义镜像。
- 使用系统盘快照，也可以创建自定义镜像。具体步骤，请参见使用快照创建自定义镜像。

RHEL（Red Hat Enterprise Linux）镜像支持哪些实例规格族？

以下实例规格族已通过RHEL的认证，对应实例规格族的详情请参见实例规格族。

- ecs.r6（只支持RHEL 7.7及以上版本）

- ecs.c6（只支持RHEL 7.7及以上版本）
- ecs.g6（只支持RHEL 7.7及以上版本）
- ecs.r5
- ecs.c5
- ecs.g5
- ecs.re4
- ecs.t5
  其中，以下实例规格因为内存小于1.5 GiB，不满足RHEL最低内存要求，因此不建议使用。
  - ecs.t5-lc2m1.nano
  - ecs.t5-lc1m1.small
- ecs.hfc5
- ecs.hfg5
- ecs.i2
- ecs.sn1ne
- ecs.sn2ne
- ecs.se1ne
- ecs.sn1
- ecs.sn2
- ecs.se1

更多信息，请参见：

- Red Hat Enterprise Linux认证信息
- Red Hat Enterprise Linux认证的ECS实例规格列表
- Red Hat Enterprise Linux对实例配置的限制

阿里云提供的RHEL（Red Hat Enterprise Linux）镜像是否包括Red Hat官方订阅？

阿里云提供的RHEL镜像包括了Red Hat官方订阅。您在购买RHEL镜像时，可以从阿里云提供的更新源中获取Red Hat的更新。该方式与传统模式区别在于，您将不会获得单独的Red Hat账号，用于从Red Hat提供的更新源获取更新。

使用Red Hat Enterprise Linux操作系统过程中遇到问题，如何获取技术支持？

与传统的登录Red Hat系统提交售后请求不同的是，您可以直接提交工单寻求技术支持，阿里云售后工程师会协助解决您遇到的问题。如果涉及阿里云无法解决的Red Hat Enterprise Linux操作系统问题，阿里云会将问题提交至Red Hat，由Red Hat负责提供最终的技术支持。

Windows系统不同版本的内存限制有何不同？

Windows系统不同的版本对应的内存上限不同。更多信息，请参见Memory Limits for Windows and Windows Server Releases。请您根据Windows系统的内存限制选配合适的实例规格。

SLES for SAP常见问题

SUSE Linux Enterprise Server for SAP Applications（SLES for SAP）是SAP和SUSE公司在SLES商业Linux操作系统的基础上，定制的SAP系统专用版本。关于SLES for SAP在使用过程中的常见问题如下：

- SUSE Linux Enterprise for SAP

- 配置SUSE linux实例的NTP/Chrony时钟同步服务
- SLES/SLES for SAP的操作系统如何升级到新版本？
- 如何判断ECS使用的镜像是否是SLES for SAP CSP镜像？

数据盘的快照是否可以创建自定义镜像？

创建自定义镜像的快照磁盘属性必须是系统盘，数据盘不能用于创建自定义镜像。

但是，使用系统盘快照创建自定义镜像时，您可以添加数据盘快照，详情请参见使用快照创建自定义镜像。

如何查看数据盘？

您可以通过df命令查看数据盘的使用情况，以及文件系统被挂载的位置。例如：df -lh。

您可以通过fdisk命令获取数据盘的分区情况。例如：fdisk -l。

如何卸载（umount）和删除disk table里的数据？

假设*/dev/hda5*已经挂载在*/mnt/hda5*上，您可以使用下列任一命令卸载已挂载的文件系统。

```
umount /dev/hda5
```

```
umount /mnt/hda5
```

```
umount /dev/hda5 /mnt/hda5
```

*/etc/fstab*是Linux系统下比较重要的配置文件，其包含了系统在启动时挂载的文件系统和存储设备的详细信息。
当您不想在启动实例时挂载指定分区，需要删除当前文件中对应的语句行。例如，删除下面的语句可以在启动的时候断开*xvdb1*。

```
/dev/xvdb1 /leejd ext4 defaults 0 0
```

Linux其他较重要的配置文件如下：

配置文件	配置说明	修改该配置文件的风险
/etc/issue*, /etc/*-release, /etc/*_version	系统发行版信息配置文件	修改*/etc/issue**会导致系统发行版无法被正常识别，导致系统创建失败。
/boot/grub/menu.lst, /boot/grub/grub.conf	系统引导启动配置文件	修改*/boot/grub/menu.lst*会导致内核无法正确加载，导致系统无法启动。
/etc/fstab	系统启动挂载分区配置文件	修改该文件会导致分区无法被加载，导致系统无法启动。
/etc/shadow	系统密码相关配置文件	修改该文件为只读会导致无法修改密码文件，导致系统创建失败。
/etc/selinux/config	系统安全策略配置文件	修改*/etc/selinux/config*开启SELinux导致系统无法启动。

如何确认已经卸载数据盘，并可以新建自定义镜像？

1. 确认*/etc/fstab*文件中对应的自动挂载数据盘分区语句行已被删除。

2. 使用mount命令查看所有设备的挂载信息，请确认执行结果中不包含对应的数据盘分区信息。

实例释放后，自定义镜像是否还存在？

存在。手动或自动释放实例后，不会影响该实例对应的自定义镜像。

用于创建自定义镜像的实例到期或释放数据后，创建的自定义镜像是否受影响？使用自定义镜像开通的实例是否受影响？

均不受影响。实例到期自动释放或者手动释放后，不会影响该实例对应的自定义镜像及使用该自定义镜像创建的实例。

使用自定义镜像创建的实例是否可以更换操作系统？更换系统后原来的自定义镜像是否还可以使用？

可以。更换后原来的自定义镜像还可以继续使用。

更换系统盘时另选操作系统，是否可以使用自定义镜像？

可以，详情请参见更换操作系统（非公共镜像）。

> **说明** 系统盘更换为自定义镜像后，原来的数据将被全覆盖。

已创建的自定义镜像，是否可以用于更换另一台云服务器ECS的系统盘数据？

可以。详情请参见更换操作系统（非公共镜像）。

> **说明** 自定义镜像将全部覆盖该服务器系统盘的所有数据。

是否可以升级自定义镜像开通的云服务器ECS的CPU、内存、带宽、硬盘等？

均可以升级，详情请参见升降配方式概述。

是否可以跨地域使用自定义镜像？

不可以。自定义镜像只能在同一个地域使用。例如：使用华东1地域的实例创建的自定义镜像，不可以直接用来开通华东2地域的云服务器ECS。

如果您需要跨地域使用自定义镜像，可以先复制镜像到目标地域，请参见复制镜像。

包年包月实例的自定义镜像，是否可以用于创建按量付费的云服务器ECS？

可以。自定义镜像功能不区分实例的付费方式，即不区分是否包年包月或按量付费。

使用自定义镜像创建的实例，系统盘自动扩容失败的原因是什么？怎么办？

使用自定义镜像创建的实例，系统盘自动扩容失败的原因可能是没有安装cloud-init服务、cloud-init服务运行失败或文件系统不支持等。

系统盘自动扩容失败时，您可以手动扩容。具体步骤，请参见扩展文件系统_Linux系统盘。

创建自定义镜像、ECS实例时为何需要注释挂载项？

使用自定义镜像创建ECS实例时，以下原因会导致挂载磁盘失败。

- 创建的ECS实例没有数据盘。
- 数据盘是新磁盘，还没有进行分区格式化。
- 创建的自定义镜像中，未注释掉*/etc/fstab*文件中的磁盘挂载条目。

下面以ECS实例数据盘未分区，且创建该实例的自定义镜像中未注释掉*/etc/fstab*中的磁盘挂载条目为例，介绍数据盘挂载失败的原因。

1. ECS实例数据盘未分区，如下图所示。

```
[root@test ~]# fdisk -l

Disk /dev/xvda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00078f9c

    Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *           1        2611    20970496   83  Linux

Disk /dev/xvdb: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

2. 使用自定义镜像创建的ECS实例中，未注释掉*/etc/fstab*中的磁盘挂载条目，如下图所示。

```
[root@test ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Aug 14 21:16:42 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=[illegible] / ext4 defaults,barrier=0 1 1
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/xvdb1              /alidata                ext4    defaults        0 0
[root@test ~]#
```

3. 实例启动时，会按照*/etc/fstab*文件中的配置挂载磁盘，但由于数据盘未分区导致挂载失败，如下图所示。

```
[root@test ~]# mount -a
mount: special device /dev/xvdb1 does not exist
[root@test ~]#
```

不用注释磁盘挂载条目的情况：一般只有在创建ECS实例时，选择了数据盘且数据盘是通过已分区、已格式化的数据盘快照生成。

如问题还未解决，请提交工单。

如何配置并使用Docker私有镜像库？

镜像管理是Docker的核心，为了满足企业或组织内部分享镜像，Docker官方在Github上建立了一个开源项目docker-registry，专门用于自建Docker的私有镜像库。

快速启动支持阿里云对象存储OSS的docker-registry：您可以从GitHub下载并安装docker-registry，运行**pip install docker-registry-driver-alioss**命令，通过pip安装OSS driver。

1. 运行docker registry。

```
docker run -e OSS_BUCKET=-e STORAGE_PATH=/docker/ -e OSS_KEY=-e OSS_SECRET=-p 5000:500
0 -d chrisjin/registry:ali_oss
```

2. 配置*config.yml*。

```
```local: &local
<<: *common
storage: alioss
storage_path: _env:STORAGE_PATH:/devregistry/
oss_bucket: _env:OSS_BUCKET[:default_value]
oss_accessid: _env:OSS_KEY[:your_access_id]
oss_accesskey: _env:OSS_SECRET[:your_access_key]```
```

3. 启动docker-registry。

```
DOCKER_REGISTRY_CONFIG=[your_config_path] gunicorn -k gevent -b 0.0.0.0:5000 -w 1 dock
er_registry.wi:application
```

如问题还未解决，请提交工单联系阿里云。

如何克隆ECS服务器？

同一账号下，新购ECS服务器时可以按照以下方式克隆现有ECS服务器的环境和数据，快速创建相同环境和配置的新ECS实例。

- 方式一：通过控制台在同地域手动克隆ECS服务器。
  i. 登录ECS管理控制台。
  ii. 找到需要克隆的ECS实例，为实例创建自定义镜像。具体请参见使用实例创建自定义镜像。
  iii. 按使用向导创建实例创建新的ECS实例。在创建过程中，需要注意以下配置：
    - 地域：必须选择与自定义镜像相同的地域。
    - 镜像：**镜像类型**选择**自定义镜像**，并选择使用系统盘创建的自定义镜像。

    > **说明** 如果您选择的自定义镜像中包含了一个或多个数据盘快照，系统会自动根据这些快照创建相同数量的云盘作为数据盘，每个云盘大小与对应的快照相同。您可以增加云盘容量，但不能缩小。

- 方式二：通过控制台在不同地域手动克隆ECS服务器。
  i. 登录ECS管理控制台。
  ii. 选择需要克隆的ECS实例，对系统盘和数据盘分别创建快照。具体请参见创建一个云盘快照。

  > **说明** 为保证数据一致性，请在实例状态为**已停止**时创建快照。

  iii. 复制快照到目标地域。具体操作请参见复制快照。
```

iv. 使用系统盘快照创建自定义镜像。创建过程中请选中**添加数据盘快照**，并单击**增加**选择并添加已创建的数据盘快照。具体请参见使用快照创建自定义镜像。

v. 按使用向导创建实例创建新的ECS实例。在创建过程中，需要注意以下配置：

- 地域：必须选择与自定义镜像相同的地域。
- 镜像：**镜像类型**选择**自定义镜像**，并选择使用系统盘创建的自定义镜像。

> **说明** 如果您选择的自定义镜像中包含了一个或多个数据盘快照，系统会自动根据这些快照创建相同数量的云盘作为数据盘，每个云盘大小与对应的快照相同。您可以增加云盘容量，但不能缩小。

vi. 按使用向导创建实例创建新的ECS实例。在创建过程中，需要注意以下配置：

- 地域：必须选择与自定义镜像相同的地域。
- 镜像：**镜像类型**选择**自定义镜像**，并选择使用系统盘创建的自定义镜像。

> **说明** 如果您选择的自定义镜像中包含了一个或多个数据盘快照，系统会自动根据这些快照创建相同数量的云盘作为数据盘，每个云盘大小与对应的快照相同。您可以增加云盘容量，但不能缩小。

- 方式三：通过运维编排服务自动化克隆ECS服务器。
  - 请访问ACS-ECS-CloneInstancesAcrossRegion，在顶部菜单栏选择当前实例所在地域后，跨地域克隆ECS实例。
  - 请访问ACS-ECS-CloneInstancesAcrossAZ，在顶部菜单栏选择当前实例所在地域后，在不同可用区克隆ECS实例。

有些自定义镜像不支持创建I/O优化的实例，我该如何操作？

部分自定义镜像不支持创建I/O优化的实例。如果想要使用这类自定义镜像来创建I/O优化的实例，请提交工单申请（提交工单时，需指定镜像名称）。

在哪里查看导入镜像的进度？导入镜像需要多少时间？

在ECS管理控制台的镜像列表页查看导入进度。导入自定义镜像是相对耗时的任务，完成的时间取决于镜像文件的大小和当前导入任务并发数，需要您耐心等待。

在哪里查看镜像创建进度？创建镜像需要多少时间？

在ECS管理控制台的镜像列表页查看。镜像制作时间取决于实例磁盘的大小。

什么情况下需要复制镜像？

自定义镜像只能在同一个地域使用，不能直接跨地域使用。如果您需要：

- 将云服务器ECS上的应用部署在多个地域。
- 将云服务器ECS迁移到其他地域。
- 跨地域使用自定义镜像。
- 变更某一自定义镜像的加密状态、加密系统盘或者加密操作系统数据。

可以通过复制镜像解决。更多信息，请参见复制镜像。

> **说明**
> - 在同地域复制自定义镜像时，仅支持加密复制。
> - 复制加密镜像的过程中不支持取消复制。

可以复制哪些镜像？

复制镜像只支持自定义镜像。不支持公共镜像，镜像市场镜像和别人共享给您的镜像。

当前有哪些支持复制镜像功能的地域？

阿里云所有地域均支持复制镜像功能。

复制一个镜像大概需要多久？

复制镜像的时间取决于网络传输速度和任务队列的排队数量。复制镜像需要通过网络把一个地域的可用区中的镜像文件传输到目标地域的可用区，需要您耐心等待。

如果您需要复制大容量镜像（例如大于2 TiB的镜像），也可以先通过复制快照功能将快照复制到目标地域，再在目标地域使用快照创建镜像。相比直接复制镜像，可节约时间。具体操作请参见复制快照和使用快照创建自定义镜像；复制快照收费说明请参见快照计费。

复制镜像怎么收费的？

复制镜像过程包括以下操作：

1. 从源地域将生成自定义镜像的快照复制到目标地域。
2. 在目标地域根据快照自动生成自定义镜像。

上述过程可能涉及以下费用：

- 不同地域之间的数据传输流量费。阿里云目前暂未对这部分流量收费，具体收费时间请以官网公告为准。
- 复制过来的快照会占用快照容量。目前快照容量已经收费，详情请参见快照计费。

在复制镜像过程中，源镜像和目标镜像有什么限制？

在复制过程中，源镜像禁止删除，目标镜像可以取消复制，不能用于更换系统盘和创建ECS实例。

怎么复制我的云账号的镜像资源到其他阿里云账号的其他地域？

您需要复制自己的镜像到目标地域，并将该镜像共享给对方的云账号。对方云账号的共享镜像列表中会显示该镜像。

能否跨地域复制来源于镜像市场镜像的自定义镜像？

如果镜像市场镜像在目标地域存在，则您可以复制基于该镜像创建的自定义镜像到目标地域。否则，复制时，会出现如下错误信息。

中国内地以外的地域迁移数据到中国内地地域有什么方法？

您可以通过复制镜像实现。具体步骤，请参见复制镜像。

我最多可以获得多少个共享镜像？

100个。

每个镜像最多可以共享给多少个用户？

50个。

我有多个站点的账号，能否互相共享镜像？

可以。支持中国站、国际站、日本站的账号之间共享镜像，但是基于镜像市场镜像创建的自定义镜像除外。

使用共享镜像是否占用我的镜像名额？

不占用。

使用共享镜像创建实例的时候存不存在地域限制？

有地域限制。同一个共享源，地域也应该相同。

使用共享镜像创建实例存在什么样的风险？

镜像拥有者可以查看该镜像的共享关系，也可以删除该镜像。共享镜像被拥有者删除后，会导致使用共享镜像的ECS实例不能重新初始化系统盘。

阿里云不保证其他账号共享镜像的完整性和安全性，使用共享镜像时您需要自行承担风险，请您选择信任的账号共享的镜像。使用共享镜像创建ECS实例时，您需要登录该ECS实例检查一下共享镜像的安全性和完整性。

我把自定义镜像共享给其他账号，存在什么风险？

有数据泄露和软件泄露的风险。在共享给其他账号之前，请确认该镜像上是否存在敏感的和安全的重要数据和软件。得到您的共享镜像的账号，可以用这个共享镜像创建ECS实例，还可以用这个ECS实例创建更多自定义镜像，其中的数据会不停传播，造成泄露风险。

我能把别人共享给我的镜像再共享给其他人吗？

不能。只有镜像的拥有者才能共享给其他账号。

我把镜像共享给他人，还能使用该镜像创建实例吗？

可以。您将镜像共享给其他账号后，还可以用该镜像创建ECS实例，在该ECS实例的基础上也可以继续创建自定义镜像。

华北地域服务器A制作的镜像能共享给华东地域的服务器B吗？

- 如果服务器A与B属于同一账号，可直接复制镜像到华东地域给服务器B使用。具体步骤，请参见复制镜像。
- 如果服务器A与B属于不同的账号，可先复制镜像到华东地域再共享给服务器B的账号。具体步骤，请参见复制镜像和共享或取消共享镜像。

导入自定义镜像时，是否支持自带许可证BYOL？

支持。您可以通过ECS管理控制台的导入镜像功能或ImportImage配置许可证类型，详情请参见导入自定义镜像和ImportImage。

导入自定义镜像支持哪些许可证类型？

导入自定义镜像时，您可以选择以下三种许可证类型：

- 阿里云（Aliyun）

由阿里云提供许可证，主要包括Windows Server操作系统许可证。在导入镜像安装了cloud-init的前提下，阿里云会使用官方密钥管理服务器（KMS）激活操作系统，且提供Windows Server更新服务（WSUS）。

- 自带许可（Bring Your Own License，简称BYOL）
  自带许可证上云的场景目前主要有以下两种：
  - Microsoft
    微软自带许可场景包含：
    - 通过软件保障协议（Software Assurance，简称SA）实现自带许可场景
      支持微软许可证移动性（License Mobility）的软件，包括SQL Server，SharePoint等，可以通过创建ECS实例实现自带许可。
    - Windows操作系统场景
      Windows客户端访问许可（Client Access License，简称CAL）不适用于许可证移动性，所以无法在共享硬件环境下使用已经拥有的Windows许可证。您需要将Windows部署在独享的物理环境中，可以使用阿里云的专有宿主机或弹性裸金属服务器，详情请参见专有宿主机产品文档和弹性裸金属服务器产品文档。
      对于此类ECS实例，阿里云不提供KMS、WSUS服务及对软件的技术支持，您可以联系微软获取软件技术支持。
    - 无SA或不支持通过SA实现自带许可的场景
      此场景类似于与Windows操作系统场景，您可以在独享的硬件环境中复用已购的软件许可证并自行下载软件进行部署。
  - Redhat
    Redhat提供云接入（Cloud Access）方式。若要迁移当前的Red Hat订阅在阿里云上使用（Bring Your Own Subscription，简称BYOS），可以注册Red Hat云接入计划。具体操作，请参见步骤一：注册Red Hat云接入计划。
- 自动（Auto）
  默认值。根据您设置的要导入操作系统的发行版，自动设置成相应的许可证类型。
  - 对于阿里云已经和厂商签署授权协议的操作系统（如Windows Server），并且阿里云可以提供官方许可证的操作系统，许可证类型会设置成阿里云（Aliyun）。
  - 其他操作系统会设置成自带许可（BYOL），例如非商业化的Linux镜像，阿里云不提供软件技术支持。

导入的自带许可BYOL镜像如何计费？

自带许可的镜像，不需要支付操作系统组件的费用，适用于新建ECS实例、续费ECS实例、实例升降配和重新初始化实例的场景。

自带许可证、订阅到期后，如何通过阿里云做认证和订阅？

您可以将BYOL镜像更换成阿里云镜像。

- Windows Server系统可使用阿里云的官方镜像。阿里云官方镜像详情，请参见公共镜像概述。
- SQL Server、Redhat镜像可通过阿里云云市场获取，详情请参见镜像市场。

我想将镜像导出到本地进行测试，具体怎么操作？

阿里云自定义镜像支持导出。具体操作，请参见导出镜像。

导出后的镜像是否支持在其他平台启动？

导出后的镜像不能保证在其他平台正常启动，但您可以挂载镜像中的磁盘获取数据。

如果使用自定义镜像创建了ECS实例，我可以删除这个镜像吗？

您可以**强制删除**这个镜像。但是，删除镜像后，使用该自定义镜像创建的ECS实例无法重新初始化云盘，详情请参见重新初始化云盘。

我曾把自己账号中的某个自定义镜像共享给其他账号，现在我可以删除这个镜像吗？

可以删除。但是当您删除共享镜像后，使用该共享镜像创建的ECS实例都不能重新初始化系统盘。所以，建议您把该自定义镜像的所有关系删除后再删除镜像。

我把某个自定义镜像（M）的共享账号（A）给删除了，会有什么影响？

您将无法通过ECS控制台或者ECS API查询到共享镜像M。无法使用镜像M创建ECS实例和更换系统盘。如果账号A在删除共享关系前，使用镜像M创建了ECS实例，那么这些实例将不能重新初始化系统盘。

删除镜像的时候提示“指定的镜像ID还存在保有实例，不能删除该镜像”，为什么？

您可能使用快照创建了镜像。如果想删除镜像，必须选择**强制删除**。强制删除镜像后，不会影响现有实例的使用，但是使用该自定义镜像创建的ECS实例无法重新初始化云盘，详情请参见删除自定义镜像。

更换系统盘时，选择的镜像中包含数据盘的话，能通过更换系统盘实现更换镜像吗？

不能。如果必须要使用这个镜像，建议您使用该镜像创建一个按量付费的ECS实例，为系统盘创建快照，然后再通过该快照创建只包含系统盘的自定义镜像，最后更换系统盘时选择该自定义镜像。

我目前有一台ECS服务器，想用现有的镜像来更换这台ECS的操作系统，怎么操作？

使用现有镜像更换ECS实例操作系统的具体步骤，请参见更换操作系统。

> **说明** 建议您操作之前创建快照备份数据。

账号A的服务器制作镜像后，能给账号B更换系统盘用吗？

您需要先共享镜像给账号B，然后再更换系统盘。共享镜像，请参见共享或取消共享镜像。

> **注意** 用于更换系统盘的镜像中，只能包含系统盘。

为什么创建实例时自定义镜像的配置费用高于公共镜像？

以下任一原因均可导致自定义镜像的配置费用高于公共镜像。

- 自定义镜像中包含数据盘。创建实例时，数据盘产生的费用，导致自定义镜像总费用高于相应的公共镜像。
- 自定义镜像基于付费公共镜像（如Windows Server、Redhat Enterprise Linux等）创建。

镜像市场的镜像有哪些功能？

镜像市场的镜像在操作系统基础上预装了软件环境和多种功能，例如PHP/.NET/JAVA/LAMP等运行环境、控制面板、建站系统等。将镜像与云服务器配套使用，您只需进行一次简单操作，就可快速部署云服务器的运行环境或软件应用。

镜像市场的镜像能带来哪些便利？

通过镜像市场的镜像开通云服务器ECS，一键部署，您即可获得与镜像一致的系统环境或软件，便捷地创建已就绪的运行环境，同时轻松地搭建并管理站点。无需自行配置环境、安装软件。

目前镜像市场的镜像支持哪些服务器环境和应用场景？

镜像市场提供上百款优质第三方镜像，不仅全面支持.NET、PHP、JAVA、LAMP和Docker虚拟容器等运行环境的部署，而且满足建站、应用开发、可视化管理等个性化需求。

镜像市场的镜像是否安全？

镜像服务商均有丰富的系统维护和环境配置经验，所有镜像都基于包含云盾的阿里云官方操作系统制作，且预先经过严格安全审核，敬请放心使用。

镜像市场的镜像安装使用过程中出问题了怎么办？

查看购买页的服务信息，通过在线旺旺、电话或邮箱直接与镜像服务商联系，实时解答您的疑问。

如何购买镜像市场镜像？

您可以在镜像市场单独购买，也可以在ECS售卖页面和ECS实例同时购买。

按次购买的镜像的使用期限是多久？

原则上可以一直使用，但要需要注意，镜像作为一种软件有自身的生命周期，另外服务商提供的服务支持实际上是有期限的，具体应以商品上的描述为准。

Red Hat和SUSE镜像支持退款吗？

不支持。使用Red Hat和SUSE镜像的ECS实例默认不支持退款。如果需要退款，请提交工单对ECS实例进行退款，Red Hat和SUSE镜像部分费用不支持退款，ECS实例退款后，相应的镜像也无法用于其他ECS实例。

镜像市场的镜像支持退款吗？

部分商品支持有限时间内无理由退款，但出现以下情况时不予退款。

- 在无理由退款时限内将购买的镜像部署在了云服务器上。
- 在提交退款的申请审批确认前，将购买的镜像部署在了云服务器上。
- 也就是说，镜像在不被使用的状态下可以退款。

镜像市场商业化后，还有免费的镜像市场镜像吗？

镜像市场还会存在一定数量的免费的镜像，可以放心使用。0元的镜像也需要购买后才能使用。

在杭州买了一个镜像市场的镜像，能否在北京创建ECS实例或者更换系统盘？

不可以，购买的镜像市场镜像只能在相同地域进行创建ECS实例或者更换系统盘。

ECS实例使用镜像市场的镜像，升级和续费ECS实例，需要为镜像继续付费吗？

不需要付费。购买一个镜像可以一直在ECS实例上使用，无需再续费。

ECS实例使用镜像市场的镜像，实例释放后，继续购买ECS实例还可以免费使用该镜像吗？

不可以。

使用镜像市场镜像创建ECS实例，该实例创建一个自定义镜像，使用该自定义镜像创建ECS实例需要为该镜像付费吗？

需要，价格和原镜像市场的镜像价格相同。

来源于镜像市场的镜像复制到其他地域创建ECS实例，是否需要为该镜像付费？

需要，价格和原镜像市场的镜像价格相同。

如果把来源于镜像市场的自定义镜像共享给其他账号（B）创建ECS实例，账号B是否需要为该镜像付费？

账号B需要支付该镜像费用，价格和原镜像市场的镜像价格相同。

如果使用镜像市场的镜像或者来源于镜像市场的镜像进行更换系统盘，需要付费吗？

需要看情况，如果当前的ECS实例使用的镜像和您要更换的镜像属于同一个镜像商品的不同版本的镜像，是不需要付费的，否则是需要付费的。

ECS实例正在使用镜像市场的镜像，更换系统盘需要收费吗？

不会。

怎么调用ECS API，使用镜像市场镜像或者来源镜像市场的自定义镜像或者共享镜像，创建ECS实例和更换系统盘？

1. 确认使用的镜像ID是镜像市场镜像或者是来源于镜像市场的镜像，调用DescribeImages查询到镜像的相关信息。
   如果您使用的镜像的商品标示（`ProductCode`）不为空，表示该镜像是镜像市场的镜像、来源于镜像市场的自定义镜像或者共享镜像。如果使用的镜像的商品标示`ProductCode`为`abcd000111`，您可以访问镜像商品的地址`http://market.aliyun.com/products/123/abcd000111.html`。
2. 需要选择镜像的版本和正确地域，只购买ECS镜像。
   购买某一地域的镜像，只能在该地域的ECS实例上使用。当前每次只能购买一个镜像，如果需要创建多个ECS实例，则需要购买多个镜像。
3. 购买完成后，您可以创建ECS实例和更换系统盘。

如果没有购买镜像市场的镜像或者来源于镜像市场的镜像，在调用ECS API使用该镜像创建ECS实例和更换系统盘，会报错吗？

会报错，错误码为`QuotaExceed.BuyImage`。

我的ESS是自动创建机器的，并且量是不固定，设置最小值为10台，最大值为100台，那么使用镜像市场的镜像如何保证我的需求实例能正常弹出来？

如果您需要弹出n台同类型的镜像，您需要提前购买n台镜像市场的镜像。

镜像市场的镜像是否支持批量购买？

暂不支持批量购买。

如果之前使用的镜像市场的镜像，已不存在该商品（如：jxsc000010、jxsc000019），怎能保证已经设置的弹性伸缩组的机器能正常弹出？

此情况建议您选择镜像市场中可替代的镜像进行替代。

1个product code能否支持不同region的镜像？

支持，前提是该地域region已经支持该商品镜像。

我买了100 product code同样值的镜像，是否可以支持在所有的地域可用？

目前镜像市场的镜像已经具备region属性，请您购买相应地域的镜像。

勾选“I/O优化实例”选项导致购买ECS实例时无法选择镜像市场的镜像，为什么？怎么解决？

有关该问题的分析及解决方案如下：

- 问题现象：在阿里云官网购买ECS实例，选择镜像时，发现无法选取任何镜像市场的镜像。
- 原因分析：该问题可能是由于购买ECS实例时，勾选了**I/O优化实例**选项导致的。
  与普通ECS实例相比，I/O优化实例可在实例与云盘之间提供更好的网络能力，可保证SSD云盘存储发挥最高性能。由于相关优化操作涉及网络、存储和镜像内部相关驱动等，因此并非所有镜像都能支持I/O优化实例。
- 解决方法：购买I/O优化实例时，建议您选择实例支持的官方标准镜像，再自行部署相关业务环境。

如问题依然未解决，请提交工单。

什么是镜像市场的包年包月和按周付费镜像？

镜像市场的包年包月和按周付费镜像是指从阿里云云市场购买的，按周、按月或按年付费使用的镜像。这些镜像由镜像供应商开发并维护，所有售前咨询和售后服务都由镜像供应商提供。在本文中，这类镜像统称为包年包月镜像。

包年包月镜像能与哪种ECS实例搭配使用？

包年包月镜像只能与包年包月实例和按周付费实例搭配使用，而且镜像与ECS实例的付费周期应保持一致。

怎么购买包年包月镜像？可以单独购买吗？

目前您还不能单独购买包年包月镜像。

您可以选择以下任一种方式购买包年包月镜像：

- 在创建ECS实例时，付费方式选择**包年包月**，并从**镜像市场**选择镜像，再选择按周、按月或按年付费。

  > **说明** 在这种情况下，您需要同时支付实例与镜像的费用。如果实例创建成功，表明您已经同时支付了实例与镜像的费用，不会出现其中一项资源购买失败的情况。

- 如果您想在一台已有的包年包月或按周付费ECS实例上使用包年包月镜像，您可以使用更换操作系统功能将操作系统更换为包年包月镜像，此时，您只能按照ECS实例的付费周期选择镜像的付费周期。具体操作方式，请参见更换操作系统（非公共镜像）。

  > **说明** 在这种情况下，您只需要支付镜像的费用。

包年包月镜像怎么付费？

包年包月镜像采用预付费，付费周期应与使用它的包年包月或按周付费ECS实例保持一致。

镜像的价格以供应商提供的信息为准。

包年包月镜像到期了就不能用了吗？怎么继续使用？

包年包月镜像到期后，如果没有及时续费就不能再正常使用。

您不能单独为包年包月镜像续费。如果您需要继续使用该镜像，可以在续费包年包月ECS实例时，同步为镜像续费。续费后即可继续使用该镜像。

购买包年包月镜像后，如果我不想再使用这个镜像，能要求退款吗？

能否退款由镜像供应商决定。您可以在购买之前咨询镜像供应商。

退款时，费用怎么结算？

如果可以退款，镜像供应商将按照您的实际使用情况退款。

包年包月镜像能转换为按量付费镜像吗？

目前不支持转换为按量付费镜像。后续我们会提供这个功能，具体时间请关注阿里云官网公告。

包年包月镜像与其它镜像之间能互换吗？更换后费用怎么计算？

可以。您可以通过ECS实例更换系统盘来更换镜像。更换镜像时有以下几种选择：

- 将其他类别的镜像（如公共镜像、自定义镜像、共享镜像）换成包年包月镜像：更换后，系统将按镜像的费用和ECS实例的剩余付费周期计算实际费用。
- 将包年包月镜像换成其它类别的镜像（如公共镜像、自定义镜像、共享镜像）：如果供应商允许退款，镜像供应商将按照您的实际使用情况退款。
- 将一个包年包月镜像（设为镜像A）换成另一个包年包月镜像（设为镜像B）：更换后，如果镜像 A 允许退款，将按退款方式结算费用，镜像B将按镜像的价格和ECS实例剩余付费周期计算实际费用。

在哪里查看并管理我购买的包年包月镜像？

您可以登录ECS管理控制台，在**镜像** > **镜像市场**中查看并管理您购买的包年包月镜像。

使用包年包月镜像制作的自定义镜像会收费吗？包年包月镜像过期对于自定义镜像有什么影响？

当您使用由包年包月镜像制作的自定义镜像时，无论是使用自定义镜像创建实例，还是更换系统盘，都是重新在镜像市场下单购买镜像的使用权。所以，用于制作自定义镜像的包年包月镜像是否过期，对使用自定义镜像没有影响。

CentOS 8 EOL（停止支持）之后相关的公共镜像会下架吗？

阿里云暂不会下线CentOS 8镜像，您使用CentOS 8创建实例不会受到影响。由于社区已停止更新，阿里云将停止更新镜像。

CentOS 8 EOL（停止支持）之后对我的ECS实例有什么影响？

已经使用CentOS 8创建的ECS实例运行不会受到影响，但是由于社区不再提供支持和安全更新，您的业务有一定的安全风险，建议您尽快迁移。更多信息，请参见CentOS Linux停止维护后如何应对？。

AMD EPYC™ MILAN处理器的实例规格族不支持哪些操作系统？

不支持Ubuntu 18或Debian 9操作系统。由于Ubuntu 18或Debian 9操作系统内核不支持AMD EPYC™ MILAN处理器，当您选用AMD EPYC™ MILAN处理器的实例规格族以及Ubuntu 18或Debian 9镜像创建实例后，实例会启动失败。目前使用AMD EPYC™ MILAN处理器的实例规格族如下所示：

- ecs.g7a
- ecs.r7a
- ecs.c7a
- ecs.ebmg7a
- ecs.ebmr7a
- ecs.ebmc7a

基于弹性裸金属实例规格的ECS实例，系统生成crash dump文件失败如何解决？

问题原因及解决方案，请参见部分ECS实例生成crash dump文件失败如何解决？。

Linux操作系统内核回写时出现softlockup异常如何解决？

部分低版本的Linux操作系统内核在回写（writeback）文件缓存时，会出现softlockup异常。具体的解决方案，请参见Linux操作系统内核回写时出现softlockup异常的解决方案。

在ECS实例内删除cgroup出现softlockup异常如何解决？

具体的解决方案，请参见在ECS实例内删除cgroup出现softlockup异常的解决方案。

ECS实例宕机相关解决方案

- ECS实例宕机并报错“Out of memory and no killable processes”如何处理？
- ECS实例宕机并产生“Objects remaining in kmalloc”告警日志，如何处理？
- ECS实例宕机并产生“RIP:get_target_pstate_use_performance”日志，如何处理？
- ECS实例宕机并产生“VFS: Unable to mount root fs on unknown-block”日志，如何处理？

为什么我无法使用ssh-rsa签名算法的SSH密钥对远程连接Fedora 33 64位系统的实例？

当您使用Fedora 33 64位操作系统的ECS实例时，如果登录凭证设置的是ssh-rsa签名算法的SSH密钥对，可能无法顺利使用SSH远程连接实例。您可以通过以下任一方式解决该问题：

- 将ssh-rsa签名算法的SSH密钥对替换为ECDSA签名算法等其他签名算法的SSH密钥对。
- 在系统中运行**update-crypto-policies --set LEGACY**命令，将加密策略 `POLICY` 切换为 `LEGACY` ，即可继续使用ssh-rsa签名算法的SSH密钥对。

FreeBSD系统如何打补丁编译内核？

阿里云的FreeBSD公共镜像已为内核添加了补丁，已满足系列V及以上的实例规格族的启动需求。具体的实例规格族可通过DescribeInstanceTypeFamilies接口的 `Generation` 参数查询。

以下情况可能导致系统无法正常启动，您可以通过FreeBSD内核源码打补丁编译内核的方式，避免或解决系统无法启动的问题。

- 使用非阿里云提供的FreeBSD镜像及相关自定义镜像创建ECS实例时，系列V及以上实例规格族的ECS实例可能出现无法正常启动的情况。
- 使用FreeBSD公共镜像创建ECS实例，并使用了freebsd-update等更新内核补丁，可能会导致系列V及以上实例规格族的ECS实例无法正常启动。

本示例以FreeBSD 12.3为例，介绍如何使用FreeBSD内核源码打补丁编译内核。

1. 下载并解压FreeBSD内核源码。

```
wget https://mirrors.aliyun.com/freebsd/releases/amd64/12.3-RELEASE/src.txz -O /src.txz
cd /
tar -zxvf /src.txz
```

2. 下载补丁包。
   本示例中，为virtio驱动打补丁包 `0001-virtio.patch` 。

```
cd /usr/src/sys/dev/virtio/
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/0001-virtio.patch
patch -p4 < 0001-virtio.patch
```

3. 复制内核文件，并编译安装内核。
   `make -j<N>` 表示指定编译时的并行数，需要根据您执行编译的环境配置来决定。例如，1 vCPU环境建议设置 `-j2` ，即vCPU核数与变量N的比值为 `1:2` 。

```
cd /usr/src/
cp ./sys/amd64/conf/GENERIC .
make -j2 buildworld KERNCONF=GENERIC
make -j2 buildkernel KERNCONF=GENERIC
make -j2 installkernel KERNCONF=GENERIC
```

4. 编译完成后，删除源码。

```
rm -rf /usr/src/*
rm -rf /usr/src/.*
```

为什么Ubuntu某些版本的ECS实例中启动安骑士进程后系统负载较高？

Ubuntu某些版本（例如Ubuntu 18.04）的ECS实例中，启动安骑士进程（AliYunDun）后，系统平均负载较高。关闭安骑士进程后，系统平均负载恢复正常。

具体的原因和解决方案请参见Ubuntu 18.04版本的ECS实例中启动安骑士进程后系统负载较高。

为什么有的ECS实例无法选择Windows操作系统？

使用Windows 操作系统创建ECS实例时，需要确保实例内存大于等于1GiB。内存低于1GiB的ECS实例（例如， 512MiB）只能选择Linux镜像和Windows Server 1709镜像。

阿里云是否支持Windows Server 2008和Windows Server 2008 R2操作系统？

微软已经于2020年1月14日停止对Windows Server 2008和Windows Server 2008 R2操作系统提供支持。因此阿里云不再对使用上述操作系统的ECS实例提供技术支持。如果您有使用上述操作系统的ECS实例，请尽快更新至Windows Server 2012或以上版本。

实例的操作系统为Windows Server，现在提示Windows副本不是正版怎么办？

激活Windows，详情请参见VPC环境下ECS Windows系统激活方法。如果在激活中遇到问题，请参见Windows系统ECS实例激活失败。

ECS实例使用操作系统需要付费吗？

使用公共镜像Windows Server、Red Hat和SUSE需付费，计费与实例规格大小有关，其余公共镜像均免费。其他类型镜像的费用详情，请参见镜像概述。

我能自己安装或者升级操作系统吗？

您可以通过以下方式安装或者升级操作系统：

- 更换系统盘重新选择操作系统。具体操作，请参见更换操作系统或批量升级操作系统。
- 从本地导入自己的镜像后使用自定义镜像创建ECS实例。
  - 关于如何导入镜像，请参见导入镜像必读。
  - 关于如何使用自定义镜像创建ECS实例，请参见使用自定义镜像创建实例。
- 为操作系统打补丁。

操作系统是否有图形界面？

除Windows Server半年渠道实例以外，Windows操作系统是桌面管理形式。有关如何使用Windows Server半年渠道操作系统，请参见Windows Server半年渠道镜像与实例管理。

Linux 操作系统是命令行形式，您可以根据需要安装图形化桌面。

如何选择操作系统？

选择操作系统，请参见选择镜像。

公共镜像自带FTP上传吗？

不自带，需要您自己安装配置。具体步骤，请参见手动搭建FTP站点（Windows）和手动搭建FTP站点（CentOS 7）。

阿里云支持哪些SUSE版本？

目前，公共镜像支持的SUSE版本，请参见Linux公共镜像列表。

SUSE操作系统提供哪些服务支持？

阿里云线上售卖的SLES（SUSE Linux Enterprise Server）操作系统会与SUSE更新源保持定时同步。使用SLES公共镜像创建的实例，其操作系统的支持服务涵盖在阿里云的企业级别支持服务中。如果您购买了企业级支持服务，可以提交工单获取帮助，阿里云工程师团队会协助您解决SLES操作系统上发生的问题。

ECS实例到期释放后，如果这个实例之前手动制作了镜像快照，能不能找回之前实例的数据？

可以。您可通过以下任一方式找回实例数据：

- 使用之前制作的镜像创建新实例。具体步骤，请参见使用自定义镜像创建实例。
- 使用之前制作的镜像为当前实例更换系统盘。具体步骤，请参见更换操作系统（非公共镜像）。

> **注意** 更换系统盘操作须注意以下两点：
> - 当前实例系统盘的内容会全部丢失，恢复为镜像的状态。
> - 镜像必须和您当前实例位于同一地域。

我先有一台ECS实例，想再买一台ECS实例并使用现有这台ECS实例的镜像部署，应该如何操作？

您可以为之前的ECS实例创建自定义镜像，然后使用该自定义镜像创建ECS实例即可。具体步骤，请参见使用实例创建自定义镜像和使用自定义镜像创建实例。

我已经购买了新的ECS实例，如何把我的共享镜像恢复到这台新购ECS服务器上？

请确保您已将镜像共享给新购服务器的账号，并根据实际情况选择下列方法之一进行操作。

- 如果共享镜像和新购服务器在同一个地域，可以更换系统盘，更换时选择您共享的镜像即可。具体步骤，请参见更换操作系统（非公共镜像）。
- 如果共享镜像和新购服务器不在同一个地域，需要先复制镜像到目标地域，再通过更换系统盘来更换镜像。具体步骤，请参见复制镜像和更换操作系统（非公共镜像）。

> **注意** 更换系统盘存在如下风险：
> - 原系统盘会被释放，建议您提前创建快照备份数据。
> - 更换系统盘需要停止实例，因此会中断您的业务。
> - 更换系统盘完成后，您需要在新的系统盘中重新部署业务运行环境，有可能会对您的业务造成长时间的中断。
> - 更换系统盘是重新为您的实例分配一个系统盘，磁盘ID会改变，所以基于旧的系统盘创建的快照将不能用于回滚新的系统盘。

我在阿里云有多个账号，想把账号A的一台ECS实例转移到账号B，或者用账号A购买一台ECS实例，把实例运行环境、应用迁移到账号B。怎么操作？

您可以通过下列步骤操作：

1. 使用账号A的实例创建自定义镜像。具体步骤，请参见使用实例创建自定义镜像。
2. 共享镜像给账号B。具体步骤，请参见共享或取消共享镜像。
3. 账号B使用共享镜像创建实例。具体步骤，请参见使用自定义镜像创建实例。

ECS实例之间如何迁移？

ECS实例间迁移步骤如下：

1. 为源ECS实例创建自定义镜像。
2. 根据源ECS实例与目标ECS实例的归属地域和归属账号，迁移分为以下几种情况。
   - 源实例与目标实例属于同地域同账号，可直接进入下一步。
   - 源实例与目标实例属于不同地域，需复制镜像至目标实例所在地域。详情请参见复制镜像。
   - 源实例与目标实例属于不同账号，需共享镜像给目标实例的账号。详情请参见共享或取消共享镜像。
   - 源实例与目标实例属于不同地域和不同账号，需先复制镜像到目标地域，再分享给目标实例的账号。详情请参见复制镜像和共享或取消共享镜像。
3. 使用镜像创建新的ECS实例，或为现有目标ECS实例更换镜像。详情请参见使用自定义镜像创建实例或更换操作系统（镜像）。

   > **说明** 为现有目标ECS实例更换镜像时，源镜像中不能包含数据盘快照。

以上迁移步骤不适用时，请参见阿里云ECS实例间迁移。

两个不同专有网络下的ECS实例能否实现网络互通？

内网互通可以通过高速通道和云企业网实现，详情请参见 *云企业网文档*使用云企业网实现跨地域网络实例互通。

如何处理CentOS DNS解析超时？

处理CentOS DNS解析超时的详情如下：

- 原因分析
  因CentOS 6和CentOS 7的DNS解析机制变动，导致2017年2月22日以前创建的ECS实例或使用2017年2月22日以前的自定义镜像创建的CentOS 6和CentOS 7实例可能出现DNS解析超时的情况。
- 解决方法
  请按下列步骤操作修复此问题：
  i. 下载脚本fix_dns.sh。

ii. 将下载的脚本放至CentOS系统的*/tmp*目录下。

iii. 运行**bash /tmp/fix_dns.sh**命令，执行脚本。

- 脚本作用
  判断DNS解析文件*/etc/resolv.conf*中是否存在 `options` > `single-request-reopen` 配置。详情请参见resolv.conf文件说明。
  CentOS 6和CentOS 7的DNS解析机制，使用相同的网络五元组发送IPV4 DNS请求和IPV6 DNS请求，此时应开启 `single-request-reopen` 配置。开启该配置后，一旦需要处理同一socket发送的两次请求时，解析端会在发送第一次请求后关闭socket，并在发送第二次请求前打开新的socket。配置成功后，无需重启实例即可生效。
- 脚本逻辑

  i. 判断实例系统是否为CentOS。
  - 如果实例为非CentOS系统（如Ubuntu和Debian）：脚本停止工作。
  - 如果实例为CentOS系统：脚本继续工作。

  ii. 查询解析文件*/etc/resolv.conf*中 `options` 的配置情况。
  - 如果不存在 `options` 配置：
    默认使用阿里云 `options` 配置 `options timeout:2 attempts:3 rotate single-request-reopen` 。

    ```
    options timeout:2 attempts:3 rotate single-request-reopen
    ; generated by /sbin/dhclient-script
    ```

  - 如果存在 `options` 配置：
    - 不存在 `single-request-reopen` 配置，则在 `options` 配置中追加该项。
    - 存在 `single-request-reopen` 配置，则脚本停止工作，不更改DNS nameserver的配置。

为什么ECS默认没有启用虚拟内存或Swap说明？

Swap分区或虚拟内存文件，是在系统物理内存不够用的时候，由系统内存管理程序将那些很长时间没有操作的内存数据，临时保存到Swap分区或虚拟内存文件中，以提高可用内存额度的一种机制。

但是，如果在内存使用率已经非常高，而同时I/O性能也不是很好的情况下，该机制其实会起到相反的效果。阿里云ECS云盘使用了分布式文件系统作为云服务器的存储，对每一份数据都进行了强一致的多份拷贝。该机制在保证用户数据安全的同时，由于3倍增涨的I/O操作，会降低本地磁盘的存储性能和I/O性能。

综上，为了避免当系统资源不足时进一步降低ECS云磁盘的I/O性能，所以Windows系统实例默认没有启用虚拟内存，Linux系统实例默认未配置Swap分区。

如何在公共镜像中开启kdump？

公共镜像中默认未开启kdump服务。若您需要实例在宕机时，生成core文件，并以此分析宕机原因，请参见以下步骤开启kdump服务。本步骤以公共镜像CentOS 7.2为例。实际操作时，请以您的操作系统为准。

1. 设置core文件生成目录。

   i. 运行**vim /etc/kdump.conf**打开kdump配置文件。vim命令使用详情，请参见Vim教程。

   ii. 设置path为core文件的生成目录。本示例中，在*/var/crash*目录下生成core文件，则path的设置如下。

   ```
   path /var/crash
   ```

   iii. 保存并关闭*/etc/kdump.conf*文件。

2. 开启kdump服务。

根据操作系统对命令的支持情况，选择开启方式。本示例中，CentOS 7.2使用方法一开启kdump服务。

- 方法一： 依次运行以下命令开启kdump服务。

```
systemctl enable kdump.service
```

```
systemctl start kdump.service
```

- 方法二： 依次运行以下命令开启kdump服务。

```
chkconfig kdump on
```

```
service kdump start
```

3. 运行以下命令模拟宕机。

```
echo c > /proc/sysrq-trigger
```

> **说明** 运行该命令后，实例会与网络失去连接。您需要重新连接实例，完成后续操作。

4. 分析core文件。
   i. 运行以下命令安装Crash分析工具。

```
yum install crash
```

   ii. 下载debug-info安装包。
   运行**uname -r**命令查看操作系统内核版本，下载相应版本的debug-info包。
   - *kernel-debuginfo-common-x86_64-<内核版本>.rpm*
   - *kernel-debuginfo-<内核版本>.rpm*

> **说明** 不同CentOS版本的debug-info包下载地址有所不同。您可以通过CentOS官网查找对应版本软件包的下载地址，具体请参见CentOS debuginfo软件包。

   本示例中，系统的内核版本为 `3.10.0-514.26.2.el7.x86_64` ，因此下载命令为：

```
wget http://debuginfo.centos.org/7/x86_64/kernel-debuginfo-common-x86_64-3.10.0-514
.26.2.el7.x86_64.rpm
```

```
wget http://debuginfo.centos.org/7/x86_64/kernel-debuginfo-3.10.0-514.26.2.el7.x86_
64.rpm
```

   iii. 依次运行下列命令，安装debug-info包。

```
rpm -ivh kernel-debuginfo-common-x86_64-3.10.0-514.26.2.el7.x86_64.rpm
```

```
rpm -ivh kernel-debuginfo-3.10.0-514.26.2.el7.x86_64.rpm
```

iv. 依次运行以下命令使用Crash工具分析core文件。

```
cd <core文件的生成目录>
```

```
crash /usr/lib/debug/lib/modules/<内核版本号>/vmlinux vmcore
```

本示例中，core文件的生成目录为*/var/crash/127.0.0.1-2019-07-08-15:52:25*，内核版本号为 `3.10.0-514.26.2.el7.x86_64` ，因此运行的命令为：

```
cd /var/crash/127.0.0.1-2019-07-08-15:52:25
```

```
crash /usr/lib/debug/lib/modules/3.10.0-514.26.2.el7.x86_64/vmlinux vmcore
```

RHEL（Red Hat Enterprise Linux）镜像中如何获取dump文件？

当前部分RHEL镜像默认未开启kdump，您可以提交工单获取dump文件。请注意，通过提交工单获取dump文件时，内存大于16 GiB的实例规格可能出现无法获取dump文件的情况，详情请以工单内信息为准。

如何在RedHat 8.1系统的ECS实例中开启kdump？

RedHat 8.1 v1版本镜像中kdump服务默认未开启。如果您需要使用kdump，请运行以下命令开启kdump服务。

```
systemctl enable kdump
systemctl start kdump
```

如何解决RedHat 8.1/8.2镜像在弹性裸金属服务器实例规格族的ECS实例下启动慢的问题？

在弹性裸金属服务器实例规格族的ECS实例中，RedHat 8.1/8.2镜像相较于RedHat 7镜像启动时长多1~2分钟。为解决该问题，您可以在RedHat 8.1/8.2系统的*/boot/grub2/grubenv*文件中，将内核启动参数 `console=ttyS0 console=ttyS0,115200n8` 修改为 `console=tty0 console=ttyS0,115200n8` ，然后重启服务器使配置生效。

vSwitch中实例数量过多导致CentOS实例夯机或异常重启，怎么办？

问题原因及解决方法，请参见vSwitch中实例数量过多导致CentOS实例夯机或异常重启的问题。

如何检查与修复CentOS 7实例和Windows实例IP地址缺失问题？

问题原因及解决方案，请参见如何检查与修复CentOS 7实例和Windows实例IP地址缺失问题。

历史Linux镜像问题修复方案有哪些？

历史Linux镜像创建的ECS云服务器，可能存在NTP、阿里云软件源没有配置的情况，还可能存在安全漏洞。修复这些问题，可以让您的云服务器更加安全，可以使用阿里云提供的免费NTP服务器进行时间同步，还可以使用阿里云提供的软件源服务安装软件。修复方法如下：

- 配置NTP服务，请参见配置Linux实例NTP服务（CentOS 6）。
- 添加阿里云软件源，请参见添加软件源。
- 主要修复目前已知的重大安全漏洞，需要升级的软件包括： bash 、glibc 、 openssl 、wget 、ntp 。在执行如下命令之前，需要确保系统当前的软件源已经正确设置。
  - CentOS和Aliyun Linux系统：**yum update bash glibc openssl wget ntp**
  - Ubuntu和Debian系统：**apt-get install bash libc6 libc-bin openssl wget ntp**

ECS实例启动时报错“UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.”，怎么办？

该问题可能是由于断电等情况，导致ECS实例内存数据丢失引发的文件系统错误。问题详情及修复方案，请参见ECS实例系统启动失败时报“UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.”的错误。

如何从RHEL 7升级到RHEL 8（Red Hat Enterprise Linux 8）？

升级文档请参见 从RHEL 7升级到RHEL 8。

如何设置Linux系统的ECS实例的静态IP地址？

您需要远程连接ECS实例进行设置，具体步骤请参见Linux系统的ECS实例如何设置静态IP地址。

CentOS/RedHat 7.x升级Systemd重启进入救援模式如何处理？

CentOS 7或RedHat 7系列的系统在升级Systemd至systemd-219-71.el7版本后，重启实例会进入救援模式，这样会导致系统网络服务和一般的应用软件服务异常。具体解决方案请参见CentOS 7.X或RedHat 7.X升级Systemd并重启后会进入救援模式。

如何在Linux实例中自定义配置DNS？

具体操作，请参见如何在Linux实例中自定义配置DNS。

在部署业务时如何让程序区分不同的ECS实例？

当您在Linux系统上部署业务时希望程序能够区分不同的ECS实例，可能会通过**systemd-machine-id-setup**命令重置*/etc/machine-id*的方式来实现，但该方式需要您在每台ECS实例上重新生成machine ID。为免去繁琐的操作，阿里云推荐您通过*/sys/class/dmi/id/product_uuid*文件来区分不同的ECS实例，该文件作为实例对外的唯一标识之一，可完全取代*/etc/machine-id*的作用，并且操作简便，只需要获取实例对应的UUID即可。您可以运行以下命令查看ECS实例的*/sys/class/dmi/id/product_uuid*信息：

```
cat /sys/class/dmi/id/product_uuid
```

返回结果示例：

```
[root@test ~]# cat /sys/class/dmi/id/product_uuid
44CC9932-AF69-[redacted]
```

为什么使用Fedora CoreOS镜像创建部分实例后，CPU信息只有实例规格的一半？

使用Fedora CoreOS镜像创建部分实例（例如，通用型实例规格族g5）后，执行**lscpu**命令查看CPU信息，`On-line CPU(s) list`的总个数只有实例实际规格的一半。例如，创建实例时选择的CPU为2核，则`On-line CPU(s) list`个数只有1个。示例如下图所示。

```
[core@iZbp1fjhzdqnsr47keavplZ ~]$ lscpu
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   46 bits physical, 48 bits virtual
CPU(s):                          2
On-line CPU(s) list:             0
Off-line CPU(s) list:            1
Thread(s) per core:              1
```

> **说明** `On-line CPU(s) list`参数值代表CPU编号，图中示例表示只有0号CPU可用。

这是因为Fedora CoreOS镜像的内核默认配置了 `mitigations=auto,nosmt` 启动参数，会自动为有漏洞的系统禁用同步多线程技术SMT（Simultaneous Multi-Threading），导致可用CPU减半。 `mitigations=auto,nosmt` 参数可以通过执行cat /proc/cmdline命令查看。

关于SMT的更多信息，请参见Automatically disable SMT when needed to address vulnerabilities和Policy for disabling SMT。

Linux操作系统配置IPv6地址后，安装了NTP服务的服务器时间无法同步，如何处理？

- 问题现象：在服务器上执行 `ntpq -p` 同步时间时，返回超时。
- 解决方法：

> **说明** 本方法适用于CentOS 7及以下、Ubuntu 20.04及以下、Anolis OS（ANCK\RHCK）、Alibaba Cloud Linux、Debian等系列操作系统。

i. 远程连接Linux实例。
具体操作，请参见通过密码或密钥认证登录Linux实例。

ii. 运行以下命令，修改*/etc/ntp.conf*配置文件。

```
vi /etc/ntp.conf
```

iii. 按*i*键进入编辑模式。

iv. 在文件中添加 `restrict -6 ::1` 内容。

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

vi. 运行以下命令，重启NTP服务。

```
systemctl restart ntp
```

13.2. 如何手动更新Windows实例的virtio驱动？

如果您需要手动更新Windows实例的virtio驱动，可以参考本文介绍的方式完成驱动更新。

操作流程

1. 创建快照备份数据。

   建议您为Windows实例创建快照备份数据，如果更新virtio驱动时造成实例异常，可通过快照回滚实例中的数据。具体操作，请参见创建一个云盘快照。

2. 关闭第三方杀毒软件。

   为确保virtio驱动的更新脚本或云助手插件顺利执行，建议您登录Windows实例，临时关闭实例中已安装的第三方杀毒软件（实例自带的杀毒软件无需关闭）。如果您确认您的Windows实例无需更新virtio驱动或者驱动已成功更新，请及时重启第三方杀毒软件。

3. 通过云安全中心或者手动检测Windows实例中的virtio驱动是否需要更新。
   - 您可以通过阿里云云安全中心的漏洞修复功能检测Windows实例中的virtio驱动是否需要更新。具体操作，请参见通过云安全中心一键更新virtio驱动。

> **注意** 云安全中心提供了多种版本，不同版本支持的功能不同。更多信息，请参见功能特性。如果您的云安全中心是免费版或其他仅支持漏洞检测，但不支持漏洞修复的版本。您可以通过漏洞修复的检测机制查看需要更新驱动的Windows实例信息，然后手动更新驱动。

- 您可以手动检查是否需要更新Windows实例的virtio驱动。具体操作，请参见手动检查是否需要更新virtio驱动。

4. 手动更新virtio驱动。

   您可以根据实际情况，选择以下任一方式手动更新virtio驱动：

   > **注意** 手动更新virtio驱动时涉及网卡驱动的更新，因此ECS实例的网络会中断10秒左右。您需要注意网络中断所造成的业务影响。

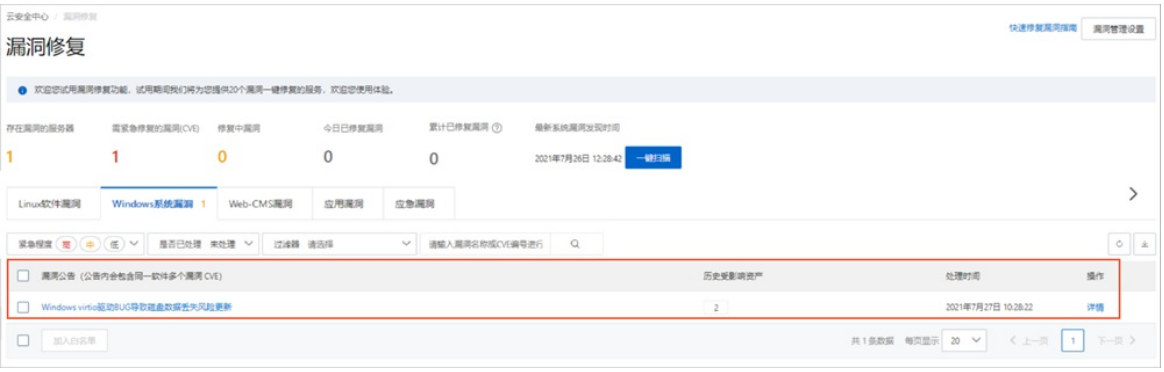
   - 如果您的Windows实例能够访问公网，建议您使用脚本快速更新。具体操作，请参见手动更新方式一：使用脚本更新驱动。
   - 如果您的Windows实例不具备公网访问能力，建议您上传virtio驱动的压缩包，手动更新驱动。具体操作，请参见手动更新方式二：通过安装包更新驱动。
   - 如果您存在多台ECS实例需要更新virtio驱动，且Windows实例能够访问公网或者专有网络VPC的内网，建议通过阿里云的云助手功能批量更新。具体操作，请参见手动更新方式三：使用云助手批量更新驱动。

   > **说明** 如果您通过脚本更新virtio驱动失败，建议您尝试使用云助手插件（`acs-plugin-manager.exe --exec --plugin=UpdateVirtIo`）更新virtio驱动。如果仍然更新失败，请提交工单。

通过云安全中心一键更新virtio驱动

阿里云云安全中心针对旧版本virtio驱动可能产生的影响，提供了检测以及一键修复功能。本操作步骤中，主要介绍如何通过云安全中心的漏洞修复功能检测并一键更新virtio驱动。关于云安全中心漏洞修复功能的更多信息，请参见漏洞修复概述。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面，单击**Windows系统漏洞**页签。
4. 从**是否已处理**下拉列表中，选择**未处理**，然后在漏洞公告列表，查看是否存在**Windows virtio驱动BUG导致磁盘数据丢失风险更新**。



漏洞公告说明：

- 如果不存在该漏洞公告，说明您的阿里云账号下没有需要更新virtio驱动的Windows实例，您无需再

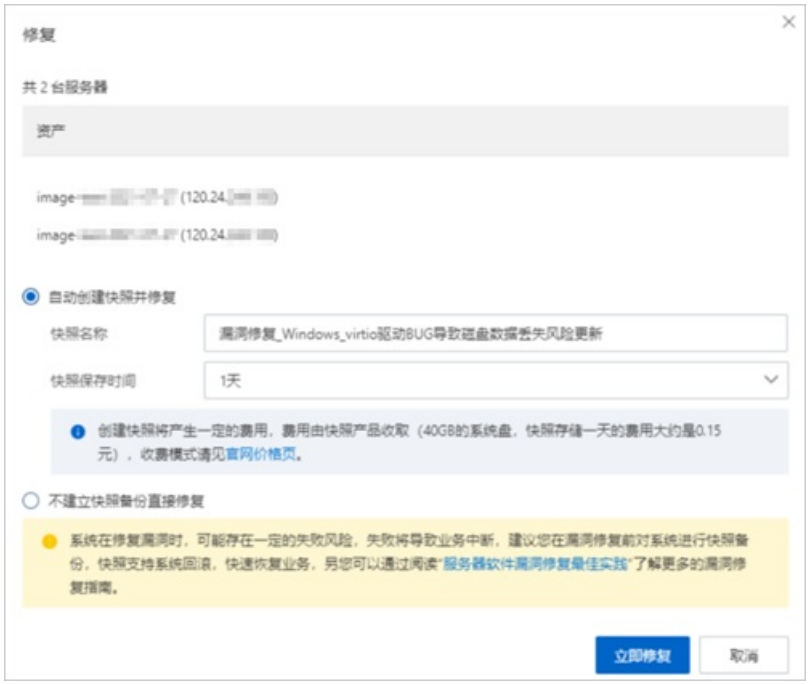
进行本文中的任何操作。

- 如果存在该漏洞公告，您可以根据云安全中心的不同版本，选择以下不同的驱动更新操作。关于云安全中心不同版本对漏洞修复的支持情况，请参见漏洞修复。
  - 如果您的云安全中心版本仅支持检测漏洞，但不支持修复漏洞。您需要根据本文提供的手动更新方式，完成virtio驱动更新。
  - 如果您的云安全中心版本支持检测并一键修复漏洞，请参考本操作步骤完成驱动更新。

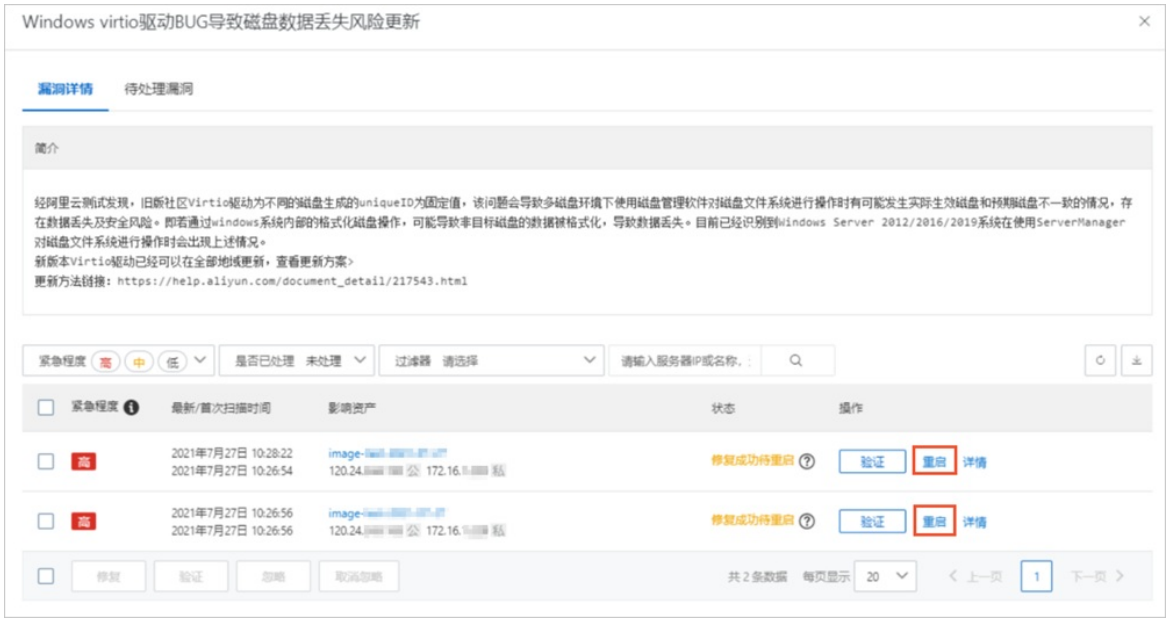
5. 单击**Windows virtio驱动BUG导致磁盘数据丢失风险更新**漏洞名称，进入漏洞详情页。
6. 在**漏洞详情**页签，选中所有待更新virtio驱动的Windows实例，然后在资源列表下方，单击**修复**。

7. 在**修复**页面，单击**立即修复**。

   您可以手动选择是否为待修复的ECS实例创建快照，建议您选择**自动创建快照并修复**。如果您确保在修复前，已经为各台实例创建了快照，可以选择**不建立快照备份直接修复**。



8. 等待修复成功后，在资源列表的**操作**列，单击**重启**，重启所有完成漏洞修复的Windows实例。



重启实例后，在**漏洞详情**页签的资源列表中，**状态**列将显示**重启成功**。

9. 查看已处理的漏洞详情。
   i. 返回**漏洞修复**页面，单击**Windows系统漏洞**页签。

ii. 从**是否已处理**下拉列表中，选择**已处理**，然后在漏洞公告列表，单击**Windows virtio驱动BUG导致磁盘数据丢失风险更新**。
如下图所示，在**漏洞详情**页签，可以查看到修复成功的资源信息。

手动检查是否需要更新virtio驱动

在更新virtio驱动前，您可以在Windows实例中运行命令检查是否需要更新驱动。当您根据本文提供的任一方式更新驱动后，也可以再次检查Windows实例中的virtio驱动是否已更新为最新版。

1. 远程连接Windows实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 在桌面按下*Win+R*组合键，打开**运行**对话框。
3. 输入**powershell**进入PowerShell命令行。
4. 运行以下命令，查看virtio驱动的版本信息。

```
[System.Diagnostics.FileVersionInfo]::GetVersionInfo("C:\Windows\System32\drivers\viostor.sys")
```

   命令行回显信息如下图所示。如果产品版本（**ProductVersion**）低于 `58017` ，阿里云建议您参考本文更新驱动。

```
PS C:\Users\Administrator> [System.Diagnostics.FileVersionInfo]::GetVersionInfo("C:\Windows\System32\drivers\viostor.sys")

ProductVersion   FileVersion      FileName
--------------   -----------      --------
100.61.101.58017 100.61.101.58017 C:\Windows\System32\drivers\viostor.sys
```

5. 运行以下命令，查看当前服务器中的磁盘唯一标识。

```
Get-Disk | Select-Object uniqueid
```

   命令行回显信息如下图所示。如果**uniqueid**的值为 `141463431303031` ，或者非 `000000` 开头的标识，阿里云建议您参考本文更新驱动。

```
PS C:\Users\Administrator> Get-Disk | Select-Object uniqueid

uniqueid
--------
0000000000000004
```

手动更新方式一：使用脚本更新驱动

如果您的Windows实例能够访问公网，可以通过该方式快速更新virtio驱动。

1. 远程连接待更新驱动的Windows实例。

   具体操作，请参见连接方式介绍。

2. 在Windows实例中，下载用于更新virtio驱动的脚本。

   下载地址：InstallVirtIo.ps1

3. 执行*InstallVirtIo.ps1*脚本更新virtio驱动。

   例如，您将脚本*InstallVirtIo.ps1*下载到了*C:\test*目录下。

   i. 打开*C:\test*文件夹。

      您需要打开*InstallVirtIo.ps1*实际的下载目录。

   ii. 选中*InstallVirtIo.ps1*文件，单击鼠标右键，然后单击**使用 PowerShell 运行**。

   您也可以在文件夹的空白区域，按下*Shift*键的同时，单击鼠标右键，然后单击**在此处打开 Powershell 窗口(S)**。在Windows PowerShell中手动执行*InstallVirtIo.ps1*脚本。

   > **说明**
   >
   > - 如果您当前Windows实例的登录用户为普通用户，需要以管理员权限执行脚本。如果是系统用户，则可以直接执行脚本。
   > - 如果您在手动执行脚本时，系统提示您禁止执行脚本，则需要您先修改PowerShell的脚本执行策略。具体操作，请参见常见问题。

4. 脚本执行完成后，重启Windows实例。

   具体操作，请参见重启实例。重启实例后，virtio驱动更新才会生效。

手动更新方式二：通过安装包更新驱动

如果您的Windows实例不具备公网访问能力，可以通过该方式更新virtio驱动。

1. 在本地主机上，下载阿里云提供的virtio驱动压缩包。

   下载地址：virtio驱动压缩包

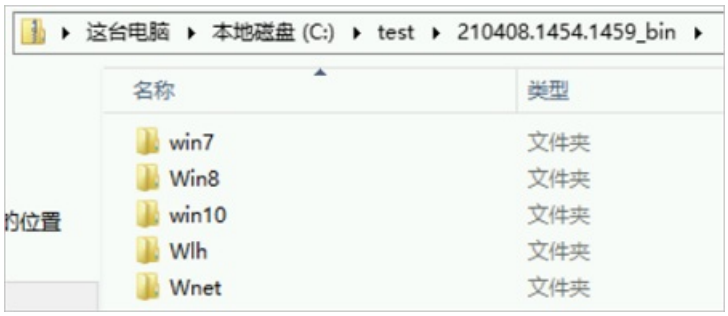
   成功下载后，您可以查看到名为*210408.1454.1459_bin.zip*的压缩包。

2. 将*210408.1454.1459_bin.zip*上传至Windows实例。

   您可以使用以下任一方式上传文件：

- 本地操作系统为Windows时，可以使用Windows远程桌面连接工具连接Windows实例，并完成文件的上传。
- 为Windows实例搭建FTP服务，然后通过FTP客户端将文件上传至Windows实例。更多信息，请参见手动搭建FTP站点（Windows）。

3. 在Windows实例中，解压*210408.1454.1459_bin.zip*，然后打开*210408.1454.1459_bin*文件夹。
   打开文件夹后，您可以查看到不同Windows操作系统版本对应的文件夹。



   各个文件夹中保存不同操作系统适用的驱动。您只需关注以下文件夹：
   - *win10*目录中保存的驱动适用于：Windows Server 2016、Windows Server 2019以及Windows 10。
   - *Win8*目录中保存的驱动适用于：Windows Server 2012 R2、Windows 8.1。
   - *win7*目录中保存的驱动适用于：Windows Server 2008 R2、Windows 7。

   每个文件夹中的驱动按照amd64架构和x86架构区分，amd64架构对应64位操作系统，x86架构对应32位操作系统。

4. 根据Windows实例当前的操作系统版本，选择打开对应的文件夹。

   例如，本示例中Windows实例的操作系统版本为Windows Server 2012 R2 64位，则打开的文件夹路径为*C:\test\210408.1454.1459_bin\Win8\amd64*。

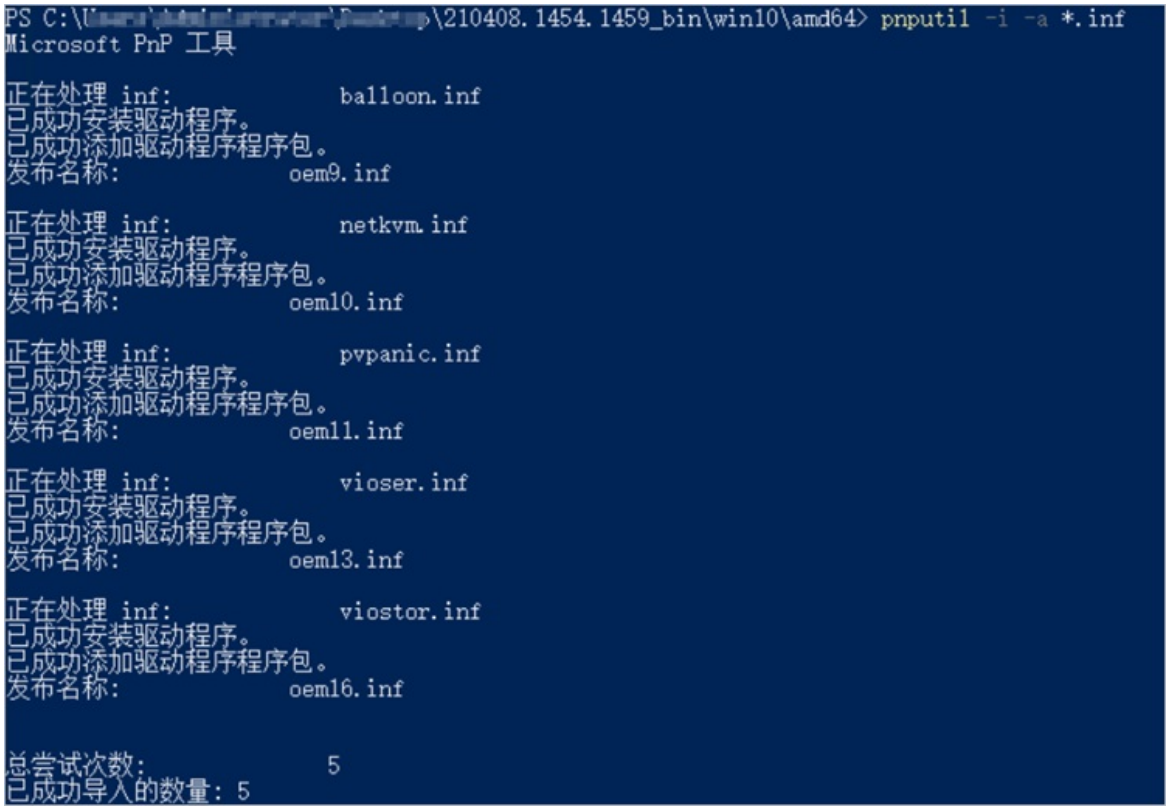
5. 在*amd64*文件夹内的空白区域，按下*Shift*键的同时，单击鼠标右键，然后单击**在此处打开Powershell 窗口(S)**。

6. 在Windows Powershell中，运行以下命令，安装新版virtio驱动。

> **说明** 如果您当前Windows实例的登录用户为普通用户，需要以管理员权限运行该命令。如果是系统用户，则可以直接运行该命令。

```
pnputil -i -a *.inf
```

如下图所示，表示virtio驱动安装成功。



7. 重启Windows实例。
   具体操作，请参见重启实例。重启实例后，virtio驱动更新才会生效。

手动更新方式三：使用云助手批量更新驱动

如果您存在多台ECS实例需要更新virtio驱动，且Windows实例能够访问公网或者专有网络VPC的内网，可以通过阿里云的云助手功能批量更新。

> **说明** 通过云助手更新virtio驱动时，需要下载驱动相关的安装包，系统会优先访问VPC内网进行下载，如果VPC内网访问受限导致下载失败，系统再访问公网进行下载。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**运维与监控 > 发送命令/文件（云助手）**。
3. 在顶部菜单栏，选择地域。

   选择的地域需要与您ECS实例所属的地域保持一致。
4. 使用云助手批量更新驱动。

   您可以通过云助手手动设置命令内容，完成驱动更新，也可以通过云助手的公共命令快速完成驱动更新。本文分别介绍不同的云助手更新驱动方式。

   - （推荐）通过公共命令批量更新驱动

a. 在**ECS云助手**页面，单击**公共命令**，然后在搜索栏中输入 `ACS-ECS-InstallVirtioDriver-windows.ps1` 进行搜索。

b. 在公共命令 `ACS-ECS-InstallVirtioDriver-windows.ps1` 的**操作**列，单击**执行**。

c. 在**执行命令**面板的**选择实例**区域，选中需要更新驱动的实例ID。

- 手动设置命令内容批量更新驱动

a. 在**ECS云助手**页面，单击**创建/执行命令**。

b. 在**创建命令**面板，完成以下配置。

- 在**命令信息**区域，必填参数说明如下表所示，其它参数保持默认值即可。

参数	说明
命令来源	单击**输入命令内容**。
命令名称	自定义名称或保持默认名称。
执行计划	单击**立即执行**。
命令类型	单击**PowerShell**。
命令内容	以下任一方式均可完成virtio驱动的更新： ■ 通过*InstallVirtIo.ps1*脚本更新virtio驱动。 您需要在本地主机下载InstallVirtIo.ps1脚本，然后将脚本的内容完整复制到云助手的命令内容中。 ■ 通过云助手插件更新virtio驱动。 将以下命令复制到云助手的命令内容中。 `acs-plugin-manager.exe --exec --plugin=UpdateVirtIo`

- 在**选择实例**区域，选中需要更新驱动的实例ID。

5. 单击**执行**。
您可以在**命令执行结果**页签查看命令的执行结果。具体操作，请参见控制台查看执行结果。多台ECS实例的其中一台实例内命令执行结果信息如下图所示，表示该实例成功更新virtio驱动。

```
发布名称：                oem8.inf

正在处理 inf:                pvpanic.inf
已成功安装驱动程序。
已成功添加驱动程序程序包。
发布名称：                oem9.inf

正在处理 inf:                vioser.inf
已成功安装驱动程序。
已成功添加驱动程序程序包。
发布名称：                oem10.inf

正在处理 inf:                viostor.inf
已成功安装驱动程序。
已成功添加驱动程序程序包。
发布名称：                oem11.inf


总尝试次数：                5
已成功导入的数量：5
```

6. 批量重启多台Windows实例。
   具体操作，请参见重启实例。重启实例后，virtio驱动更新才会生效。

常见问题

- 问题一：PowerShell中禁止运行脚本怎么办？

```
PS C:\[illegible]> .\InstallVirtIo.ps1
.\InstallVirtIo.ps1 : 无法加载文件 C:\[illegible]\InstallVirtIo.ps1，因为在此系统上禁止运行脚本。有关详
细信息，请参阅 https:/go.microsoft.com/fwlink/?LinkID=135170 中的 about_Execution_Policies。
所在位置 行:1 字符: 1
+ .\InstallVirtIo.ps1
+
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\[illegible]>
```

解决方案：部分Windows操作系统版本中，PowerShell为保障安全性，默认禁止运行脚本。您可以修改PowerShell的脚本执行策略，使PowerShell支持运行脚本。具体操作如下：

i. 运行以下命令，使PowerShell支持运行脚本。

```
Set-ExecutionPolicy Unrestricted
```

ii. 在命令行输入 `A` ，然后按下*Enter*键，更改策略。

```
PS C:\[illegible]> Set-ExecutionPolicy Unrestricted

执行策略更改
执行策略可帮助你防止执行不信任的脚本。更改执行策略可能会产生安全风险，如 https:/go.microsoft.com/fwlink/?LinkID=135170
中的 about_Execution_Policies 帮助主题所述。是否要更改执行策略？
[Y] 是(Y)  [A] 全是(A)  [N] 否(N)  [L] 全否(L)  [S] 暂停(S)  [?] 帮助 (默认值为“N”): A
```

iii. 再次手动运行脚本。

iv. PowerShell为保证系统安全，将在命令行中回显安全警告，您需要在命令行输入 `R` ，然后按下*Enter*键，运行一次脚本。

v. 当脚本被成功运行后，建议运行以下命令，恢复PowerShell的默认配置，以保证系统安全。

```
Set-ExecutionPolicy Restricted
```

vi. 在命令行输入 `A` ，然后按下*Enter*键，更改策略。

- 问题二：更新virtio驱动后，网卡驱动提示没有数字签名如何解决？
  解决方案：您可以手动下载最新的Windows驱动程序包，替换存在问题的网卡驱动，以解决该问题。具体操作如下：

  i. 远程连接目标Windows实例。
     具体操作，请参见通过密码认证登录Windows实例。

  ii. 下载最新的Windows驱动程序包。

> **说明** 如果您的Windows实例不能成功下载该驱动包，您可以先将驱动包下载至本地物理主机，然后通过远程桌面连接工具、FTP等方式将驱动包上传至Windows实例。搭建FTP站点的具体操作，请参见手动搭建FTP站点（Windows）。

成功下载后，您可以查看到名为*new_virtio.zip*的驱动程序包。

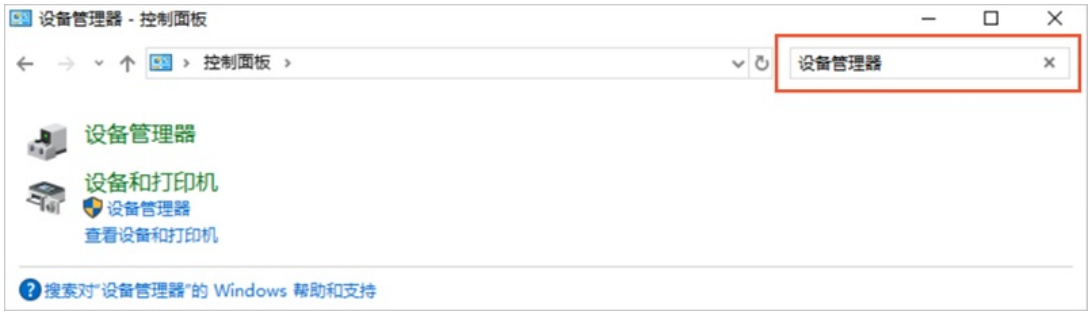
iii. 解压Windows驱动程序包，然后打开*new_virtio*文件夹进行查看。
打开文件夹后，您可以查看到不同Windows操作系统版本对应的文件夹。

各个文件夹中保存不同操作系统适用的驱动。您只需关注以下文件夹：

- *win10*目录中保存的驱动适用于：Windows Server 2016、Windows Server 2019以及Windows 10。
- *Win8*目录中保存的驱动适用于：Windows Server 2012 R2、Windows 8.1。
- *win7*目录中保存的驱动适用于：Windows Server 2008 R2、Windows 7。

iv. 卸载Windows实例中的网卡驱动。
本示例以Windows Server 2019 64位为例，介绍具体的操作步骤，其他Windows操作系统版本的操作步骤与之类似。

a. 打开Windows控制面板，在**搜索控制面板**文本框，输入 `设备管理器` 进行搜索。



b. 单击**设备管理器**，打开设备管理器。

c. 单击**网络适配器**，然后右键单击**Red Hat VirtIO Ethernet Adapter**。

d. 单击**卸载设备(U)**。

e. 在**卸载设备**对话框，选中**删除此设备的驱动程序软件**前的复选框，然后单击**卸载**。
成功卸载后，设备管理器中将不再显示**网络适配器**。

v. 安装最新版Windows网卡驱动。

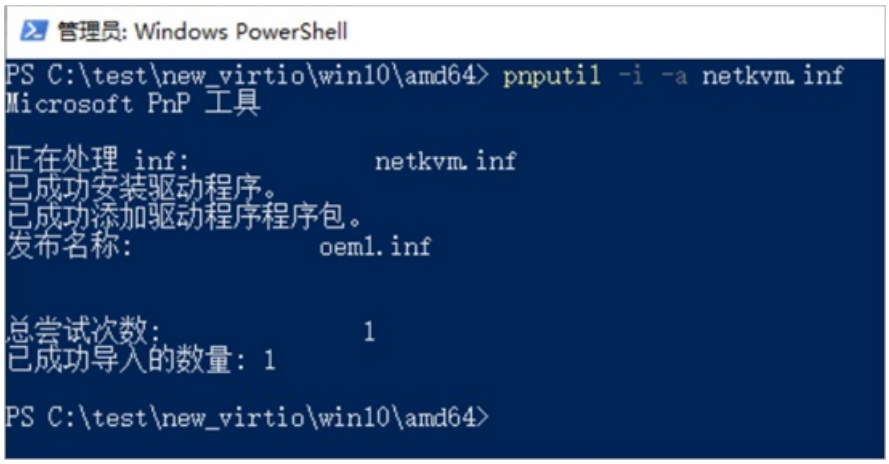
a. 根据Windows实例当前的操作系统版本，选择打开对应的Windows驱动程序文件夹。
例如，本示例中Windows实例的操作系统版本为Windows Server 2019 64位，且Windows驱动程序保存在*C:\test*文件夹中，则需要打开的文件夹路径为*C:\test\new_virtio\win10\amd64*。

b. 在*amd64*文件夹内的空白区域，按下*Shift*键的同时，单击鼠标右键，然后单击**在此处打开Powershell 窗口(S)**。

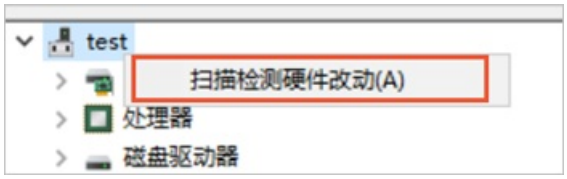
c. 在Powershell窗口中，运行以下命令，安装最新版Windows网卡驱动。

```
pnputil -i -a netkvm.inf
```

如下图所示，表示网卡驱动成功安装。



vi. 返回或重新打开设备管理器，右键单击主机名称，然后单击**扫描检测硬件改动(A)**。
例如，本示例中Windows实例的主机名称为 `test` ，则操作示例如下图所示：



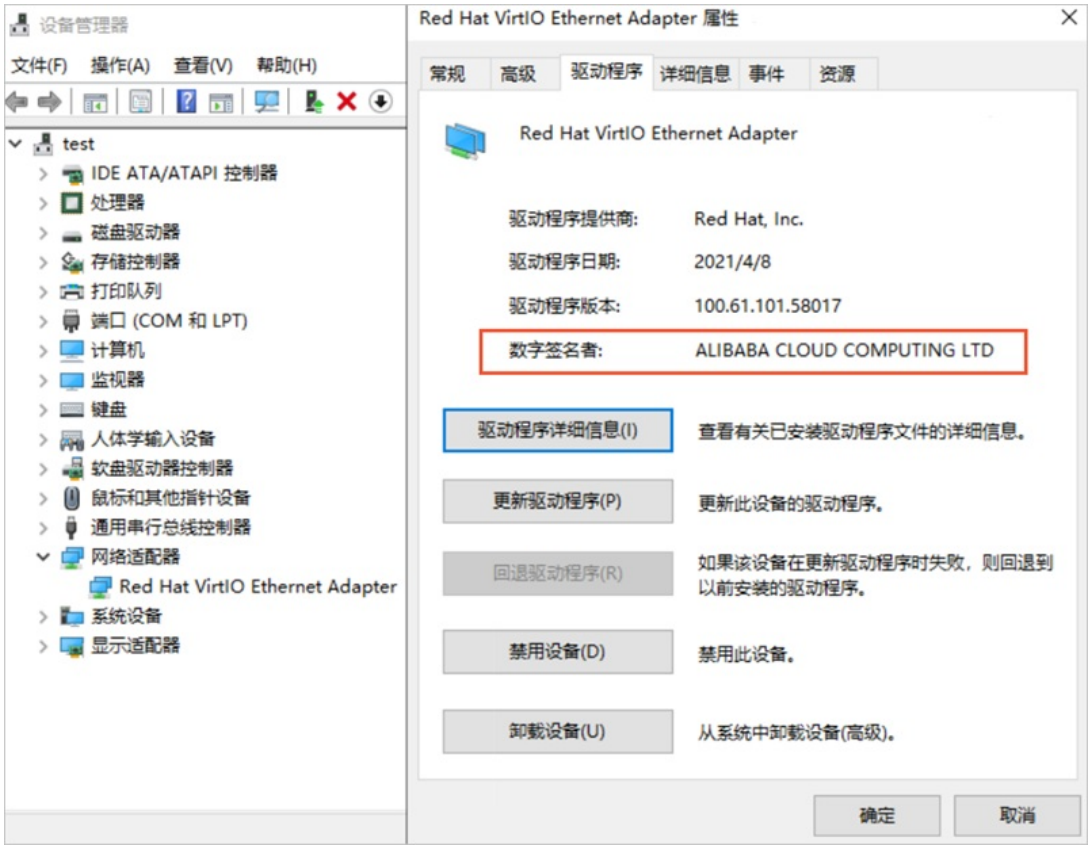
扫描检测完成后，您可以在设备管理器中查看到新增的**网络适配器**。

vii. 查看最新版的网卡驱动信息。

a. 单击**网络适配器**，然后右键单击Red Hat VirtIO Ethernet Adapter。

b. 单击**属性(R)**。

c. 在Red Hat VirtIO Ethernet Adapter 属性对话框，单击**驱动程序**页签。
如下图所示，在页签内，您可以查看到最新版网卡驱动的数字签名信息。



viii. 重启Windows实例。
具体操作，请参见重启实例。重启实例后，新版的驱动才会生效。

13.3. CentOS Linux停止维护后如何应对？

CentOS官方已计划停止维护CentOS Linux项目，阿里云上CentOS Linux公共镜像来源于CentOS官方，当CentOS Linux停止维护后，阿里云将会同时停止对该操作系统的支持。本文主要介绍CentOS Linux操作系统停止维护带来的影响，并针对影响提供应对策略。

背景信息

2020年12月08日，CentOS官方宣布了停止维护CentOS Linux的计划，并推出了CentOS Stream项目。更多信息，请参见CentOS官方公告。CentOS计划把Red Hat Enterprise Linux（RHEL）的复刻版本CentOS Linux转向CentOS Stream，因此对CentOS Linux存在以下影响：

- CentOS Linux 7作为RHEL 7的复刻版本于2020年08月06日停止更新，但会延续当前的支持计划，于2024年6月30日停止维护（EOL）。
- CentOS Linux 8作为RHEL 8的复刻版本，生命周期缩短，于2021年12月31日停止更新并停止维护（EOL）。
- CentOS官方不再提供CentOS Linux 9及后续版本，而是提供CentOS Stream版本。

影响

基于CentOS官方的变更计划，对CentOS操作系统的使用者产生的影响如下所述：

- 2021年12月31日以后，CentOS Linux 8的使用者将无法获得包括问题修复和功能更新在内的任何软件维护和支持。
- 2024年06月30日以后，CentOS Linux 7的使用者将无法获得包括问题修复和功能更新在内的任何软件维护和支持。

基于CentOS Linux 8提前结束生命周期，CentOS官方提供的建议为：对于开发或测试环境，可以将环境迁移至CentOS Stream版本；对于生产环境或部署关键业务的系统，建议使用稳定的Red Hat Enterprise Linux。针对该建议，您需要关注以下影响：

- CentOS Stream是一个滚动升级的版本，而不是Red Hat Enterprise Linux的复刻版本。因此无法保障系统稳定性与兼容性，当CentOS Stream被运用于生产环境时，可能存在的风险仍未知。
- Red Hat Enterprise Linux是付费镜像，需要购买订阅服务。因此您需要关注业务成本的变化。
- 对于阿里云的公共镜像及服务支持存在一定影响：
  - 阿里云暂不会下线CentOS 8镜像，同时已经使用CentOS 8创建的ECS实例运行不会受到影响，但将停止更新镜像。更多信息，请参见2022年。
  - 阿里云对于CentOS操作系统的服务支持将和CentOS官方日期保持同步。2021年12月31日以后将不再对CentOS Linux 8提供服务支持；对CentOS Linux 7的服务支持将持续至2024年6月30日。

关于CentOS变更计划的更多问答信息，请参见FAQ - CentOS Project shifts focus to CentOS Stream。

应对策略

替换CentOS Linux操作系统的方式分为两类，更换操作系统和迁移操作系统。阿里云提供了多种操作系统的公共镜像供您选择，您可以根据业务的实际情况，选择适用的操作系统替代CentOS Linux，具体说明如下表所示。

- 无需保留系统盘数据，下表中所有的操作系统均支持。具体操作，请参见更换操作系统。
- 服务器迁移中心SMC提供了产品化的操作系统迁移能力，可保留系统盘数据，有效减少业务中断时长。SMC迁移目前仅支持以下场景：
  - CentOS 7操作系统迁移为Alibaba Cloud Linux 2/Anolis OS 7操作系统。
  - CentOS 8操作系统迁移为Alibaba Cloud Linux 3/Anolis OS 8操作系统。

  具体操作，请参见迁移操作系统。

操作系统	概述	适用人群
Alibaba Cloud Linux	Alibaba Cloud Linux由阿里云官方提供，完全兼容RHEL/CentOS生态和操作方式。该操作系统针对阿里云做了大量优化，并由阿里云免费提供长期支持和维护（LTS）。阿里云公共镜像提供了Alibaba Cloud Linux的两个发行版镜像。更多信息，请参见Alibaba Cloud Linux概述或Alibaba Cloud Linux概述。	适用于希望使用免费镜像，并需要获得服务支持的个人或企业。
Anolis OS	Anolis OS由龙蜥社区（OpenAnolis）提供，100%兼容CentOS 8软件生态，且兼容其它主流Linux发行版。该操作系统是完全开源、中立且开放的发行版，具备企业级的高性能、稳定性、安全性以及可靠性。更多信息，请参见龙蜥社区。	适用于希望使用免费镜像，并延续开源社区镜像使用习惯的个人或企业。
Red Hat Enterprise Linux	Red Hat Enterprise Linux是Red Hat公司提供的企业版操作系统，您需要付费使用并可以享受Red Hat的订阅服务。更多信息，请参见红帽企业 Linux。	适用于希望延续CentOS使用习惯，并需要获得服务支持的个人或企业。

操作系统	概述	适用人群
CentOS Stream	CentOS Stream是一个滚动升级的版本，由CentOS官方提供。	适用于希望延续CentOS使用习惯，并希望获得滚动升级的个人或企业。
Rocky Linux	Rocky Linux是一个社区化的企业级操作系统，位于Red Hat Enterprise Linux（RHEL）下游。Rocky Linux与CentOS一样，提供了适用于服务器的稳定版本，旨在作为CentOS完全兼容的替代版本。	适用于希望使用免费镜像，并延续开源社区镜像使用习惯的个人或企业。
AlmaLinux	AlmaLinux是CloudLinux团队宣布构建的一个稳定版CentOS社区分支。该操作系统实现了与Red Hat Enterprise Linux（RHEL）二进制文件的*1:1*兼容，并提供了不停机更换操作系统的能力。	适用于希望使用免费镜像，并延续开源社区镜像使用习惯的个人或企业。
Debian、Ubuntu等其他操作系统	Linux的其他发行版操作系统，不同操作系统在使用习惯和应用兼容性上存在一定差异。阿里云提供了丰富的操作系统镜像供您选择，更多信息，请参见选择镜像。	适用于可以自行应对操作系统切换成本的个人或企业。

相关链接

- 操作系统停止支持计划
- 2022年
- 镜像FAQ

13.4. CentOS 8 EOL如何切换源？

CentOS 8操作系统版本结束了生命周期（EOL），Linux社区已不再维护该操作系统版本。建议您切换到Anolis或Alinux。如果您的业务过渡期仍需要使用CentOS 8系统中的一些安装包，请根据下文切换CentOS 8的源。

背景信息

2021年12月31日CentOS 8 EOL。按照社区规则，CentOS 8的源地址 `http://mirror.centos.org/centos/8/` 内容已移除，目前第三方的镜像站中均已移除CentOS 8的源。阿里云的源 `http://mirrors.cloud.aliyuncs.com`和`http://mirrors.aliyun.com` 也无法同步到CentOS 8的源。当您在阿里云上继续使用默认配置的CentOS 8的源会发生报错。报错示例如下图所示：

```
CentOS Linux 8 - AppStream                                      20 kB/s | 2.3 kB     00:00
Errors during downloading metadata for repository 'appstream':
  - Status code: 404 for http://mirrors.cloud.aliyuncs.com/centos/8/AppStream/x86_64/os/repodata/repomd.xml (IP: 100.100.2.148)
Error: Failed to download metadata for repo 'appstream': Cannot download repomd.xml: Cannot download repodata/repomd.xml: All mi
rrors were tried
```

您可以通过下文的操作步骤，在CentOS 8操作系统的ECS实例中将源配置按照网络环境不同进行切换。

- yum源
  - 专有网络VPC类型实例需切换为 `http://mirrors.cloud.aliyuncs.com/centos-vault/8.5.2111/` 源。
  - 经典网络类型实例需切换为 `http://mirrors.aliyuncs.com/centos-vault/8.5.2111/` 源。
- epel源：
  - 专有网络VPC类型实例需切换为 `http://mirrors.cloud.aliyuncs.com/epel-archive/8/` 源。
  - 经典网络类型实例需切换为 `http://mirrors.aliyuncs.com/epel-archive/8/` 源。

> **说明** 本文主要说明ECS实例中的相关操作与配置。如果您的服务器不是ECS实例，需保证服务器具有公网访问能力，并且源地址 `http://mirrors.cloud.aliyuncs.com` 需要替换为 `http://mirrors.aliyun.com` 。例如，切换yum源为 `http://mirrors.aliyun.com/centos-vault/8.5.2111/` ；切换epel源为 `http://mirrors.aliyun.com/epel-archive/8/` 。

操作步骤

1. 登录CentOS 8系统的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 运行以下命令备份之前的repo文件。

```
rename '.repo' '.repo.bak' /etc/yum.repos.d/*.repo
```

3. 运行以下命令下载最新的repo文件。

```
wget http://mirrors.cloud.aliyuncs.com/repo/Centos-vault-8.5.2111.repo -O /etc/yum.repos.d/Centos-vault-8.5.2111.repo
wget http://mirrors.cloud.aliyuncs.com/repo/epel-archive-8.repo -O /etc/yum.repos.d/epel-archive-8.repo
```

> **说明** 如果您的服务器具备公网访问能力，请将命令中的源地址 `http://mirrors.cloud.aliyuncs.com` 替换为 `http://mirrors.aliyun.com` 。您也可以直接参考CentOS 镜像社区说明进行下载。

4. 运行以下命令替换repo文件中的链接。

```
sed -i 's/mirrors.cloud.aliyuncs.com/url_tmp/g'  /etc/yum.repos.d/Centos-vault-8.5.2111.repo &&  sed -i 's/mirrors.aliyun.com/mirrors.cloud.aliyuncs.com/g' /etc/yum.repos.d/Centos-vault-8.5.2111.repo && sed -i 's/url_tmp/mirrors.aliyun.com/g' /etc/yum.repos.d/Centos-vault-8.5.2111.repo
sed -i 's/mirrors.aliyun.com/mirrors.cloud.aliyuncs.com/g' /etc/yum.repos.d/epel-archive-8.repo
```

5. 运行以下命令重新创建缓存。

```
yum clean all && yum makecache
```

   yum源和epel源切换完成后，即可使用yum install命令在实例上安装您所需要的软件包。

相关文档

- CentOS Product Specifications
- 操作系统停止支持计划

13.5. CentOS 6 EOL如何切换源？

CentOS 6操作系统版本结束了生命周期（EOL），Linux社区已不再维护该操作系统版本。建议您升级操作系统至CentOS 7及以上，如果您的业务过渡期仍需要使用CentOS 6系统中的一些安装包，请根据下文切换CentOS 6的源。

背景信息

2020年11月30日CentOS 6 EOL。按照社区规则，CentOS 6的源地址 `http://mirror.centos.org/centos-6/` 内容已移除，目前第三方的镜像站中均已移除CentOS 6的源。阿里云的源 `http://mirrors.cloud.aliyuncs.com` 和 `http://mirrors.aliyun.com` 也无法同步到CentOS 6的源。当您在阿里云上继续使用默认配置的CentOS 6的源会发生报错。报错示例如下图所示：

```
http://mirrors.cloud.aliyuncs.com/centos/6/os/x86_64/repodata/repomd.xml: [Errno 14] PYCURL ERROR 22 - "The requested URL returned error: 404 Not Found"
Trying other mirror.
http://mirrors.cloud.aliyuncs.com/centos/6/extras/x86_64/repodata/repomd.xml: [Errno 14] PYCURL ERROR 22 - "The requested URL returned error: 404 Not Found"
Trying other mirror.
http://mirrors.cloud.aliyuncs.com/centos/6/updates/x86_64/repodata/repomd.xml: [Errno 14] PYCURL ERROR 22 - "The requested URL returned error: 404 Not Found"
```

您可以通过下文的操作步骤，在CentOS 6操作系统的ECS实例中将源配置按照网络环境不同进行切换。

- yum源
  - 专有网络VPC类型实例需切换为 `http://mirrors.cloud.aliyuncs.com/centos-vault/6.10/` 源。
  - 经典网络类型实例需切换为 `http://mirrors.aliyuncs.com/centos-vault/6.10/` 源。
- epel源
  - 专有网络VPC类型实例需切换为 `http://mirrors.cloud.aliyuncs.com/epel-archive/6/` 源。
  - 经典网络类型实例需切换为 `http://mirrors.aliyuncs.com/epel-archive/6/` 源。

> **说明** 本文主要说明ECS实例中的相关操作与配置。如果您的服务器不是ECS实例，需保证服务器具有公网访问能力，并且源地址 `http://mirrors.cloud.aliyuncs.com` 需要替换为 `http://mirrors.aliyun.com` 。例如，切换yum源为 `http://mirrors.aliyun.com/centos-vault/6.10/` ；切换epel源为 `http://mirrors.aliyun.com/epel-archive/6/` 。

操作步骤

1. 登录CentOS 6系统的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 运行以下命令编辑 `CentOS-Base.repo` 文件。

   ```
   vim /etc/yum.repos.d/CentOS-Base.repo
   ```

3. 按进入编辑模式，修改以下内容切换源。

   请根据实例不同的网络类型进行修改，具体内容如下：

   - 专有网络VPC类型实例

```
[base]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.cloud.aliyuncs.com/centos-vault/6.10/os/$basearch/
gpgcheck=1
gpgkey=http://mirrors.cloud.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
[updates]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.cloud.aliyuncs.com/centos-vault/6.10/updates/$basearch/
gpgcheck=1
gpgkey=http://mirrors.cloud.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
[extras]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.cloud.aliyuncs.com/centos-vault/6.10/extras/$basearch/
gpgcheck=1
gpgkey=http://mirrors.cloud.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
```

- 经典网络类型实例

```
[base]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.aliyuncs.com/centos-vault/6.10/os/$basearch/
gpgcheck=1
gpgkey=http://mirrors.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
[updates]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.aliyuncs.com/centos-vault/6.10/updates/$basearch/
gpgcheck=1
gpgkey=http://mirrors.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
[extras]
name=CentOS-6.10
enabled=1
failovermethod=priority
baseurl=http://mirrors.aliyuncs.com/centos-vault/6.10/extras/$basearch/
gpgcheck=1
gpgkey=http://mirrors.aliyuncs.com/centos-vault/RPM-GPG-KEY-CentOS-6
```

编辑完成后，按*Esc*键，并输入 `:wq` 保存退出文件。

4. 运行以下命令编辑 `epel.repo` 文件。

```
vim /etc/yum.repos.d/epel.repo
```

5. 按*i*进入编辑模式，修改以下内容切换源。

   请根据实例不同的网络类型进行修改，具体内容如下：

- 专有网络VPC类型实例

```
[epel]
name=Extra Packages for Enterprise Linux 6 - $basearch
enabled=1
failovermethod=priority
baseurl=http://mirrors.cloud.aliyuncs.com/epel-archive/6/$basearch
gpgcheck=0
gpgkey=http://mirrors.cloud.aliyuncs.com/epel-archive/RPM-GPG-KEY-EPEL-6
```

- 经典网络类型实例

```
[epel]
name=Extra Packages for Enterprise Linux 6 - $basearch
enabled=1
failovermethod=priority
baseurl=http://mirrors.aliyuncs.com/epel-archive/6/$basearch
gpgcheck=0
gpgkey=http://mirrors.aliyuncs.com/epel-archive/RPM-GPG-KEY-EPEL-6
```

编辑完成后，按*Esc*键，并输入 `:wq` 保存退出文件。

后续步骤

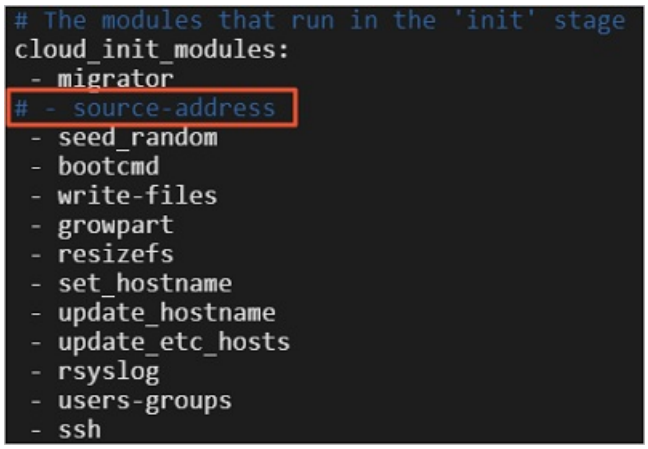
yum源和epel源切换完成后，即可使用**yum install**命令在实例上安装您所需要的软件包。

使用自定义镜像创建新的ECS实例，在启动实例时 `cloud-init` 会自动初始化系统的源配置。如果您后续需要通过已切换源的ECS实例创建自定义镜像，并且需要保留已切换的源配置，需要您在创建自定义镜像前，按照以下操作在已切换源的ECS实例中修改 `cloud-init` 的配置文件*/etc/cloud/cloud.cfg*。

1. 运行以下命令编辑*/etc/cloud/cloud.cfg*文件。

```
vim /etc/cloud/cloud.cfg
```

2. 按*i*进入编辑模式，使用 `#` 注释掉 `cloud_init_modules:` 下的 `- source-address` 模块。
   注释后，文件内的配置信息如下所示：



3. 编辑完成后，按*Esc*键，并输入 `:wq` 保存退出文件。

相关文档

- CentOS Product Specifications
- 操作系统停止支持计划

13.6. 阿里云针对CentOS EOL迁移方案

CentOS计划停止CentOS Linux项目，如果您是CentOS系统的使用者，将面临CentOS停止维护（EOL，End Of Life）后如何更新、维护、系统迁移等问题。因此，阿里云针对CentOS停止维护提供了迁移方案以及迁移案例。

背景信息

2020年12月08日，CentOS官方宣布CentOS Linux项目将停止。更多信息，请参见CentOS官网公告。

CentOS未来将会从Red Hat Enterprise Linux（RHEL）复刻版本的CentOS Linux转向CentOS Stream。对于当前处于生命周期中的CentOS版本后续影响如下：

- CentOS Linux 7（简称CentOS 7）将会延续当前的支持计划，于2024年6月30日停止维护。
- CentOS Linux 8（简称CentOS 8）将提前到2021年12月31日停止维护。

CentOS EOL产生的影响

基于CentOS官方公告及阿里云所获得的信息，此次变更会产生如下影响：

- 2021年12月31日以后，CentOS Linux 8的使用者将无法获得包括问题修复和功能更新在内的任何软件维护和支持。
- 2024年06月30日以后，CentOS Linux 7的使用者将无法获得包括问题修复和功能更新在内的任何软件维护和支持。

阿里云提供的应对方案

阿里云联合龙蜥社区（OpenAnolis）为您提供了完备的操作系统迁移方案：您可以直接选择把现在使用的CentOS迁移到龙蜥操作系统（Anolis OS）或者Alibaba Cloud Linux操作系统，阿里云将为您提供包括迁移评估、迁移工具、长期稳定支持在内的完整迁移解决方案。

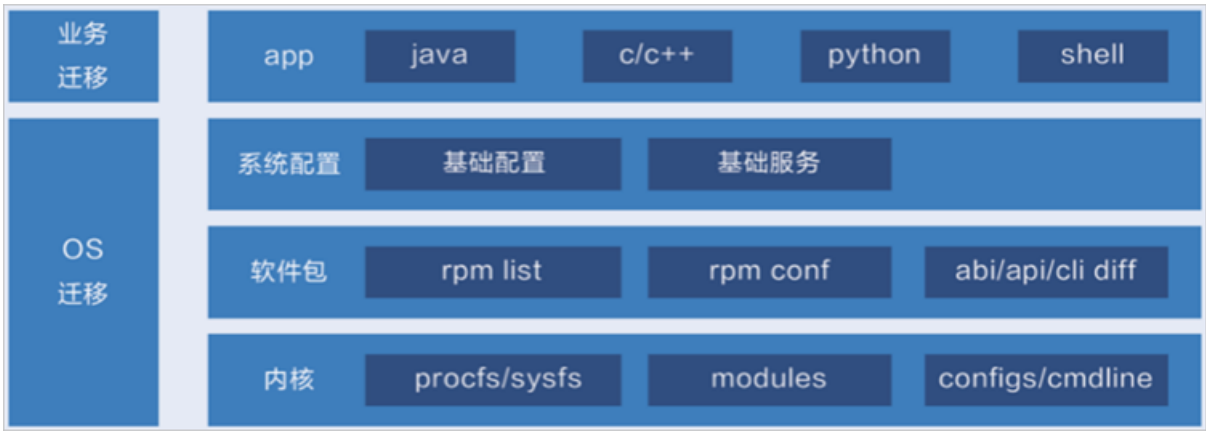
该迁移方案相比其他开源方案的优势：阿里云提供系统化解决方案、迁移配套工具平台、长期稳定支持、全面兼容CentOS生态、差异化技术优势、丰富的场景验证以及用户迁移案例实践等。

操作系统迁移方案介绍

迁移方案主要分为迁移评估和迁移实施。

迁移评估

迁移评估通过扫描获取原CentOS系统信息，并与目标操作系统（Anolis OS/Alibaba Cloud Linux）进行对比，来判断迁移风险，并据此来实施迁移。迁移评估主要包含OS评估和业务评估，如下图所示：



具体说明：

- 业务迁移评估：主要对迁移业务的应用类型进行评估，并根据不同的业务类型来制定相应的业务迁移方案。

- OS迁移评估：差异评估工具从OS的内核、软件包、系统配置等方面判断差异，并据此来实施迁移。

迁移实施

按照您实际的使用场景可以分为全新部署和原地迁移。具体说明如下：

- 全新部署
  全新部署是指重新安装操作系统，所有的应用程序以及配置数据信息需要重新部署。该方式适用于集群扩容，节点替换等场景。
- 原地迁移
  原地迁移指线上系统的原地升级，对所有的应用程序、系统配置、应用配置进行保留，无需再重新部署和迁移数据。原地迁移适用于对OS底层变更不敏感的业务。例如Java类程序，JDK做了对底层OS的适配，只要迁移前后JDK版本一致，OS迁移后，业务无需重新适配部署即可正常运行。示例场景：在CentOS 8上基于java-1.8.0-openjdk部署hadoop多节点集群，通过原地迁移工具迁移到Anolis OS 8后，主节点配置不丢失，数据节点数据存储正常，集群能够正常工作。

迁移指引

CentOS迁移方案分为两类，通过服务器迁移中心SMC（Server Migration Center）迁移和操作系统迁移工具迁移。

- SMC提供了产品化的操作系统迁移能力，可保留系统盘数据，有效减少业务中断时长，因此推荐您使用该迁移方式。SMC迁移目前仅支持以下场景：
  - CentOS 7操作系统迁移为Alibaba Cloud Linux 2/Anolis OS 7操作系统。
  - CentOS 8操作系统迁移为Alibaba Cloud Linux 3/Anolis OS 8操作系统。

  具体操作，请参见迁移操作系统。
- 迁移工具迁移目前支持以下场景：

  > **注意** 在使用操作系统迁移工具前，您需要注意：操作系统的迁移操作不可逆，其中涉及到系统内软件包的重新安装。因此您需要在迁移前为ECS实例创建快照备份数据。关于快照的更多信息，请参见快照概述。

  - CentOS 7迁移到Anolis OS 7详细迁移步骤，请参见CentOS 7迁移Anolis OS 7手册。
  - CentOS 8迁移到Anolis OS 8详细迁移步骤，请参见CentOS 8迁移Anolis OS 8手册。
  - CentOS 7迁移Alibaba Cloud Linux 2详细迁移步骤，请参见CentOS 7迁移Alibaba Cloud Linux 2。

    > **说明** Alibaba Cloud Linux 2使用4.19内核，CentOS 7使用3.10内核，两个版本的内核无法相互兼容，依赖于内核接口编程的业务，例如涉及内核OOT模块开发、硬件使能等，需提前做好评估，明确是否适合直接迁移，以免OS迁移后业务无法运行。

  - CentOS 8迁移Alibaba Cloud Linux 3详细迁移步骤，请参见CentOS 8迁移Alibaba Cloud Linux 3。

    > **说明** Alibaba Cloud Linux 3使用5.10内核，CentOS 8使用4.18内核，两个版本的内核无法相互兼容，依赖于内核接口编程的业务，例如涉及内核OOT模块开发、硬件使能等，需提前做好评估，明确是否适合直接迁移，以免OS迁移后业务无法运行。

迁移案例

- 龙蜥社区助力中国联通完成核心业务CentOS试点替换
- 浙江移动完成全国首例基于“龙芯5000系列芯片+统信UOS操作系统”技术端到端投产商用

13.7. Ubuntu 16.04 LTS停止支持维护后如何继续安全更新？

2021年04月，Ubuntu 16.04 LTS（Xenial Xerus）将停止为期5年的标准支持维护，同时阿里云也将停止Ubuntu 16.04 LTS公共镜像的更新。Ubuntu 16.04 LTS后续将过渡到扩展安全维护（ESM）的阶段。您可以参考本文的操作，通过Ubuntu订阅服务（UA-I）为Ubuntu 16.04实例获取ESM更新支持。

背景信息

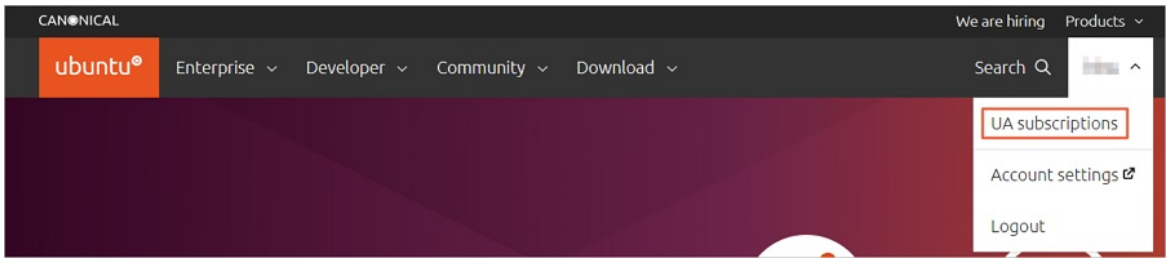
当Ubuntu 16.04 LTS处于扩展安全维护（ESM）阶段时，您可以通过Ubuntu订阅服务（UA-I）内的扩展安全维护（ESM），继续获取基础操作系统、关键软件包和基础设置组件的安全更新。更多信息，请参见Ubuntu Advantage for Infrastructure以及Extended Security Maintenance。

如果您需要在Ubuntu 16.04实例中继续获取操作系统的安全更新，请参见以下操作步骤。

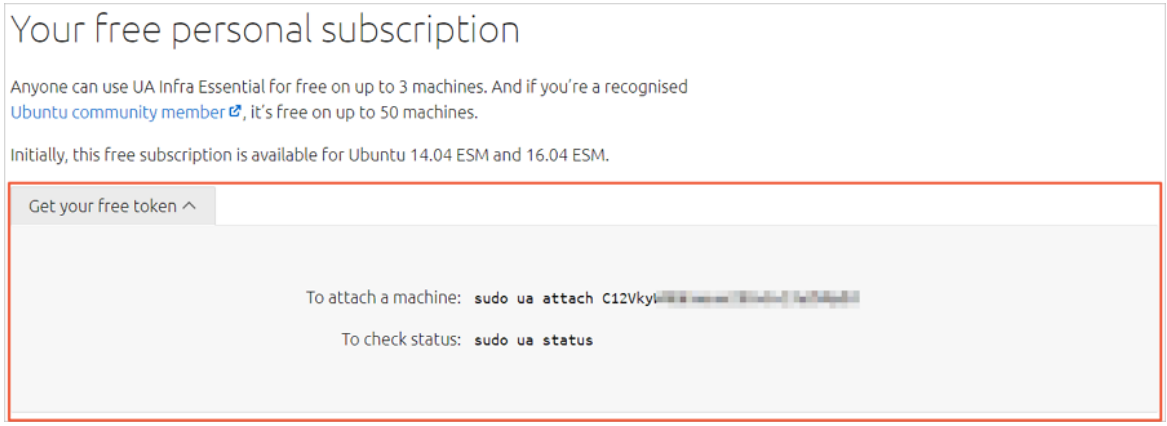
步骤一：在Ubuntu官网订阅UA-I服务

1. 在本地主机，访问Ububtu官网（`https//ubuntu.com`）。
2. 在顶部菜单栏，单击Sign in。

   您需要使用Ubuntu账号登录，如果您没有Ubuntu账号，需要根据实际的页面提示完成注册并登录Ubuntu官网。
3. 在顶部菜单栏，单击Ubuntu账号的用户名，然后单击UA subscriptions。



4. 在Your free personal subscription区域，单击Get your free token。



   您需要自行保存To attach a machine后的命令信息。

步骤二：在Ubuntu 16.04实例中添加UA-I并进行安全更新

1. 远程连接Ubuntu 16.04实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。
2. 依次运行以下命令，安装Ubuntu最新的Ubuntu Advantage（UA）客户端。

i. 升级软件包。

```
sudo apt update
```

ii. 安装UA客户端。

```
sudo apt install ubuntu-advantage-tools
```

3. 运行步骤一中保存的To attach a machine命令。

   命令格式如下所示，您需要将*<token>*替换为实际保存的数值。

```
sudo ua attach <token>
```

   如下图所示，表示已启用ESM。

```
SERVICE       ENTITLED  STATUS    DESCRIPTION
cis           yes       disabled  Center for Internet Security Audit Tools
esm-infra     yes       enabled   UA Infra: Extended Security Maintenance (ESM)
fips          yes       disabled  NIST-certified core packages
fips-updates  yes       disabled  NIST-certified core packages with priority security updates
livepatch     yes       enabled   Canonical Livepatch service
```

4. （可选）运行以下命令，启用ESM。

   如果您不确定ESM是否启用，可以运行以下命令确保ESM已启用。

```
sudo ua enable esm-infra
```

5. 依次运行以下命令，升级软件包并更新安全补丁。

   i. 升级软件包。

```
sudo apt update
```

   ii. 更新安全补丁。

```
sudo apt upgrade
```

13.8. 如何共享加密自定义镜像？

如果ECS实例挂载的云盘开启了加密功能，则通过该ECS实例所创建的自定义镜像为加密自定义镜像。本文介绍如何共享加密自定义镜像。

背景信息

关于加密功能的更多信息，请参见加密概述。当您需要共享加密自定义镜像时，需要先通过阿里云的访问控制创建名为 `AliyunECSShareEncryptImageDefaultRole` 的角色并授予指定的权限与策略，然后才可以将加密自定义镜像共享给其他阿里云账号。

> **说明** 共享加密自定义镜像的功能目前支持华北2（北京）、华东2（上海）、中国（香港）、新加坡地域。

操作步骤

1. 准备工作。

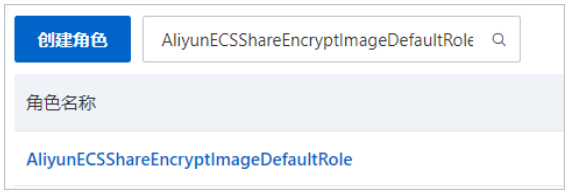
   在共享您的加密自定义镜像之前，您需要先明确被共享者的阿里云账号ID（必须是主账号ID）。阿里云账号ID的获取方式为：将鼠标移至控制台右上角的用户头像，在弹出的用户信息框中，如果标识了账号为**主账号**，则显示的账号ID即为阿里云账号ID。

本文示例中，被共享者的阿里云账号ID为 `125****` 。

2. 使用共享者的阿里云账号（即拥有加密自定义镜像的阿里云账号）登录RAM控制台。
3. 在左侧导航栏，选择**身份管理 > 角色**。
4. 单击**创建角色**，然后在**创建角色**面板中完成以下配置。
   i. 在**选择类型**页面，选择**阿里云账号**，然后单击**下一步**。
   ii. 在**配置角色**页面，**角色名称**下的文本框中输入 `AliyunECSShareEncryptImageDefaultRole` ，并在**选择信任的云账号**区域单击**当前云账号**，然后单击**完成**。
   iii. 在**创建完成**页面，单击**为角色授权**。
   iv. 在**添加权限**面板的**选择权限**区域，单击**系统策略**，然后在搜索框中输入 `AliyunKMSFullAccess` 进行搜索。

   其他未说明的配置项保持默认配置即可。

   v. 添加 `AliyunKMSFullAccess` 权限，单击**确定**，然后单击**完成**。
5. 返回**角色**页面，通过**创建角色**后的搜索框，搜索 `AliyunECSShareEncryptImageDefaultRole` 角色，然后单击角色名进入角色详情页。



6. 在角色详情页修改信任策略。
   i. 单击**信任策略管理**。

ii. 单击**修改信任策略**，然后将默认的信任策略替换为以下信任策略。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "<UID>@ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

其中，*<UID>*为变量，您需要修改为被共享者的阿里云账号ID。例如，本文示例中被共享者的阿里云账号ID为 `125****` ，则修改后的信任策略如下所示：

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "125[redacted]@ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

如果您的加密自定义镜像需要共享给多个阿里云账号，则您需要分别为这些阿里云账号设置信任策略。格式为：

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "<UID-1>@ecs.aliyuncs.com",
          "<UID-2>@ecs.aliyuncs.com",
          "<UID-3>@ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

iii. 单击**确定**。

后续步骤

完成 `AliyunECSShareEncryptImageDefaultRole` 角色的创建与配置后，您可以使用共享者的阿里云账号将加密的自定义镜像共享给已添加在信任策略中的阿里云账号。共享镜像的具体操作，请参见共享或取消共享镜像。

13.9. Linux自定义镜像如何适配NVMe系统盘？

部分实例规格族支持基于NVMe协议挂载云盘（例如ecs.g7se、ecs.c7se、ecs.r7se等），如果您需要在该类实例规格族上使用自定义镜像启动ECS实例，且需要保证实例稳定运行，则您在创建自定义镜像前，需要在对应的操作系统中进行NVMe相关的配置操作。

背景信息

支持基于NVMe协议挂载云盘的实例规格族信息，请参见实例规格族。

在您完成NVMe相关配置并创建自定义镜像前，建议您先为操作系统所在实例的系统盘以及数据盘创建快照，备份数据。更多信息，请参见快照概述。

本文提供了如何在以下操作系统中进行NVMe相关的配置操作：

- CentOS
- Debian
- Ubuntu
- SUSE Linux Enterprise Server（SLES）

此外，阿里云云助手提供了自动化插件，如果您的操作系统符合云助手插件的支持范围，则您也可以使用云助手插件自动进行NVMe相关的配置操作。具体操作，请参见使用云助手插件自动化配置。

CentOS

1. 远程连接待创建自定义镜像的CentOS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 根据您的操作系统的配置信息，完成NVMe相关的配置。

   i. 运行以下命令，查看系统内核是否已经加载了NVMe驱动。

   ```
   cat /boot/config-`uname -r` | grep -i nvme | grep -v "^#"
   ```

   返回结果如下所示，如果 `CONFIG_BLK_DEV_NVME=y` 则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动，您需要跳过后续的步骤2、步骤3，直接进行步骤4的参数配置。否则，您需要依次完成以下操作步骤。

   ```
   [root@test ~]# cat /boot/config-`uname -r` | grep -i nvme | grep -v "^#"
   CONFIG_NVME_CORE=m
   CONFIG_BLK_DEV_NVME=m
   CONFIG_NVME_MULTIPATH=y
   CONFIG_NVME_FABRICS=m
   CONFIG_NVME_RDMA=m
   CONFIG_NVME_FC=m
   CONFIG_NVME_TCP=m
   CONFIG_NVME_TARGET=m
   CONFIG_NVME_TARGET_LOOP=m
   CONFIG_NVME_TARGET_RDMA=m
   CONFIG_NVME_TARGET_FC=m
   CONFIG_NVME_TARGET_FCLOOP=m
   CONFIG_NVME_TARGET_TCP=m
   CONFIG_RTC_NVMEM=y
   CONFIG_NVMEM=y
   ```

ii. 运行以下命令，查看initramfs中是否包含NVMe驱动。

```
lsinitrd /boot/initramfs-`uname -r`.img | grep -i nvme | awk '{print $NF}'
```

如果有类似于如下图所示的返回结果，则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动，您需要跳过后续的步骤3，直接进行步骤4的参数配置。否则，您需要依次完成以下操作步骤。

```
[root@test ~]# lsinitrd /boot/initramfs-`uname -r`.img | grep -i nvme | awk '{print $NF}'
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-core.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-fabrics.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-fc.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-rdma.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-tcp.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvme-loop.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvmet-fc.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvmet.ko.xz
```

iii. 依次运行以下命令，使initramfs支持NVMe驱动。

```
mkdir -p /etc/dracut.conf.d
```

```
echo 'add_drivers+=" nvme nvme-core nvme-fabrics nvme-fc nvme-rdma nvme-loop nvmet
nvmet-fc nvme-tcp "' >/etc/dracut.conf.d/nvme.conf
```

```
dracut -v -f
```

> **说明** 如果您的操作系统没有安装dracut工具，您需要先运行yum -y install dracut安装dracut工具。

iv. 在GRUB中添加NVMe相关的nvme timeout参数。

a. 运行以下命令，打开*grub*文件。

```
vi /etc/default/grub
```

b. 按*i*键进入编辑模式，在 `GRUB_CMDLINE_LINUX=` 一行中，添加 `nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295` 参数信息。
添加参数后，文件内容如下图所示：

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet net.ifnames=0 console=tty0 console=ttyS0,115200n8 nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
~
```

> **说明** 如果配置文件中默认已存在相同的参数信息，则无需再次添加。

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

v. 运行以下命令，使配置的GRUB生效。

根据操作系统的启动方式不同，选择以下适用于您的操作系统的命令：

- Legacy启动方式

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- UEFI启动方式

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

vi. 重新运行以下命令，查看是否有NVMe相关的返回信息。

```
lsinitrd /boot/initramfs-`uname -r`.img | grep -i nvme | awk '{print $NF}'
```

如果有类似于如下图所示的返回结果，则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动。

```
[root@test ~]# lsinitrd /boot/initramfs-`uname -r`.img | grep -i nvme | awk '{print $NF}'
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-core.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-fabrics.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-fc.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-rdma.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/host/nvme-tcp.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvme-loop.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvmet-fc.ko.xz
usr/lib/modules/4.18.0-193.28.1.el8_2.x86_64/kernel/drivers/nvme/target/nvmet-ko.xz
```

3. 为实例创建自定义镜像。

当您在操作系统中完成了NVMe相关的配置后，即可为对应的实例创建自定义镜像。具体操作以及操作前的注意事项，请参见使用实例创建自定义镜像。

> **说明** 如果您是在本地环境中自行创建的自定义镜像，可以通过导入镜像功能将自定义镜像导入云上。具体操作，请参见Linux镜像导入流程。

创建自定义镜像需要一定的时间，您需要等待自定义镜像成功创建并处于**可用**状态后，再执行下一步。

4. 通过自定义镜像创建新的ECS实例。

通过自定义镜像创建ECS实例的具体操作，请参见使用自定义镜像创建实例。在创建过程中，实例规格请设置为您需要的支持基于NVMe协议挂载云盘的实例规格。

5. 远程连接新建的ECS实例。

具体操作，请参见连接方式概述ECS远程连接操作指南。

6. 在新建的ECS实例内，依次运行以下命令，查看NVMe相关配置是否正常。

i. 运行以下命令，查看支持NVMe协议的云盘信息。

```
lsblk
```

ii. 运行以下命令，查看*/proc/cmdline*文件中是否存在nvme timeout参数的相关信息。

```
cat /proc/cmdline
```

操作示例的返回结果如下，表示自定义镜像已成功适配NVMe系统盘。

```
[root@test ~]# lsblk
NAME        MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1     259:0    0  40G  0 disk
└nvme0n1p1 259:1    0  40G  0 part /
[root@test ~]# cat /proc/cmdline
BOOT_IMAGE=(hd0,msdos1)/boot/vmlinuz-4.18.0-193.28.1.el8_2.x86_64 root=UUID=edf839fd-8e1a-4373-946a-[illegible] ro
 crashkernel=auto rhgb quiet net.ifnames=0 console=tty0 console=ttyS0,115200n8 nvme_core.io_timeout=4294967295 nvme
_core.admin_timeout=4294967295
[root@test ~]#
```

Debian

1. 远程连接待创建自定义镜像的Debian实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 完成NVMe相关的配置。

   i. 运行以下命令，查看initrd中包含的NVMe驱动。

   Debian操作系统的initrd中默认已经加载了NVMe驱动。

```
lsinitramfs /boot/initrd.img-`uname -r` | grep -i nvme
```

   返回结果如下所示：

```
root@test:~# lsinitramfs /boot/initrd.img-`uname -r` | grep -i nvme
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host/nvme-core.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host/nvme-fabrics.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host/nvme-fc.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host/nvme-rdma.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/host/nvme.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/target
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/target/nvmet-fc.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/target/nvmet-rdma.ko
usr/lib/modules/4.19.0-13-amd64/kernel/drivers/nvme/target/nvmet.ko
root@test:~#
```

   ii. 在GRUB中添加NVMe相关的nvme timeout参数。

   a. 运行以下命令，打开*/etc/default/grub*文件。

```
vi /etc/default/grub
```

   b. 按*i*键进入编辑模式，在 `GRUB_CMDLINE_LINUX=` 一行中，添加 `nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295` 参数信息。

   添加参数后，文件内容如下图所示：

```
GRUB_DEFAULT=0
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX="" vga=792 console=tty0 console=ttyS0,115200n8 net.ifnames=0 noibrs nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295"
```

> **说明** 如果配置文件中默认已存在相同的参数信息，则无需再次添加。

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

iii. 运行以下命令，使配置的GRUB生效。

根据操作系统的启动方式不同，选择以下适用于您的操作系统的命令：

- Legacy启动方式

```
grub-mkconfig -o /boot/grub/grub.cfg
```

- UEFI启动方式

```
grub-mkconfig -o /boot/efi/EFI/debian/grub.cfg
```

> **说明** 除以上方式外，您还可以选择Debian系统提供的脚本使配置的GRUB生效，运行脚本的命令如下所示。该脚本不区分操作系统的启动方式，适用于Legacy或UEFI启动方式。
>
> ```
> update-grub2
> ```

3. 为实例创建自定义镜像。

当您在操作系统中完成了NVMe相关的配置后，即可为对应的实例创建自定义镜像。具体操作以及操作前的注意事项，请参见使用实例创建自定义镜像。

> **说明** 如果您是在本地环境中自行创建的自定义镜像，可以通过导入镜像功能将自定义镜像导入云上。具体操作，请参见Linux镜像导入流程。

创建自定义镜像需要一定的时间，您需要等待自定义镜像成功创建并处于**可用**状态后，再执行下一步。

4. 通过自定义镜像创建新的ECS实例。

通过自定义镜像创建ECS实例的具体操作，请参见使用自定义镜像创建实例。在创建过程中，实例规格请设置为您需要的支持基于NVMe协议挂载云盘的实例规格。

5. 远程连接新建的ECS实例。

具体操作，请参见连接方式概述ECS远程连接操作指南。

6. 在新建的ECS实例内，依次运行以下命令，查看NVMe相关配置是否正常。

i. 运行以下命令，查看支持NVMe协议的云盘信息。

```
lsblk
```

ii. 运行以下命令，查看*/proc/cmdline*文件中是否存在nvme timeout参数的相关信息。

```
cat /proc/cmdline
```

操作示例的返回结果如下，表示自定义镜像已成功适配NVMe系统盘。

```
root@test:~# lsblk
NAME        MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1     259:0    0  40G  0 disk
└nvme0n1p1 259:1    0  40G  0 part /
root@test:~# cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-4.19.0-13-amd64 root=UUID=a82ffd5b-6af8-4766-9da4-[redacted] ro vga=792 console=tty0 con
sole=ttyS0,115200n8 net.ifnames=0 noibrs nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_time
out=4294967295 quiet
root@test:~#
```

Ubuntu

1. 远程连接待创建自定义镜像的Ubuntu实例。

具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 完成NVMe相关的配置。
   i. 运行以下命令，查看initrd中包含的NVMe驱动。

      Ubuntu操作系统的initrd中默认已经加载了NVMe驱动。

      ```
      lsinitramfs /boot/initrd.img-`uname -r` | grep -i nvme
      ```

      返回结果如下所示：

      ```
      root@test:~# lsinitramfs /boot/initrd.img-`uname -r` | grep -i nvme
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host/nvme-fabrics.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host/nvme-core.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host/nvme-fc.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host/nvme-rdma.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/host/nvme.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/target
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/target/nvmet-fc.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/target/nvme-loop.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/target/nvmet.ko
      lib/modules/4.15.0-166-generic/kernel/drivers/nvme/target/nvmet-rdma.ko
      root@test:~#
      ```

   ii. 在GRUB中添加NVMe相关的nvme timeout参数。
      a. 运行以下命令，打开*/etc/default/grub*文件。

         ```
         vi /etc/default/grub
         ```

      b. 按*i*键进入编辑模式，在 `GRUB_CMDLINE_LINUX=` 一行中，添加 `nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295` 参数信息。

         添加参数后，文件内容如下图所示：

         ```
         GRUB_DEFAULT=0
         GRUB_TIMEOUT_STYLE=hidden
         GRUB_TIMEOUT=1
         GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
         GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
         GRUB_CMDLINE_LINUX="" vga=792 console=tty0 console=ttyS0,115200n8 net.ifnames=0 noibrs nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295"
         ```

         > **说明** 如果配置文件中默认已存在相同的参数信息，则无需再次添加。

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

   iii. 运行以下命令，使配置的GRUB生效。

      根据操作系统的启动方式不同，选择以下适用于您的操作系统的命令：

      - Legacy启动方式

        ```
        grub-mkconfig -o /boot/grub/grub.cfg
        ```

      - UEFI启动方式

        ```
        grub-mkconfig -o /boot/efi/EFI/ubuntu/grub.cfg
        ```

      > **说明** 除以上方式外，您还可以选择Ubuntu系统提供的脚本使配置的GRUB生效，运行脚本的命令如下所示。该脚本不区分操作系统的启动方式，适用于Legacy或UEFI启动方式。
      >
      > ```
      > update-grub2
      > ```

3. 为实例创建自定义镜像。

当您在操作系统中完成了NVMe相关的配置后，即可为对应的实例创建自定义镜像。具体操作以及操作前的注意事项，请参见使用实例创建自定义镜像。

> **说明** 如果您是在本地环境中自行创建的自定义镜像，可以通过导入镜像功能将自定义镜像导入云上。具体操作，请参见Linux镜像导入流程。

创建自定义镜像需要一定的时间，您需要等待自定义镜像成功创建并处于**可用**状态后，再执行下一步。

4. 通过自定义镜像创建新的ECS实例。

   通过自定义镜像创建ECS实例的具体操作，请参见使用自定义镜像创建实例。在创建过程中，实例规格请设置为您需要的支持基于NVMe协议挂载云盘的实例规格。

5. 远程连接新建的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

6. 在新建的ECS实例内，依次运行以下命令，查看NVMe相关配置是否正常。

   i. 运行以下命令，查看支持NVMe协议的云盘信息。

   ```
   lsblk
   ```

   ii. 运行以下命令，查看*/proc/cmdline*文件中是否存在nvme timeout参数的相关信息。

   ```
   cat /proc/cmdline
   ```

   操作示例的返回结果如下，表示自定义镜像已成功适配NVMe系统盘。

   ```
   root@test:~# lsblk
   NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme0n1      259:0    0  40G  0 disk
   └nvme0n1p1 259:1    0  40G  0 part /
   root@test:~# cat /proc/cmdline
   BOOT_IMAGE=/boot/vmlinuz-4.15.0-166-generic root=UUID=13c57707-3bef-4381-b0c7-14506e17ee7a ro vga=792 console=tty0
   console=ttyS0,115200n8 net.ifnames=0 noibrs nvme_core.multipath=n nvme_core.io_timeout=4294967295 nvme_core.admin_t
   imeout=4294967295 quiet splash vt.handoff=1
   root@test:~#
   ```

SUSE Linux Enterprise Server（SLES）

1. 远程连接待创建自定义镜像的SLES实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 根据您的操作系统的配置信息，完成NVMe相关的配置。

i. 运行以下命令，查看系统内核是否已经加载了内核驱动。

```
cat /boot/config-`uname -r` | grep -i nvme | grep -v "^#"
```

返回结果如下所示，如果 `CONFIG_BLK_DEV_NVME=y` 则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动，您需要跳过后续的步骤2、步骤3，直接进行步骤4的参数配置。否则，您需要依次完成以下操作步骤。

```
sles125:~ # cat /boot/config-`uname -r` | grep -i nvme | grep -v "^#"
CONFIG_NVME_CORE=m
CONFIG_BLK_DEV_NVME=m
CONFIG_NVME_MULTIPATH=y
CONFIG_NVME_FABRICS=m
CONFIG_NVME_RDMA=m
CONFIG_NVME_FC=m
CONFIG_NVME_TCP=m
CONFIG_NVME_TARGET=m
CONFIG_NVME_TARGET_LOOP=m
CONFIG_NVME_TARGET_RDMA=m
CONFIG_NVME_TARGET_FC=m
CONFIG_NVME_TARGET_FCLOOP=m
CONFIG_NVME_TARGET_TCP=m
CONFIG_NVMEM=m
```

ii. 运行以下命令，查看initrd中是否包含NVMe驱动。

```
lsinitrd /boot/initrd-`uname -r` | grep -i nvme | awk '{print $NF}'
```

如果有类似于如下图所示的返回结果，则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动，您需要跳过后续的步骤3，直接进行步骤4的参数配置。否则，您需要依次完成以下操作步骤。

```
sles125:~ # lsinitrd /boot/initrd-`uname -r` | grep -i nvme | awk '{print $NF}'
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-core.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-fabrics.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-fc.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-rdma.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-tcp.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvme-loop.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvmet-fc.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvmet.ko
```

iii. 依次运行以下命令，使initrd支持NVMe驱动。

```
mkdir -p /etc/dracut.conf.d
```

```
echo 'add_drivers+=" nvme nvme-core nvme-fabrics nvme-fc nvme-rdma nvme-loop nvmet
nvmet-fc nvme-tcp "' >/etc/dracut.conf.d/nvme.conf
```

```
dracut -v -f
```

> **说明** 如果您的操作系统没有安装dracut工具，您需要运行zypper install -y dracut安装dracut工具。

iv. 在GRUB中添加NVMe相关的nvme timeout参数。

a. 运行以下命令，打开*grub*文件。

```
vi /etc/default/grub
```

b. 按*i*键进入编辑模式，在 `GRUB_CMDLINE_LINUX=` 一行中，添加 `nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295` 参数信息。

添加参数后，文件内容如下图所示：

```
GRUB_DISTRIBUTOR=
GRUB_DEFAULT=saved
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=1
GRUB_CMDLINE_LINUX_DEFAULT="mitigations=auto splash=silent quiet showopts"
GRUB_CMDLINE_LINUX=" net.ifnames=0 console=tty0 console=ttyS0,115200n8 nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295"
```

> **说明** 如果配置文件中默认已存在相同的参数信息，则无需再次添加。

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

v. 运行以下命令，使配置的GRUB生效。

根据操作系统的启动方式不同，选择以下适用于您的操作系统的命令：

- Legacy启动方式

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- UEFI启动方式

```
grub2-mkconfig -o /boot/efi/EFI/sles/grub.cfg
```

vi. 重新运行以下命令，查看是否有NVMe相关的返回信息。

```
lsinitrd /boot/initrd-`uname -r` | grep -i nvme | awk '{print $NF}'
```

如果有类似于如下图所示的返回结果，则表示该操作系统可以直接在支持NVMe协议的实例规格族上启动。

```
sles125:~ # lsinitrd /boot/initrd-`uname -r` | grep -i nvme | awk '{print $NF}'
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-core.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-fabrics.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-fc.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-rdma.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/host/nvme-tcp.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvme-loop.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvmet-fc.ko
lib/modules/4.12.14-122.80-default/kernel/drivers/nvme/target/nvmet.ko
```

3. 为实例创建自定义镜像。

   当您在操作系统中完成了NVMe相关的配置后，即可为对应的实例创建自定义镜像。具体操作以及操作前的注意事项，请参见使用实例创建自定义镜像。

   > **说明** 如果您是在本地环境中自行创建的自定义镜像，可以通过导入镜像功能将自定义镜像导入云上。具体操作，请参见Linux镜像导入流程。

   创建自定义镜像需要一定的时间，您需要等待自定义镜像成功创建并处于**可用**状态后，再执行下一步。

4. 通过自定义镜像创建新的ECS实例。

   通过自定义镜像创建ECS实例的具体操作，请参见使用自定义镜像创建实例。在创建过程中，实例规格请设置为您需要的支持基于NVMe协议挂载云盘的实例规格。

5. 远程连接新建的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

6. 在新建的ECS实例内，依次运行以下命令，查看NVMe相关配置是否正常。

   i. 运行以下命令，查看支持NVMe协议的云盘信息。

   ```
   lsblk
   ```

   ii. 运行以下命令，查看*/proc/cmdline*文件中是否存在nvme timeout参数的相关信息。

   ```
   cat /proc/cmdline
   ```

   操作示例的返回结果如下，表示自定义镜像已成功适配NVMe系统盘。

   ```
   test:~ # lsblk
   NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme0n1      259:0    0  40G  0 disk
   `-nvme0n1p1 259:1    0  40G  0 part /
   test:~ # cat /proc/cmdline
   BOOT_IMAGE=/boot/vmlinu[illegible] root=UUID=35aa893d-9[illegible] net.ifnames=0 conso
   le=tty0 console=ttyS0,115200n8 idle=nomwait nvme_core.io_timeout=4294967295 nvme_core.admin_timeout=4294967295 spla
   sh=silent mitigations=auto quiet
   test:~ #
   ```

使用云助手插件自动化配置

云助手提供了 `ecs_nvme_config` 插件，帮助您快速完成操作系统内NVMe相关的配

置。`ecs_nvme_config` 插件目前支持以下操作系统：

- Alibaba Cloud Linux
- Anolis OS
- CentOS/CentOS Stream
- Debian
- Ubuntu
- OpenSUSE
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux
- Fedora
- Rocky Linux
- AlmaLinux

不支持 `ecs_nvme_config` 插件的操作系统版本信息：

- CentOS/Red Hat Enterprise Linux：低于6.6的操作系统版本
- Debian：低于9的操作系统版本
- Ubuntu：低于16的操作系统版本
- OpenSUSE：42操作系统版本
- SUSE Linux Enterprise Server：低于11.4的操作系统版本

1. 远程连接待创建自定义镜像的实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

2. 运行以下命令，检查实例内是否已安装云助手客户端，并检查客户端内是否提供了 `ecs_nvme_config` 插件。

   ```
   acs-plugin-manager --list
   ```

   如果已安装云助手客户端，则会返回如下图所示的信息。如果您运行命令后没有返回云助手相关信息，则需要先在实例内安装云助手客户端。具体操作，请参见安装云助手客户端。

   ```
   [root@test ~]# acs-plugin-manager --list
   +-----------------------------------------------------------------+
   |                          Name|   version| publisher|        os|
   +-----------------------------------------------------------------+
   |                   ecsgo-helper|      0.12|    aliyun|     LINUX|
   |                       oosutil|      1.11|    aliyun|     LINUX|
   |                          sysak|      0.38|    aliyun|     LINUX|
   |        ecs_tools_sysak-iosdiag|       2.3|    aliyun|     LINUX|
   |          ecs-metrics-collector|      0.13|    aliyun|     LINUX|
   |                 ecs-utils-ipv6|       1.3|    aliyun|     LINUX|
   |                  patch_manager|      1.10|    aliyun|     LINUX|
   |                ecs_nvme_config|       1.0|    aliyun|     LINUX|
   |                kms-rotate-secret|       1.0|    aliyun|     LINUX|
   |             app-snapshot-plugin|       1.8|    aliyun|     LINUX|
   |             ecs-hibernate-linux|       0.3|    aliyun|     LINUX|
   |               smc-client-plugin|       1.1|    aliyun|     LINUX|
   |ecs_disable_intel_hyper-threading|       1.0|    aliyun|     LINUX|
   |                  multi-nic-util|       1.0|    aliyun|     LINUX|
   |           ecs_tools_multiqueue|       1.2|    aliyun|     LINUX|
   |                ecs_dump_config|       1.0|    aliyun|     LINUX|
   |       bare_metal_shutdown_util|       1.0|    aliyun|     LINUX|
   |             ecs_inventory_test|       3.3|    aliyun|     LINUX|
   +-----------------------------------------------------------------+
   ```

   如果您可以查看到返回的云助手插件列表，但插件列表中没有 `ecs_nvme_config` 插件，则表示该插件在当前的地域和可用区下没有发布。您需要根据不同的操作系统，选择适用的手动配置方式，进行NVMe相关的配置操作。

- CentOS
- Debian
- Ubuntu
- SUSE Linux Enterprise Server（SLES）

如果您的实例内已安装云助手客户端，且存在 `ecs_nvme_config` 插件，请继续下一步。

3. 使用 `ecs_nvme_config` 插件，完成NVMe相关的配置。

   i. 运行以下命令，使用 `ecs_nvme_config` 插件检查当前实例内是否有NVMe模块，以及是否可以配置NVMe模块。

   ```
   acs-plugin-manager --exec --plugin ecs_nvme_config --params --check
   ```

   返回结果说明：

   - 如果返回结果中存在如下提示，则表示您无需进行NVMe相关的配置，可直接创建自定义镜像。

     ```
     [SUCCESS]  Summary: Your image can Runnig on nvme instance
     ```

   - 如果返回结果中存在 `[ERROR]` 相关提示，则您需要继续执行下一步操作。

   ii. 根据检查结果中的提示信息，配置NVMe驱动以及相关参数信息。

   例如，检查结果中提示如下信息：

   ```
   [ERROR]  1.initrd/initramfs not has nvme module, Please run acs-plugin-manager --ex
   ec --plugin ecs_nvme_config --params -f/--fix to enable nvme;
   ```

   则您需要根据提示内容，运行以下命令，完成NVMe相关的配置。

   ```
   acs-plugin-manager --exec --plugin ecs_nvme_config --params --fix
   ```

   iii. 完成配置后，运行以下命令，重启实例。

   ```
   reboot
   ```

   iv. 重启实例后，重新检查NVMe模块是否配置成功。

   ```
   acs-plugin-manager --exec --plugin ecs_nvme_config --params --check
   ```

   配置成功的返回示例如下：

   ```
   [OK]  1.initrd/initramfs already contain nvme module;
   [OK]  2.fstab file looks fine and does not contain any device names;
   [OK]  3.The nvme parameters already included.
   [SUCCESS]  Summary: Your image can Runnig on nvme instance
   ```

4. 为实例创建自定义镜像。

   当您在操作系统中完成了NVMe相关的配置后，即可为对应的实例创建自定义镜像。具体操作以及操作前的注意事项，请参见使用实例创建自定义镜像。

   > **说明** 如果您是在本地环境中自行创建的自定义镜像，可以通过导入镜像功能将自定义镜像导入云上。具体操作，请参见Linux镜像导入流程。

   创建自定义镜像需要一定的时间，您需要等待自定义镜像成功创建并处于**可用**状态后，再执行下一步。

5. 通过自定义镜像创建新的ECS实例。

通过自定义镜像创建ECS实例的具体操作，请参见使用自定义镜像创建实例。在创建过程中，实例规格请设置为您需要的支持基于NVMe协议挂载云盘的实例规格。

6. 远程连接新建的ECS实例。

   具体操作，请参见连接方式概述ECS远程连接操作指南。

7. 在新建的ECS实例内，依次运行以下命令，查看NVMe相关配置是否正常。

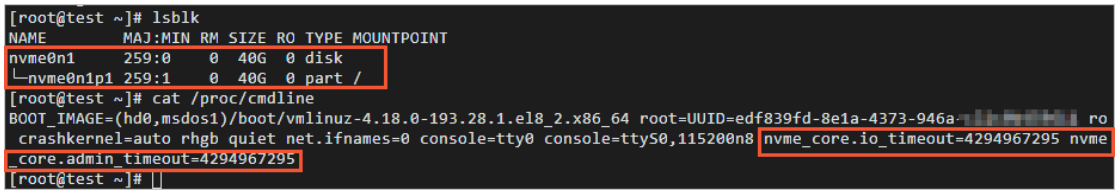
   i. 运行以下命令，查看支持NVMe协议的云盘信息。

   ```
   lsblk
   ```

   ii. 运行以下命令，查看*/proc/cmdline*文件中是否存在nvme timeout参数的相关信息。

   ```
   cat /proc/cmdline
   ```

   操作示例的返回结果如下，表示自定义镜像已成功适配NVMe系统盘。



13.10. 存量SUSE Linux Enterprise Server实例的镜像如何升级为商业版？

阿里云的SUSE Linux Enterprise Server（SLES）公共镜像已于2021年10月30日正式开启收费。如果您存量的ECS实例内仍有使用原免费SLES镜像的实例，从2022年04月01日起，针对该部分实例需要升级到商业版镜像，才能获取SLES镜像更新和SUSE的售后支持。您可以参考本文将免费镜像升级为商业版镜像。

背景信息

存量的SLES操作系统的ECS实例是指基于历史免费版的SLES公共镜像创建的ECS实例，或者基于您原有的免费SLES自定义镜像创建的ECS实例。这类ECS实例目前支持通过云服务器ECS控制台选择是否升级为商业版。选择升级商业版后，您可以继续获取SLES镜像更新以及技术支持。您也可以选择不升级商业版，ECS实例的延续性不会受到影响，但从2022年04月01日起，该类实例不能获取镜像更新和SUSE的售后支持。

关于SUSE Linux Enterprise Server（SLES）公共镜像商业化的具体公告，请参见【其他】SUSE Enterprise Linux Server将于2021年10月30日开启收费。

注意事项

- 当您升级SLES镜像为商业版时，需要支付镜像费用。费用详情以您升级时的询价价格为准。
- 如果您不希望继续使用SLES镜像，阿里云推荐您使用免费的Alibaba Cloud Linux操作系统来替代SLES操作系统。
- 本次镜像商业化变更只包含SUSE Linux Enterprise Server操作系统，不包含SUSE Linux Enterprise Server for SAP操作系统。
- 本次存量SLES实例升级，不支持经典网络实例。如果您拥有存量的SLES经典网络实例，请将ECS实例从经典网络迁移到专有网络之后再进行升级。如有问题，请提交工单。

操作步骤

如果您的阿里云账号内具有存量待升级商业版的SLES公共镜像创建的ECS实例，当您登录ECS控制台后，可以通过实例列表页面查看到为SLES镜像升级为商业版的提示消息，您可以根据实际情况进行升级。

升级前，您需要先通过阿里云账号（主账号）手动完成授权操作，授权阿里云在您升级支付费用后运行注册命令，以便获取SLES更新源。具体操作说明如下所示。

1. 使用阿里云账号（主账号）登录RAM控制台。
2. 创建角色为AliyunECSAssistantRunCommandRole，并修改该角色的信任策略为以下内容。

   说明 角色名称必须是AliyunECSAssistantRunCommandRole，否则注册命令会失败。

```
{
            "Statement": [
            {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                "Service": [
                    "ecs.aliyuncs.com"
                ]
                }
            }
],
            "Version": "1"
}
```

   具体操作，请参见授予实例RAM角色。

3. 在该角色下，添加自定义策略AliyunECSAssistantRunCommandRolePolicy，策略内容如下。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:RunCommand",
            "Resource": "*"
        }
    ]
}
```

   具体操作，请参见通过RAM用户控制资源访问。

4. 登录ECS管理控制台。
5. 在左侧导航栏，选择**实例与镜像 > 实例**。

   在实例列表上方区域，可以看到SLES镜像的升级提醒。

6. 单击**立即升级**。
7. 根据页面提示完成SLES镜像升级为商业版的操作。

   您也可以根据实际情况，选择暂不升级镜像至商业版。

升级并支付费用后，即代表您已授权RunCommand执行注册命令，系统会自动为您完成升级注册。注册过程通常持续数秒，建议您稍作等待，再进入到实例列表页刷新并确认剩余待升级实例数量，并针对剩余实例进行升级。
升级完成后，您即可获取SLES更新源和SUSE的售后支持。

13.11. Linux时间和时区说明

本文主要介绍Linux操作系统中时间和时区相关的基本概念与操作，并介绍部分阿里云Linux公共镜像中时钟配置的相关变化。

背景信息

Linux操作系统中时间和时区相关的基本概念如下表所述：

基本概念	说明
时钟	Linux时钟分为以下两种： • 硬件时钟（Real Time Clock，简称RTC）：由物理层面的主板上电池供电的时钟，该硬件时钟可以在Linux的BIOS（Basic Input Output System）中进行设置。 • 系统时钟（System Clock）：Linux内核中的时钟。当Linux系统启动时，硬件时钟会读取系统时钟的设置，然后系统时钟会独立于物理层面的硬件运作。Linux系统中所有的命令（包括函数）均使用系统时钟。
时间标准	Linux内的时间标准分为以下两种： • localtime标准：基于操作系统所在本地时区的时间标准。 • UTC（Coordinated Universal Time）标准：与时区无关的全球时间标准。

时间相关操作

- 运行以下命令，可以查看当前Linux系统内的时间设置。

```
timedatectl status
```

返回结果示例如下图所示，您可以查看Linux系统内的本地时间、全球标准时间、RTC时间以及时区等信息。

```
root@test:~# timedatectl status
               Local time: Fri 2022-01-21 17:56:58 CST
           Universal time: Fri 2022-01-21 09:56:58 UTC
                 RTC time: Fri 2022-01-21 09:56:58
                Time zone: Asia/Shanghai (CST, +0800)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@test: #
```

- 通过timedatectl命令设置硬件时钟的时间标准。
  - 将硬件时钟的时间标准设置为localtime：

    ```
    timedatectl set-local-rtc 1
    ```

    当硬件时钟的时间标准为localtime时，通过timedatectl status命令查看时间设置中的 `RTC in local TZ` 参数值为 `yes` 。
  - 将硬件时钟的时间标准设置为UTC：

    ```
    timedatectl set-local-rtc 0
    ```

    当硬件时钟的时间标准为UTC时，通过timedatectl status命令查看时间设置中的 `RTC in local TZ` 参数值为 `no` 。

> **说明** */etc/adjtime*文件是同步系统时钟的配置文件。上述操作命令会自动更新*/etc/adjtime*文件，因此您无需单独对该文件进行设置。

阿里云RTC时钟使用UTC时间标准的公共镜像列表

阿里云公共镜像中的RTC时钟默认使用localtime时间标准，但您需要注意，在最新发布的公共镜像中，阿里云已把RTC时钟默认使用的localtime时间标准修改为UTC时间标准，且该类镜像的后续版本会保持RTC时钟使用UTC时间标准。关于RTC时钟使用UTC时间标准的公共镜像发布的更多信息，请参见：

- 2022年

- Alibaba Cloud Linux 3镜像发布记录
- Alibaba Cloud Linux 2镜像发布记录

13.12. AMD实例的兼容性

本文主要说明AMD实例与不同版本的操作系统镜像之间的兼容性问题。

背景信息

AMD实例是阿里云新推出的重磅产品，基于AMD EPYC™ Zen 2微处理器架构（代号Rome），该架构属于x86架构。AMD实例将大量虚拟化功能卸载到专用硬件，降低虚拟化开销，提供稳定可预期的超高性能。
AMD实例规格族目前有以下三种：

- 通用型实例规格族g6a
- 计算型实例规格族c6a
- 内存型实例规格族r6a

更多信息，请参见实例规格族。
AMD实例可以兼容不同版本的操作系统，AMD Zen架构发布于2017年，处理器的部分新特性在旧版操作系统上会出现部分功能支持上的缺陷。请您根据应用的实际情况，自行决定需要使用的操作系统版本。下文列出了各主流操作系统建议使用的版本。

各操作系统对AMD Rome处理器支持说明

下表列出了支持AMD Rome处理器的不同操作系统版本。

操作系统	操作系统版本	官方文档
Windows	• Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019	Windows Server support and installation instructions for the AMD Rome family of processors
Linux	• Alibaba Cloud Linux 2 • CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3 • Ubuntu 16.04/18.04/20.04	• Red Hat Enterprise Linux：AMD CPUs and Supported Red Hat Enterprise Linux (RHEL) Versions • Ubuntu：AMD EPYC Rome support in Ubuntu Server

相关文档

- 2022年

13.13. 镜像常见格式

ECS支持导入多种镜像格式，本文对ECS支持导入的QCOW2、VHD及RAW镜像格式进行对比说明。
常用镜像格式说明如下表所示。

镜像格式	镜像简介	镜像特点

镜像格式	镜像简介	镜像特点
QCOW2	QCOW2是QEMU实现的一种虚拟机镜像格式，是用一个文件的形式来表示一块固定大小的块设备磁盘。	• 支持更小的磁盘占用。 • 支持写时拷贝（CoW，Copy-On-Write），镜像文件只反映底层磁盘变化。 • 支持快照，可以包含多个历史快照。 • 支持压缩和加密，可以选择ZLIB压缩和AES加密。
VHD	VHD是微软提供的一种虚拟磁盘文件格式。VHD文件格式可以被压缩成单个文件存放到本地物理主机的文件系统上，主要包括云服务器启动所需的文件系统。	• 维护简单。可以在不影响物理分区的前提下对它进行分区、格式化、压缩、删除等操作。 • 轻松备份。备份时仅需要将创建的VHD文件进行备份，也可以用备份工具将VHD文件所在的整个物理分区进行备份。 • 迁移方便。当有一个VHD文件需要在多台计算机上使用时，只要先将此VHD文件从当前计算机上分离，将其复制到目的计算机上，再做附加操作即可。 • 可直接用于系统部署。可以使用Imagex工具将已经捕获的映像释放到VHD虚拟磁盘，或通过WDS服务器部署系统到VHD虚拟磁盘。
RAW	RAW格式是直接给云服务器进行读写的文件。RAW不支持动态增长空间，是镜像中I/O性能最好的一种格式。	• 寻址简单，访问效率较高。 • 可以通过格式转换工具方便地转换为其他格式。 • 可以方便地被本地物理主机挂载，可以在不启动虚拟机的情况下和宿主机进行数据传输。

13.14. 如何为Linux服务器安装GRUB？

通过服务器迁移中心SMC迁移Linux源服务器时，若Linux源服务器未安装GRUB、系统版本较低（如CentOS 5和Debian 7）、自带的系统引导程序GRUB（GRand Unified Bootloader）版本低于2.02，日志文件提示Do Grub Failed时，您需要安装GRUB的2.02及以上版本。

背景信息

本文以GRUB 2.02版本为例，介绍在Linux服务器上安装系统引导程序GRUB的操作步骤。安装其他版本的操作步骤与此相同，主要差异在于安装过程中需下载相应版本的GRUB源码包。详情请参见下载相应版本的GRUB源码包。

操作步骤

1. 登录Linux源服务器。
2. 依次运行以下命令查看原grub、grub-install以及grub-mkconfig的路径。

```
which grub
```

```
which grub-install
```

```
which grub-mkconfig
```

- 如果任一命令提示路径不存在，说明源服务器中未安装GRUB或者文件缺失。您需要参见下文的操作步骤安装GRUB。
- 如果能够查看到文件路径，则需要运行以下命令为旧版本grub、grub-install以及grub-mkconfig改名以备份文件，然后参见下文的操作步骤安装新版本GRUB，覆盖当前版本。

```
mv /sbin/grub /sbin/grub-old
```

```
mv /sbin/grub-install /sbin/grub-install-old
```

```
mv /sbin/grub-mkconfig /sbin/grub-mkconfig-old
```

> **说明** 您可以在使用SMC迁移服务器后，恢复原名以使用原配置。

3. 安装GRUB依赖的bison、gcc以及make工具。

```
yum install -y bison gcc make
```

4. 依次运行以下命令安装flex。
   i. 判断是否存在文件夹tools，如果不存在则创建。

   ```
   test -d /root/tools || mkdir -p /root/tools
   ```

   ii. 进入tools文件夹，并下载flex安装包。

   ```
   cd /root/tools
   wget https://github.com/westes/flex/releases/download/v2.6.4/flex-2.6.4.tar.gz
   ```

   iii. 解压flex安装包。

   ```
   tar xzf flex-2.6.4.tar.gz
   ```

   iv. 进入安装包并创建build文件夹。

   ```
   cd flex-2.6.4
   mkdir -p build
   ```

   v. 进入build文件夹，编译安装flex。

   ```
   cd build
   ../configure
   ```

   ```
   make && make install
   ```

   vi. 创建软连接。

   ```
   ln -s /usr/local/bin/flex /usr/bin/flex
   ```

5. 依次运行以下命令安装GRUB。

   CentOS 5、Red Hat Enterprise Linux 5、Debian 7、Amazon Linux或Oracle Linux等低版本操作系统，更新GRUB至2.02及以上版本。

   i. 判断是否存在文件夹tools，如果不存在则创建。

   ```
   test -d /root/tools || mkdir -p /root/tools
   ```

ii. 进入tools文件夹，并下载GRUB 2.02安装包。

```
cd /root/tools
wget https://alpha.gnu.org/gnu/grub/grub-2.02~rc1.tar.gz
```

iii. 解压GRUB 2.02安装包。

```
tar xzf grub-2.02~rc1.tar.gz
```

iv. 进入安装包并创建build文件夹。

```
cd grub-2.02~rc1
mkdir -p build
```

v. 进入build文件夹，编译安装GRUB。

```
cd build
../configure
```

```
sed -i -e "s/-Werror//" ./grub-core/Makefile
sed -i -e "s/-Werror//" ./Makefile
make && make install
```

vi. 创建软连接。

```
ln -s /usr/local/sbin/grub-install /sbin/grub-install
ln -s /usr/local/sbin/grub-mkconfig /sbin/grub-mkconfig
```

说明 若编译过程中出现了 `-Werror` 报错，您可以定位到编译对象的编译文件*makefile*中，去掉 `-Werror` 选项重新编译。

6. 运行以下命令，检查是否已成功安装或更新至GRUB 2.02版本。

```
grub-install --version
```

后续步骤

- 成功安装新版本系统引导程序GRUB后，您可以使用SMC迁移服务器至阿里云。具体操作，请参见迁移流程。
- （可选）迁云成功后，如果您需要使用旧版本的GRUB，可以运行以下命令将GRUB恢复为旧版本。

```
rm /sbin/grub-install
rm /sbin/grub-mkconfig
rm /boot/grub/grub.cfg
mv /sbin/grub-old /sbin/grub
mv /sbin/grub-install-old /sbin/grub-install
```

13.15. Windows Server半年渠道镜像与实例管理

云服务器ECS提供Windows Server半年渠道镜像，本文介绍如何管理由该类镜像创建的Windows Server半年渠道实例。

背景信息

背景信息

Windows Server半年渠道镜像是一款纯Server Core模式运行的操作系统，不提供图形化用户界面。Windows Server半年渠道镜像对硬件要求宽松许多，降低了更新频率并且支持远程管理。Windows Server半年渠道实例不再包含资源管理器、控制面板、Windows Explorer，不支持*.msc功能（如devmgmt.msc等）。Windows Server半年渠道实例支持使用Sconfig、Server Manager、PowerShell和Windows Admin Center等工具管理服务器。

创建实例时，您可以在公共镜像列表中看到Windows Server半年渠道镜像，包括：

- Windows Server Version 1809 数据中心版
- Windows Server Version 1709 数据中心版
- Windows Server Version 1903 数据中心版
- Windows Server Version 1909 数据中心版
- Windows Server Version 2004 数据中心版

由于Windows Server半年渠道实例使用Server Core模式，本文推荐您使用功能更为完善的PowerShell和Windows Admin Center。更多信息，请参见微软文档如何管理 Server Core 模式服务器。

远程管理PowerShell

PowerShell依赖于.NET Framework实现了强大的面向对象的脚本，可以做到SSH功能一样远程管理Windows实例。我们假设您的实例公网IP为172.16.1XX.183，您可以按以下步骤实现PowerShell远程管理。

1. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
2. 在命令行里输入**PowerShell**打开PowerShell。
3. 在实例PowerShell中运行以下命令。

```
Enable-PSRemoting -Force
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
```

4. 在实例所在安全组中添加规则放行HTTP 5985端口和HTTPS 5986端口。添加安全组规则的具体操作，请参见添加安全组规则。
5. 在客户端计算机命令行里输入**PowerShell**打开PowerShell。
6. 在客户端PowerShell中运行以下命令。

```
Set-Item WSMan:localhost\client\trustedhosts -value 172.16.1XX.183 -Force
```

> **说明** `172.16.1XX.183` 代表只授信您的实例，您也可以使用 `*` 表示授信所有计算机。

7. 在客户端PowerShell中运行 `Enter-PSSession '172.16.1XX.183' -Credential:'administrator'` 并按提示输入实例密码。

现在您可以在客户端计算机管理您的Windows实例了。

安装Windows Admin Center

Windows Admin Center是一个基于浏览器的图形管理工具，可以在Server Core运行环境中取代服务器管理和MMC。我们假设您的实例公网IP为172.16.1XX.183，您可以按以下任一方法安装Windows Admin Center。

- 通过命令行安装Windows Admin Center
  i. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
  ii. 在实例所在安全组中添加规则放行HTTP 5985端口和HTTPS 5986端口。具体操作，请参见添加安全组规则。

iii. 在命令行里输入**PowerShell**打开PowerShell。

iv. 在实例PowerShell中运行以下命令。

```
Enable-PSRemoting -Force
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
```

v. 运行以下命令下载Windows Admin Center。

```
wget -Uri http://download.microsoft.com/download/E/8/A/E8A26016-25A4-49EE-8200-E4BCBF
292C4A/HonoluluTechnicalPreview1802.msi -UseBasicParsing -OutFile c:\HonoluluTechnica
lPreview1802.msi
msiexec /i c:\HonoluluTechnicalPreview1802.msi /qn /L*v log.txt SME_PORT=443 SSL_CERT
IFICATE_OPTION=generate
```

vi. 运行*cat log.txt*命令查看下载进度。
当日志文件出现下列信息，说明Windows Admin Center已经成功安装。

```
MSI (s) (14:44) [09:48:37:885]: Product: Project 'Honolulu'(技术预览版) -- Installatio
n completed successfully.
MSI (s) (14:44) [09:48:37:885]: Windows Installer 已安装产品。产品名称: Project 'Honolul
u'(技术预览版)。产品版本: 1.1.10326.0。产品语言: 1033。制造商: Microsoft Corporation。安装
成功或错误状态: 0。
```

- 通过浏览器安装Windows Admin Center
  - 前提条件
    通过浏览器安装Windows Admin Center需要在客户端计算机中完成，请确保您已经通过配置PowerShell管理实例。更多信息，请参见PowerShell 远程管理。
  - 操作步骤
    a. 下载并安装Windows Admin Center。更多信息，请参见Windows Admin Center概述。
    b. 完成安装后，打开https://localhost/。
    c. 单击**添加**，在弹窗中添加实例的IP地址。

现在，您可以通过Microsoft Edge或者Chrome使用Windows Admin Center管理实例。

常见问题

问题一：如何复制文件到Windows Server半年渠道实例？

假设需要复制的文件在您的客户端计算机上，并且您已经配置了PowerShell远程管理或者已安装Windows Admin Center。

- 通过RDP应用
  i. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
  ii. 在客户端计算机上，复制目标文件。
  iii. 在实例CMD环境中输入*notepad*。
  iv. 单击**文件 > 打开**，在打开对话框里，选择文件要复制的目标目录，右键单击选择**粘贴**。
- 通过PowerShell远程
  i. 启动目标Windows实例。
  ii. 在客户端计算机上打开CMD，输入**PowerShell**进入PowerShell。
  iii. 通过PowerShell远程管理目标实例。更多信息，请参见远程管理PowerShell。
  iv. 在客户端计算机上运行以下命令。

```
$session = New-PSSession -ComputerName 172.16.1XX.183
Copy-Item -ToSession $session -Path C:\1.txt -Destination c:\2.txt
```

说明 *C:\1.txt*是客户端计算机的文件位置，*C:\2.txt*是要拷贝到的Windows实例目录。

- 通过Windows Admin Center
  i. 启动目标Windows 实例。
  ii. 配置Windows Admin Center工具。具体操作，请参见安装Windows Admin Center。
  iii. 打开Windows Admin Center，选择被管理的实例，单击**文件**，选中文件后单击**上传**。

问题二：如何从内部关闭或者重启Windows Server半年渠道实例？

- 通过RDP应用
  i. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
  ii. 在CMD中输入*sconfig*，根据需要选择 `13` 重启实例或者 `14` 停止实例并回车。
- 通过PowerShell
  i. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
  ii. 在CMD中输入**PowerShell**进入PowerShell。
  iii. 选择并输入以下命令行重启或者停止实例。

```
shutdown -r -t 00 ::命令行 在0秒后重启
shutdown -s -t 00 ::命令行 在0秒后关机
Stop-Computer -Force # Powershell 立即关机
Restart-Computer -Force # Powershell 立即重启
```

- 通过PowerShell远程管理
  i. 启动目标 Windows 实例。
  ii. 在客户端计算机上打开CMD，输入**PowerShell**进入PowerShell。
  iii. 通过PowerShell远程管理目标实例。更多信息，请参见远程管理PowerShell。
  iv. 在客户端计算机上选择性运行以下PowerShell命令。

```
Enter-PsSession -ComputerName 172.16.1XX.183
Restart-Computer -Force #重启
Stop-Computer -Force #关机
```

- 通过Windows Admin Center
  i. 启动目标Windows实例。
  ii. 配置Windows Admin Center工具。具体操作，请参见安装Windows Admin Center。
  iii. 打开Windows Admin Center，选择被管理的实例，单击**概述**，选择性单击**重启**或者**关机**。

问题三：如何安装IIS服务？

- 通过RDP应用
  i. 远程连接Windows实例。具体操作，请参见通过密码认证登录Windows实例。
  ii. 在CMD中输入**PowerShell**进入PowerShell。
  iii. 运行以下命令安装IIS。

```
Import-Module ServerManager
Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
```

- 通过PowerShell远程管理
  i. 启动目标 Windows 实例。
  ii. 在客户端计算机上打开CMD，输入**PowerShell**进入 PowerShell。
  iii. 通过PowerShell远程管理目标实例。更多信息，请参见远程管理PowerShell。
  iv. 在客户端计算机上运行以下PowerShell命令。

```
Enter-PsSession -ComputerName 172.16.1XX.183
Import-Module ServerManager
Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
```

- 通过Windows Admin Center
  i. 启动目标Windows实例。
  ii. 配置Windows Admin Center工具，具体操作，请参见安装Windows Admin Center。
  iii. 打开Windows Admin Center，选中被管理的实例，单击**角色和功能**，单击**Web 服务器**，选择您需要的功能后单击**是**。

问题四：如何重新建立不小心在RDP会话中关闭了的命令行窗口？

如果在远程会话中不小心关闭了命令行窗口，远程应用将变成纯黑界面，无法操作。这时您可以：

1. 通过mstsc连接的情况下按Ctrl + Alt + End组合键，其他情况按Ctrl + Alt + Del组合键。
2. 在出现的界面选择**任务管理器**并回车。
3. 在任务管理器中，依次单击**文件** > **新建任务**文件，输入cmd后单击**确定**。

相关文档

相关文档

- Windows Server 半年渠道概述
- Introducing Windows Server, version 1709
- Windows Admin Center
- About Remote Troubleshooting

13.16. 如何解决实例迁移后的宕机问题？

因Xen环境裁撤项目、ECS过保迁移、经典网络迁移到VPC等涉及虚拟化环境迁移需求，可能会导致一部分实例系统在迁移后出现kernel panic宕机、蓝屏、找不到引导设备（INACCESSIBLE_BOOT_DEVICE）等问题。本文主要为您介绍这些问题的解决方案。

背景信息

阿里云为您提供了丰富的实例规格族以及主流操作系统镜像。不同实例规格实现的虚拟化技术不同：

- 以已经停售的ecs.t1和ecs.s1规格族为例，该规格族基于Xen虚拟化技术，该规格族需要操作系统镜像内有Xen等相关驱动。
- 以ecs.g5规格为例，该规格基于KVM虚拟化技术，该规格需要操作系统镜像有virtio驱动。
- 以ecs.g7规格为例，该规格基于神龙架构的虚拟化技术，该规格实例同样需要操作系统镜像有virtio驱动。

这些驱动是由ECS镜像中的内核提供的，内核版本不同，驱动支持的ECS规格也不同。一些比较旧版本系统中的内核默认没有相关驱动，需要用户自行安装，或者版本较低的内核的驱动不支持一些新版本的实例规格。

迁移前注意事项

如果您的实例系统环境有异常，Xen迁移到KVM环境后实例可能会运行异常，例如注册表损坏、文件系统损坏、系统启动异常等。因此建议您在迁移前做一些准备工作，确保迁移正常。

- 建议您在迁移前重启实例，检查系统是否正常重启，确保系统和业务在迁移前状态正常。
- 建议您在迁移前对实例创建快照，对重要数据备份。具体操作，请参见创建一个云盘快照。
- 除了现有的迁移方案，您也可以对原有实例创建自定义镜像，然后使用自定义镜像创建KVM规格的实例。具体操作，请参见使用实例创建自定义镜像和使用自定义镜像创建实例。

神龙环境不兼容部分旧版本操作系统

已知旧版本操作系统列表如下：

- Windows Server 2003及以下版本（Windows Server 2008 标准版本支持，但是需要清理Xen注册表信息）
- CentOS/RedHat 5.8及以下版本，包括基于CentOS/RedHat 5内核系统（内核版本2.6.18-348及以下）
- Debian 6.09以下版本（6.09以下版本对KVM支持也存在一定问题，建议升级到6.09以上版本）
- FreeBSD 11以下版本（FreeBSD 11/12版本需要安装对应的阿里云补丁。具体操作，请参见FreeBSD系统如何打补丁编译内核？。）
- Ubuntu 10及以下版本（Ubuntu 12基于内核3.2可以正常启动，官方镜像未提供过低于Ubuntu 12的版本）
- SUSE Linux Enterprise Server 10及以下版本（官方镜像未提供过低于SUSE Linux Enterprise Server 11的版本）
- OpenSUSE 13以下版本（官方镜像未提供过低于OpenSUSE 13的版本）
- Gentoo（阿里云提供的Gentoo只支持Xen版本，如果需要支持KVM，建议升级到最新版本，阿里云于2016年后未再提供Gentoo操作系统）

上述仅是6代实例规格的神龙环境不兼容情况，对于7代及以上版本实例规格的约束会更高一些。

解决方案一：更换系统盘升级系统

以上涉及的旧版本操作系统很早就已经停止维护更新。更多信息，请参见操作系统停止支持计划。停止维护更新的系统面临各种功能和安全风险、系统安全漏洞无法更新等问题，因此阿里云建议您尽快升级操作系统版本。

阿里云官方提供了以下公共镜像覆盖主流Linux和Windows操作系统 。更多信息，请参见公共镜像概述。

Linux：

- Alibaba Cloud Linux 2/3
- Anolis OS 7/8
- CentOS 7/8
- Debian 8/9/10
- FreeBSD 11/12
- OpenSUSE 15
- Ubuntu 16.04/18.04/20.04
- Fedora 33/34
- Rocky Linux 8.5
- AlmaLinux 8.5

Windows：

- Windows Server 2012
- Windows Server 2016
- Windows Server 2019

ECS支持更换系统盘操作，您可以一键更换实例的系统盘，完成系统升级。具体操作，请参见更换操作系统。

- 原系统盘数据如何拷贝出来？
  您可以通过卸载系统盘挂载为数据盘的方式将原实例系统盘内容拷贝出来。具体操作，请参见卸载或挂载系统盘。
- 原系统盘中部署的服务应用怎么迁移出来？
  - 在新的系统盘中重新部署服务。
  - 迁移数据库等应用。具体操作，请参见数据库和应用迁移服务。

采用方案一的优点和缺点如下：

- 优点：方便易操作，阿里云有丰富的公共镜像可以选择，一键切换到新版本操作系统。
- 缺点：原系统盘中的数据需要客户自行备份处理， 一些应用服务可能需要重新部署。

解决方案二：升级系统到OS的最高版本

您可以进行系统升级，将系统版本升级到该OS的最高版本。例如，可以将CentOS 5升级到CentOS 5的最高版本CentOS 5.11。更多信息，请参见：

- 如何将RedHat和CentOS 5系统升级到5.11版本？
- FreeBSD系统如何打补丁编译内核？
- 如何将Debian 6系统升级到最新的6.0.10版本？
- gentoo 升级或者使用Gentoo的cloud image 镜像

采用方案二的优点和缺点如下：

- 优点：原系统中的数据及服务不受影响。
- 缺点：即使升级到OS的最高版本（例如CentOS 5升级到CentOS 5.11），该版本仍然是已不维护更新的版本，系统漏洞风险依然存在，无法使用新OS发行版（例如CentOS 7/8）上的新特性和功能。

解决方案三：使用旧版本的实例规格

您可以尝试非神龙MOC环境的5代旧版本实例规格，例如ecs.n、ecs.xn、ecs.c5系列。更多信息，请参见实例规格族。

虚拟化virtio驱动安装配置不成功

系统在迁移后，发生了虚拟化环境从Xen到KVM的变化，如果系统内部虚拟化驱动没有安装或者配置好KVM virtio驱动，就会发生系统宕机、蓝屏等问题。可能有以下原因：

- Linux系统未安装配置virtio驱动
- Windows ISO阶段驱动安装失败
- Windows系统注册表损坏
- Windows安装有360软件等安全软件限制

解决方案

- 安装virtio驱动
- 如果检查Linux系统是内核损坏，请下载安装官方内核再次尝试
- Windows请联系售后技术支持挂载Winpe 3.0 ISO，并用内置工具修复virtio驱动

- Windows建议迁移前用SFC（System File Checker）检查系统的完整性，包括注册表等，并卸载类似360等安全软件

13.17. 如何收集操作系统宕机后的内核转储信息?

ECS实例宕机后会生成一个转储信息文件，您可以将转储信息提交给阿里云，便于阿里云技术支持人员定位分析问题。本文为您介绍如何收集操作系统宕机后的内核转储信息。

背景信息

阿里云技术支持人员可以通过在转储文件中找到对应的信息，从而分析操作系统宕机的原因，并同步给用户。

> **说明** 您也可以通过Windows平台的WinDbg工具和Linux平台的crash工具来检查操作系统内核的转储文件。

Linux实例

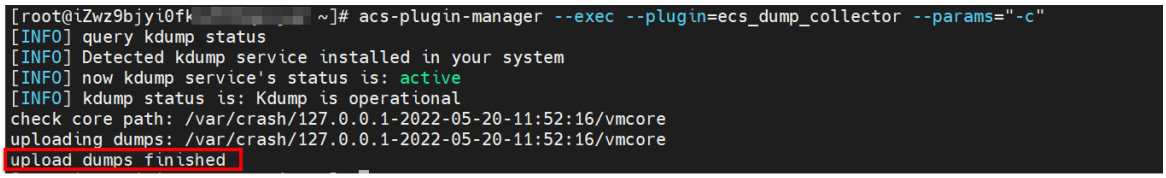
1. 远程连接ECS实例。

   具体操作，请参见通过密码或密钥认证登录Linux实例。

2. 运行以下命令，收集转储信息。

```
acs-plugin-manager --exec --plugin=ecs_dump_collector --params="-c"
```

   显示如下信息，表示收集成功。



Windows实例

1. 远程连接ECS实例。

   具体操作，请参见通过密码或密钥认证登录Windows实例。

2. 打开CMD命令行窗口。
3. 运行以下命令，进入到*assist*目录。

```
cd C:\ProgramData\aliyun\assist
```

4. 运行以下命令，查询*assist*目录下的文件信息。

```
dir
```

5. 运行以下命令，进入目录的最新版本，例如 `2.1.3.282` 。

```
cd 2.1.3.282
```

6. 运行以下命令，收集转储信息。

```
acs-plugin-manager.exe --exec --plugin=ecs_dump_collector_win --params="-c"
```

显示如下信息，表示收集成功。

```
C:\ProgramData\aliyun\assist\2.1.3.282>acs-plugin-manager.exe --exec --plugin=ecs_dump_collector_win --params="-c"
[06/01/2022 15:23:32] [info] Crash status is ON.
check core path: c:/windows/MEMORY.DMP
uploading dumps: c:/windows/MEMORY.DMP
upload dumps finished
```

常见问题

如果在收集转储信息过程中出现类似如下提示信息，表示当前操作系统未开启dump配置。

```
[INFO] Detected kdump service installed in your system
[INFO] now kdump service's status is: unknown
[INFO] kdump service is NOT enabled in system, please run --enable
[INFO] kdump status is: Kdump is not operational
```

解决方案：

1. 运行以下命令，开启操作系统的dump配置。
   - Linux操作系统：`acs-plugin-manager --exec --plugin=ecs_dump_collector --params="--enable"`
   - Windows操作系统：`acs-plugin-manager.exe --exec --plugin=ecs_dump_collector_win --params="--enable"`
2. 在控制台重启实例，使配置生效。
   具体操作，请参见重启实例。

13.18. Red Hat云接入和Windows许可证

13.18.1. Red Hat云接入

13.18.1.1. Red Hat云接入概述

本教程介绍如何将Red Hat Enterprise Linux（RHEL）虚拟机镜像导入阿里云，并使用它在控制台中创建ECS实例。本教程适用于RHEL 6.9/6.10、7.4及以上版本、8.0及以上版本。

背景说明

在以下场景下，您才需要执行Red Hat云接入操作：

- 将自定义镜像导入阿里云ECS时，**许可证类型**选择**自带许可**。更多信息，请参见导入自定义镜像。
- 使用服务器迁移中心SMC迁移任务时，各目标类型中的**许可证类型**选择**自带许可**。更多信息，请参见创建并启动迁移任务。

ECS实例和自定义RHEL镜像要求

导入阿里云ECS实例的RHEL镜像必须满足以下要求：

- 镜像导入不支持多个网络接口或者IPv6地址。
- 确认已为远程访问启用了SSHD服务。
- 确认已禁用防火墙，并且已打开SSH 22端口。否则，您无法连接到已创建的ECS实例。
  建议您使用安全组来控制一台或多台ECS实例的入流量或出流量。更多信息，请参见安全组概述。
- 确认操作系统是RHEL 6.9/6.10、7.4及以上版本、8.0及以上版本，并且包括最新的cloud-init和安全更新。
  关于RHEL版本的更多信息，请参见公共镜像概述。

- 确认在根分区上使用了以下文件系统之一：xfs、ext3或ext4。
- ECS仅支持导入RAW、QCOW2或VHD格式的镜像。建议导入QCOW2或VHD格式的镜像，其传输容量较小。如果需要导入其他格式的镜像，请在导入镜像之前使用qemu-img工具转换格式。
- 确认*/etc/issue**文件未被修改，否则，将无法正确识别Guest操作系统的分发，并且您可能无法成功创建ECS实例。
- 正确配置了系统的GRUB配置文件。否则，系统可能无法启动。
- 确认*/etc/fstab*配置正确，否则，可能会出现阻止加载分区的异常，从而导致系统启动失败。
- 必须使用*/etc/shadow*上的默认权限。否则，无法修改密码文件，并且系统启动将失败。
- 只存在系统盘上的单个根分区，并且系统盘具有足够的空间容纳镜像文件。
- 确认已正确配置关键系统文件，例如：*/sbin*、*/bin*和*/lib**。

有关ECS实例和自定义RHEL镜像要求的更多信息，请参见导入镜像必读。

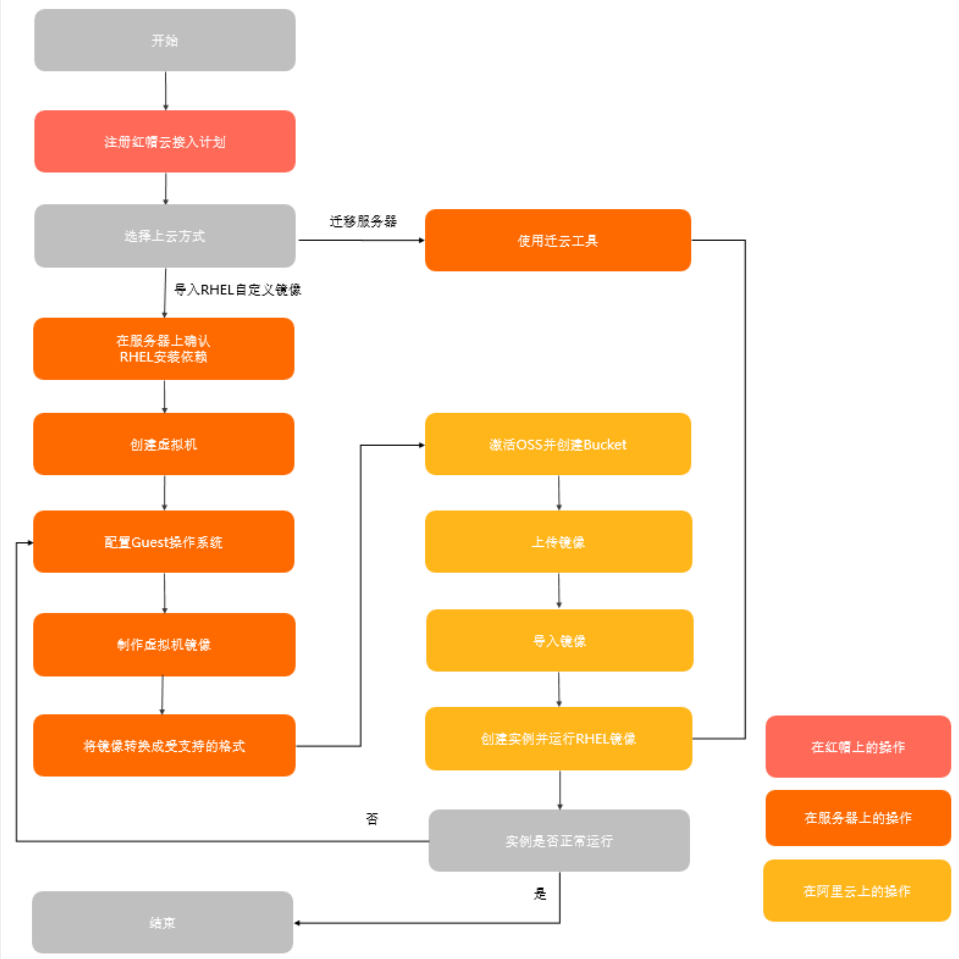
前提条件

在开始之前，请确保以下事项：

- 您同时具有Red Hat账号和阿里云账号。
  - 如果没有阿里云账号，请先注册阿里云账号。具体操作，请参见阿里云账号注册流程。
  - 如果没有Red Hat账号，请在Red Hat官网创建Red Hat门户账号。
- 您将物理Red Hat Enterprise Linux 7服务器作为脱机环境定制已下载的虚拟镜像，以满足阿里云镜像要求。更多信息，请参见步骤二：创建RHEL镜像。
- 如果您希望在位于中国内地的地域中创建ECS实例，根据相关政策，请使用您的真实姓名注册阿里云账号。

操作流程

下图展示了如何导入RHEL虚拟机镜像，并在ECS控制台上通过该镜像创建RHEL实例。



步骤概述

1. 步骤一：注册Red Hat云接入计划
2. 步骤二：创建RHEL镜像
3. （可选）步骤三：将镜像转换为受支持的格式
4. 步骤四：将镜像导入阿里云ECS
5. 步骤五：创建ECS实例并运行RHEL镜像

13.18.1.2. 步骤一：注册Red Hat云接入计划

本文介绍如何注册Red Hat云接入计划，供迁移当前的Red Hat订阅以在阿里云上使用。

操作步骤

1. 使用Red Hat账号登录Red Hat官网。

   Red Hat官网链接，请参见Red Hat官网。

2. 转到注册页面，并单击**GET STARTED**。

   注册页面链接，请参见注册页面。

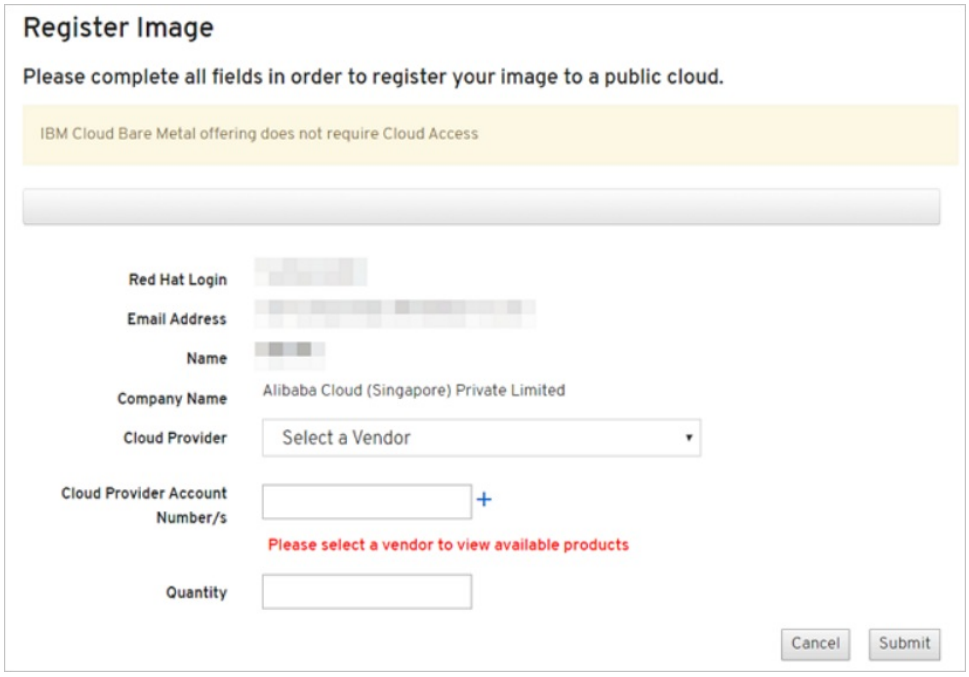
3. 单击**Verifying eligibility for Cloud Access**，确认您符合Red Hat云接入的资格要求。

   操作页面链接，请参见Verifying eligibility for Cloud Access。

4. 向上滚动页面并转到Enrollment Links部分，然后单击Enroll with Use your own image。

   操作页面链接，请参见Enroll with Use your own image。

5. 在Register Image对话框，完成以下参数配置。
   - Cloud Provider：选择Alibaba Cloud。
   - Cloud Provider Account：输入您的阿里云账号ID。
     您可以在ECS管理控制台的**账号管理 > 基本资料**里查看阿里云账号ID。
   - Quantity：指定您的镜像数量。



6. 单击Submit，将镜像注册到阿里云ECS。

13.18.1.3. 步骤二：创建RHEL镜像

本文以RHEL 7服务器为例，为您介绍如何将脱机IDC中的物理主机或经典虚拟化平台中的虚拟机迁移到阿里云。

背景信息

您可以将物理服务器或虚拟机迁移到阿里云。

- 将物理服务器迁移到阿里云ECS（P2V和V2V）
  您可以使用服务器迁移中心SMC（Server Migration Center）将物理服务器的操作系统镜像迁移到阿里云ECS，在将镜像导入ECS后，再通过已导入的镜像创建RHEL实例。
- 将虚拟机迁移到阿里云ECS（V2V）
  在本地物理服务器上创建阿里云支持的虚拟机镜像。您可以参考本文操作完成迁移，也可以使用阿里云的服务器迁移中心SMC进行迁移。

关于SMC迁移的更多信息，请参见迁移流程。

将虚拟机迁移到阿里云ECS

按照以下步骤将虚拟机迁移到阿里云ECS：

1. 步骤1 准备一台物理RHEL 7服务器
2. 步骤2 创建虚拟机

3. 步骤3 配置Guest操作系统
4. 步骤4 创建虚拟镜像

> **说明** 如果RHEL 7服务器上已运行满足步骤1 准备一台物理RHEL 7服务器中提到的要求的虚拟机，则可以直接从步骤3 配置Guest操作系统开始。

步骤1 准备一台物理RHEL 7服务器

1. 登录到物理RHEL 7服务器。
2. 确认下表中列出的所有包都已安装在您的RHEL服务器上。

   您可以运行 `yum info 包名` 查看已安装的包。

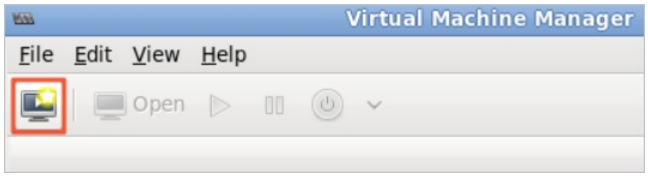
包	存储库	描述
libvirt	rhel-7-server-rpms	用于管理平台虚拟化的开源API、守护进程和管理工具。
virt-manager	rhel-7-server-rpms	桌面虚拟机管理器。
libguestfs	rhel-7-server-rpms	一组用于访问和修改虚拟机（VM）磁盘镜像的工具。
libguestfs-tools	rhel-7-server-rpms	用于虚拟机的系统管理工具，包括Guestfish。
qemu-img	rhel-7-server-rpms	用于将虚拟机磁盘镜像文件从一种格式转换为另一种格式的工具。

步骤2 创建虚拟机

1. 从Red Hat下载页面下载最新的**Red Hat Enterprise Linux 7.5 更新 KVM Guest镜像**或**Red Hat Enterprise Linux 7.4 更新 KVM Guest镜像**。

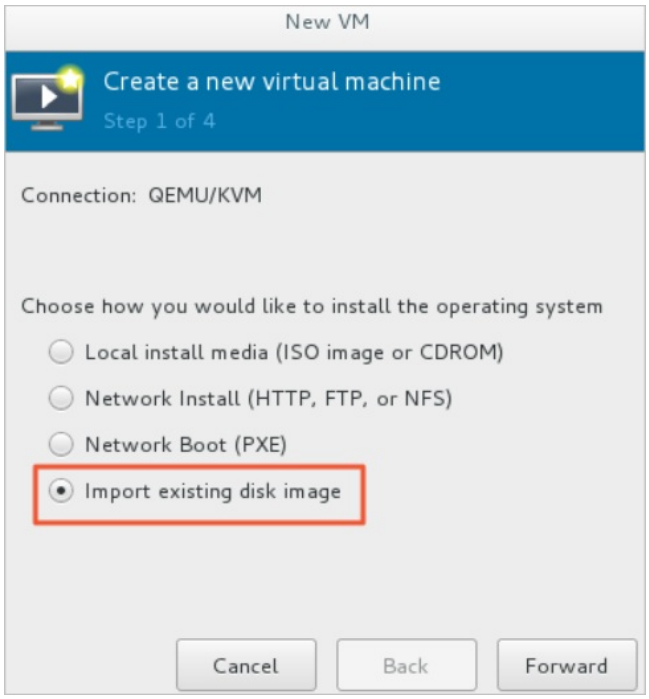
   > **说明** 建议您下载RHEL 7.5版本，RHEL 7.5相比较于RHEL 7.4功能更全面。

2. 将镜像保存到在步骤1准备的RHEL服务器中。
3. 将镜像移动到*/var/lib/libvirt/images*目录中。
4. 在**Virtual Machine Manager**窗口上，单击 图标创建新的虚拟机。

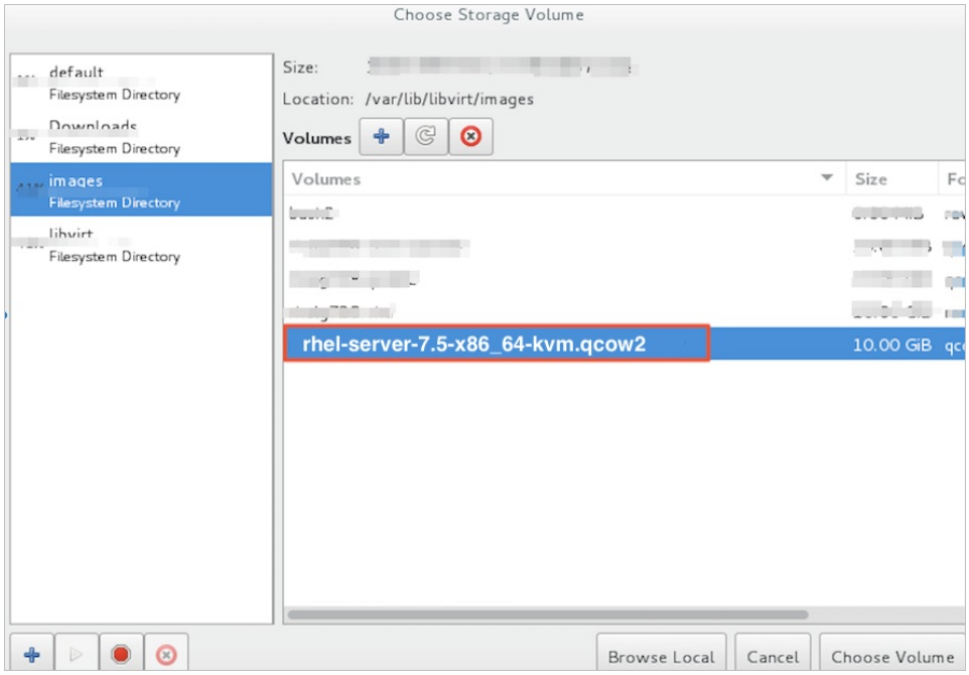


5. 按照**Create a new virtual machine**向导完成配置。

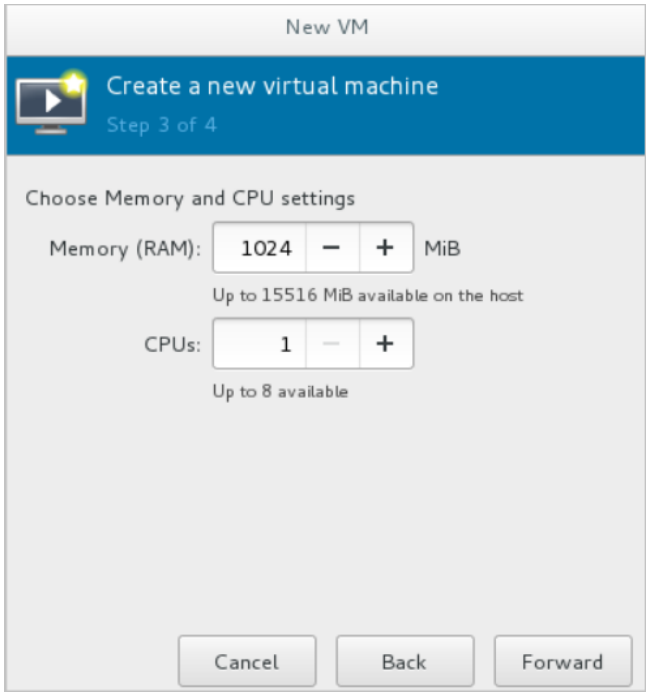
i. 选择**Import existing disk image**安装Guest操作系统，然后单击**Forward**。



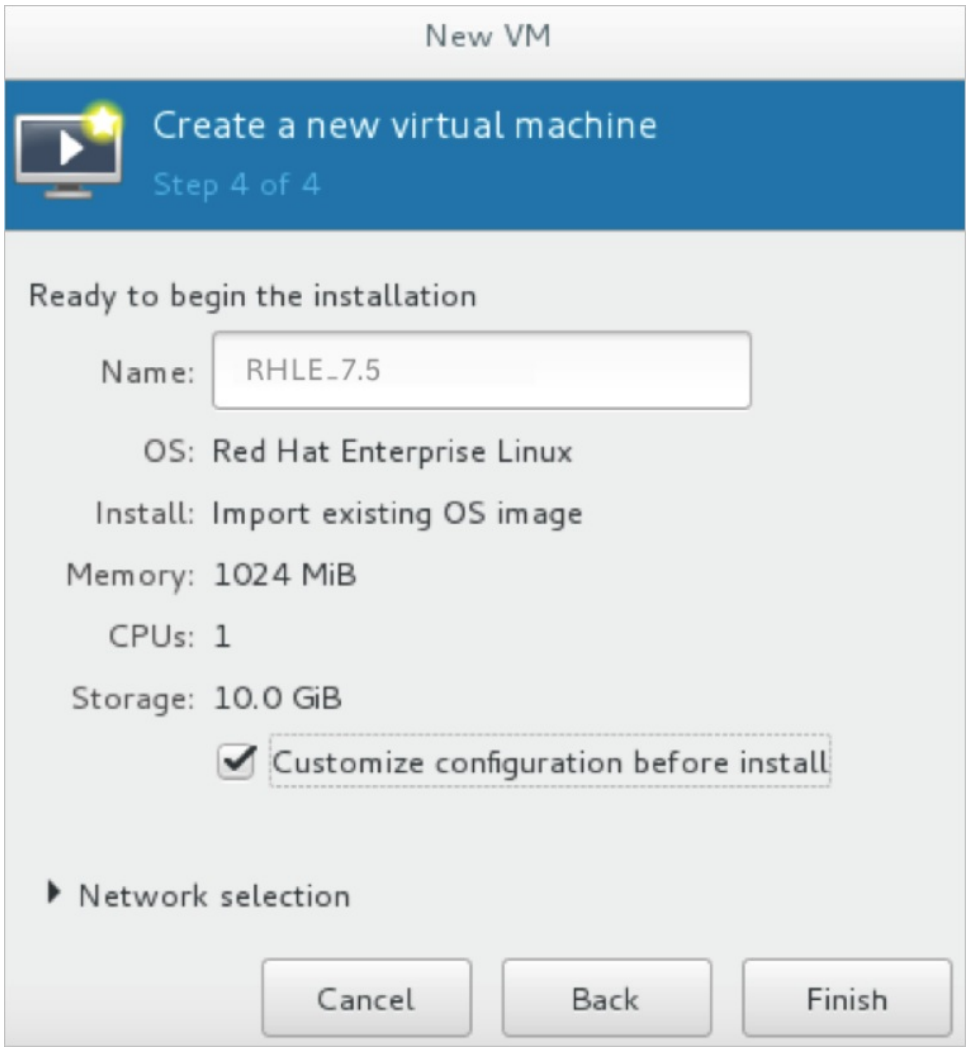
ii. 浏览*/var/lib/libvirt/images*目录并选择qcow2 KVM Guest镜像。



iii. 为新虚拟机设置内存和CPU内核。



iv. 查看新虚拟机的配置，指定名称，然后选中**Customize configuration before install**。



v. 在自定义配置对话框的左侧窗格中，单击**NIC**，然后设置**Device model**为**virtio**。

vi. 单击**Begin Installation**。
将开始创建新虚拟机。在此过程中，虚拟机控制台将显示并引导到登录提示。

vii. 当登录提示出现时，关闭虚拟机。

6. 运行以下命令，为虚拟机的根用户设置密码。

```
virt-customize -a /var/lib/libvirt/images/rhel-server-7.5-x86_64-kvm.qcow2 --root-passw
ord password:<密码>
```

本示例中为虚拟机根用户设置的密码为 `redhat!` ，命令示例如下：

```
 # virt-customize -a /var/lib/libvirt/images/rhel-server-7.5-x86_64-kvm.qcow2 --root-pa
ssword password:redhat!
 [   0.0] Examining the guest ...
 [ 103.0] Setting a random seed
 [ 103.0] Setting passwords
 [ 112.0] Finishing off
```

7. 启动RHEL虚拟机并以根用户身份登录。

步骤3 配置Guest操作系统

在您登录到虚拟机后，前往配置Guest操作系统。

1. 确保RHEL虚拟机的Guest操作系统满足要求。

   具体要求，请参见Red Hat云接入概述中的ECS限制及自定义RHEL镜像条件部分。
   需要验证的Guest操作系统配置如下表所示。

项目	要求
/etc/shadow	通过运行**chattr**命令使*/etc/shadow*处于未锁定状态。
qemu-ga	已卸载qemu-ga。
网络	已禁用或已卸载网络管理器，并且已启用网络服务。
ssh	已启用SSH服务，并且未设置PermitRootLogin。
防火墙	已禁用防火墙。
文件系统	使用xfs、ext3或ext4。不要使用具有64位功能的ext4。
passwd	已安装passwd。
分区	使用MBR分区或者GPT分区。
逻辑卷管理器（LVM）	未使用逻辑卷管理器（LVM）。
/lib	只能对*/lib*和*/lib64*使用相对路径。
cloud-init	Guest操作系统必须安装了cloud-init。 **说明** cloud-init缺省配置会禁止密码方式登录，如需启用密码登录，请参见文档安装cloud-init，根据其中安装cloud-init段落中的第5步，修改*/etc/cloud/cloud.cfg*配置文件中cloud_init_modules段落。

2. 配置ntp.conf文件。

   按照以下步骤配置ntp.conf文件，文件位于*/etc/ntp.conf*目录中。

   i. 运行以下命令，将ntp.conf文件备份为ntp.conf.bk。

   ```
   cp /etc/ntp.conf /etc/ntp.conf.bk
   ```

   ii. 编辑*/etc/ntp.conf*文件并将其内容替换为以下内容。

```
driftfile  /var/lib/ntp/drift
pidfile    /var/run/ntpd.pid
logfile    /var/log/ntp.log
# Access Control Support
restrict    default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict 192.168.0.0 mask 255.255.0.0 nomodify notrap nopeer noquery
restrict 172.16.0.0 mask 255.240.0.0 nomodify notrap nopeer noquery
restrict 100.64.XX.XX mask 255.192.0.0 nomodify notrap nopeer noquery
restrict 10.0.0.0 mask 255.0.0.0 nomodify notrap nopeer noquery
# local clock
server 127.127.1.0
fudge  127.127.1.0 stratum 10
restrict ntp1.aliyun.com nomodify notrap nopeer noquery
restrict ntp1.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp10.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp11.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp12.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp2.aliyun.com nomodify notrap nopeer noquery
restrict ntp2.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp3.aliyun.com nomodify notrap nopeer noquery
restrict ntp3.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp4.aliyun.com nomodify notrap nopeer noquery
restrict ntp4.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp5.aliyun.com nomodify notrap nopeer noquery
restrict ntp5.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp6.aliyun.com nomodify notrap nopeer noquery
restrict ntp6.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp7.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp8.cloud.aliyuncs.com nomodify notrap nopeer noquery
restrict ntp9.cloud.aliyuncs.com nomodify notrap nopeer noquery
server ntp1.aliyun.com iburst minpoll 4 maxpoll 10
server ntp1.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp10.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp11.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp12.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp2.aliyun.com iburst minpoll 4 maxpoll 10
server ntp2.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp3.aliyun.com iburst minpoll 4 maxpoll 10
server ntp3.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp4.aliyun.com iburst minpoll 4 maxpoll 10
server ntp4.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp5.aliyun.com iburst minpoll 4 maxpoll 10
server ntp5.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp6.aliyun.com iburst minpoll 4 maxpoll 10
server ntp6.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp7.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp8.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
server ntp9.cloud.aliyuncs.com iburst minpoll 4 maxpoll 10
```

修改完成后按*Esc*键，并输入 `:wq` 后按下回车键，保存并退出。

在确认Guest操作系统的配置后，便可以创建虚拟机镜像了。您也可以使用阿里云提供的服务器迁

移中心SMC创建和导入虚拟镜像，更多信息，请参见什么是服务器迁移中心。

步骤4 创建虚拟镜像

1. 在RHEL虚拟机菜单上，选择View > Snapshots。
2. 单击+图标并创建快照。

   在创建快照后，将创建虚拟机镜像。虚拟机镜像采用QCOW2格式。

后续步骤

（可选）步骤三：将镜像转换为受支持的格式

13.18.1.4. （可选）步骤三：将镜像转换为受支持的格式

ECS仅支持导入QCOW2、RAW或VHD格式的镜像文件。如果镜像没有采用QCOW2、RAW或VHD格式，需要转换格式后再导入。本文介绍如何使用qemu-img工具将其他格式的镜像文件转换成QCOW2、RAW或VHD格式。

背景信息

qemu-img支持以下镜像格式的转换：

- RAW、qcow2、qcow1、VMDK、VDI、VHD（vpc）、VHDX或QED格式的镜像转换成VHD格式
- RAW和VHD格式的互相转换

更多信息，请参见转换镜像格式。

操作步骤

1. 运行以下命令，安装qemu-img工具。

```
yum install qemu-img
```

2. 运行以下命令，转换镜像文件格式。

```
qemu-img convert -f VHDX -O vhd rhel.vhdx rhel.vhd
```

   参数说明如下：

   - -f：后跟源镜像格式。
   - -O：必须大写，后跟目标格式、源文件名和目标文件名。

   转换完成后，目标文件会出现在源镜像文件所在的目录下。

13.18.1.5. 步骤四：将镜像导入阿里云ECS

将镜像导入阿里云ECS之前，您必须先将其上传到OSS Bucket。本文介绍如何将自定义RHEL镜像导入阿里云ECS。

前提条件

- 请确保OSS Bucket、镜像和实例在同一地域中，并且由一个账号所有。
- 您已开通OSS（Object Storage Service）服务。具体操作，请参见开通OSS服务。
- 如果您使用的是RAM用户，应预先联系阿里云账号授权AliyunECSImageImportDefaultRole角色策略获得操作许可。

背景信息

对象存储OSS是阿里云提供的海量、安全、低成本、高持久性的云存储服务。更多信息，请参见什么是对象

存储OSS。

操作步骤

1. 步骤1 创建Bucket
2. 步骤2 在OSS Bucket上传镜像
3. 步骤3 在ECS中导入镜像

步骤1 创建Bucket

1. 登录OSS控制台。
2. 在左侧导航栏，选择**Bucket列表**。
3. 在**Bucket列表**页面，单击**创建Bucket**。
4. 在**创建Bucket**对话框中，完成以下配置，然后单击**确定**。
   - **Bucket名称**：输入有效的Bucket名称。例如，在本教程中为import rhel。
   - **地域**：从下拉列表中，选择一个地域。

     > **说明** Bucket和要创建的实例必须在同一地域中。

   - **存储类型**：选择默认类。在此示例中，请选择**标准存储**。
   - **读写权限**：选择默认方法。在此示例中，请选择**私有**。

   其他详细的参数配置，请参见创建存储空间。

步骤2 在OSS Bucket上传镜像

如果镜像文件大于5 GiB，请使用API或ossutil上传。

- 有关API的更多信息，请参见分片上传。
- 有关ossutil的更多信息，请参见命令行工具ossutil概述。

在此示例中，镜像文件小于5 GiB，直接在OSS控制台将其上传到OSS Bucket。

1. 登录OSS控制台。
2. 在左侧导航栏，选择**Bucket列表**。
3. 在Bucket列表中，单击Bucket名称，例如import rhel。
4. 在**文件管理**页面，单击**新建目录**页签。
5. 在**新建目录**对话框中，为目录输入有效的名称，例如在本教程中为*rhel/*，然后单击**确定**。
6. 单击目录名称，然后在目录页面上，单击**上传文件**。
7. 在**上传文件**页面，完成以下配置。
   - **上传到**：单击**当前目录**。
   - **文件ACL**：单击**继承Bucket**。
   - **待上传文件**：您可以单击**扫描文件**或**扫描文件夹**选择本地文件或文件夹，或者直接拖拽镜像文件到待上传文件区域。

   其他详细的参数配置，请参见简单上传。
8. 单击**上传文件**。

   此时，您可以在**上传列表**页签查看各个文件的上传进度。当进度为100%时，您可以在*rhel/*目录中查看镜像信息。

9. 单击镜像名称，然后在**详情**对话框中的URL字段下，单击**复制文件URL**。

> **说明**
> - 导入镜像阶段，您需要填入文件URL。
> - 如果文件的ACL为**私有**，则URL包含**过期**和**签名**信息。

步骤3 在ECS中导入镜像

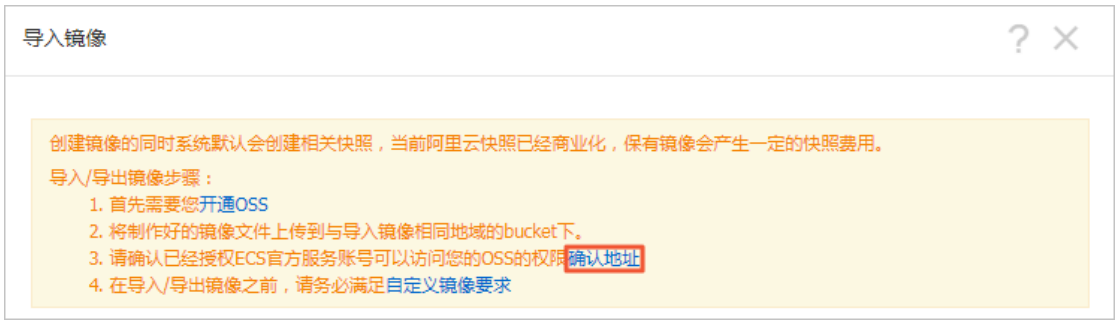
上传镜像后，您可以按照以下步骤在ECS控制台中导入镜像。您还可以使用ECS API ImportImage导入镜像。

> **说明** 建议您使用阿里云账号导入镜像，或者必须授予RAM用户AliyunECSImageImportDefaultRole权限。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像** > **镜像**。
3. 选择地域。

> **说明** 创建实例的地域必须与OSS Bucket在同一地域中。

4. 授权ECS服务访问您的OSS资源。
   i. 在**镜像**页面右上角，单击**导入镜像**。
   ii. 在**导入镜像**对话框里，单击提示信息第3步中的**确认地址**。



   iii. 在**云资源访问授权**页面，查看到 `AliyunECSImageImportDefaultRole` 和 `AliyunECSExportDefaultRole` ，单击**同意授权**。
5. 导入自定义镜像。
   i. 在**镜像**页面右上角，再次单击**导入镜像**。

ii. 在**导入镜像**对话框中，完成以下设置。

- **OSS Object地址**：粘贴镜像文件的OSS URL。
- **镜像名称**：输入镜像的有效名称。在创建ECS实例时，您可以使用此名称搜索镜像。
- **操作系统/平台**：选择Linux、RedHat。
- **系统架构**：选择x86_64。
- **系统盘大小(GiB)**：输入介于40和500 GiB之间的值作为系统盘的大小以满足您的业务需求。
- **镜像格式**：选择VHD。
- **许可证类型**：选择**自带许可**。

其他详细的参数配置，请参见导入自定义镜像。

iii. 信息确认无误后，单击**确定**。系统会创建一个导入自定义镜像的任务。

6. （可选）在目标地域的镜像列表中查看导入进度。在任务完成前，您都可以通过任务管理找到该导入的自定义镜像，取消导入镜像任务。

   导入自定义镜像所需时间，取决于镜像文件的大小和当前导入任务的并发数，需要您耐心等待。
   导入自定义镜像时，系统会自动生成一份快照，您可以在**快照列表**里看到快照信息。导入镜像任务未完成前，快照的状态会显示为**失败**。任务完成后，快照的状态自动更新为**成功**，镜像的状态自动更新为**可用**。快照的容量为导入的自定义镜像文件大小，与导入自定义镜像时设置的系统盘大小无关。目前快照容量已经收费，更多信息，请参见快照计费。

后续步骤

步骤五：创建ECS实例并运行RHEL镜像

13.18.1.6. 步骤五：创建ECS实例并运行RHEL镜像

在导入镜像后，您可以使用该镜像创建ECS实例。本文介绍如何在ECS控制台中使用RHEL镜像创建ECS实例，您还可以使用ECS API RunInstances创建实例。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例**页面，单击**创建实例**。
5. 完成**基础配置**。

   i. 配置付费模式。

   有关付费模式的更多信息，请参见计费方式概述。

   ii. 配置地域及可用区。

   选择已导入的镜像所在的地域，然后选择可用区。更多信息，请参见地域和可用区。

   iii. 配置实例规格及实例购买数量。

   选择Red Hat支持的ECS实例类型。更多信息，请参见阿里云上 RHEL Guest支持哪些实例类型。

   iv. 配置镜像。

   单击**自定义镜像**，并从下拉列表中按名称选择已导入的镜像。

   v. 配置存储信息。

   选择系统盘和数据盘的云盘类型并指定其大小。其中系统盘的大小不得小于镜像文件大小。

vi. （可选）配置快照服务。

vii. 单击**下一步：网络和安全组**。

6. （可选）完成网络和安全组配置、系统配置、分组设置，并确认订单。

   详细的操作步骤和参数配置，请参见使用向导创建实例。

执行结果

实例创建完成后，前往实例列表页面查看实例的状态，当实例的状态为**运行中**时，表明已在阿里云上成功创建了RHEL实例。

后续步骤

您可以通过Workbench、VNC和第三方客户端工具等多种方式连接实例。更多信息，请参见连接方式概述ECS远程连接操作指南。

相关文档

- RunInstances

13.18.2. Windows许可证

13.18.2.1. 微软许可证与软件保障

当您需要将业务部署在基于微软（Microsoft）软件的环境里时，我们能够为您提供在云端使用的微软许可证（Microsoft License）。

在阿里云使用微软许可证有两种方式：

- 使用阿里云提供的许可证
  直接购买和使用阿里云提供的微软许可证，包括运行Windows Server操作系统的公共镜像和预装了SQL Server的云市场镜像。
- 使用自带许可证
  根据软件保障条款和微软许可证迁移性在阿里云继续使用您当前拥有的许可证。

使用阿里云提供的许可证

阿里云通过服务提供商许可协议SPLA（Service Provider License Agreement）获得了提供微软许可证的权限。目前，ECS和RDS提供带有微软正版授权软件，包括Windows Server操作系统和SQL Server数据库。阿里云提供的Windows Server镜像和SQL Server数据库均含有合规正版许可。其中，运行了Windows Server系统镜像的ECS实例无需客户端访问许可证CAL（Client Access License）。每个Windows实例默认附带两个仅用于管理用途的远程连接。如果您需要两个以上的远程连接，或者需要将这些远程连接用于管理以外的用途，则需要引入额外的远程桌面服务的客户端访问许可证（Remote Desktop Services CAL）。

您可以在创建ECS实例时选择合适的Windows Server镜像或者数据库类型，创建ECS实例的具体操作，请参见使用向导创建实例。阿里云提供的Windows Server操作系统镜像版本如下表所示。

Windows Server操作系统	SQL Server数据库
• Windows Server 2019 with Container 数据中心版 64位中文版 • Windows Server 2019 with Container 数据中心版 64位英文版 • Windows Server 2019 数据中心版 64位中文版 • Windows Server 2019 数据中心版 64位英文版 • Windows Server 2016 数据中心版 64位中文版 • Windows Server 2016 数据中心版 64位英文版 • Windows Server 2012 R2 数据中心版 64位中文版 • Windows Server 2012 R2 数据中心版 64位英文版 • Windows Server Version **** 数据中心版 64位中文版 • Windows Server Version **** 数据中心版 64位英文版 Windows Server的更多版本信息，请参见2022年。	• Windows Server 2016 SQL Server 2014企业版 • Windows Server 2016 SQL Server 2014标准版 • Windows Server 2012 R2 SQL Server 2012 SP3企业版 • Windows Server 2012 R2 SQL Server 2012 SP3标准版

说明 微软已经于2020年1月14日停止对Windows Server 2008和Windows Server 2008 R2操作系统提供支持。因此阿里云不再对使用上述操作系统的ECS实例提供技术支持。如果您有使用上述操作系统的ECS实例，请尽快更新至Windows Server 2012或以上版本。

使用自带许可证

如果您已经拥有微软许可证，在阿里云可以继续使用自带许可证BYOL（Bring Your Own License）。请了解您的微软许可证是否有软件保障，更多信息，请参见微软官网。根据您的微软许可证有无软件保障，有两种选择：

说明 您可以将自带许可证（BYOL）的自定义镜像导入至阿里云，并通过该自定义镜像创建相应的ECS实例。注意在导入自定义镜像时，需要将**许可证类型**设置为**自带许可**。具体操作，请参见导入自定义镜像。

- 无软件保障
  如果您所拥有的许可证没有软件保障（Software Assurance），您可以使用阿里云弹性裸金属服务器或专有宿主机。由于弹性裸金属服务器和专有宿主机是您独享物理资源的云主机，即使没有软件保障，您也能使用自带的微软许可证。更多信息，请参见弹性裸金属服务器概述和什么是专有宿主机DDH。

  注意 为了满足合规要求，许可证必须于2019年10月01日前获取，同时操作系统版本的发布时间必须早于2019年10月01日。

  您可以在弹性裸金属服务器或专有宿主机中部署微软产品条款中涵盖的所有微软许可证的软件，包括但不限于：
  - Microsoft Windows Server
  - Microsoft Exchange Server
  - Microsoft SharePoint Server
  - Microsoft SQL Server
  - Microsoft System Center

- Microsoft Dynamics
- MSDN
- Microsoft远程桌面服务（用户CAL）

- 有软件保障
  如果您所拥有的许可证具有软件保障，您可以通过软件保障和批量许可投资将微软许可证迁入阿里云继续使用。对于有效微软产品条款中涵盖的微软许可证的软件，您可以通过享有的许可移动性权利申请迁移到ECS后继续使用自带许可证。更多信息，请参见申请许可移动性和什么是服务器迁移中心。
  以下列表为符合条件的微软产品：
  - Microsoft Exchange Server
  - Microsoft SharePoint Server
  - Microsoft SQL Server
  - Microsoft System Center
  - Microsoft Dynamics
  - Microsoft BizTalk Server
  - Microsoft远程桌面服务（用户CAL）
  - 适用于Business Server的Microsoft Skype

权责声明

微软发行的正版软件具有高性能、高稳定性和高安全性的优点，请您根据自己的业务需求选择合适的正版软件，并遵守产品使用条款和授权条款。本文档仅作为参考指南不构成法律意见，请勿依赖于本文描述。如果您对微软正版软件的授权或权利有任何疑问，请咨询您的法务团队、律师咨询所、微软官方渠道或者相关分销商。

13.18.2.2. 申请许可移动性

本章节旨在阐述如何基于软件保障（Software Assurance）申请微软产品许可移动性。如果您打算使用ECS专有宿主机或者直接购买阿里云提供的许可证，可以跳过此章节。

背景信息

阿里云作为微软的授权移动性合作伙伴（Authorized Mobility Partner），接受有效软件保障合同所覆盖的微软软件产品许可。您可以向微软提交许可迁移申请，在阿里云继续使用自带许可证BYOL（Bring Your Own License），无需再次购买。

如果需要使用软件许可移动性继续使用已有的许可证，请确保许可证符合以下情况：

- 您的微软许可证必须具有有效软件保障（Software Assurance）。更多信息，请参见Software Assurance。
- 软件产品必须支持许可移动性协议，主要包括以下产品：
  - Exchange Server
  - SharePoint Server
  - SQL Server Standard Edition
  - SQL Server Enterprise Edition
  - Skype for Business Server
  - System Center Server
  - Project Server
  - Visual Studio Team Foundation Server

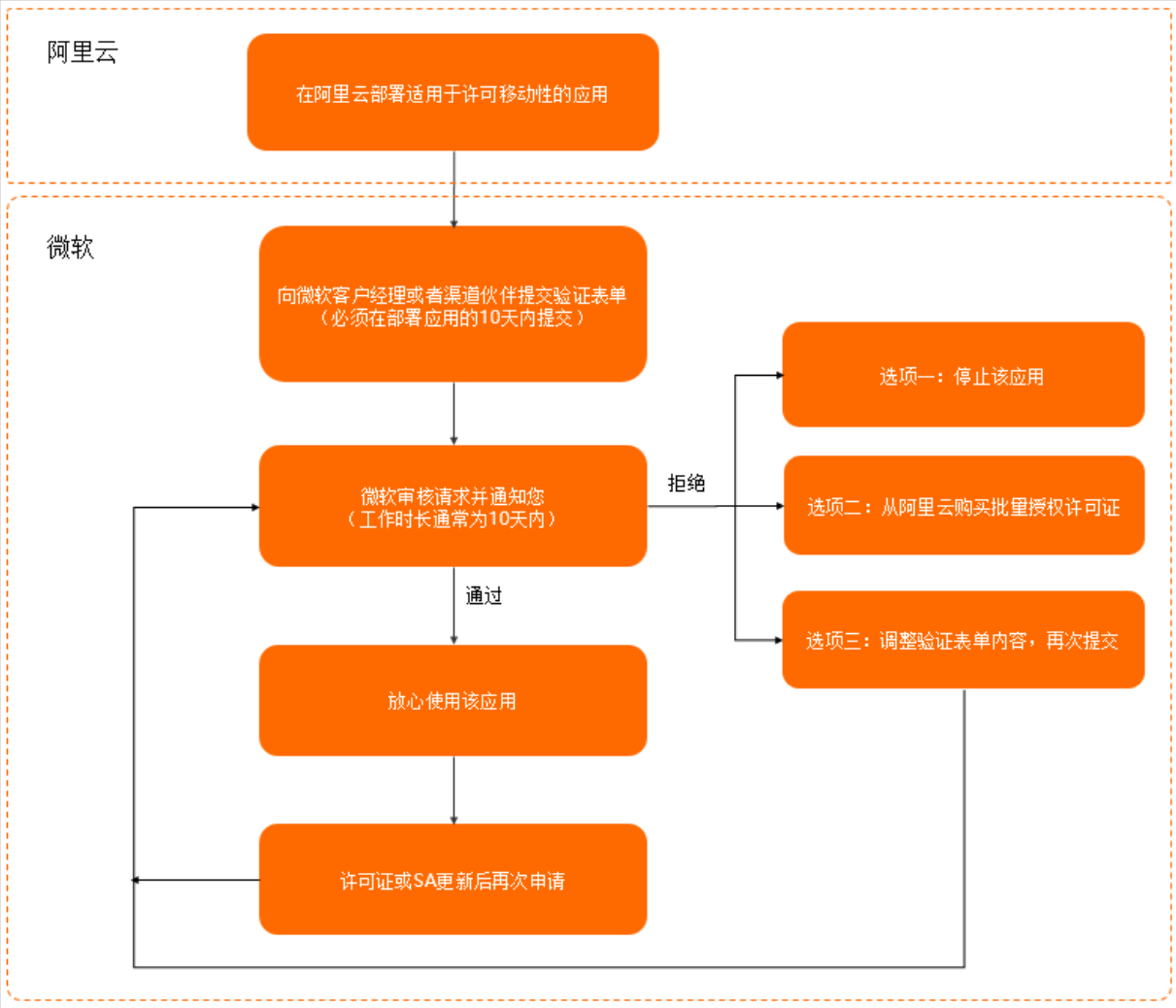
- BizTalk Server
- Remote Desktop Services

更多支持的微软产品详情，请参见许可条款。

- 适用的批量许可计划包括具有软件保障选项的企业协议、企业订阅协议、Microsoft Open Value协议以及其他Microsoft批量许可计划，如Microsoft Open License或Select Plus。
- 许可证不能是Microsoft Windows客户端操作系统或者桌面应用程序产品，例如Microsoft Office和Microsoft Windows Server操作系统。

申请步骤

根据微软许可移动性条款，您可以在微软确认您的申请之前部署应用环境。并且在应用环境部署完成后10天内提交许可移动性审核。参考申请流程如下图所示。



1. 在阿里云部署适用于许可移动性的应用。
2. 向微软提交许可迁移使用申请。

   具体操作请参见微软文档通过软件保障获取的许可移动性。在验证表单中提供阿里云作为微软授权移动性合作伙伴的认证信息，包括：

   - 授权移动性合作伙伴名称：Alibaba Cloud Computing Ltd.
   - 授权移动性合作伙伴网站：www.alibaba-inc.com
   - 授权移动性合作伙伴邮箱：microsoft@alibaba-inc.com

3. 等待微软审核与答复。

后续步骤

基于微软产品条款，对于已获得许可移动性的许可证，您可以根据需要：

- 将具有许可移动性的许可证重新分配给同一阿里云可用区内的其他ECS实例，关于可用区的更多信息，请参见地域和可用区。
- 将具有许可移动性的许可证重新分配给不同阿里云可用区内的其他ECS实例。但两次分配的时间间隔不得少于90天。更多信息，请参见许可条款。