

目录

目录	1
安装操作系统	2
购买时安装操作系统	2
重装操作系统	2
设置RAID级别	2
购买时设置RAID级别	2
重装系统时设置RAID级别	2
更改网络配置	3
SSH密钥管理	3
创建密钥对	3
查看和修改密钥对	3
删除密钥对	3
镜像使用说明	4
自定义镜像管理	4
创建自定义镜像	4
查看自定义镜像	4
删除自定义镜像	4
安全组管理	5
创建安全组	5
编辑安全组进站规则/出站规则	5
复制安全组	5
删除安全组	6
操作前提	6
操作步骤	6
管理裸金属服务器成员	6
远程登录	6
操作步骤	6
RoCE网络IP分发	7
RDMA的概念	7
RDMA 的网络协议	7
RoCE网络 IP的分发方式	7

安装操作系统

在购买或者重装裸金属服务器时，用户需指定想要安装的操作系统的。裸金属服务器控制台中提供的可选操作系统，都已经过服务器厂商和金山云的测试认证，保证裸金属服务器可以在数据中心正常运行。

购买时安装操作系统

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 单击裸金属服务器，进入新建裸金属服务器页面。
3. 在选择镜像步骤中，选择所需镜像。关于创建裸金属服务器的其他步骤说明，请参见[创建裸金属服务器](#)。



重装操作系统

非标准化租赁机型不支持重装系统操作，标准化租赁机型可在线重装系统。

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在目标裸金属服务器列表上方选择重装系统，或在对应的操作列中，选择更多 > 重装系统。



3. 选择要使用的镜像、Bond选型和RAID类型等，并单击 下一步。



4. 选择SSH密钥，设置管理员密码，并单击确定。

若要创建新的SSH密钥，请参见[SSH密钥管理](#)。



设置RAID级别

独立冗余磁盘阵列（Redundant Arrays of Independent Disks，简称RAID）以提高读写性能以及容错能力为目标，与单块硬盘相比，具有更快的传输速率，可大幅提高存储系统的数据吞吐量。

用户可以像管理独立硬盘或逻辑存储单元一样来管理磁盘阵列，并根据业务场景，在购买时或者重装系统时设置RAID级别。

RAID级别的说明如下：

- RAID 1：通过数据镜像保障数据的安全性，读写性能等同于单块盘，数据有镜像备份，存储空间利用率为50%，适用于对数据安全要求较高的场合。
- RAID 10（推荐使用）：结合了RAID 0数据条带分布与RAID 1镜像冗余两者的特性，既能够提供较高的读写速度，又能够使数据得到镜像保护，存储空间利用率为50%，实际应用比较常用。
- RAID 5：提供了对数据的奇偶冗余，且采用数据条带分布，读写性能很高，存储空间利用率高于50%，但安全性略低于RAID 10和RAID 1。适合多读少写场景，是性能、数据冗余与成本最佳的折中方案。
- RAID 50：结合了RAID 5冗余校验和RAID 0条带分布的优势，可以在确保数据安全性的同时保障存储IO的性能，存储空间的利用率是(N-2)/N，利用率比较高。
- 单盘RAID 0：采用数据条带分布，具有最高的读写性能，磁盘利用率为 100%，但无冗余保证，不能应用于对数据安全要求较高的场合。

购买时设置RAID级别

在购买裸金属服务器时，在选择镜像步骤中设置数据盘RAID参数。关于其他步骤说明，请参见[创建裸金属服务器](#)。



重装系统时设置RAID级别

在为裸金属服务器重装系统时，可以设置数据盘RAID参数。但注意此操作会格式化磁盘，需要提前做好数据备份。

有关重装系统的详细步骤，请参见[安装操作系统](#)。

更改网络配置

裸金属服务器使用内网IP与处于同一VPC的其他裸金属服务器或云服务器实现内网互访，产生的流量不收取费用。

内网IP由系统统一分配，用户可以在控制台进行更换网络配置的操作。不支持在操作系统内部自行变更内网IP，否则会导致内网通信失败。

更换网络配置的具体操作如下：

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 找到目标裸金属服务器，在对应的操作列中，选择更多 > 更换网络。

注意： 仅支持为未绑定弹性IP的裸金属服务器更换网络。

3. 选择虚拟私有网络、子网与IP地址，单击 **确定** 。

SSH密钥管理

裸金属服务器支持使用SSH密钥对认证登录，用户在创建裸金属服务器时需要指定SSH密钥对，所有已创建的密钥对在SSH密钥页面统一管理。

创建密钥对

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在左侧导航栏中，选择SSH密钥。
3. 在SSH密钥对列表页面，单击**创建密钥**。
4. 选取一种方式创建密钥对：
 - **创建新密钥对：**输入密钥对名称，单击“确定”后在弹出框中单击“下载”，保存私钥到本地。私钥只有一次下载机会，后续无法找回，只能创建其他密钥对。

- **使用已有公钥：**输入密钥对名称和公钥，单击“确定”。

查看和修改密钥对

密钥对通过ID/指纹作为唯一标识，用户可以查看密钥对应的公钥内容，或批量修改密钥对名称。

1. 进入[裸金属服务器 > SSH密钥](#)页面。
2. 选择想要查看的密钥对，可以看到创建时间、密钥ID和公钥内容。

3. 选择一个或多个想要修改名称的密钥对，单击**修改**。

4. 输入新的密钥对名称，单击**确定**。

密钥对将修改为新名称。如果是批量修改，命名方式为“新名称 + 后缀”。

删除密钥对

用户可根据需要删除密钥对，但需要注意删除后无法恢复。

1. 进入[裸金属服务器 > SSH密钥](#)页面。
2. 选择一个或多个想要删除的密钥对，单击列表上方**删除**。

3. 在弹出页面确认信息，单击**确定**。

镜像使用说明

裸金属服务器提供标准镜像，也支持自定义镜像。每个镜像都是裸金属服务器运行环境的模板，包含了操作系统和预装软件以及配置。

目前裸金属服务器支持以下标准镜像：

操作系统	内核版本
CentOS-6.5 64位	2.6.32-431.el6.x86_64
CentOS-7.2 64位	3.10.0-327.el7.x86_64
CentOS-6.7 64位	2.6.32-573.el6.x86_64
CentOS-7.0 64位	3.10.0-123.el7.x86_64
CentOS-7.1 64位	3.10.0-229.el7.x86_64
CentOS-7.3 64位	3.10.0-514.el7.x86_64
centos-7.2-x86_64-cuda8	3.10.0-327.el7.x86_64
centos-7.3-x86_64-cuda8	3.10.0-514.el7.x86_64
Ubuntu-12.04 64位	3.13.0-32-generic
Ubuntu-14.04 64位	4.4.0-31-generic
Ubuntu-16.04 64位	4.4.0-62-generic
ubuntu-16.04-x86_64-cuda8	4.4.0-62-generic
ubuntu-14.04-x86_64-cuda8	4.4.0-31-generic
Windows Server 2008 R2 英文 数据中心版 NT 6.1	
Windows Server 2008 R2 中文 数据中心版 NT 6.1	
Windows Server 2012 R2 英文 数据中心版 NT 6.3	
Windows Server 2012 R2 中文 数据中心版 NT 6.3	

自定义镜像管理

用户可以制作自定义镜像，并对自定义镜像进行集中管理。

创建自定义镜像

1. 登录[裸金属服务器控制台](#)，默认进入**裸金属服务器** > **裸金属服务器**页面。
2. 选择目标裸金属服务器，并单击列表上方的**关机**。
3. 在目标裸金属服务器对应的“操作”列中，选择**更多** > **制作镜像**。

4. 填写镜像名称，单击 **确定** 。

查看自定义镜像

1. 登录[裸金属服务器控制台](#)，默认进入**裸金属服务器** > **裸金属服务器**页面。
2. 在左侧导航栏中，选择**自定义镜像**。

在列表中可以查看自定义镜像的相关属性，包括ID、操作系统和创建时间。

删除自定义镜像

1. 登录[裸金属服务器控制台](#)，默认进入**裸金属服务器** > **裸金属服务器**页面。
2. 在左侧导航栏中，选择**自定义镜像**。
3. 选择一个或多个想要删除的自定义镜像，并单击列表上方的**删除**。

4. 在弹出页面中确认信息，单击**删除**。

安全组管理

安全组是一种有状态的服务器虚拟防火墙，它用于设置单台或多台裸金属服务器的网络访问控制。有关安全组的详细介绍，请参见[安全组（防火墙）](#)介绍。

用户在创建裸金属服务器实例时，可以将一个或多个安全组与该实例相关联，为安全组添加规则，规定流入或流出其关联裸金属服务器实例的流量。安全组规则按照从上到下的顺序与数据包进行逐条匹配。

创建安全组

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在左侧导航栏中，选择安全组。
3. 单击**新建安全组**。

4. 在新建安全组页面，输入安全组名称，选择虚拟私有网络，并配置规则：
 - a. 在入站规则或出站规则页签上，单击**新增**一行。
 - b. 选择协议，输入起始端口、结束端口、源IP和备注。
 - c. 重复上述步骤添加更多入站或者出站规则。

注意： 安全组中必须包含至少一条入站规则或出站规则。

5. 单击**确定**。

系统开始创建安全组并弹出**创建成功**提示。

编辑安全组入站规则/出站规则

编辑出站规则与入站规则步骤基本一致，本节以入站规则的编辑作为示例进行介绍。

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在左侧导航栏中，选择安全组。
3. 选择需要编辑的某个安全组，单击列表上方或入站规则页签下**编辑入站规则**。

4. 在规则列表中编辑已有入站规则，并使用页面其他功能辅助规则的编辑：
 - 新增一行：单击**新增**一行为列表增加新的规则。
 - 导出规则：单击**导出规则**将现有入站规则列表另存为.xlsx文件，并在本地编辑保存。
 - 批量导入：单击**批量导入**并选择文件，将当前入站规则列表替换为所选文件中的规则列表。
5. 单击**确定**。

复制安全组

用户可以将已有安全组快速地复制到其它地域或VPC。

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器>裸金属服务器页面。
2. 在左侧导航栏中，选择安全组。
3. 选择需要复制的安全组，单击**复制安全组**。

4. 在**复制安全组**页面，完成下列配置：

- 选择目标地域和目标VPC。
- 输入新的安全组名称。
- 编辑入站规则和出站规则。

5. 单击“确定”。

当出现“复制成功”的提示时，表示安全组复制成功，用户可以在安全组页面查看复制的安全组信息。

删除安全组

用户可以删除不再使用的安全组，但是VPC中的默认安全组不能删除。

操作前提

安全组中不包含任何裸金属服务器和云服务器，否则安全组不能删除。取消关联裸金属服务器和取消关联云服务器的操作步骤类似，请参见[管理裸金属服务器成员](#)。

操作步骤

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在左侧导航栏中，选择**安全组**。
3. 选择一个或多个需要删除的安全组，并单击**删除**。
4. 在删除确认页面，单击**删除**。当出现**删除成功**的提示时，表示安全组成功删除。

管理裸金属服务器成员

1. 登录[裸金属服务器控制台](#)，默认进入裸金属服务器 > 裸金属服务器页面。
2. 在左侧导航栏中，选择**安全组**。
3. 选择想要管理的安全组，单击列表上方的**管理裸金属服务器**。
4. 在管理裸金属服务器页面，单击**添加**或**移除**来管理此安全组下的裸金属服务器。左侧列表展示未加入此安全组的网卡，右侧列表展示已加入此安全组的网卡。

5. 单击**确定**。

远程登录

绑定公网IP地址的裸金属服务器，支持远程登录。

本节以Xshell 6软件为例进行介绍。

操作步骤

1. 在Xshell左上角选择**文件** > **新建**。
2. 在新建会话窗口中，输入裸金属服务器的公网IP地址，单击**确定**。

3. 在左侧导航栏中，选择**连接** > **用户身份验证**，并根据认证类型配置验证信息。本例采用默认的**root**用户。
 - 如果采用密码登录，选择“Password”方法并输入密码。

- 如果采用SSH密钥登录，选择“Public Key”方法，并单击**浏览**导入SSH密钥。

4. 单击确定。

RoCE网络IP分发

RDMA的概念

RDMA的内核旁路机制，允许应用与网卡之间的直接数据读写，将服务器内的数据传输时延降低到1us以下。RDMA的内存零拷贝机制，允许接收端直接从发送端的内存读取数据，极大的减少了CPU的负担，提升CPU的效率。

RDMA 的网络协议

1. InfiniBand (IB)：从一开始就支持RDMA的新一代网络协议。由于这是一种新的网络技术，因此需要支持该技术的IB网卡和IB交换机。
2. RDMA over Ethernet (RoCE)：即RDMA over Ethernet，允许通过以太网执行RDMA的网络协议。这允许在标准以太网基础架构(交换机)上使用RDMA，只不过网卡必须是支持RoCE的特殊的NIC。
3. 互联网广域RDMA协议(iWARP)：即RDMA over TCP，允许通过TCP执行RDMA的网络协议。这允许在标准以太网基础架构(交换机)上使用RDMA，只不过网卡要求是支持iWARP(如果使用CPU offload的话)的NIC。否则，所有iWARP栈都可以在软件中实现，但是失去了大部分的RDMA性能优势。

RoCE网络 IP的分发方式

4. 基础网络给每台交换机分配26位网段，NOC定时抓取获取交换机VLAN20记录的网段信息通过接口提供给EPC服务端。
5. 服务器上架后系统部确认RoCE网卡状态无异常后，抓取ROCE网卡收到的LLDP报文，将服务器上联的8台ROCE交换机主机名、端口号、400G网卡MAC地址推送给EPC服务端。
6. EPC服务端在控制台装机时根据交换机主机名匹配网段信息，对服务器的每张网卡分配IP并传递网关掩码信息，同时将以上信息与服务器SN关联记录在metadata中。
7. RoCE网络通过白名单形式开放，加白后控制台可以选择开启/关闭RoCE选择不同的库存服务器进行创建实例。
8. 创建完成后控制台实例详情页可以查看该实例网卡所分配的IP、网关、掩码信息。