**Amazon EC2用户使用手册**

**产品介绍**

**什么是Amazon EC2**

Amazon Elastic Compute Cloud（EC2）是亚马逊云科技（AWS）提供的安全、可弹性伸缩的云端计算服务。它允许用户在云端快速启动和管理虚拟机实例（称为“EC2实例”），这些实例具备高度灵活性、可扩展性且完全可控，能满足各种应用程序和工作负载的多样化需求，为企业和开发者提供了便捷高效的云端计算资源。

**产品核心价值**

|  |  |
| --- | --- |
| 产品核心价值 | 具体说明 |
| 稳定可靠高可用 | 来自弗若斯特沙利文在《云服务韧性取决于什么？》调研中看到AWS机器在各大云提供商中区域内云服务终端风险等级最低，说明其稳定性高。 |
| 服务稳定性 | 亚马逊云科技在研究周期内的整体故障时长低于其他云提供商整体故障时长平均值的1/5。 |
| 全球骨干网 | 安全性：数据传输通过Amazon骨干网，不会经过互联网。骨干网数据传输流量默认加密。  高可用性：骨干网由多条400GbE冗余线路组成。物理设备高可用的设计。  高可靠性：根据网络状态实时调优。  就近接入：全球边缘站点多，客户可以就近接入PoP点，经由Amazon骨干网入云。 |
| 弹性伸缩优势 | 秒级启动实例，快速响应业务需求。 |
| 全球部署优势 | 覆盖全球30+地理区域，构建广泛服务网络；  支持就近部署，大幅降低网络延迟；  适配全球合规要求，保障业务合法运营。 |

**Amazon EC2产品实例类型特性**

|  |  |  |  |
| --- | --- | --- | --- |
| 实例类型 | 核心特性 | 适配业务类型 | 业务说明 |
| 通用型实例 | 平衡的 CPU、内存与网络资源配比，支持突发性能（可通过 CPU 积分实现短时间性能提升），适用于资源需求均衡且负载波动较小的场景。 | 中小型网站/博客 | 无需高计算或大内存支撑，日常访问量稳定，突发流量可通过实例的突发性能应对，如企业官网、个人博客、内容展示类网站。 |
| 开发与测试环境 | 开发团队搭建代码编译、功能测试、接口调试环境，对资源需求灵活，通用型实例的性价比可降低研发成本。 |
| 轻量级应用服务 | 小型 API 服务、轻量数据库（如 MySQL 单机部署）、缓存服务（如 Redis 小规模集群），无需极致性能但需资源均衡。 |
| 办公协作工具 | 企业内部的 OA 系统、文档协作平台（如自建 Confluence）、小型 CRM 系统，用户访问量有限且功能需求简单。 |
| 计算优化型实例 | 高 CPU 核心占比（CPU / 内存配比高），搭载高性能处理器，适合密集型计算场景，能高效处理并行任务与计算密集型负载。 | 批处理作业 | 大规模数据处理（如日志分析、数据清洗）、批量渲染（如影视动画渲染、建筑设计效果图渲染），需多 CPU 核心并行运算。 |
| Web服务器集群 | 高并发访问的电商网站（如促销活动期间的商品详情页服务）、内容分发节点，需大量 CPU 资源处理用户请求。 |
| 游戏服务器（轻量型） | 中小型多人在线游戏的服务端，需处理玩家实时操作指令，但对内存需求较低。 |
| 计算密集型应用 | 科学计算（如简单的数值模拟）、机器学习训练（小规模模型，如分类算法训练）、实时数据分析（如用户行为实时统计）。 |
| 内存优化型实例 | 超大内存配置（内存容量远高于通用型，部分实例内存可达 TB 级），内存带宽高，支持高效数据读写，适合需将大量数据加载到内存中进行实时处理的场景。 | 内存数据库 | Redis、Memcached 等缓存数据库（大规模集群，需缓存海量数据）、MongoDB（文档型数据库，高频次读取场景），需内存快速存取数据以降低延迟。 |
| 大数据分析引擎 | Apache Spark、Hadoop 集群（内存计算模式），需将全量数据集加载到内存中进行实时分析，如用户画像实时构建、实时推荐系统。 |
| 企业级数据库 | Oracle、SQL Server 等关系型数据库（大规模部署，如千万级用户的交易数据存储），需内存支撑高频次查询与事务处理。 |
| 内存密集型应用 | 实时数据分析平台（如金融市场实时行情分析）、大规模机器学习推理（预训练模型加载到内存，快速响应预测请求）。 |
| 存储优化型实例 | 搭载高 IOPS（每秒输入输出操作）的本地存储（如 NVMe SSD、HDD），存储容量大，适合需频繁读写大规模数据的场景，兼顾存储性能与容量需求。 | 数据仓库 | 企业级数据仓库（如 Amazon Redshift 自建部署）、数据湖存储（存储海量结构化 / 非结构化数据），需高效读写历史数据用于分析。 |
| NoSQL数据库（存储密集型） | 分布式数据库，需存储海量数据且高频次读写，如用户行为日志存储、物联网设备数据存储。 |
| 文件存储服务 | 大规模文件共享（如媒体公司的素材库）、备份与恢复系统（需快速读取备份数据进行恢复），如影视公司的视频素材存储、企业的异地备份服务。 |
| 物联网（loT）数据处理 | 接收并存储海量物联网设备上传的实时数据（如传感器数据、设备状态数据），需高存储容量与稳定的 IO 性能。 |
| 高性能计算（HPC）实例 | 搭载高性能 GPU 或 CPU（如 NVIDIA A100 GPU、AMD EPYC 处理器），支持高速网络（如Elastic Fabric Adapter，EFA，低延迟互联），可组建大规模集群，适合超大规模计算任务。 | 科学与工程模拟 | 计算流体动力学（CFD，如飞机气动性能模拟）、分子动力学（如药物分子与靶点结合模拟）、天体物理模拟（如星系演化计算），需超大规模并行计算。 |
| 深度学习训练 | 大规模 AI 模型训练（如大语言模型 LLM、计算机视觉模型），GPU 提供强大的浮点运算能力，加速模型训练过程。 |
| 高性能数据分析 | 超大规模数据集处理（如全基因组测序数据分析、全球气象数据模拟），需多节点协同计算以缩短处理时间。 |
| 高端制造业仿真 | 汽车碰撞模拟、航空发动机结构强度分析、芯片设计验证，需高精度计算以确保产品性能与安全性。 |

**购买指南**

**购买指引**

* 前提条件：

购买Amazon EC2前，您需要完成快快网络账号注册，并完成实名认证。

* 操作步骤

**方式一：介绍页购买**

|  |
| --- |
| 请在购买前先登录快快网络控制台》Amazon EC2》密钥对，创建需要购买地域的密钥对。否则将无法成功完成服务的购买。 |

1. 登录快快网络官网。在顶部导航栏选择【弹性云服务器】（https://www.kkidc.com/ecs/index.html），进入产品介绍页面。
2. 单击“立即购买”。
3. 在弹性云服务器购买页面，选择“Amazon EC2”，跟进您的业务需求，选择服务器地域、镜像、实例配置、存储、网络带宽、安全组、密钥对、购买量等信息。
4. 单击底部右侧“立即购买”，完成支付流程。

**方式二：控制台购买**

1. 登录快快官网控制台，选择【Amazon EC2】。
2. 单击列表左上方“购买产品”按钮进行购买。

* 请等待1-2分钟请刷新页面。成功开通Amazon EC2实例后，您可以在官网控制台Amazon EC2页面查看和管理实例。

**计费方式**

|  |
| --- |
| 1. **Amazon EC2实例到期仅保留1天时间，若该时间内没有及时操作续费，则实例将被删除，数据无法恢复。** 2. Amazon EC2实例流量按量使用计费。请保障账户余额充足，账号欠费后，系统会发送对应的欠费通知，**若未在流量欠费1小时内补足欠款，实例将自动禁用**。 |

Amazon EC2仅提供包年包月购买方式。

**实例**

实例决定了用于实例的主机硬件配置，每一个实例类型提供不同的计算和存储能力，您可以基于需要提供的服务规模而选择实例计算能力、存储空间和网络访问方式。

计费模式：包年包月

**存储**

Amazon EC2的实例提供了数据存储设备，包括系统盘、数据盘。

注：部分地域镜像的存储默认包括多个盘，这是Amazon EC2的硬性要求。

计费模式：包年包月

**网络**

Amazon EC2覆盖全球30+地理区域，构建广泛服务网络。具备安全性、高可用性、高可靠性、就近接入等优势。目前网络仅提供按流量计费方式。

按流量计费：按公网传输的数据总量（单位为GB）计费。

免费流量包：不同地域规则赠送的流量包额度有所差异，请参考购买页。

流量计费：根据Amazon不同地区的流量计费方式。

计费周期：每小时。

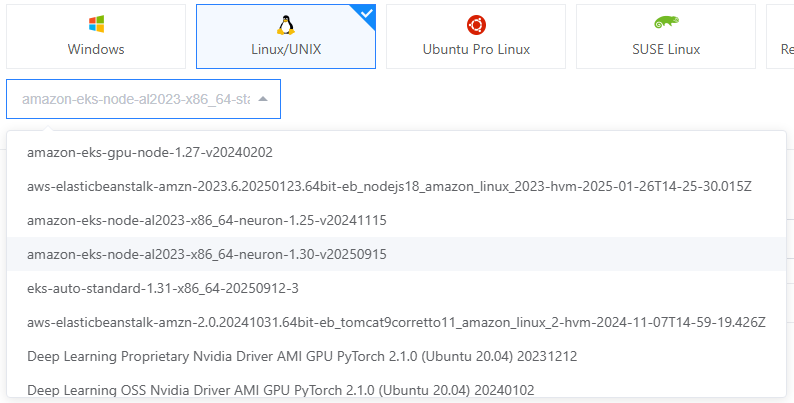
**镜像**

Amazon EC2提供多种主流镜像免费服务。

|  |
| --- |
| 选择建议  **按用途分类**：  Web 开发: Ubuntu 22.04 LTS  企业应用: RHEL 9 或 Amazon Linux 2  容器应用: ECS/EKS 优化镜像  Windows 应用: Windows Server 2022  机器学习: Deep Learning AMI  成本敏感: Amazon Linux 2 (免费)  **按稳定性分类**:  生产环境: LTS 版本 (Ubuntu LTS, RHEL, Amazon Linux 2)  开发测试: 最新版本 (Amazon Linux 2023, Ubuntu 最新)  **特殊需求**: 专用优化镜像 |

**镜像选择规则参考：**

* 以Linux/UNIX为例：



Amazon EC2通常遵循以下命名模式，您可通过对比该模式规则关键词内容选择合适的镜像信息。

* **镜像类型**：表示镜像的用途，例如Deep Learing（深度学习）、EKS（Elastic Kubernetes Service节点）、ECS（Elastic Container Service）等。
* **特殊支持**：例如GPU（图像处理器）、Neuron（AWS机器学习加速器）、NVIDIA（NVIDIA驱动支持）。
* **版本号**：包括软件版本（如Kubernetes版本）和日期版本（如v20240227，表示镜像创建日期）
* 其它镜像描述参考（这些是AWS官方维护的主要镜像类型）：
* **Amazon Linux2系列版本**，特点：免费、AWS优化、长期支持到2025年
* amzn2-ami-hvm-\*-x86\_64-gp2 （标准版本）
* amzn2-ami-minimal-hvm-\*-x86\_64-gp2 （最小化安装）
* amzn2-ami-ecs-hvm-\*-x86\_64-gp2 - ECS （容器优化）
* amzn2-ami-ecs-hvm-\*-x86\_64-gp2 - ECS （容器优化）
* **Amazon Linux 2023**，特点：现代内核、容器优化、滚动更新
* al2023-ami-\*-kernel-6.1-x86\_64（最新版本）
* al2023-ami-minimal-\*-kernel-6.1-x86\_64（最小化版本）
* **Ubuntu 22.04 LTS (Jammy)**
* ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-\*（标准服务器版）
* ubuntu-minimal/images/hvm-ssd/ubuntu-jammy-22.04-amd64-minimal-\* （最小化版本）
* ubuntu-pro-server/images/hvm-ssd/ubuntu-jammy-22.04-amd64-pro-server-\* （Pro 版本 (扩展安全更新)）
* **Ubuntu 20.04 LTS (Focal)**
* ubuntu/images/hvm-ssd/ubuntu-focal-20.04-amd64-server-\*（标准版）
* ubuntu-pro-server/images/hvm-ssd/ubuntu-focal-20.04-amd64-pro-server-\* （Pro 版本）
* **Red Hat Enterprise Linux**
* RHEL-9.\_HVM--x86\_64-\*-Hourly2-GP2 - 按小时付费版本
* RHEL-9.\_HVM--x86\_64-\*-Access2-GP2 - 自带许可版本 (BYOL)
* RHEL-HA-9.\_HVM--x86\_64-\*-Hourly2-GP2 - 高可用版本
* RHEL-8.\_HVM--x86\_64-\*-Hourly2-GP2 - 标准版本
* RHEL-SAP-8.\_HVM--x86\_64-\*-Hourly2-GP2 - SAP 优化版本
* **Windows Server 系列**
* Windows\_Server-2022-English-Full-Base-\* - 完整版 (桌面体验)
* Windows\_Server-2022-English-Core-Base-\* - 核心版 (无 GUI)
* Windows\_Server-2022-English-Full-SQL\_\*\_Standard-\* - 包含 SQL Server 标准版
* Windows\_Server-2022-English-Full-SQL\_\*\_Enterprise-\* - 包含 SQL Server 企业版
* Windows\_Server-2019-English-Full-Base-\* - 完整版
* Windows\_Server-2019-English-Core-Base-\* - 核心版
* Windows\_Server-2019-English-Full-ContainersLatest-\* - 容器优化版
* **SUSE Linux 系列**
* suse-sles-15-sp-v-hvm-ssd-x86\_64\*\* - 标准版 (按小时付费)
* suse-sles-15-sp-byos-v-hvm-ssd-x86\_64\*\* - 自带许可版本
* suse-sles-sap-15-sp-v-hvm-ssd-x86\_64\*\* - SAP 优化版本
* **CentOS/Rocky Linux 系列**
* Rocky-9-EC2-Base-\*-x86\_64 - 标准版本
* Rocky-9-EC2-LVM-\*-x86\_64 - LVM 配置版本
* Rocky-8-EC2-Base-\*-x86\_64 - Rocky Linux 8
* CentOS-Stream-ec2-9-\*-x86\_64 - CentOS Stream 9
* CentOS-Stream-ec2-8-\*-x86\_64 - CentOS Stream 8
* **Debian 系列**
* debian-12-amd64-\*-x86\_64 - 标准版本
* debian-12-arm64-\*-arm64 - ARM64 版本
* debian-11-amd64-\*-x86\_64 - 稳定版本
* **容器优化镜像**
* amzn2-ami-ecs-hvm-\*-x86\_64-ebs - ECS 标准优化
* amzn2-ami-ecs-gpu-hvm-\*-x86\_64-ebs - ECS GPU 优化
* amzn2-ami-ecs-inf-hvm-\*-x86\_64-ebs - ECS Inferentia 优化
* **ECS 优化镜像**
* amazon-eks-node--v - EKS 工作节点
* amazon-eks-gpu-node--v - EKS GPU 工作节点
* amazon-eks-arm64-node--v - EKS ARM64 节点
* **深度学习镜像（Deep Learning AMI）**
* \*Deep Learning AMI GPU PyTorch -Amazon Linux 2 - PyTorch GPU 版本
* \*Deep Learning AMI GPU TensorFlow -Amazon Linux 2 - TensorFlow GPU 版本
* Deep Learning AMI (Ubuntu 20.04) - Ubuntu 基础的深度学习环境
* **特殊用途镜像（FreeBSD）**
* FreeBSD 13.\*-RELEASE-amd64 - FreeBSD 系统
* **macOS (仅限 Mac 实例)**
* amzn-ec2-macos-12.-x86\_64- - macOS Monterey
* amzn-ec2-macos-13.-x86\_64- - macOS Ventura

**欠费说明**

如果您账号的余额小于待结算的账单，账号会进入欠费状态，

**欠费影响**

* 包年包月

账号欠费后，您可以使用已有的包年包月EC2资源，但存在以下限制：无法执行涉及管理的操作，如添加弹性IP、添加磁盘、启动、重启，也无法远程连接进入服务器。

|  |
| --- |
| **Amazon EC2实例到期仅保留1天时间，若该时间内没有及时操作续费，则实例将被删除，数据无法恢复。** |

* 按流量计费

账号欠费后，系统会发送对应的欠费通知，**若未在流量欠费1小时内补足欠款，实例将自动禁用**。为了避免业务影响，请及时充值。

* 结清欠费账单

账号结清欠款账单后，实例使用将自动恢复。

**续费指引**

**续费单台Amazon EC2**

登录快快官网控制台，选择Amazon EC2。

选择需要续费的Amazon EC2，点击列表操作栏“续费”按钮，按照页面提示选择需要续费的时长，并完成支付。

**操作指南**

**实例管理**

**管理实例状态**

您可以在控制台实现Amazon EC2服务器管理操作，包括启动、停止、重启等。

**启动**

* 前提条件：

实例处于【已停止】状态。

实例处于正常服务周期内。

* 操作步骤

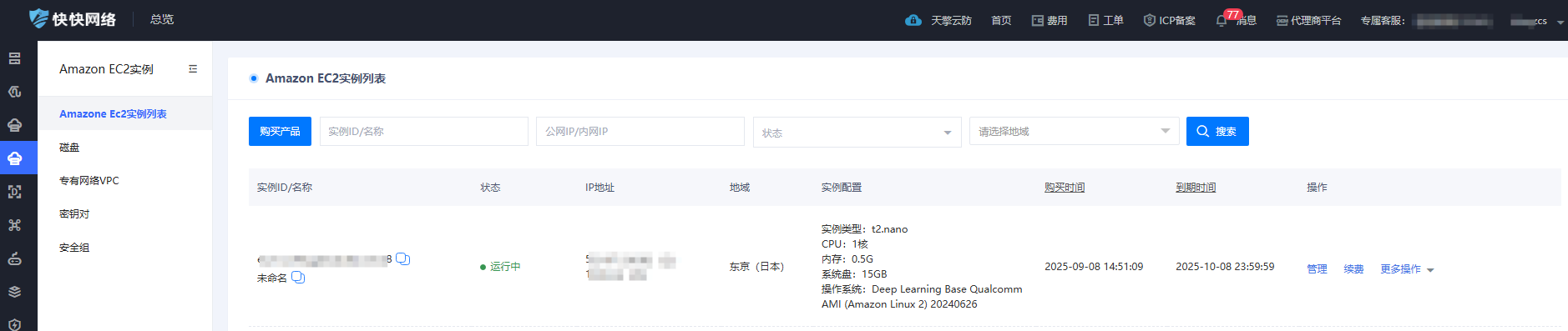
1. 登录快快官网控制台，选择Amazon EC2实例。
2. 选择需要操作启动的Amazon EC2实例，选择更多操作，单击【启动】。



1. 在启动实例确认框中确认实例信息，并单击确认，实例将进入启动中状态。



1. 请耐心等待1-2分钟后，刷新页面查看启动情况。若状态显示【运行中】，则实例启动成功。



**停止**

* 前提提交

实例处于【运行中】状态。

实例处于正常服务周期内。

* 操作步骤

1. 登录快快官网控制台，选择Amazon EC2实例。
2. 选择需要操作停止的Amazon EC2实例，选择更多操作，单击【停止】。



1. 在停止实例确认框中确认实例信息，并单击确认，实例将进入停止中状态。



1. 请耐心等待1-2分钟后，刷新页面查看停止情况。若状态显示【已停止】，则实例停止成功。



**重启**

* 前提条件

实例处于【运行中】状态。

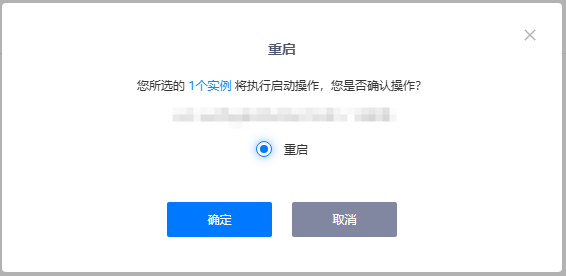
实例处于正常服务周期内。

* 操作步骤

1. 登录快快官网控制台，选择Amazon EC2实例。
2. 选择需要操作重启的Amazon EC2实例，选择更多操作，单击【重启】。



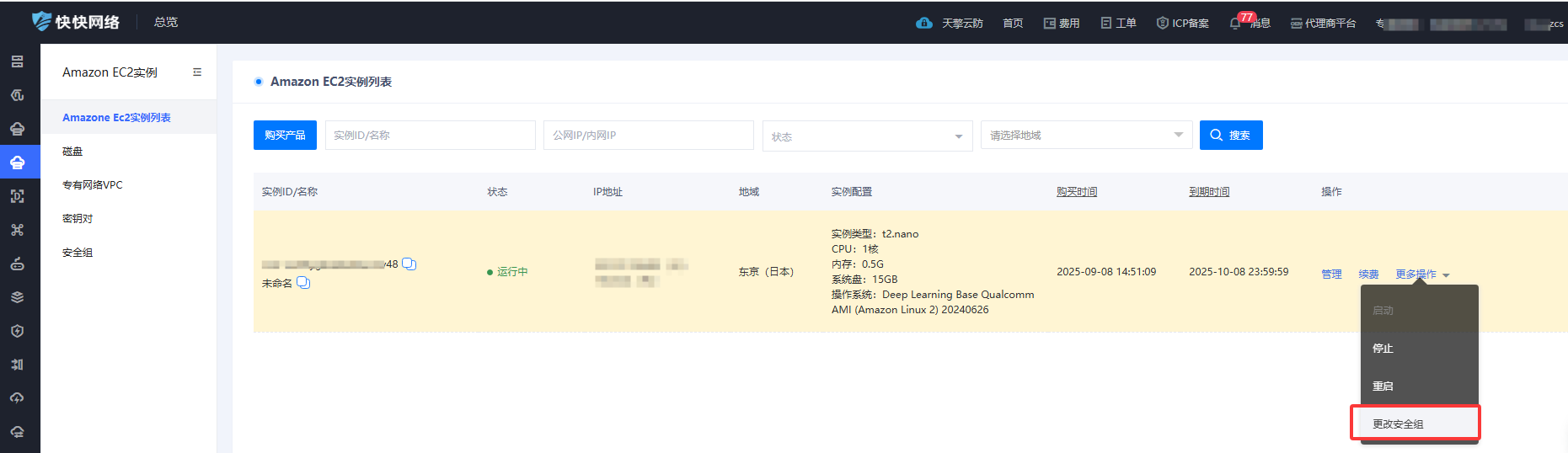
1. 在重启实例确认框中确认实例信息，并单击确认，实例将进入运行中状态。



**更改安全组**

|  |
| --- |
| 1. 一台实例最多关联5个安全组。 2. 建议为实例设置简介的安全规则。如果给一台服务器分配了多个安全规则，有可能导致服务器同时遵循数百条安全设置，设置变更都可能引起网络不通的故障。 3. 实例更改安全组时，可选的安全组内VPC需要关联该实例。 |

当您购买实例时，将默认为实例配置该地域下的默认安全组，您可以通过Amazon EC2》安全组新增对应地域的安全组信息。



**磁盘管理**

磁盘是Amazon EC2提供的块设备产品，具有高性能和低时延的特点，支持随机读写，满足大部分通用业务场景下的数据存储需求。您可以像使用物理硬盘一样，在Amazon EC2上进行格式化并建立文件系统来使用块存储。

**磁盘属性**

1. 系统盘：是Amazon EC2的启动盘，用于存储操作系统和程序文件等系统相关的数据，只能随实例创建，生命周期与实例相同。
2. 数据盘：用于存储用户数据，日志和其他应用程序等非系统相关的数据，生命周期与实例相同。

**使用限制：**

当前系统盘默认1块，数据盘至多支持10块。

**专有网络VPC**

专有网络VPC是您在Amazon EC2创建的自定义私有网络，不同的VPC之间二层逻辑隔离。您可以创建自己的VPC，例如可以自定义IP地址范围、子网、路由表和网络安全策略等，确保数据和应用的安全性，实现对网络架构的完全控制；随着业务需求的变化，可以轻松地扩展或缩减VPC内的资源，支持业务的连续性和快速迭代及增长。通过专有网络VPC，您可以更好地控制自己的资源访问、提高数据安全性和灵活性。

**专有网络段：**专有网络网段在创建专有网络和交换机时，您需要以CIDR地址块的形式指定专有网络使用的私网网段。允许的块大小介于 /16 网络掩码 (65,536 个 IP 地址) 和 /28 网络掩码 (16 个 IP 地址) 之间。在创建 VPC 后，您可以将额外的 IPv4 CIDR 块与 VPC 关联。您可以使用下表中标准的私网网段及其子网作为VPC的私网网段，也可以使用自定义地址段作为VPC的私网网段。

|  |  |
| --- | --- |
| 网段 | 说明 |
| 10.0.0.0/16 | 默认网段：您可以在掩码17-28进行扩展 |
| 172.16.0.0/16 | 您可以在掩码17-28进行扩展 |
| 192.168.0.0/16 | 您可以在掩码17-28进行扩展 |

**子网：**您可以通过对专有网络划分一个或多个子网。同一专有网络内的不同交换机之间内网互通。您可以将应用部署在不同可用区的交换机内，提高应用的可用性。

**创建和管理专有网络VPC**

专有网络 VPC是您在云上的私有网络，您可以自主选择IP地址范围、配置路由表和网关等。创建VPC后，还可以添加子网来扩展网络范围。

* 操作步骤

1. 登录快快官网控制台，选择Amazon EC2》专有网络VPC。
2. 单击【创建专有网络】
3. 选择与实例相应的地域。
4. 专有网络名称：输入VPC的名称。
5. IPv4网段：输入VPC的主IPv4网段，当前仅支持（192.168.0.0/16、172.16.0.0/16、10.0.0.0/16）网段。
6. 初始子网信息：
7. 子网名称：请输入您子网的名称
8. IPv4子网网段：配置子网IPv4网段，子网网段必须是其所属VPC网段的真子集。



**创建和管理子网**

创建VPC后，您可以通过创建子网为VPC划分一个或多个子网。默认同VPC下的子网互通。

**约束条件：**

您需要先创建对应的专有网络VPC。

* 操作步骤

1. 登录快快网络官网，选择Amazon EC2》专有网络VPC》子网。
2. 单击【创建子网】。
3. 所属专有网络：选择需要添加子网的专网网络。
4. 名称：子网对应的名称。
5. IPv4子网 CIDR：配置子网IPv4网段，子网网段必须是其所属VPC网段的真子集。

**密钥对**

远程登录Amazon EC2服务器实例必须通过密钥对核验身份。购买实例前，您需要先登录控制台创建对应地域的密钥对。

|  |
| --- |
| 创建密钥对后，系统将通过浏览器自动下载私钥。**您只有1次下载私钥的机会**，我们不会保管您的私钥信息，请您务必保存好创建完成后下载的私钥。 |

**什么是密钥对？**

Amazon EC2 密钥对（Key Pair）是 Amazon Elastic Compute Cloud（EC2）服务中用于身份验证的核心安全组件，替代了传统的密码登录方式，为 EC2 实例（虚拟机）提供更安全的远程访问机制。它本质上是一对关联的加密密钥 —— 公钥（Public Key）和私钥（Private Key），通过非对称加密算法确保只有持有私钥的用户才能访问对应的 EC2 实例。

EC2 密钥对基于非对称加密技术，由两个功能互补的密钥组成，二者一一对应、不可分割：

|  |  |  |  |
| --- | --- | --- | --- |
| 密钥类型 | 存储位置 | 核心作用 | 安全要求 |
| 公钥（Public Key） | WS 云端（与 EC2 实例绑定） | 加密数据：EC2 实例使用公钥对登录请求的验证信息进行加密，只有对应的私钥能解密 | 可公开（如配置到 EC2 实例、代码仓库等），无泄露风险 |
| 私钥（Private Key） | 用户本地（如电脑、安全存储设备） | 密数据：用户通过私钥解密 EC2 实例的加密信息，完成身份验证（类似 “数字钥匙”） | 绝对保密，仅用户持有，泄露会导致实例被未授权访问 |

**密钥对的注意事项**

1. Linux和Windows系统请选择 RAS类型密钥对。Linux和mac OS系统请选择 ED25519 类型密钥对。
2. 创建密钥对时，请务必确认好远程工具支持的格式。（当前支持的格式包括.pem（推荐远程工具：OpenSSH）和.ppk（推荐远程工具： PuTTY）。
3. 每个密钥对创建成功后通过浏览器下载，私钥仅可下载一次。**请务必保管并记录好私钥文件及登录密码。若私钥文件或者登录密码遗失，AWS不支持自助更换密钥对。**
4. Linux实例通过SSH远程登录时，ec2-user 是 EC2 实例的默认用户名（不同系统镜像用户名不同，如 Ubuntu 是 ubuntu）
5. Windows实例通过RDP远程登录时，需先转换密钥格式。通过控制台》实例列表》获取Windows密码》上传密钥对解密出首次登录密码后，通过解密密码登录。

**创建密钥对**

* 操作步骤

1. 登录快快网络官网，选择Amazon EC2》密钥对。
2. 单击【创建密钥对】。
3. 密钥对名称：填写对应实例的密钥对名称信息。
4. 地域：请选择与您购买的实例相关的地域。
5. 密钥对类型：请选择支持您实例系统的密钥对类型。
6. 私钥文件格式：请选择与您第三方远程软件支持的私钥文件格式（该项请您确认后选择，EC2不支持自助更换密钥对。）

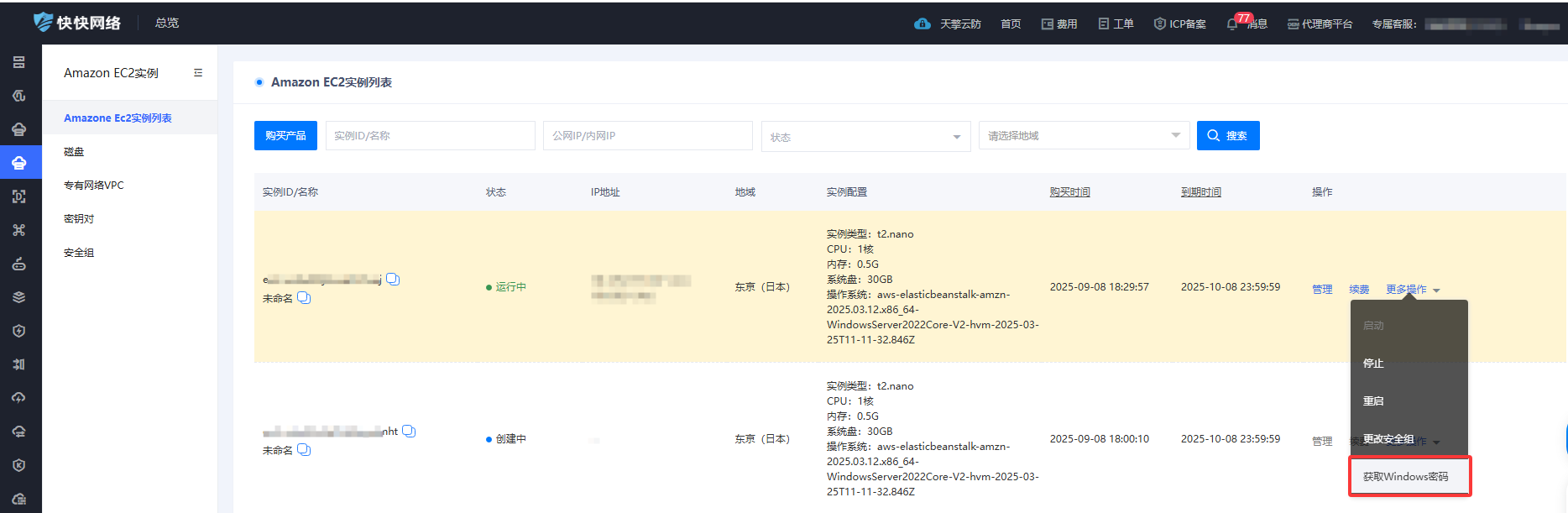
**实例远程登录**

**Windows实例登录：**

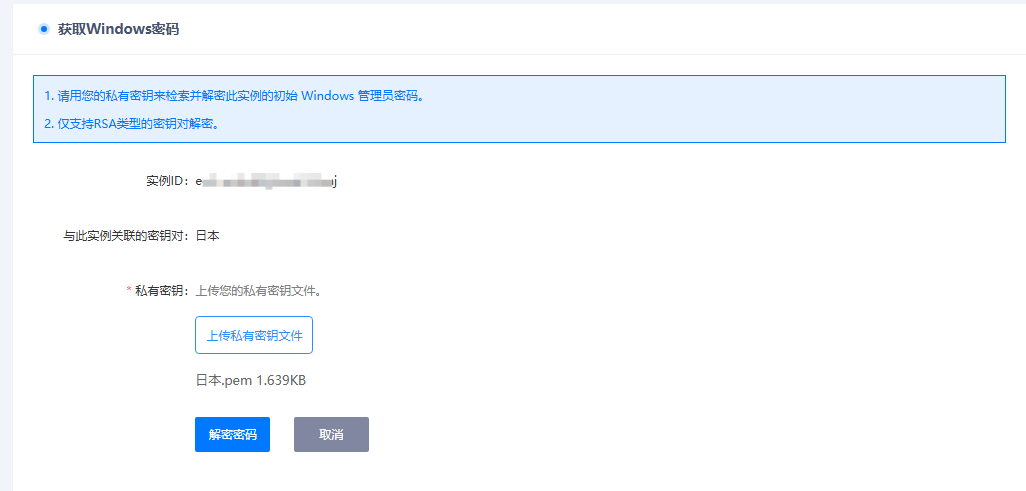
若您开通了Windows实例，您可通过本地RDP远程登录方式登录您的Amazon EC2。

* 操作步骤

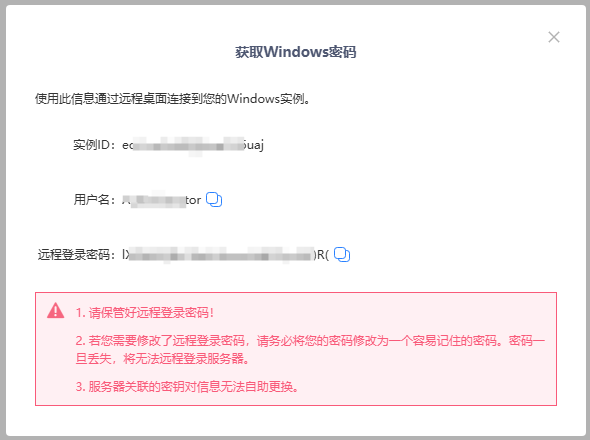
1. 登录快快官网控制台，在Amazon EC2实例列表找到需远程的实例。
2. 更多操作》获取Windows密码。



1. 将该实例对应的私钥文件上传后解密。



1. 请将解密的用户名和远程登录密码，通过Windows本地的远程窗口（RDP）进行实例的远程连接。



|  |
| --- |
| 1. 该密码为远程初始登录密码。请务必保管好！ 2. 若需求修改了初始远程登录密码，请将密码修改为一个您容易记住的密码，若该密码丢失，则无法远程登录服务器。 3. Amazon EC2的密钥对信息无法自助更换。 |

**Linux实例登录：**

若您开通了Linux实例，您可通过本地第三方远程工具导入密钥的方式登录您的Amazon EC2。

* 操作步骤（以第三方远程工具为例）

1. 点击"新建连接"：在FinalShell主界面,点击左上角新建连接按钮。
2. 配置基本信息:
3. 名称：自定义连接名称(如AWS-Linux)。
4. 主机：填入实例的公网IP地址。
5. 端口：默认22 (SSH端口)。
6. 用户名：通常为ec2-user (Amazon Linux)或ubuntu (Ubuntu系统)，具体取决于你使用的AMI。
7. 配置密钥认证:
8. 在"密码/密钥"区域，点击选择密钥。
9. 从已导入的密钥列表中，选择之前导入的密钥(如aws-key)。
10. 测试连接:点击测试连接，若提示"连接成功"，保存配置即可。

**安全组**

安全组是一种虚拟防火墙，能够控制实例的出入站流量。安全组的入方向规则控制实例的入站流量，出方向规则控制实例的出站流量。

购买Amazon EC2时，系统会默认关联到指定安全组，如您有特定的出入规则需要，可以前往控制台进行创建自定义安全组，进行关联。

合理使用安全组可以有效提高实例的安全性。

**安全组使用实践：**

* 规划：您可以为安全组设置名称、描述，便于进行分类运维。建议您合理设置这些信息，方便快速识别安全组的用途，在管理较多安全组时更加清晰。
* 以白名单的方式使用安全组：即默认拒绝所有访问，添加允许规则来放通指定的端口范围和授权对象。
* 添加安全组规则时遵循最大原则：例如，开放Linux实例的22端口用于远程登录时，建议仅允许特定的IP访问，而非所有IP（0.0.0.0/0）。
* 如果特定端口具有多个规则，Amazon EC2将应用最宽松的规则。例如，如果有一条规则允许从IP地址203.0.113.1访问TCP端口22（SSH），而另一条规则允许从任何地方访问TCP端口22，则所有人都可以访问TCP端口22。
* 您可以将多个安全组与一个实例关联。因此，一个实例可以有数百条适用的规则。访问该实例时，可能会导致问题。我们建议您尽可能让规则简洁。
* 不同类型应用的实例加入不同的安全组，分别维护安全组规则
* 例如，将允许公网访问的实例关联到同一个安全组，仅放通对外提供服务的端口，例如80、443等，默认拒绝其他所有访问。避免在允许公网访问的实例上提供其他服务，例如MySQL、Redis等，建议将内部服务部署在不允许公网访问的实例上，并关联其他的安全组。
* 避免直接修改线上环境使用的安全组：可以先克隆一个安全组在测试环境调试，确保修改后实例流量正常，再对线上环境的安全组规则进行修改。

**创建安全组**

安全组是一种虚拟防火墙，能够控制实例的出入站流量。每台实例必须至少加入一个安全组。

* 操作步骤

1. 登录快快官网控制台》Amazon EC2》安全组。
2. 单击【创建安全组】。

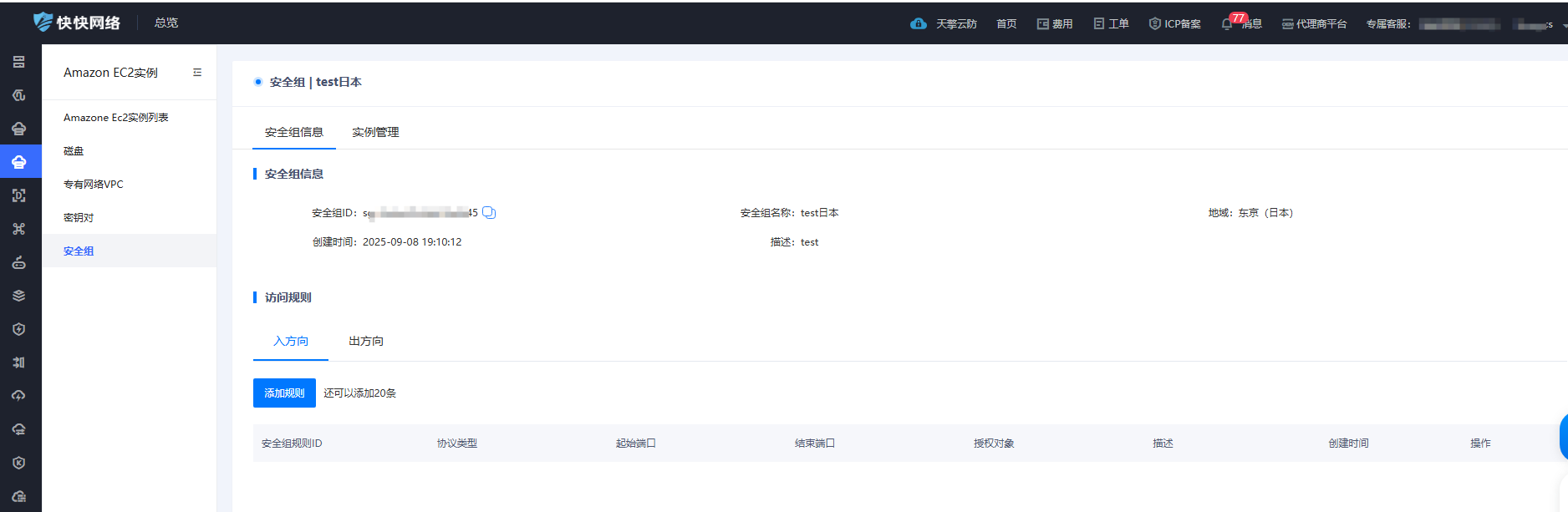


1. 地域：选择需要匹配实例的地域信息，不同地域之间安全组不互通。
2. 安全组名称：标识您此时安全组的记录，便于您识别安全组规则。
3. 安全组描述：描述该安全组的详细信息。
4. 专有网络VPC：请为该安全组选择对应的VPC网络。
5. 提交后，安全组此时无具体的入规则，需要通过管理规则进行编辑具体的规则后，才能正常远程该实例。

**管理规则**

* 操作步骤

1. 登录快快官网控制台》Amazon EC2》安全组。
2. 选择需要【管理规则】的安全组，单击【管理规则】。



1. 在管理安全组规则页面中，编辑对应的出入方向规则：
2. 协议：您可以根据实际使用的出入协议规则进行设置。
3. 起始端口：协议放行的开始端口。
4. 结束端口：协议放行的结束端口。
5. 授权对象：实际允许放行的源地址。



1. 提交后，对应安全组仅放行添加的规则，其他访问为禁止。

**VPC关联**

如果您的工作负载在具有共同网络安全要求的多个 VPC 中运行，则可以使用安全组 VPC 关联功能将安全组与同一区域中的多个 VPC 关联。这样，您就可以在一个位置管理和维护账户中多个 VPC 的安全组。

**安全组 VPC 关联功能的要求**

* 您必须拥有 VPC 或共享其中一个 VPC 子网才能将安全组与 VPC 关联。
* VPC 和安全组必须位于同一 地域域。
* 您不能将默认安全组与其他 VPC 关联，也不能将安全组与默认 VPC 关联。
* 安全组所有者和 VPC 所有者都可以查看安全组 VPC 关联。
* 安全组首次关联的VPC无法单独取消关联。

**取消关联VPC**

当您网络调整需要取消安全组内关联的VPC时，可通过【关联VPC】页面选择取消。

|  |
| --- |
| 安全组取消关联VPC时，已关联实例的VPC无法取消。 |

**删除安全组**

已关联实例的安全组无法删除。

* 操作步骤

1. 登录快快官网控制台》Amazon EC2》安全组。
2. 选择需要删除的安全组，单击【删除】
3. 若【删除】按钮灰选。请到实例列表》对应实例》更改安全组，删除关联的安全组信息。
4. 在删除安全组确认弹窗中，选择确认。
5. 提交后安全组将删除，且数据不可恢复。