
Amazon Elastic Compute Cloud

Linux 实例用户指南



Amazon Elastic Compute Cloud: Linux 实例用户指南

Copyright © 2017 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

| | |
|--|----|
| 什么是 Amazon EC2 ? | 1 |
| Amazon EC2 的功能 | 1 |
| 如何开始使用 Amazon EC2 | 1 |
| 相关服务 | 2 |
| 访问 Amazon EC2 | 3 |
| Amazon EC2 定价 | 3 |
| PCI DSS 合规性 | 4 |
| 实例和 AMI | 4 |
| 实例 | 4 |
| AMI | 5 |
| 地区和可用区域 | 7 |
| 区域和可用区域概念 | 7 |
| 可用区域 | 8 |
| 区域和终端节点 | 8 |
| 描述您的区域和可用区域 | 9 |
| 为资源指定区域 | 9 |
| 在可用区中启动实例 | 10 |
| 将实例迁移到其他可用区 | 10 |
| 根设备卷 | 11 |
| 根设备存储概念 | 11 |
| 根据根设备类型选择 AMI | 12 |
| 确定实例的根设备类型 | 13 |
| 将根设备卷更改为持久保留 | 13 |
| 设置 | 15 |
| 注册 AWS | 15 |
| 创建 IAM 用户 | 16 |
| 创建密钥对 | 17 |
| 创建 Virtual Private Cloud (VPC) | 18 |
| 创建安全组 | 18 |
| 入门 | 20 |
| 概述 | 20 |
| 先决条件 | 21 |
| 步骤 1 : 启动实例 | 21 |
| 步骤 2 : 连接到您的实例 | 22 |
| 步骤 3 : 清除您的实例 | 22 |
| 后续步骤 | 23 |
| 最佳实践 | 24 |
| 教程 | 26 |
| 教程 : 在 Amazon Linux 上安装 LAMP Web 服务器 | 26 |
| 故障排除 | 34 |
| 相关主题 | 35 |
| 教程 : 托管 WordPress 博客 | 35 |
| 先决条件 | 36 |
| 安装 WordPress | 36 |
| 后续步骤 | 42 |
| 帮助 ! 我的公有 DNS 名称发生更改导致我的博客瘫痪 | 42 |
| 教程 : 将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS | 43 |
| 先决条件 | 44 |
| 步骤 1 : 在服务器上启用 SSL/TLS | 44 |
| 步骤 2 : 获取 CA 签名的证书 | 45 |
| 步骤 3 : 测试和强化安全配置 | 48 |
| 故障排除 | 50 |
| 教程 : 提高应用程序的可用性 | 51 |
| 先决条件 | 51 |

| | |
|--|-----|
| 对应用程序进行扩展和负载均衡 | 51 |
| 测试负载均衡器 | 53 |
| 教程 : 远程管理您的实例 | 53 |
| 向您的用户账户授予对 Systems Manager 的访问权限 | 54 |
| 安装 SSM 代理 (Linux) | 54 |
| 使用 EC2 控制台发送命令 | 55 |
| 使用适用于 Windows PowerShell 的 AWS 工具 发送命令 | 56 |
| 使用 AWS CLI 发送命令 | 56 |
| 相关内容 | 57 |
| Amazon 系统映像 | 58 |
| 使用 AMI | 58 |
| 创建您自己的 AMI | 58 |
| 购买、共享和出售 AMI | 59 |
| 取消注册您的 AMI | 59 |
| Amazon Linux | 59 |
| AMI 类型 | 59 |
| 启动许可 | 59 |
| 根设备存储 | 60 |
| 虚拟化类型 | 62 |
| 查找 Linux AMI | 62 |
| 使用 Amazon EC2 控制台查找 Linux AMI | 63 |
| 使用 AWS CLI 查找 AMI | 63 |
| 共享 AMI | 64 |
| 查找共享 AMI | 64 |
| 将 AMI 设为公用 | 66 |
| 将 AMI 与特定 AWS 账户共享 | 67 |
| 使用书签 | 68 |
| 共享 Linux AMI 指导原则 | 68 |
| 付费 AMI | 72 |
| 出售 AMI | 73 |
| 查找付费 AMI | 73 |
| 购买付费 AMI | 73 |
| 获取实例的产品代码 | 74 |
| 使用付费支持 | 74 |
| 付费和支持 AMI 的账单 | 75 |
| 管理 AWS Marketplace 订阅 | 75 |
| 创建 Amazon EBS 支持的 Linux AMI | 75 |
| 创建 Amazon EBS 支持的 AMI 的概述 | 76 |
| 从实例创建 Linux AMI | 76 |
| 从快照创建 Linux AMI | 78 |
| 创建由实例存储支持的 Linux AMI | 78 |
| 由实例存储支持的 AMI 的创建过程概述 | 79 |
| 先决条件 | 79 |
| 设置 AMI 工具 | 80 |
| 通过实例存储支持的 实例创建 AMI | 104 |
| 转换为 Amazon EBS 支持的 AMI | 113 |
| 带加密快照的 AMI | 116 |
| 涉及加密的 EBS 快照的 AMI 情景 | 116 |
| 复制 AMI | 117 |
| 权限 | 118 |
| 跨区域 AMI 复制 | 118 |
| 跨账户 AMI 复制 | 119 |
| 加密和 AMI 复制 | 119 |
| 复制 AMI | 120 |
| 停止待处理的 AMI 复制操作 | 121 |
| 取消注册您的 AMI | 121 |
| 清除由 Amazon EBS 支持的 AMI | 122 |

| | |
|-------------------------------------|-----|
| 清除由实例存储支持的 AMI | 122 |
| Amazon Linux | 123 |
| 查找 Amazon Linux AMI | 123 |
| 启动并连接到 Amazon Linux 实例 | 123 |
| 识别 Amazon Linux AMI 映像 | 123 |
| 包含的 AWS 命令行工具 | 124 |
| cloud-init | 125 |
| 存储库配置 | 126 |
| 添加软件包 | 127 |
| 访问源软件包获取参考信息 | 127 |
| 开发应用程序 | 127 |
| 实例存储访问 | 128 |
| 产品生命周期 | 128 |
| 安全更新 | 128 |
| 支持 | 128 |
| 用户提供的内核 | 129 |
| HVM AMI (GRUB) | 129 |
| 半虚拟化 AMI (PV-GRUB) | 130 |
| 实例 | 135 |
| 实例类型 | 135 |
| 可用实例类型 | 136 |
| 硬件规格 | 137 |
| 虚拟化类型 | 137 |
| 联网和存储功能 | 137 |
| 实例限量 | 139 |
| T2 实例 | 139 |
| 计算优化型实例 | 141 |
| 内存优化型实例 | 144 |
| 存储优化型实例 | 146 |
| 加速计算实例 | 150 |
| T1 微型实例 | 154 |
| 调整实例大小 | 156 |
| 实例购买选项 | 160 |
| 实例生命周期 | 160 |
| 预留实例 | 161 |
| 计划实例 | 184 |
| 竞价型实例 | 187 |
| 专用主机 | 227 |
| 专用实例 | 237 |
| 实例生命周期 | 241 |
| 实例启动 | 241 |
| 停止和启动实例 (仅限 Amazon EBS 支持的实例) | 241 |
| 实例重启 | 242 |
| 实例停用 | 242 |
| 实例终止 | 242 |
| 重启、停止与终止之间的区别 | 242 |
| 启动 | 243 |
| 连接 | 252 |
| 停止和启动 | 263 |
| 重启 | 265 |
| 停用 | 266 |
| 终止 | 267 |
| 恢复 | 272 |
| 配置实例 | 272 |
| 常见配置方案 | 273 |
| 管理软件 | 273 |
| 管理用户 | 280 |

| | |
|----------------------------------|-----|
| 处理器状态控制 | 282 |
| 设置时间 | 286 |
| 更改主机名 | 289 |
| 设置动态 DNS | 291 |
| 启动时运行命令 | 292 |
| 实例元数据和用户数据 | 295 |
| 识别混合计算环境中的 EC2 实例 | 308 |
| 检查 Xen 域 UUID | 308 |
| 检查实例标识文档 | 309 |
| 监控 | 310 |
| 自动和手动监控 | 311 |
| 自动监控工具 | 311 |
| 手动监控工具 | 312 |
| 监控的最佳实践 | 313 |
| 监控实例状态 | 313 |
| 实例状态检查 | 313 |
| 计划的事件 | 317 |
| 使用 CloudWatch 监控您的实例 | 320 |
| 启用详细监控 | 321 |
| 列出可用指标 | 322 |
| 获取指标的统计数据 | 326 |
| 绘制指标图形 | 331 |
| 创建警报 | 331 |
| 创建停止、终止、重启或恢复实例的警报 | 332 |
| 使用 CloudWatch Events 实现自动化 | 339 |
| 监控内存和磁盘指标 | 339 |
| 支持的系统 | 339 |
| 程序包内容 | 340 |
| 先决条件 | 340 |
| 入门 | 341 |
| mon-put-instance-data.pl | 342 |
| mon-get-instance-stats.pl | 344 |
| 在控制台中查看自定义指标 | 345 |
| 故障排除 | 345 |
| 网络与安全性 | 346 |
| 密钥对 | 346 |
| 使用 Amazon EC2 创建密钥对 | 347 |
| 将您自己的公有密钥导入 Amazon EC2 | 348 |
| 在 Linux 上检索密钥对的公有密钥 | 349 |
| 在 Windows 上检索密钥对的公有密钥 | 350 |
| 验证您的密钥对指纹 | 350 |
| 删除您的密钥对 | 351 |
| 丢失私有密钥时连接到 Linux 实例 | 351 |
| 安全组 | 354 |
| EC2-Classic 安全组 | 354 |
| EC2-VPC 安全组 | 355 |
| 安全组规则 | 355 |
| 默认安全组 | 357 |
| 自定义安全组 | 357 |
| 使用安全组 | 357 |
| 安全组规则引用 | 361 |
| Controlling Access | 366 |
| 网络访问您的实例 | 366 |
| Amazon EC2 权限属性 | 366 |
| IAM 和 Amazon EC2 | 367 |
| IAM 策略 | 368 |
| IAM 角色 | 422 |

| | |
|--|-----|
| 网络访问 | 429 |
| Amazon VPC | 431 |
| 使用 VPC 的优势 | 432 |
| EC2-Classic 与 EC2-VPC 的区别 | 432 |
| 在 EC2-Classic 与 EC2-VPC 之间共享和访问资源 | 433 |
| 实例类型仅在 VPC 中可用 | 434 |
| Amazon VPC 文档 | 435 |
| 支持的平台 | 435 |
| ClassicLink | 436 |
| 从 EC2-Classic 迁移到 VPC | 445 |
| 实例 IP 寻址 | 453 |
| 私有 IPv4 地址和内部 DNS 主机名 | 453 |
| 公有 IPv4 地址和外部 DNS 主机名 | 454 |
| 弹性 IP 地址 (IPv4) | 455 |
| Amazon DNS 服务器 | 455 |
| IPv6 地址 | 455 |
| EC2-Classic 和 EC2-VPC 之间的 IP 地址区别 | 455 |
| 使用实例的 IP 地址 | 456 |
| 多个 IP 地址 | 460 |
| 弹性 IP 地址 | 467 |
| 弹性 IP 地址基础信息 | 467 |
| EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别 | 468 |
| 使用弹性 IP 地址 | 469 |
| 将反向 DNS 用于电子邮件应用程序 | 472 |
| 弹性 IP 地址限额 | 473 |
| 网络接口 | 473 |
| 每个实例类型的每个网络接口的 IP 地址 | 474 |
| 网络接口的使用场景 | 477 |
| 网络接口最佳配置实践 | 477 |
| 使用 ec2-net-utils 配置网络接口 | 478 |
| 使用网络接口 | 479 |
| 置放群组 | 487 |
| 置放群组的限制 | 487 |
| 将实例启动到置放群组中 | 488 |
| 删除置放群组 | 489 |
| 网络 MTU | 489 |
| 极大帧 (9001 MTU) | 490 |
| 路径 MTU 发现 | 490 |
| 查看两台主机之间的路径 MTU | 490 |
| 在您的 Amazon EC2 实例上检查并设置 MTU | 491 |
| 故障排除 | 492 |
| 增强型联网 | 492 |
| 增强联网类型 | 492 |
| 在实例上启用增强联网 | 492 |
| 启用增强联网 : Intel 82599 VF | 492 |
| 启用增强联网 : ENA | 501 |
| ENA 问题排查 | 509 |
| 存储 | 515 |
| Amazon EBS | 516 |
| Amazon EBS 的功能 | 517 |
| EBS 卷 | 517 |
| EBS 快照 | 559 |
| EBS 优化 | 564 |
| EBS 加密 | 568 |
| EBS 性能 | 571 |
| EBS CloudWatch Events | 586 |
| 实例存储 | 591 |

| | |
|-----------------------------------|-----|
| 实例存储生命周期 | 592 |
| 实例存储卷 | 592 |
| 添加实例存储卷 | 595 |
| SSD 实例存储卷 | 597 |
| 实例存储交换卷 | 599 |
| 优化磁盘性能 | 601 |
| Amazon EFS | 602 |
| 先决条件 | 602 |
| 步骤 1：创建 EFS 文件系统 | 603 |
| 步骤 2：挂载文件系统 | 603 |
| 步骤 3：测试文件系统 | 604 |
| 步骤 4：清除 | 605 |
| Amazon S3 | 605 |
| Amazon S3 和 Amazon EC2 | 605 |
| 实例卷限制 | 607 |
| 特定于 Linux 的卷限制 | 607 |
| 特定于 Windows 的卷限制 | 607 |
| 带宽与容量 | 608 |
| 设备命名 | 608 |
| 可用设备名称 | 608 |
| 设备名称注意事项 | 609 |
| 块储存设备映射 | 609 |
| 块储存设备映射的概念 | 609 |
| AMI 块储存设备映射 | 611 |
| 实例块储存设备映射 | 613 |
| 使用公用数据集 | 617 |
| 公用数据集概念 | 617 |
| 查找公用数据集 | 617 |
| 从快照创建公用数据集卷 | 618 |
| 连接和装载公用数据集卷 | 618 |
| 资源和标签 | 619 |
| 资源位置 | 619 |
| 资源 ID | 620 |
| 使用较长的 ID | 621 |
| 控制对较长 ID 设置的访问 | 623 |
| 列出并筛选您的资源 | 623 |
| 高级搜索 | 624 |
| 使用控制台列出资源 | 624 |
| 使用控制台筛选资源 | 625 |
| 使用 CLI 和 API 列出并筛选 | 625 |
| 标记您的成员资源 | 626 |
| 有关标签的基本知识 | 626 |
| 标记您的成员资源 | 626 |
| 标签限制 | 628 |
| 标记资源以便于计费 | 628 |
| 通过控制台使用标签 | 629 |
| 通过 CLI 或 API 使用标签 | 631 |
| 服务限制 | 633 |
| 查看当前限制 | 633 |
| 申请提高限制 | 633 |
| 使用率报告 | 633 |
| 可用报告 | 634 |
| 开始设置使用率报告 | 634 |
| 向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限 | 635 |
| 实例使用率 | 636 |
| 预留实例使用率 | 638 |
| 故障排除 | 642 |

| | |
|--|-----|
| 启动实例 | 642 |
| 了解实例终止的原因 | 643 |
| 连接到您的实例 | 643 |
| 连接到您的实例时出错：连接超时 | 644 |
| 错误：服务器无法识别用户密钥 | 645 |
| 错误：未找到主机密钥，权限被拒绝 (publickey)，或者 身份验证失败，权限被拒绝 | 646 |
| 错误：未保护的私钥文件 | 647 |
| 错误：服务器拒绝我们的密钥或 没有支持的身份验证方法 | 648 |
| 在 Safari 浏览器上使用 MindTerm 时的错误 | 648 |
| 使用 Mac OS X RDP 客户端时出错 | 648 |
| 无法对实例执行 Ping 操作 | 648 |
| 停止实例 | 649 |
| 终止实例 | 650 |
| 延迟的实例终止 | 650 |
| 已终止实例仍然显示 | 650 |
| 自动启动或终止实例 | 650 |
| 实例恢复故障 | 650 |
| 故障状态检查 | 650 |
| 初始步骤 | 651 |
| 检索系统日志 | 651 |
| 诊断基于 Linux 的实例的系统日志错误 | 652 |
| 内存不足：终止进程 | 653 |
| 错误：mmu_update 失败（内存管理更新失败） | 653 |
| I/O 错误（块储存设备故障） | 654 |
| IO 错误：既不是本地磁盘也不是远程磁盘（破损的分布式块储存设备） | 655 |
| request_module：runaway loop modprobe（在较旧的 Linux 版本上循环旧内核 modprobe） | 656 |
| “严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”（内核与 AMI 不匹配） | 656 |
| “FATAL: Could not load /lib/modules”或者“BusyBox”（内核模块缺失） | 657 |
| ERROR：无效内核（EC2 不兼容内核） | 658 |
| request_module：runaway loop modprobe（在较旧的 Linux 版本上循环旧内核 modprobe） | 659 |
| fsck：尝试打开时没有找到此文件或目录...（未找到文件系统） | 660 |
| 安装文件系统时出现一般性错误（安装失败） | 661 |
| VFS：无法在未知块上安装根 fs（根文件系统不匹配） | 663 |
| 错误：无法确定根设备的主/次编号...（根文件系统/设备不匹配） | 663 |
| XENBUS：设备没有驱动程序 | 664 |
| ... 没有检查时，已强制执行检查的工作日（文件系统检查要求） | 665 |
| fsck 卡在退出状态...（缺少设备） | 666 |
| GRUB 提示（grubdom>） | 666 |
| 提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。（硬编码的 MAC 地址）。 | 668 |
| 无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。（SELinux 配置错误） | 669 |
| XENBUS：连接设备时超时（Xenbus 超时） | 670 |
| 实例容量 | 670 |
| 错误：InsufficientInstanceCapacity | 670 |
| 错误：InstanceLimitExceeded | 671 |
| 获取控制台输出和重启实例 | 671 |
| 实例重启 | 671 |
| 实例控制台输出 | 671 |
| 捕获无法访问的实例的屏幕截图 | 672 |
| 主机发生故障时的实例恢复 | 672 |
| 正在从错误的卷启动我的实例 | 673 |
| 文档历史记录 | 675 |
| AWS 词汇表 | 687 |

什么是 Amazon EC2？

Amazon Elastic Compute Cloud (Amazon EC2) 在 Amazon Web Services (AWS) 云中提供可扩展的计算容量。使用 Amazon EC2 可避免前期的硬件投入，因此您能够快速开发和部署应用程序。通过使用 Amazon EC2，您可以根据自身需要启动任意数量的虚拟服务器、配置安全和网络以及管理存储。Amazon EC2 允许您根据需要进行缩放以应对需求变化或流行高峰，降低流量预测需求。

有关云计算的更多信息，请参阅[何为“云计算”？](#)

Amazon EC2 的功能

Amazon EC2 提供以下功能：

- 虚拟计算环境，也称为实例
- 实例的预配置模板，也称为 Amazon 系统映像 (AMI)，其中包含您的服务器需要的程序包（包括操作系统和其他软件）。
- 实例 CPU、内存、存储和网络容量的多种配置，也称为实例类型
- 使用密钥对的实例的安全登录信息 (AWS 存储公有密钥，您在安全位置存储私有密钥)
- 临时数据（停止或终止实例时会删除这些数据）的存储卷，也称为实例存储卷
- 使用 Amazon Elastic Block Store (Amazon EBS) 的数据的持久性存储卷，也称为 Amazon EBS 卷。
- 用于存储资源的多个物理位置，例如实例和 Amazon EBS 卷，也称为区域和可用区
- 防火墙，让您可以指定协议、端口，以及能够使用安全组到达您的实例的源 IP 范围
- 用于动态云计算的静态 IPv4 地址，称为弹性 IP 地址
- 元数据，也称为标签，您可以创建元数据并分配给您的 Amazon EC2 资源
- 您可以创建的虚拟网络，这些网络与其余 AWS 云在逻辑上隔离，并且您可以选择连接到您自己的网络，也称为 Virtual Private Cloud (VPC)

有关 Amazon EC2 功能的更多信息，请参阅[Amazon EC2 产品页](#)。

有关在 AWS 上运行网站的更多信息，请参阅[网站和网站托管](#)。

如何开始使用 Amazon EC2

您需要做的第一件事是为使用 Amazon EC2 进行设置。设置完毕后，您便基本上完成了 Amazon EC2 入门教程。如果需要关于 Amazon EC2 功能的更多信息，可阅读技术文档。

设置和运行

- [Amazon EC2 的设置 \(p. 15\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 20\)](#)

基础知识

- [实例和 AMI \(p. 4\)](#)
- [地区和可用区域 \(p. 7\)](#)
- [实例类型 \(p. 135\)](#)
- [标签 \(p. 626\)](#)

网络和安全性

- [Amazon EC2 密钥对 \(p. 346\)](#)
- [安全组 \(p. 354\)](#)
- [弹性 IP 地址 \(p. 467\)](#)
- [Amazon EC2 和 Amazon VPC \(p. 431\)](#)

存储

- [Amazon EBS \(p. 516\)](#)
- [实例存储 \(p. 591\)](#)

使用 Linux 实例

- [远程管理 \(Run Command\)](#)
- [教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)
- [教程：将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS \(p. 43\)](#)
- [AWS 入门：托管适用于 Linux 的 Web 应用程序](#)

对于 AWS 是否适合您，如果有任何疑问，请联系 [AWS 销售](#)。如果遇到有关 Amazon EC2 的技术问题，请使用 [Amazon EC2 forum](#)。

相关服务

您可以直接使用 Amazon EC2 预配置 Amazon EC2 资源，例如示例和卷。您也可以使用其他 AWS 服务预配置 Amazon EC2 资源。有关更多信息，请参阅以下文档：

- [Auto Scaling 用户指南](#)
- [AWS CloudFormation 用户指南](#)
- [AWS Elastic Beanstalk 开发人员指南](#)
- [AWS OpsWorks 用户指南](#)

要跨多个实例自动分配应用程序的传入流量，可使用 Elastic Load Balancing。有关更多信息，请参阅 [Elastic Load Balancing 用户指南](#)。

要监控您的实例和 Amazon EBS 卷的基本统计数据，可使用 Amazon CloudWatch。有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。

要自动执行操作，例如在新的 Amazon EC2 实例启动时激活 Lambda 函数或在另一个 AWS 服务中发生事件时调用 SSM Run Command，请使用 Amazon CloudWatch Events。有关更多信息，请参阅 [Amazon CloudWatch Events 用户指南](#)。

要监控对您的账户的 Amazon EC2 API 的调用（包括由 AWS 管理控制台、命令行工具和其他服务进行的调用），请使用 AWS CloudTrail。有关更多信息，请参阅 [AWS CloudTrail User Guide](#)。

要获取云中托管的关系数据库，可使用 Amazon Relational Database Service (Amazon RDS) 启动数据库实例。尽管可以在 EC2 实例上设置数据库，但是 Amazon RDS 为您处理数据库管理任务提供了优势，例如修补软件、备份以及存储备份。有关更多信息，请参阅 [Amazon Relational Database Service 开发人员指南](#)。

要从您的本地环境将虚拟机 (VM) 映像导入到 AWS 并将其转换为立即可用的 AMI 或实例，请使用 VM Import/Export。有关更多信息，请参阅 [VM Import/Export 用户指南](#)。

访问 Amazon EC2

Amazon EC2 提供基于 Web 的用户界面，即 Amazon EC2 控制台。如果您已注册 AWS 账户，可以通过登录 AWS 管理控制台并从控制台主页选择 EC2 来访问 Amazon EC2 控制台。

如果倾向于使用命令行界面，您可使用以下选项：

AWS 命令行界面 (CLI)

提供大量 AWS 产品的相关命令，同时被 Windows、Mac 和 Linux 支持。要了解其用法，请参阅 [AWS Command Line Interface 用户指南](#)。有关 Amazon EC2 的命令的更多信息，请参阅 AWS Command Line Interface Reference 中的 `ec2`。

适用于 Windows PowerShell 的 AWS 工具

为在 PowerShell 环境中编写脚本的用户提供大量 AWS 产品的相关命令。要开始使用，请参阅 [适用于 Windows PowerShell 的 AWS 工具 用户指南](#)。有关 Amazon EC2 的 Cmdlet 的更多信息，请参阅 [适用于 Windows PowerShell 的 AWS 工具 Reference](#)。

Amazon EC2 提供查询 API。这些请求属于 HTTP 或 HTTPS 请求，需要使用 HTTP 动词 GET 或 POST 以及一个名为 Action 的查询参数。有关 Amazon EC2 的 API 操作的更多信息，请参阅 Amazon EC2 API Reference 中的 [Actions](#)。

如果您倾向于使用特定语言的 API 而非通过 HTTP 或 HTTPS 提交请求来构建应用程序，AWS 为软件开发人员提供了库文件、示例代码、教程和其他资源。这些库文件提供可自动执行任务的基本功能，例如以加密方式对请求签名、重试请求和处理错误响应，因此您可以更轻松地上手。有关更多信息，请参阅 [AWS SDKs and Tools](#)。

Amazon EC2 定价

注册 AWS 后，您可以通过 [AWS 免费套餐](#)开始免费使用 Amazon EC2。

Amazon EC2 为实例提供以下购买选项：

按需实例

您只需要按小时支付使用实例的费用，无需长期购买或预付款。

预留实例

以极低的费率支付一次性前期费用，可预留实例一年或三年，并大幅降低这些实例的每小时费率。

竞价型实例

指定您愿意为运行特定实例类型支付的最高小时价格。现货价格随供需浮动，但您支付的价格不会超过您所指定的最高价。当现货价格高于您的最高价格时，Amazon EC2 会关闭您的竞价型实例。

有关 Amazon EC2 收费和具体价格的完整列表，请参阅 [Amazon EC2 定价](#)。

要计算示例设置环境的成本，请参阅 [AWS 成本中心](#)。

要查看您的账单，请转至 [AWS 账户活动页面](#)。您的账单中包含了提供您的账单详情的使用情况报告的链接。要了解有关 AWS 账户账单的更多信息，请参阅 [AWS 账户账单](#)。

如果您有关于 AWS 账单、账户和事件的问题，请[联系 AWS Support](#)。

Trusted Advisor 可帮助您优化成本、安全性和您的 AWS 环境性能，有关其概述，请参阅 [AWS Trusted Advisor](#)。

PCI DSS 合规性

Amazon EC2 支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。有关 PCI DSS 的更多信息，包括如何请求 AWS PCI Compliance Package 的副本，请参阅 [PCI DSS 第 1 级](#)。

实例和 AMI

Amazon 系统映像 (AMI) 是一种包含软件配置 (例如，操作系统、应用程序服务器和应用程序) 的模板。通过 AMI，您可以启动实例，实例是作为云中虚拟服务器运行的 AMI 的副本。您可以启动多个 AMI 实例，如下图所示。

您的实例会保持运行，直到您停止或终止运行，或实例失败。如果实例失败了，您可以从 AMI 启动一个新实例。

实例

您可以从一个单一的 AMI 启动不同类型的实例。实例类型从本质上决定了用于您的实例的主机硬件。每一个实例类型提供不同的计算和存储能力。选择一种基于您打算在实例上运行的应用程序或软件所需的存储容量和计算能力的实例类型。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

启动一个实例后，该实例看上去像一个传统主机，您可以像与任何计算机交互一样与其进行交互。您对实例有完全控制权；您可以使用 sudo 运行需要根特权的命令。

您的 AWS 账户对于保持运行状态的实例数量有限制。有关此限制的更多信息，以及如何请求调高限制，请参阅“[Amazon EC2 一般常见问题](#)”中的 [我能在 Amazon EC2 中运行多少个实例](#)。

实例的存储

实例的根设备包含用于启动实例的映像。有关更多信息，请参阅 [Amazon EC2 根设备卷 \(p. 11\)](#)。

实例可能包括本地存储卷 (称为实例存储卷)，可以在启动时使用块储存设备映射配置这些卷。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。这些卷已添加到实例并进行映射之后，便可供您进行装载和使用。如果实例失败，或是实例停止或终止，则这些卷上的数据会丢失；因此，这些卷最好用于临时数据。对于

重要数据，应在多个实例间使用复制策略以保证数据安全，或将持久性数据存储在 Amazon S3 或 Amazon EBS 卷中。有关更多信息，请参阅 [存储 \(p. 515\)](#)。

安全最佳实践

- 使用 AWS Identity and Access Management (IAM) 控制对 AWS 资源 (包括您的实例) 的访问。您可以在 AWS 账户下创建 IAM 用户和组，向每个用户和组分配安全证书并控制他们对 AWS 中资源和服务的访问权限。有关更多信息，请参阅 [控制对 Amazon EC2 资源的访问 \(p. 366\)](#)。
- 通过仅允许受信任主机或网络访问实例的端口来限制访问。例如，您可以通过限制端口 22 的入站流量来限制 SSH 访问。有关更多信息，请参阅 [Linux 实例的 Amazon EC2 安全组 \(p. 354\)](#)。
- 定期审查安全组中的规则并确保应用最小权限原则 (即仅开启您需要的权限)。您还可以创建不同的安全组来处理具有不同安全要求的实例。考虑创建一个可允许外部登录的堡垒安全组，同时在不允许外部登录的组内保留实例提醒程序。
- 对于从 AMI 启用的实例，禁用基于密码的登录。由于密码可以被查到或破解，因此存在安全风险。有关更多信息，请参阅 [对根禁用基于密码的远程登录 \(p. 69\)](#)。有关安全共享 AMI 的更多信息，请参阅 [共享 AMI \(p. 64\)](#)。

停止、启动和终止实例

停止实例

实例停止后，该实例将执行正常关闭操作，然后过渡到 `stopped` 状态。其所有 Amazon EBS 卷都将保持附加状态，并且您可以在稍后重新启动实例。

当实例处于停止状态时，您不必支付额外的实例小时费用。而每次从停止状态过渡到运行状态时，都需要支付一整个实例小时费用，即使是在一小时内进行多次操作也是如此。当实例停止时，如果实例类型发生变化，则在实例启动后，您需要就新实例类型支付费用。您实例的所有相关 Amazon EBS 用量 (包括根设备用量) 都按照一般 Amazon EBS 价格计费。

当实例处于停止状态时，您可以附加或分离 Amazon EBS 卷。您还可以从实例创建 AMI，以及更改内核、RAM 磁盘和实例类型。

终止实例

当终止实例后，实例将执行正常关闭操作，然后将删除附加的 Amazon EBS 卷，除非将该卷的 `deleteOnTermination` 属性设置为 `false`。实例本身也将被删除，并且您不能在稍后重新启动该实例。

要防止意外终止，您可以禁用实例终止。如果禁用，请确保将实例的 `disableApiTermination` 属性设置为 `true`。若要控制实例关闭时的行为 (如在 Linux 中为 `shutdown -h`，在 Windows 中为 `shutdown`)，则可根据需要将 `instanceInitiatedShutdownBehavior` 实例属性设为 `stop` 或 `terminate`。根设备的 Amazon EBS 卷默认为 `stop` 的实例和带有实例存储根设备的实例，总会因实例关闭而终止。

有关更多信息，请参阅 [实例生命周期 \(p. 241\)](#)。

AMI

Amazon Web Services (AWS) 发布了许多包含常见软件配置的Amazon 系统映像 (AMI) 供公众使用。此外，AWS 开发人员社区的会员也发布了他们的定制 AMI。您也可以创建一个或多个定制 AMI；这样能让您快速轻松地启动能满足您一切需求的新实例。例如，如果您的应用程序是网站或 Web 服务，则您的 AMI 可能包含 Web 服务器、相关静态内容和动态页面代码。因此，您从这个 AMI 启动实例之后，您的 Web 服务器将启动，并且您的应用程序已准备好接受请求。

所有 AMI 都被分类为由 Amazon EBS 支持或由实例存储支持，前者意味着从 AMI 启动的实例的根设备是 Amazon EBS 卷，后者意味着从 AMI 启动的实例的根设备是依据 Amazon S3 中存储的模板创建的实例存储卷。

对 AMI 的描述显示了根设备类型 (ebs 或 instance store)。这很重要，因为您使用每种 AMI 可进行的操作有很大区别。有关这些区别的更多信息，请参阅 [根设备存储 \(p. 60\)](#)。

地区和可用区域

Amazon EC2 托管在全球多个位置。这些位置由区域和可用区构成。每个区域 都是一个独立的地理区域。每个区域都有多个相互隔离的位置，称为可用区。Amazon EC2 让您可以在多个位置放置资源（如实例）和数据。除非您特意这样做，否则资源不会被跨区域复制。

Amazon 运行着具有高可用性的先进数据中心。数据中心有时会发生影响托管于同一位置的所有实例的可用性的故障，虽然这种故障极少发生。如果您将所有实例都托管在受此类故障影响的同一个位置，则您的所有实例都将不可用。

内容

- [区域和可用区域概念 \(p. 7\)](#)
- [可用区域 \(p. 8\)](#)
- [区域和终端节点 \(p. 8\)](#)
- [描述您的区域和可用区域 \(p. 9\)](#)
- [为资源指定区域 \(p. 9\)](#)
- [在可用区中启动实例 \(p. 10\)](#)
- [将实例迁移到其他可用区 \(p. 10\)](#)

区域和可用区域概念

每一个区域都是完全独立的。每个可用区都是独立的，但区域内的可用区通过低延迟链接相连。下图阐明了区域和可用区之间的关系。

Amazon EC2 资源要么具有全球性，要么与区域或可用区相关联。有关更多信息，请参阅 [资源位置 \(p. 619\)](#)。

区域

每个 Amazon EC2 区域都被设计为与其他 Amazon EC2 区域完全隔离。这可实现最大程度的容错能力和稳定性。

当您查看您的资源时，您只会看到与您指定的区域相关联的资源。这是因为区域间彼此隔离，而且我们不会自动跨区域复制资源。

当您启动实例时，必须选择位于同一地区的 AMI。如果 AMI 在其他区域，您可将该 AMI 复制到您使用的区域。有关更多信息，请参阅 [复制 AMI \(p. 117\)](#)。

区域之间的所有通信都是通过公共 Internet 进行的。因此，您应使用合适的加密方法来保护您的数据。请注意，在区域之间传输数据需要收费。有关更多信息，请参阅 [Amazon EC2 定价 - 数据传输](#)。

可用区

当您启动实例时，您可以自己选择一个可用区或让我们为您选择。如果您的实例分布在多个可用区域且其中的某个实例发生故障，则您可对您的应用程序进行相应设计，以使另一可用区域中的实例可代为处理相关请求。

您也可使用弹性 IP 地址来掩蔽某个可用区中的实例所发生的故障，方法是快速将该地址重新映射到另一可用区中的实例。有关更多信息，请参阅 [弹性 IP 地址 \(p. 467\)](#)。

可用区由区域代码后跟一个字母标识符表示；例如，us-east-1a。为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的标识符。例如，您的可用区 us-east-1a 与其他账户的可用区 us-east-1a 所表示的可能不是同一个位置。您无法在不同账户之间协调可用区。

随着可用区中内容的增加，我们对其进行扩展的能力会逐渐受限。如果发生此情况，我们可能会阻止您在扩展能力受限的可用区内启动实例，除非您在此可用区中已拥有实例。最终，我们还可能将扩展能力受限的可用区从新客户的可用区列表中删除。因此，您的不同账户在一个区域中可用的可用区数量可能不同。

您可以列出您的账户可用的可用区。有关更多信息，请参阅 [描述您的区域和可用区域 \(p. 9\)](#)。

可用区域

您的账户会确定适用于您的地区。例如：

- AWS 账户提供多个区域，因此您可在满足您要求的位置启动Amazon EC2实例。例如，您可能希望在欧洲区域启动实例以更多符合欧洲客户的要求或满足法律要求。
- 您只能通过AWS GovCloud（美国）账户访问AWS GovCloud（美国）区域。有关更多信息，请参阅[AWS GovCloud（美国）区域](#)。
- 您只能通过 Amazon AWS（中国）账户访问中国（北京）区域。

下表列出的是 AWS 账户提供的地区。您不能通过 AWS 账户描述或访问其他区域，例如AWS GovCloud（美国）或中国（北京）。

| 代码 | 名称 |
|----------------|---------------|
| us-east-1 | 美国东部（弗吉尼亚北部） |
| us-east-2 | 美国东部（俄亥俄州） |
| us-west-1 | 美国西部（加利福尼亚北部） |
| us-west-2 | 美国西部（俄勒冈） |
| ca-central-1 | 加拿大（中部） |
| eu-west-1 | 欧洲（爱尔兰） |
| eu-central-1 | 欧洲（法兰克福） |
| eu-west-2 | 欧洲（伦敦） |
| ap-northeast-1 | 亚太区域（东京） |
| ap-northeast-2 | 亚太区域（首尔） |
| ap-southeast-1 | 亚太区域（新加坡） |
| ap-southeast-2 | 亚太区域（悉尼） |
| ap-south-1 | 亚太地区（孟买） |
| sa-east-1 | 南美洲（圣保罗） |

有关更多信息，请参阅 [AWS 全球基础设施](#)。

每个区域的可用区的数量和映射可能因 AWS 账户不同而异。要获取可用于您的账户的可用区列表，您可以使用 Amazon EC2 控制台或命令行界面。有关更多信息，请参阅 [描述您的区域和可用区域 \(p. 9\)](#)。

区域和终端节点

当您通过命令行界面或 API 操作使用实例时，您必须指定其区域终端节点。有关 Amazon EC2 区域和终端节点的更多信息，请参阅 Amazon Web Services 一般参考 中的[区域和终端节点](#)。

若要了解有关AWS GovCloud (美国) 内的终端节点和协议的更多信息 , 请参阅 AWS GovCloud (US) User Guide 内的 [AWS GovCloud \(美国 \) 终端节点](#)。

描述您的区域和可用区域

您可使用 Amazon EC2 控制台或命令行界面来确定您的账户可用哪些区域和可用区。有关这些命令行界面的更多信息 , 请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

使用控制台查找您的区域和可用区

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中 , 查看区域选择器中的选项。
3. 在服务运行状况、可用区状态下的控制面板上查看可用区。

使用命令行查找您的区域和可用区

1. [AWS CLI] 使用如下 `describe-regions` 命令描述您账户的区域。

```
aws ec2 describe-regions
```

2. [AWS CLI] 使用如下 `describe-availability-zones` 命令描述指定区域内的可用区。

```
aws ec2 describe-availability-zones --region region-name
```

3. [适用于 Windows PowerShell 的 AWS 工具] 使用如下 `Get-EC2Region` 命令描述您账户的区域。

```
Get-EC2Region
```

4. [适用于 Windows PowerShell 的 AWS 工具] 使用如下 `Get-EC2AvailabilityZone` 命令描述指定区域内的可用区。

```
Get-EC2AvailabilityZone -Region region-name
```

为资源指定区域

每次创建 Amazon EC2 资源时 , 您都可为该资源指定区域。您可以使用 AWS 管理控制台或命令行为资源指定区域。

Note

一些 AWS 资源可能不是在所有区域和可用区都可用。在具体的可用区内启动实例前 , 请确保您可以在所需的区域或可用区内能够创建您需要的资源。

使用控制台为资源指定区域

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 使用导航栏中的区域选择器。

使用命令行指定默认区域

可以将环境变量的值设置为所需的区域终端节点 (例如 , `https://ec2.us-west-1.amazonaws.com`) :

- AWS_DEFAULT_REGION (AWS CLI)
- Set-AWSDefaultRegion (适用于 Windows PowerShell 的 AWS 工具)

或者，您可针对各个单独的命令使用 --region (AWS CLI) 或 -Region (适用于 Windows PowerShell 的 AWS 工具) 命令行选项。例如：--region us-west-1。

有关 Amazon EC2 终端节点的更多信息，请参阅 [Amazon Elastic Compute Cloud 终端节点](#)。

在可用区中启动实例

当您启动实例时，请选择能让您的实例更接近特定客户的区域，或选择能够满足法律或您的其他要求的区域。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。

当您启动实例时，可以选择指定所用区域中的可用区。如果您未指定可用区，我们将为您选择一个。启动初始实例时，我们建议您采用默认可用区，因为这有助于我们根据系统运行状况和可用容量为您选择最佳可用区。如果您要启动其他实例，则除非您的新实例必须接近正在运行的实例或必须与正在运行的实例相隔离，否则请不要为新实例指定可用区。

使用控制台为您的实例指定可用区

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 按照向导中的指示操作。在 Configure Instance Details (配置实例详细信息) 页面中，执行以下操作：
 - [EC2-Classic] 从列表中的可用区选项中选择一项，或选择 No Preference (无首选项)，让我们为您选择最佳可用区。
 - [EC2-VPC] 从列表中的子网选项中选择一项，或选择 No Preference (default subnet in any Availability Zone) (无首选项(任何可用区的默认子网))，让我们为您选择最佳可用区。

使用 AWS CLI 为您的实例指定可用区

您可以将 `run-instances` 命令与下面的一个选项结合使用：

- [EC2-Classic] `--placement`
- [EC2-VPC] `--subnet-id`

使用 适用于 Windows PowerShell 的 AWS 工具 为您的实例指定可用区

您可以将 `New-EC2Instance` 命令与下面的一个选项结合使用：

- [EC2-Classic] `-AvailabilityZone`
- [EC2-VPC] `-SubnetId`

将实例迁移到其他可用区

如果需要，您可以将实例迁移从一个可用区迁移到另一个可用区。例如，如果您尝试修改实例的类型，且我们无法在当前可用区中启动新实例类型的实例，则您可以将该实例迁移到我们可以启动该实例类型的实例的可用区中。

如以下步骤所示，迁移过程包括从原始实例创建 AMI、在新可用区中启动实例以及更新新实例的配置。

将实例迁移到其他可用区

1. 从该实例创建 AMI。迁移过程取决于操作系统和实例的根设备卷的类型。有关更多信息，请参阅对应于您的操作系统和根设备卷的文档：
 - [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)
 - [创建由实例存储支持的 Linux AMI \(p. 78\)](#)
 - [创建 Amazon EBS 支持的 Windows AMI](#)
 - [创建实例存储支持的 Windows AMI](#)
2. [EC2-VPC] 如果需要保留实例的私有 IPv4 地址，必须删除当前可用区中的子网，然后在新可用区中用与原始子网相同的 IPv4 地址范围创建子网。请注意，在删除子网前，您必须终止该子网中的所有实例。因此，您应从子网中的所有实例创建 AMI，这样您就可以将当前子网的所有实例迁移到新子网。
3. 指定新的可用区或子网，从您刚创建的 AMI 启动一个实例。您可以使用与初始实例相同的实例类型，也可以选择新实例类型。有关更多信息，请参阅 [在可用区中启动实例 \(p. 10\)](#)。
4. 如果原始实例有关联的弹性 IP 地址，则请将其与新实例相关联。有关更多信息，请参阅 [取消关联弹性 IP 地址，并将它与其他实例重新关联 \(p. 470\)](#)。
5. 如果原始实例是预留实例，请更改预留的可用区。(如果您还更改了实例类型，则可以更改预留的实例类型。)有关更多信息，请参阅 [提交修改请求 \(p. 180\)](#)。
6. (可选) 终止原始实例。有关更多信息，请参阅 [终止实例 \(p. 268\)](#)。

Amazon EC2 根设备卷

当您启动一个实例时，根设备卷 包含用于启动该实例的映像。当我们介绍 Amazon EC2 时，所有 AMI 都由 Amazon EC2 实例存储提供支持，也就是说从该 AMI 启动的实例的根设备是从存储在 Amazon S3 中的模板创建的实例存储卷。介绍完 Amazon EBS 之后，我们将介绍由 Amazon EBS 提供支持的 AMI。这意味着从 AMI 启动的实例的根设备是一个从 Amazon EBS 快照创建的 Amazon EBS 卷。

您可以在 Amazon EC2 实例存储支持的 AMI 和 Amazon EBS 支持的 AMI 之间进行选择。我们建议您使用由 Amazon EBS 提供支持的实例，因为它们启动速度更快，而且采用了持久性存储。

有关用于您的根卷的设备名称Amazon EC2的更多信息，请参阅[Linux 实例上的设备命名 \(p. 608\)](#)。

主题

- [根设备存储概念 \(p. 11\)](#)
- [根据根设备类型选择 AMI \(p. 12\)](#)
- [确定实例的根设备类型 \(p. 13\)](#)
- [将根设备卷更改为持久保留 \(p. 13\)](#)

根设备存储概念

您可以从实例存储支持 AMI 或Amazon EBS支持 AMI 启动实例。AMI 的说明中包括 AMI 的类型；您会看到根设备在一些地方被称为 ebs(表示由 Amazon EBS 提供支持) 或 instance store (表示由实例存储提供支持)。这很重要，因为您可以使用每种 AMI 进行哪些操作有很大区别。有关这些区别的更多信息，请参阅[根设备存储 \(p. 60\)](#)。

实例存储支持的实例

使用实例存储作为根设备的实例自带可用的一个或多个实例存储卷，其中一个卷充当根设备卷。当一个实例被启动时，用于启动该实例的映像被复制到根卷。请注意，您可以根据实例类型选择使用其他实例存储卷。

只要实例正在运行，实例存储卷上的所有数据便会存在，但是在实例终止时 (实例存储支持的实例不支持 Stop (停止) 操作) 或是实例失败时 (例如底层硬盘有问题时)，会删除这些数据。

由 Amazon 实例存储支持的实例失败或终止后，该实例不能被恢复。如果您打算使用由 Amazon EC2 实例存储支持的实例，我们强烈建议您将数据跨多个可用区分配到实例存储中。您还应该定期将您的实例存储卷上的关键数据备份至持久性存储。

有关更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#)。

由 Amazon EBS 提供支持的实例

使用 Amazon EBS 作为根设备的实例自动附加 Amazon EBS 卷。当您启动由 Amazon EBS 提供支持的实例时，系统会为您使用的 AMI 所参考的每一个 Amazon EBS 快照创建 Amazon EBS 卷。您可以根据实例类型选择使用其他 Amazon EBS 卷或实例存储卷。

由 Amazon EBS 提供支持的实例可以停止然后再重新启动，所连接的卷中存储的数据不会受影响。当由 Amazon EBS 提供支持的实例处于停止状态时，您可以完成各种与该实例和卷有关的任务。例如，您可以修改实例的属性，您可以更改实例的大小或更新实例使用的内核，或者您可以将您的根卷连接到另一个的运行的实例，以进行调试或达到任何其他目的。

如果由 Amazon EBS 提供支持的实例失败，您可以通过以下方法之一恢复您的会话：

- 停止，然后再次启动 (先尝试此方法)。
- 自动为相关卷拍摄快照并创建新的 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。
- 通过以下步骤将卷连接到一个新实例：
 1. 创建根卷的快照。
 2. 使用快照注册一个新的 AMI。
 3. 从新的 AMI 启动一个新实例。
 4. 从旧的实例中分离其余 Amazon EBS 卷。
 5. 将 Amazon EBS 卷重新连接到新实例。

有关更多信息，请参阅 [Amazon EBS 卷 \(p. 517\)](#)。

根据根设备类型选择 AMI

您在启动实例时指定的 AMI 决定着实例的根设备卷类型。

使用控制台选择 Amazon EBS 支持的 AMI

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从筛选条件列表中，选择映像类型 (例如 Public images (公有映像))。在 搜索栏中选择 Platform 选择操作系统 (例如 Amazon Linux)，单击 Root Device Type 选择 EBS images。
4. (可选) 为了获取其他信息以帮助您进行选择，请选择 Show/Hide Columns (显示/隐藏列) 图标，更新要显示的列，然后选择 Close (关闭)。
5. 选择一个 AMI 并写下其 AMI ID。

使用控制台选择实例存储支持的 AMI

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从筛选条件列表中，选择映像类型 (例如 Public images (公有映像))。在 搜索栏中选择 Platform 选择操作系统 (例如 Amazon Linux)，单击 Root Device Type 选择 Instance store。
4. (可选) 为了获取其他信息以帮助您进行选择，请选择 Show/Hide Columns (显示/隐藏列) 图标，更新要显示的列，然后选择 Close (关闭)。

5. 选择一个 AMI 并写下其 AMI ID。

使用命令行验证 AMI 的根设备卷的类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

确定实例的根设备类型

使用控制台确定实例的根设备类型

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 检查说明选项卡上根设备类型的值，如下所示：
 - 如果值为 ebs，那么这是一个由 Amazon EBS 支持的实例。
 - 如果值为 instance store，则表示这是由实例存储支持的实例。

使用命令行确定实例的根设备类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

将根设备卷更改为持久保留

默认情况下，当实例终止时，由 Amazon EBS 提供支持的 AMI 的根设备卷会被删除。要更改默认操作，请使用块储存设备映射将 DeleteOnTermination 属性设置为 false。

使用控制台将根卷更改为持久保留

当您启动实例时，可以使用控制台更改 DeleteOnTermination 属性。要对正在运行的实例更改此属性，您必须使用命令行。

使用控制台在启动时将实例的根设备卷更改为持久保留

1. 打开 Amazon EC2 控制台。
2. 从 Amazon EC2 控制台控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面上，取消选中根卷的 Delete On Termination (终止时删除)。
6. 完成其余向页面上的操作，然后选择 Launch。

您可以通过实例的详细信息窗格查看根设备卷的详细信息以验证设置。在 Block devices (块储存设备) 旁，选择根设备卷的条目。默认情况下，Delete on termination (终止时删除) 为 true。如果您更改默认行为，Delete on termination (终止时删除) 将为 false。

使用 AWS CLI 将实例的根卷更改为持久保留

使用 AWS CLI，您可以在启动实例或者在实例正在运行时更改 `DeleteOnTermination` 属性。

Example 在启动时

使用 `run-instances` 命令并在其中包括将根卷的 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射，来保留根卷。

```
aws ec2 run-instances --block-device-mappings file://mapping.json other parameters...
```

在 `mapping.json` 中指定以下内容。

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

您可以通过使用 `describe-instances` 命令，并如此处所示，在命令输出中查找设备的 `BlockDeviceMappings` 条目，确认 `DeleteOnTermination` 为 `false`。

```
...  
"BlockDeviceMappings": [  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "Status": "attached",  
      "DeleteOnTermination": false,  
      "VolumeId": "vol-1234567890abcdef0",  
      "AttachTime": "2013-07-19T02:42:39.000Z"  
    }  
  }  
...  
]
```

Example 当实例正在运行时

使用 `modify-instance-attribute` 命令，并在命令中包括将根卷的 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射，来保留根卷。

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings  
file://mapping.json
```

在 `mapping.json` 中指定以下内容。

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

Amazon EC2 的设置

如果您已注册了 Amazon Web Services (AWS) , 则可以立即开始使用 Amazon EC2。您可以打开 Amazon EC2 控制台 , 单击 Launch Instance (启动实例) , 然后按照启动向导的步骤启动第一个实例。

如果您尚未注册 AWS , 或如果需要帮助启动第一个实例 , 请完成以下任务以便为使用 Amazon EC2 进行设置 :

1. [注册 AWS \(p. 15\)](#)
2. [创建 IAM 用户 \(p. 16\)](#)
3. [创建密钥对 \(p. 17\)](#)
4. [创建 Virtual Private Cloud \(VPC\) \(p. 18\)](#)
5. [创建安全组 \(p. 18\)](#)

注册 AWS

当您注册 Amazon Web Services (AWS) 时 , 您的 AWS 账户会自动注册 AWS 中的所有服务 , 包括 Amazon EC2。您只需为使用的服务付费。

使用 Amazon EC2 , 您可以按实际用量付费。如果您是 AWS 新客户 , 还可以免费试用 Amazon EC2。有关更多信息 , 请参阅 [AWS 免费套餐](#)。

如果您已有一个 AWS 账户 , 请跳到下一个任务。如果您还没有 AWS 账户 , 请使用以下步骤创建。

如何创建 AWS 账户

1. 打开 <https://aws.amazon.com/> , 然后选择 Create an AWS Account。
2. 按照屏幕上的说明进行操作。

作为注册流程的一部分 , 您会收到一个电话 , 需要您使用电话键盘输入一个 PIN 码。

请记住您的 AWS 账户 , 因为进行下一个任务时需要用到该账户。

创建 IAM 用户

AWS 中的服务（例如 Amazon EC2）要求您在访问时提供证书，以便服务可以确定您是否有权限访问其资源。控制台要求您的密码。您可以为您的 AWS 账户创建访问密钥以访问命令行界面或 API。但是，我们不建议您使用 AWS 账户的凭证访问 AWS，而建议您使用 AWS Identity and Access Management (IAM)。创建 IAM 用户，然后将该用户添加到具有管理权限的 IAM 组或授予此用户管理权限。然后您就可以使用特别的 URL 和 IAM 用户的证书访问 AWS。

如果您已注册 AWS 但尚未为自己创建一个 IAM 用户，则可以使用 IAM 控制台自行创建。如果您不熟悉如何使用控制台，请参阅[使用 AWS 管理控制台](#)中的概述内容。

为您自己创建一个 IAM 用户并将该用户添加到管理员组

1. 在 <https://console.aws.amazon.com/iam/> 处登录 IAM 控制台。
2. 在导航窗格中，选择 Users，然后选择 Add user。
3. 对于 User name，键入用户名，例如 Administrator。名称可包含字母、数字以及以下字符：加号 (+)、等号 (=)、逗号 (,)、句点 (.)、at 符号 (@)、下划线 (_) 和连字符 (-)。名称不区分大小写，且最大长度可为 64 个字符。
4. 选中 AWS 管理控制台 access 旁边的复选框，选择 Custom password，然后在文本框中键入新用户的密码。您可以选择 Require password reset 以强制用户在下次登录时选择新密码。
5. 选择 Next: Permissions。
6. 在 Set permissions for user 页面上，选择 Add user to group。
7. 选择 Create group。
8. 在 Create group 对话框中，为新组键入名称。名称可包含字母、数字以及以下字符：加号 (+)、等号 (=)、逗号 (,)、句点 (.)、at 符号 (@)、下划线 (_) 和连字符 (-)。名称不区分大小写，且最大长度可为 128 个字符。
9. 对于 Filter，选择 Job function。
10. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group。
11. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh 以在列表中查看该组。
12. 选择 Next: Review 以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user。

您可使用此相同的流程创建更多的组和用户，并允许您的用户访问 AWS 账户资源。要了解有关使用策略将用户权限限制到特定 AWS 资源的信息，请转到[访问管理和管理 AWS 资源的策略示例](#)。

要以该新 IAM 用户的身份登录，请从 AWS 控制台退出，然后使用以下 URL，其中 your_aws_account_id 是您的不带连字符的 AWS 账户（例如，如果您的 AWS 账户是 1234-5678-9012，则您的 AWS 账户 ID 是 123456789012）：

`https://your_aws_account_id.signin.aws.amazon.com/console/`

输入您刚创建的 IAM 用户名（而不是电子邮件地址）和密码。登录后，导航栏显示 your_user_name @ your_aws_account_id。

如果您不希望您的登录页面 URL 包含 AWS 账户 ID，可以创建账户别名。从 IAM 控制台中，单击导航窗格中的控制面板。从控制面板中，单击 Customize，然后输入一个别名，例如您的公司名称。要在创建账户别名后登录，请使用以下 URL：

`https://your_account_alias.signin.aws.amazon.com/console/`

要为您的账户验证 IAM 用户的登录链接，请打开 IAM 控制台并在控制面板的 IAM users sign-in link (IAM 用户登录链接) 下进行检查。

有关 IAM 的更多信息，请参阅 [IAM 和 Amazon EC2 \(p. 367\)](#)。

创建密钥对

AWS 使用公共密钥密码术来保护您实例的登录信息。Linux 实例没有密码；您可以使用密钥对安全地登录您的实例。您可以在启动实例时指定密钥对的名称，然后提供私有密钥（使用 SSH 登录时）。

如果您尚未创建密钥对，则可以通过 Amazon EC2 控制台自行创建。请注意，如果您计划在多个区域启动实例，则需要在每个区域中创建密钥对。有关区域的更多信息，请参阅[地区和可用区域 \(p. 7\)](#)。

创建密钥对

1. 使用您在上节中创建的 URL 登录到 AWS。
2. 从 AWS 控制面板中，选择 EC2 以打开 Amazon EC2 控制台。
3. 从导航栏中，选择密钥对区域。您可以选择向您提供的任何区域，无需理会您身处的位置。但是，密钥对是特定于区域的；例如，如果您计划在美国西部（俄勒冈）区域中启动实例，则必须在 美国西部（俄勒冈）区域中创建实例的密钥对。
4. 在导航窗格中的 NETWORK & SECURITY 下，单击 Key Pairs。

Tip

导航窗格位于控制台的左侧。如果您看不到窗格，它可能被最小化了；单击箭头扩展窗格。您可能必须向下滚动才能看到 Key Pairs 链接。

5. 单击创建键前缀。
6. 在 Create Key Pair (创建密钥对) 对话框的 Key pair name (密钥对名称) 字段中输入新密钥对的名称，然后单击 Create (创建)。选择一个容易记住的名称，例如，您的 IAM 用户名称，后跟 -key-pair 加区域名称。例如，me-key-pair-uswest2。
7. 您的浏览器会自动下载私有密钥文件。基本文件名是您为密钥对指定的名称，文件扩展名为 .pem。将私有密钥文件保存在安全位置。

Important

这是您保存私有密钥文件的唯一机会。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

8. 如果您将在 Mac 或 Linux 计算机上使用 SSH 客户端连接到您的 Linux 实例，请使用以下命令设置您私有密钥文件的权限，以确保只有您可以读取它。

```
$ chmod 400 your_user_name-key-pair-region_name.pem
```

有关更多信息，请参阅 [Amazon EC2 密钥对 \(p. 346\)](#)。

使用密钥对连接到实例

要从运行 Mac 或 Linux 的计算机连接到 Linux 实例，需要使用 -i 选项对 SSH 客户端指定 .pem 文件和私有密钥的路径。若要从运行 Windows 的计算机连接到 Linux 实例，可以使用 MindTerm 或 PuTTY。如果您计划使用 PuTTY，则需要安装它并按以下过程将 .pem 文件转换为 .ppk 文件。

(可选) 准备使用 PuTTY 从 Windows 连接到 Linux 实例

1. 从 <http://www.chiark.greenend.org.uk/~sgtatham/putty/> 下载并安装 PuTTY。确保安装整个套件。
2. 启动 PuTTYgen（例如，在“Start”菜单中，依次单击“All Programs > PUTTY > PuTTYgen”）。
3. 在 Type of key to generate (要生成的密钥类型) 下，选择 SSH-2 RSA。

4. 单击“Load”。在默认情况下，PuTTYgen 仅显示扩展名为 .ppk 的文件。要找到您的 .pem 文件，请选择显示所有类型的文件的选项。
5. 选择您在上一个步骤中创建的私有密钥文件，然后单击 Open (打开)。单击 OK (确定) 关闭确认对话框。
6. 单击 Save private key (保存私钥)。PuTTYgen 显示一条关于在没有口令的情况下保存密钥的警告。单击 Yes (是)。
7. 指定与密钥对相同的密钥名称。PuTTY 自动添加 .ppk 文件扩展名。

创建 Virtual Private Cloud (VPC)

Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。如果您有默认 VPC，则可以跳过此部分并进入下一个任务，即 [创建安全组 \(p. 18\)](#)。若要确定您是否有默认的 VPC，请参阅在 [Amazon EC2 控制台中所支持的平台 \(p. 435\)](#)。否则，您可以使用以下步骤在账户中创建非默认 VPC。

Important

如果您的账户在某个区域中支持 EC2-Classic，则您在该区域没有默认 VPC。T2 实例必须在 VPC 中启动。

创建非默认 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 从导航栏中，为 VPC 选择区域。VPC 特定于某一区域，因此您应选择已创建密钥对的区域。
3. 在 VPC 控制面板上，单击 Start VPC Wizard (启动 VPC 向导)。
4. 在 Step 1: Select a VPC Configuration (步骤 1: 选择 VPC 配置) 页面上，确保选择 VPC with a Single Public Subnet (带有单个公有子网的 VPC)，然后单击 Select (选择)。
5. 在 Step 2: VPC with a Single Public Subnet (步骤 2: 带有单个公有子网的 VPC) 页面上，在 VPC name (VPC 名称) 字段中为您的 VPC 输入友好名称。保留其他默认配置设置，然后单击 Create VPC (创建 VPC)。在确认页面上，单击 OK (确定)。

有关 Amazon VPC 的更多信息，请参阅 [Amazon VPC 是什么？\(在 Amazon VPC 用户指南 中\)](#)。

创建安全组

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须在安全组中添加规则，以便能够使用 SSH 从您的 IP 地址连接到实例。您还可以添加允许来自任意位置的入站和出站 HTTP 和 HTTPS 访问的规则。

请注意，如果您计划在多个区域中启动实例，则需要在每个区域中创建安全组。有关区域的更多信息，请参阅 [地区和可用区域 \(p. 7\)](#)。

先决条件

您需要使用本地计算机的公有 IPv4 地址。Amazon EC2 控制台中的安全组编辑器可以为您自动检测公有 IPv4 地址。此外，您可以在 Internet 浏览器中搜索“什么是我的 IP 地址”，或使用以下服务：<http://checkip.amazonaws.com/>。如果您正通过 Internet 服务提供商 (ISP) 连接或者在不使用静态 IP 的情况下从防火墙后面连接，则您需要找出客户端计算机使用的 IP 地址范围。

为您的 VPC 创建具有最小特权的

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

Tip

另外，您可以使用 Amazon VPC 控制台创建安全组。但是，此过程中的说明不适用于 Amazon VPC 控制台。因此，如果您在以前的部分中切换到了 Amazon VPC 控制台，请切换回 Amazon EC2 控制台并使用这些说明，或者使用 Amazon VPC 入门指南 中的[为您的 VPC 设置安全组](#)。

2. 从导航栏中选择安全组的区域。安全组特定于某一区域，因此您应选择已创建密钥对的区域。
3. 单击导航窗格中的 Security Groups (安全组)。
4. 单击 Create Security Group (创建安全组)。
5. 输入新安全组的名称和描述。选择一个容易记住的名称，例如，您的 IAM 用户名称，后跟 _SG_ 加区域名称。例如，me_SG_uswest2。
6. 在 VPC 列表中选择您的 VPC。如果您有默认 VPC，则该 VPC 会带有星号 (*) 标记。

Note

如果您的账户支持 EC2-Classic，请选择您在上一个任务中创建的 VPC。

7. 在 Inbound 选项卡上，创建以下规则 (为每个新规则单击 Add Rule)，然后单击 Create：
 - 从 Type (类型) 列表中选择 HTTP，确保 Source (源) 设置为 Anywhere (任何位置) (0.0.0.0/0)。
 - 从 Type (类型) 列表中选择 HTTPS，确保 Source (源) 设置为 Anywhere (任何位置) (0.0.0.0/0)。
 - 从 Type (类型) 列表中选择 SSH。在源框中，选择 My IP 以便使用本地计算机的公有 IPv4 地址自动填充该字段。或者，选择自定义并用 CIDR 表示法指定计算机的公有 IPv4 地址或网络。要采用 CIDR 表示法指定单个 IP 地址，请添加路由前缀 /32，例如 203.0.113.25/32。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 203.0.113.0/24。

Warning

出于安全原因，我们建议您不要允许从所有 IPv4 地址 (0.0.0.0/0) 对您的实例进行 SSH 访问，但以测试为目的的短暂访问除外。

有关更多信息，请参阅 [Linux 实例的 Amazon EC2 安全组 \(p. 354\)](#)。

Amazon EC2 Linux 实例入门

让我们通过启动、连接以及使用 Linux 实例来实现 Amazon Elastic Compute Cloud (Amazon EC2) 入门。实例是 AWS 云中的虚拟服务器。您可以使用 Amazon EC2 来创建和配置在实例上运行的操作系统和应用程序。

注册 AWS 后，您可以通过 [AWS 免费套餐](#)开始免费使用 Amazon EC2。如果您在过去 12 个月内创建过 AWS 账户，并且还没有超出 Amazon EC2 的免费套餐权益范围，则学完本教程不需要任何费用，因为我们会帮助您选择免费套餐权益范围内的选项。否则，您将从启动实例的那一刻开始承担标准的 Amazon EC2 使用费，直至终止实例（本教程最后一项任务），即使实例处于闲置状态也要计费。

内容

- [概述 \(p. 20\)](#)
- [先决条件 \(p. 21\)](#)
- [步骤 1：启动实例 \(p. 21\)](#)
- [步骤 2：连接到您的实例 \(p. 22\)](#)
- [步骤 3：清除您的实例 \(p. 22\)](#)
- [后续步骤 \(p. 23\)](#)

概述

该实例为 Amazon EBS 支持的实例（即，根卷为 EBS 卷）。您可以指定在其中运行您的实例的可用区，也可以让 Amazon EC2 为您选择可用区。启动您的实例时，您可以通过指定密钥对和安全组保障其安全。连接到您的实例时，您必须指定您在启动实例时指定的密钥对的私有密钥。

任务

要完成本教程，请执行以下任务：

1. [启动实例 \(p. 21\)](#)
2. [连接到您的实例 \(p. 22\)](#)
3. [清除您的实例 \(p. 22\)](#)

相关教程

- 如果您希望启动 Windows 实例，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的以下教程：[Amazon EC2 Windows 实例入门](#)。
- 如果您希望使用命令行，请参阅 AWS Command Line Interface 用户指南 中的以下教程：[通过 AWS CLI 使用 Amazon EC2](#)。

先决条件

开始之前，请确保您已完成[Amazon EC2 的设置 \(p. 15\)](#)中的步骤。

步骤 1：启动实例

您可以根据以下过程所述使用 AWS 管理控制台启动 Linux 实例。本教程旨在帮助您快速启动第一个实例，因此不会涵盖所有可能的选项。有关高级选项的更多信息，请参阅[启动实例](#)。

启动实例

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 从控制台控制面板中，选择 Launch Instance。
- Choose an Amazon Machine Image (AMI) 页面显示一组称为 Amazon 系统映像 (AMI) 的基本配置，作为您的实例的模板。选择 Amazon Linux AMI 的 HVM 版本。请注意，此 AMI 标记为“符合条件的免费套餐。”
- 在 Choose an Instance Type (选择实例类型) 页面上，您可以选择实例的硬件配置。选择 t2.micro 类型（默认情况下的选择）。请注意，此实例类型适用免费套餐。

Note

T2 实例 (如 t2.micro) 必须在 VPC 中启动。如果您的 AWS 账户支持 EC2-Classic 并且您在所选区域中没有 VPC，则启动向导会为您创建 VPC，然后您可以继续执行下一个步骤。否则，Review and Launch 按钮会被禁用，并且您必须选择 Next: Configure Instance Details 并按照说明选择一个子网。

- 选择 Review and Launch 让向导为您完成其他配置设置。
- 在 Review Instance Launch (查看实例启动) 页面上的 Security Groups (安全组) 下，您将看到向导为您创建并选择了安全组。使用以下步骤，您可以使用此安全组，或者也可以选择在设置时创建的安全组：
 - 选择 Edit security groups。
 - 在 Configure Security Group 页面上，确保 Select an existing security group 处于选中状态。
 - 从现有安全组列表中选择您的安全组，然后选择 Review and Launch。
- 在 Review Instance Launch 页面上，选择 Launch。
- 当系统提示提供密钥对时，选择 Choose an existing key pair，然后选择您在进行设置时创建的密钥对。

另外，您也可以新建密钥对。选择 Create a new key pair，输入密钥对的名称，然后选择 Download Key Pair。这是您保存私有密钥文件的唯一机会，因此务必单击进行下载。将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

Warning

请勿选择 Proceed without a key pair (在没有密钥对的情况下继续) 选项。如果您启动的实例没有密钥对，就不能连接到该实例。

准备好后，选中确认复选框，然后选择 Launch Instances。

9. 确认页面会让您知道自己的实例已启动。选择 View Instances 以关闭确认页面并返回控制台。
10. 在实例屏幕上，您可以查看启动状态。启动实例只需很短的时间。启动实例时，其初始状态为 pending。实例启动后，其状态变为 running，并且会收到一个公有 DNS 名称。(如果 Public DNS (IPv4) 列已隐藏，请选择页面右上角的“显示/隐藏”图标，然后选择 Public DNS (IPv4)。)
11. 需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查；您可以在 Status Checks 列中查看此信息。

步骤 2：连接到您的实例

有几种方法可以连接到 Linux 实例。在此过程中，您将使用浏览器连接。或者，您也可以使用 PuTTY 或 SSH 客户端进行连接。我们还假定您按照之前的步骤操作并从 Amazon Linux AMI 启动了一个实例，该实例有特定的用户名。其他 Linux 发行版可能使用不同的用户名。有关更多信息，请参阅 [使用 PuTTY 从 Windows 连接到 Linux 实例 \(p. 256\)](#) 或 [使用 SSH 连接到 Linux 实例 \(p. 252\)](#)。

Important

除非您在启动它时使用 .pem 文件的键前缀以及允许访问 SSH 的安全组，否则您无法连接到您的实例。如果您无法连接到实例，请参阅 [排查实例的连接问题 \(p. 643\)](#) 以获得帮助。

使用 Web 浏览器连接到您的 Linux 实例

1. 您必须安装了 Java 并已在浏览器中启用。如果您还未安装 Java，可以联系您的系统管理员进行安装，也可以遵循以下页面中概括的步骤：[安装 Java 和在您的 Web 浏览器中启用 Java](#)。
2. 从 Amazon EC2 控制台中，在导航窗格中选择 Instances。
3. 选择该实例，然后选择 Connect。
4. 选择 A Java SSH client directly from my browser (Java required)。
5. Amazon EC2 自动检测您实例的公有 DNS 名称并为您填写 Public DNS (公有 DNS)。它还检测您在启动实例时指定的密钥对。完成以下步骤，然后选择 Launch SSH Client。
 - a. 在 User name (用户名) 中，输入 ec2-user。
 - b. 在 Private key path 中，输入私有密钥 (.pem) 文件的完全限定路径，包括密钥对名称。
 - c. (可选) 选择 Store in browser cache 以将私有密钥的位置存储在您的浏览器缓存中。这使得 Amazon EC2 可在后续的浏览器会话中检测私有密钥的位置，直到您清除浏览器缓存为止。
6. 如有必要，请选择 Yes 以信任证书，然后选择 Run 以运行 MindTerm 客户端。
7. 如果这是您第一次运行 MindTerm，则会出现一系列对话框，要求您接受许可协议、确认主目录的设置以及确认已知主机目录的设置。确认这些设置。
8. 一个对话框会提示您向已知主机集添加主机。如果您不想在本地计算机上存储主机密钥信息，请选择 No。
9. 此时会打开一个窗口并且您连接到了您的实例。

Note

如果您在上一步中选择了 No，则将看到以下消息：

```
Verification of server key disabled in this session.
```

步骤 3：清除您的实例

在您完成为本教程创建的实例后，应通过终止该实例进行清除。如果在清除该实例前要对其进行更多操作，请参阅 [后续步骤 \(p. 23\)](#)。

Important

终止实例可有效地删除实例；无法在终止实例后重新连接到实例。

如果您启动的实例不在 [AWS 免费套餐](#) 范围内，则该实例一旦变为 `shutting down` 或 `terminated` 状态，就会停止产生费用。如果您希望在不产生费用的情况下保留实例以供将来使用，您可以立即停止该实例，然后在稍后再次启动它。有关更多信息，请参阅[停止实例](#)。

终止您的实例

1. 在导航窗格中，选择 Instances。在实例列表中选择实例。
2. 依次选择 Actions、Instance State 和 Terminate。
3. 当系统提示您确认时，选择 Yes, Terminate。

Amazon EC2 关闭并终止您的实例。您的实例在终止之后，短时间内仍将在控制台上可见，然后该条目将被删除。

后续步骤

启动实例后，您可能想尝试以下的一些练习：

- 了解如何使用 Run Command 远程管理您的 EC2 实例。有关更多信息，请参阅[教程：远程管理您的 Amazon EC2 实例 \(p. 53\)](#)和[Systems Manager 远程管理 \(Run Command\)](#)。
- 配置 CloudWatch 警报以便在您的使用量超出免费套餐时向您发出通知。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的[创建账单警报](#)。
- 添加 EBS 卷。有关更多信息，请参阅[创建 Amazon EBS 卷 \(p. 527\)](#) 和 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
- 安装 LAMP 堆栈。有关更多信息，请参阅[教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)。

针对 Amazon EC2 的最佳实践

此核对清单旨在帮助您从 Amazon EC2 获得最大好处和满意度。

安全与网络

- 使用联合身份验证、IAM 用户和 IAM 角色可管理对 AWS 资源和 API 的访问。建立证书管理策略和过程，以便创建、分配、轮换和撤销 AWS 访问证书。有关更多信息，请参阅 IAM 用户指南 中的 [IAM 最佳实践](#)。
- 为安全组实现最严格的规则。有关更多信息，请参阅 [安全组规则 \(p. 355\)](#)。
- 定期修补、更新和保护实例上的操作系统和应用程序。有关更新 Amazon Linux 的更多信息，请参阅 [管理 Linux 实例上的软件](#)。有关更新您的 Windows 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [更新 Windows 实例](#)。
- 在 VPC (而不是 EC2-Classic) 中启动您的实例。请注意，如果您在 2013-12-04 后创建 AWS 账户，我们会自动将实例启动到 VPC。有关所获好处的更多信息，请参阅 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 431\)](#)。

存储

- 了解根设备类型对数据持久性、备份和恢复的影响。有关更多信息，请参阅 [根设备存储 \(p. 60\)](#)。
- 对操作系统与您的数据分别使用单独的 Amazon EBS 卷。确保含有您数据的卷可在实例终止后保留。有关更多信息，请参阅 [在实例终止时保留 Amazon EBS 卷 \(p. 270\)](#)。
- 使用您的实例可用的实例存储来存储临时数据。请注意，当您停止或终止您的实例时，会删除存储在实例存储中的数据。如果将实例存储用于数据库存储，请确保您拥有一个具有重复因子的群集，从而确保容错。

资源管理

- 使用实例元数据和自定义资源标签跟踪并确定您的 AWS 资源。有关更多信息，请参阅 [实例元数据和用户数据 \(p. 295\)](#) 和 [标记 Amazon EC2 资源 \(p. 626\)](#)。
- 查看您的 Amazon EC2 的当前限制。需要时请提前计划请求提高限制。有关更多信息，请参阅 [Amazon EC2 服务限制 \(p. 633\)](#)。

备份和恢复

- 使用 [Amazon EBS 快照 \(p. 559\)](#)定期备份您的 EBS 卷，并从您的实例创建 [Amazon 系统映像 \(AMI\) \(p. 58\)](#)，以便保存配置以作为启动未来实例的模板。

- 跨多个可用区部署应用程序的关键组件，并适当地复制数据。
- 设计您的应用程序，以便在实例重新启动时处理动态 IP 地址分配。有关更多信息，请参阅 [Amazon EC2 实例 IP 寻址 \(p. 453\)](#)。
- 监控和响应事件。有关更多信息，请参阅 [监控 Amazon EC2 \(p. 310\)](#)。
- 确保您已准备好处理故障转移。对于基本解决方案，您可以手动将网络接口或弹性 IP 地址附加到替换实例。有关更多信息，请参阅 [弹性网络接口 \(p. 473\)](#)。对于自动解决方案，您可以使用 Auto Scaling。有关更多信息，请参阅 [Auto Scaling 用户指南](#)。
- 定期测试在您实例和 Amazon EBS 卷发生故障时恢复它们的过程。

运行 Linux 的 Amazon EC2 实例的相关教程

以下教程为您介绍了如何使用运行 Linux 的 EC2 实例执行常见任务。

教程

- [教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)
- [教程：使用 Amazon Linux 托管 WordPress 博客 \(p. 35\)](#)
- [教程：将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS \(p. 43\)](#)
- [教程：提高应用程序在 Amazon EC2 上的可用性 \(p. 51\)](#)
- [教程：远程管理您的 Amazon EC2 实例 \(p. 53\)](#)

教程：在 Amazon Linux 上安装 LAMP Web 服务器

通过以下步骤，您可以将支持 PHP 和 MySQL 的 Apache Web 服务器（有时称为 LAMP Web 服务器或 LAMP 堆栈）安装到您 Amazon Linux 实例上。您可以使用此服务器来托管静态网站或部署能对数据库中的信息执行读写操作的动态 PHP 应用程序。

先决条件

本教程假定您已经启动具有可从 Internet 访问的公有 DNS 名称的新实例。有关更多信息，请参阅 [步骤 1：启动实例 \(p. 21\)](#)。还必须将安全组配置为允许 SSH(端口 22)、HTTP((口 80) 和 HTTPS(端口 443) 连接。有关这些先决条件的更多信息，请参阅 [Amazon EC2 的设置 \(p. 15\)](#)。

Important

如果您尝试在 Ubuntu 实例上设置 LAMP Web 服务器，则本教程不适合您。这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。有关 Ubuntu 上的 LAMP Web 服务器的信息，请参阅 Ubuntu 社区文档 [ApacheMySQLPHP](#) 主题。

在 Amazon Linux 上安装和启动 LAMP Web 服务器

1. [连接到您的实例 \(p. 22\)](#)。
2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

Note

-y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略此选项。

```
[ec2-user ~]$ sudo yum update -y
```

3. 您的实例处于最新状态后，便可以安装 Apache Web 服务器、MySQL 和 PHP 软件包。

Note

一些应用程序可能与以下建议的软件环境不兼容。在安装这些软件包之前，请检查您的 LAMP 应用程序（如 WordPress 或 phpMyAdmin）是否与其相兼容。如果出现问题，您可能需要按照[我想在我的服务器上运行的应用程序软件与所安装的 PHP 版本或其他软件不兼容 \(p. 34\)](#) 中所述安装替代环境

使用 yum install 命令可同时安装多个软件包和所有相关依赖项。

```
[ec2-user ~]$ sudo yum install -y httpd24 php70 mysql56-server php70-mysqld
```

4. 启动 Apache Web 服务器。

```
[ec2-user ~]$ sudo service httpd start
Starting httpd: [ OK ]
```

5. 使用 chkconfig 命令将 Apache Web 服务器配置为在每次系统启动时启动。

```
[ec2-user ~]$ sudo chkconfig httpd on
```

Tip

当您成功地使用 chkconfig 启用服务时，此命令不提供任何确认消息。
您可通过运行以下命令验证 httpd 是否启用：

```
[ec2-user ~]$ chkconfig --list httpd
httpd      0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

在此处，httpd 在运行级别 2、3、4 和 5（您需要查看的运行级别）为 on。

6. 测试您的 Web 服务器。在 Web 浏览器中，输入您实例的公有 DNS 地址（或公有 IP 地址），您应该可以看到 Apache 测试页面。您可以使用 Amazon EC2 控制台获取实例的公有 DNS（查看 Public DNS 列；如果此列处于隐藏状态，请选择 Show/Hide，然后选择 Public DNS）。

Tip

如果您未能看到 Apache 测试页面，请检查您使用的安全组是否包含允许 HTTP（端口 80）流量的规则。有关将 HTTP 规则添加到安全组的信息，请参阅[向安全组添加规则 \(p. 359\)](#)。

Important

如果您使用的不是 Amazon Linux，则还可能需要在实例上配置防火墙才能允许这些连接。有关如何配置防火墙的更多信息，请参阅适用于特定分配的文档。

Amazon Linux AMI Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The [Amazon Linux AMI](#) is a supported and maintained Linux image provided by [Amazon Web Services](#) for use on [Amazon Elastic Compute Cloud \(Amazon EC2\)](#). It is designed to provide a stable, secure, and high performance execution environment for applications running on [Amazon EC2](#). It also includes packages that enable easy integration with [AWS](#), including launch configuration tools and many popular AWS libraries and tools. [Amazon Web Services](#) provides ongoing security and maintenance updates to all instances running the [Amazon Linux AMI](#). [The Amazon Linux AMI](#) is provided at no additional charge to [Amazon EC2 users](#).

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and Amazon Linux AMI powered HTTP servers. Thanks for using Apache and the Amazon Linux AMI!



2.4

Note

该测试页面仅在 `/var/www/html` 无内容时显示。将内容添加到文档根目录后，您的内容将显示在您实例的公有 DNS 地址中，而不显示在本测试页面。

Apachehttpd 提供的文件保存在称为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录是 `/var/www/html`，默认情况下归 `root` 所有。

```
[ec2-user ~]$ ls -l /var/www
total 16
drwxr-xr-x 2 root root 4096 Jul 12 01:00 cgi-bin
drwxr-xr-x 3 root root 4096 Aug 7 00:02 error
drwxr-xr-x 2 root root 4096 Jan 6 2012 html
drwxr-xr-x 3 root root 4096 Aug 7 00:02 icons
```

要允许 `ec2-user` 操作此目录中的文件，您需修改其所有权和权限。有多种方法可以完成此任务；在本教程中，您可以将 `www` 组添加到您的实例，然后赋予该组 `/var/www` 目录的所有权并为该组添加写入权限。随后，该组的所有成员都将能够为 Web 服务器添加、删除和修改文件。

设置文件权限

1. 将 www 组添加到您的实例。

```
[ec2-user ~]$ sudo groupadd www
```

2. 将您的用户 (这里指 ec2-user) 添加到 www。

```
[ec2-user ~]$ sudo usermod -a -G www ec2-user
```

Important

您必须先退出，再重新登录，然后才能接受新组。您可以使用 exit 命令，也可以关闭终端窗口。

3. 先退出，再重新登录，然后验证您是否为 www 组的成员。

- a. 退出。

```
[ec2-user ~]$ exit
```

- b. 重新连接到实例，然后运行以下命令，以验证您是否为 www 组的成员。

```
[ec2-user ~]$ groups  
ec2-user wheel www
```

4. 将 /var/ 及其内容的组所有权更改到 www 组。

```
[ec2-user ~]$ sudo chown -R root:www /var/www
```

5. 更改 /var/www 及其子目录的目录权限，以添加组写入权限和设置未来子目录上的组 ID。

```
[ec2-user ~]$ sudo chmod 2775 /var/www  
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
```

6. 递归更改 /var/www 及其子目录的文件权限，以添加组写入权限。

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

现在，ec2-user (以及 www 组的任何未来成员) 可以在 Apache 根目录中添加、删除和编辑文件。现在您已准备好添加内容，例如静态网站或 PHP 应用程序。

(可选) 保护您的 Web 服务器

运行 HTTP 协议的 Web 服务器不为其发送或接收的数据提供传输安全。当您使用 Web 浏览器连接 HTTP 服务器时，对于您输入的 URL、您接收的网页内容以及您提交的任何 HTML 表的内容 (包括密码)，窃取者可在网络路径上的任何位置看到。保护您的 Web 服务器的最佳实践是安装 HTTPS (HTTP Secure) 支持，它将使用 SSL/TLS 加密保护您的数据。

有关在您的服务器上启用 HTTPS 的信息，请参阅[教程：将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS](#)。

测试您的 LAMP Web 服务器

如果您的服务器已安装并运行，且文件权限设置正确，则您的 ec2-user 账户应该能够在 /var/www/html 目录 (可从 Internet 访问) 中创建一个简单的 PHP 文件。

1. 在 Apache 文档根目录中创建一个简单的 PHP 文件。

```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Tip

尝试运行此命令时，如果出现“Permission denied”错误，请尝试先退出，再重新登录，以接受您在[设置文件权限 \(p. 29\)](#)中配置的适当组权限。

2. 在 Web 浏览器中，输入您刚刚创建的文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。例如：

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该可以看到 PHP 信息页面：

PHP Version 5.6.6

| | |
|---|---|
| System | Linux ip-172-31-7-35 3.14.35-28.38.amzn1.x86_64 #1 SMP Wed Mar 11 22:50:37 UTC 2015 x86_64 |
| Build Date | Mar 5 2015 23:26:53 |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc |
| Loaded Configuration File | /etc/php.ini |
| Scan this dir for additional .ini files | /etc/php-5.6.d |
| Additional .ini files parsed | /etc/php-5.6.d/20-bz2.ini, /etc/php-5.6.d/20-calendar.ini, /etc/php-5.6.d/20-ctype.ini, /etc/php-5.6.d/20-crypt.ini, /etc/php-5.6.d/20-dom.ini, /etc/php-5.6.d/20-exif.ini, /etc/php-5.6.d/20-fileinfo.ini, /etc/php-5.6.d/20-ftp.ini, /etc/php-5.6.d/20-gettext.ini, /etc/php-5.6.d/20-iconv.ini, /etc/php-5.6.d/20-mysqlnd.ini, /etc/php-5.6.d/20-pdo.ini, /etc/php-5.6.d/20-phar.ini, /etc/php-5.6.d/20-posix.ini, /etc/php-5.6.d/20-shmop.ini, /etc/php-5.6.d/20-simplexml.ini, /etc/php-5.6.d/20-sockets.ini, /etc/php-5.6.d/20-sqlite3.ini, /etc/php-5.6.d/20-sysvmsg.ini, /etc/php-5.6.d/20-sysvshm.ini, /etc/php-5.6.d/20-tokenizer.ini, /etc/php-5.6.d/20-xml.ini, /etc/php-5.6.d/20-xmlreader.ini, /etc/php-5.6.d/20-xsl.ini, /etc/php-5.6.d/20-zip.ini, /etc/php-5.6.d/30-mysql.ini, /etc/php-5.6.d/30-pdo.ini, /etc/php-5.6.d/30-mysqli.ini, /etc/php-5.6.d/30-pdo_mysql.ini, /etc/php-5.6.d/30-pdo_sqlite.ini, /etc/php-5.6.d/30-wddx.ini, /etc/php-5.6.d/30-xmlreader.ini, /etc/php-5.6.d/40-json.ini, /etc/php-5.6.d/php.ini |
| PHP API | 20131106 |
| PHP Extension | 20131226 |
| Zend Extension | 220131226 |
| Zend Extension Build | API220131226,NTS |
| PHP Extension Build | API20131226,NTS |

Note

如果您未看到此页面，请验证上一步中是否已正确创建 `/var/www/html/phpinfo.php` 文件。您也可以使用以下命令验证是否安装了所有必需的程序包（第二列中的程序包版本不需要与此示例输出匹配）：

```
[ec2-user ~]$ sudo yum list installed httpd24 php70 mysql56-server php70-mysqlnd
Loaded plugins: priorities, update-motd, upgrade-helper
Installed Packages
httpd24.x86_64                               2.4.25-1.68.amzn1
@amzn-updates
mysql56-server.x86_64                          5.6.35-1.23.amzn1
@amzn-updates
php70.x86_64                                  7.0.14-1.20.amzn1
@amzn-updates
php70-mysqlnd.x86_64                           7.0.14-1.20.amzn1
@amzn-updates
```

如果输出中未列出任何必需的程序包，请使用 `sudo yum install package` 命令安装它们。

3. 删除 `phpinfo.php` 文件。尽管此信息可能对您很有用，但出于安全考虑，不应将其传播到 Internet。

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

保障 MySQL 服务器的安全

MySQL 服务器的默认安装提供有多种功能，这些功能对于测试和开发都很有帮助，但对于产品服务器，应禁用或删除这些功能。`mysql_secure_installation` 命令可引导您设置根密码并删除安装中的不安全功能。即使您不打算使用 MySQL 服务器，执行此步骤也是一个不错的建议。

1. 启动 MySQL 服务器。

```
[ec2-user ~]$ sudo service mysqld start
Initializing MySQL database:
...
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
...
Starting mysqld: [ OK ]
```

2. 运行 `mysql_secure_installation`。

```
[ec2-user ~]$ sudo mysql_secure_installation
```

- a. 在系统提示时，输入 `root` 账户的密码。

- i. 输入当前 `root` 密码。默认情况下，`root` 账户没有设置密码，因此按 Enter。
- ii. 键入 Y 设置密码，然后输入两次安全密码。有关创建安全密码的更多信息，请参阅 <http://www.pctools.com/guides/password/>。确保将此密码存储在安全位置。

Note

设置 MySQL 根密码仅是保护数据库的最基本措施。在您构建或安装数据库驱动的应用程序时，您通常可以为该应用程序创建数据库服务用户，并避免使用根账户执行除数据库管理以外的操作。

- b. 键入 Y 删除匿名用户账户。
- c. 键入 Y 禁用远程 `root` 登录。
- d. 键入 Y 删除测试数据库。
- e. 键入 Y 重新加载权限表并保存您的更改。

3. (可选) 如果不打算立即使用 MySQL 服务器，请停止。您可以在需要时再次重新启动该服务器。

```
[ec2-user ~]$ sudo service mysqld stop
Stopping mysqld: [ OK ]
```

4. (可选) 如果您希望每次启动时 MySQL 服务器都启动，请输入以下命令。

```
[ec2-user ~]$ sudo chkconfig mysqld on
```

现在，您应该有了一个功能完善的 LAMP Web 服务器。如果您将内容添加到位于 `/var/www/html` 的 Apache 文档根目录，您应该能够在实例的公有 DNS 地址处看到这些内容。

(可选) 安装 phpMyAdmin

[phpMyAdmin](#) 是一种基于 Web 的数据库管理工具，可用于在 EC2 实例上查看和编辑 MySQL 数据库。按照以下步骤操作可在您的 Amazon Linux 实例上安装和配置 phpMyAdmin。

Important

除非您在 Apache 中启用了 SSL/TLS，否则我们不建议您使用 phpMyAdmin 访问 LAMP 服务器；如果您使用 phpMyAdmin，您的数据库管理员密码和其他数据将无法安全地通过 Internet 传输。

有关在 EC2 实例上配置安全的 Web 服务器的信息，请参阅[教程：将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS](#)。

Note

这些说明假定已在 Amazon Linux 和 Extra Packages for Enterprise Linux (EPEL) 中指定同一默认 PHP 版本。如果您遇到与 EPEL 软件包有关的兼容性问题，建议您手动安装 phpMyAdmin。有关最新版本，请参阅[phpMyAdmin 下载页面](#)。确保验证安装要求是否与您的 Amazon Linux (或其他 Linux) 实例的环境相匹配。

另请参阅以下的问题排查帮助：[我想在我的服务器上运行的应用程序软件与所安装的 PHP 版本或其他软件不兼容 \(p. 34\)](#)。

1. 在您的实例上从 Fedora 项目启用 Extra Packages for Enterprise Linux (EPEL) 存储库。

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

2. 安装 phpMyAdmin 软件包。

```
[ec2-user ~]$ sudo yum install -y phpMyAdmin
```

Note

在系统提示时，回答 **y** 以导入 EPEL 存储库的 GPG 密钥。

3. 将您的 phpMyAdmin 安装配置为允许从本地计算机进行访问。默认情况下，phpMyAdmin 仅允许从其运行于的服务器进行访问，这不是很有用，因为 Amazon Linux 不包括 Web 浏览器。
 - a. 通过访问服务 (例如 whatismyip.com) 查找您的本地 IP 地址。
 - b. 编辑 `/etc/httpd/conf.d/phpMyAdmin.conf` 文件，然后使用以下命令将服务器 IP 地址 (127.0.0.1) 替换为您的本地 IP 地址，并将 `your_ip_address` 替换为您在上一步中找到的本地 IP 地址。

```
[ec2-user ~]$ sudo sed -i -e 's/127.0.0.1/'your_ip_address/g' /etc/httpd/conf.d/phpMyAdmin.conf
```

4. 重启 Apache Web 服务器，让新配置生效。

```
[ec2-user ~]$ sudo service httpd restart
Stopping httpd:                                     [  OK  ]
Starting httpd:                                     [  OK  ]
```

5. 重启 MySQL 服务器，让新配置生效。

```
[ec2-user ~]$ sudo service mysqld restart
Stopping mysqld:                                     [  OK  ]
Starting mysqld:                                     [  OK  ]
```

6. 在 Web 浏览器中，输入 phpMyAdmin 安装的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和 `phpmyadmin`。例如：

```
http://my.public.dns.amazonaws.com/phpmyadmin
```

您应该可以看到 phpMyAdmin 登录页面：



Note

如果您收到 403 Forbidden 错误，请验证您是否在 /etc/httpd/conf.d/phpMyAdmin.conf 文件中设置了正确的 IP 地址。您可以使用以下命令查看 Apache 访问日志，以了解 Apache 服务 器实际从哪个 IP 地址获取您的请求：

```
[ec2-user ~]$ sudo tail -n 1 /var/log/httpd/access_log | awk '{ print $1 }'  
205.251.233.48
```

重复 Step 3.b (p. 32) , 使用此处返回的地址替换您以前输入的错误地址 ; 例如 :

```
[ec2-user ~]$ sudo sed -i -e 's/previous_ip_address/205.251.233.48/g' /etc/  
httpd/conf.d/phpMyAdmin.conf
```

替换 IP 地址后 , 请使用Step 4 (p. 32) 重新启动 httpd 服务。

7. 使用您先前创建的 root 用户名和 MySQL 根密码登录到安装的 phpMyAdmin。有关使用 phpMyAdmin 的更多信息 , 请参阅 [phpMyAdmin 用户指南](#)。

故障排除

本部分提供了解决在设置新 LAMP 服务器时可能遇到的常见问题的建议。

我无法使用 Web 浏览器连接到我的服务器。

执行以下检查以查看您的 Apache Web 服务器是否正在运行且可以访问。

- Web 服务器正在运行吗 ? 您可通过运行以下命令验证 httpd 是否启用 :

```
[ec2-user ~]$ chkconfig --list httpd  
httpd           0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

在此处 , httpd 在运行级别 2、3、4 和 5 (您需要查看的运行级别) 为 on。

如果 httpd 进程未运行 , 请重复[在 Amazon Linux 上安装和启动 LAMP Web 服务器 \(p. 27\)](#) 中描述的步骤。

- 防火墙是否配置正确 ?

如果您未能看到 Apache 测试页面 , 请检查您使用的安全组是否包含允许 HTTP (端口 80) 流量的规则。有关将 HTTP 规则添加到安全组的信息 , 请参阅[向安全组添加规则 \(p. 359\)](#)。

我想在我的服务器上运行的应用程序软件与所安装的 PHP 版本或其他软件不兼容

本教程建议安装最新版本的 Apache Web 服务器、PHP 和 MySQL。在安装其他 LAMP 应用程序之前 , 请检查其要求以确认它们与已安装的环境兼容。如果不支持最新版本的 PHP , 则可以 (并且完全安全) 降级到较旧的受支持配置。您还可以并行安装 PHP 的多个版本 , 至少可以解决部分兼容性问题。有关如何从安装的多个版本 PHP 中选择其一配置为首选项的信息 , 请参阅 [Amazon Linux AMI 2016.09 发行说明](#)。

如何降级

本教程的以前版本经过良好测试 , 需要以下核心 LAMP 程序包 :

- httpd24
- php56
- mysql55-server
- php56-mysqlnd

如果您已按照本教程开头所述的建议安装了最新的软件包，您首先需要卸载如下这些软件包和其他依赖项：

```
[ec2-user ~]$ sudo yum remove -y httpd24 php70 mysql56-server php70-mysqlnd perl-DBD-MySQL56
```

其次，安装替代环境：

```
[ec2-user ~]$ sudo yum install -y httpd24 php56 mysql55-server php56-mysqlnd
```

如果您以后决定升级为建议的环境，您首先需要删除自定义软件包和依赖项：

```
[ec2-user ~]$ yum remove -y httpd24 php56 mysql55-server php56-mysqlnd perl-DBD-MySQL55
```

现在，您可以按照本教程开头所述安装最新版的软件包。

相关主题

有关将文件传输到您的实例或在 Web 服务器上安装 WordPress 博客的更多信息，请参阅以下主题：

- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 259)
- 使用 SCP 将文件从 Linux 传输到 Linux 实例 (p. 254)
- 教程：使用 Amazon Linux 托管 WordPress 博客 (p. 35)

有关本主题中使用的命令和软件的更多信息，请参阅以下网页：

- Apache Web 服务器：<http://httpd.apache.org/>
- MySQL 数据库服务器：<http://www.mysql.com/>
- PHP 编程语言：<http://php.net/>
- chmod 命令：<https://en.wikipedia.org/wiki/Chmod>
- chown 命令：<https://en.wikipedia.org/wiki/Chown>

如果您想注册 Web 服务器的域名或将现有域名转移到此主机，请参阅 Amazon Route 53 开发人员指南 中的[创建域和子域并将其迁移到 Amazon Route 53](#)。

教程：使用 Amazon Linux 托管 WordPress 博客

以下步骤将帮助您在 Amazon Linux 实例上安装、配置和保护 WordPress 博客。本教程是很好的 Amazon EC2 入门教程，因为您可以完全控制托管您 WordPress 博客的 Web 服务器，这对传统的托管服务来说并不是一个典型的方案。

您负责更新软件包并为您的服务器维护安全补丁。对于不需要与 Web 服务器配置直接交互的更自动化 WordPress 安装来说，AWS CloudFormation 服务还会提供可让您快速入门的 WordPress 模板。有关更多信息，请参阅 AWS CloudFormation 用户指南 中的[入门](#)。如果您更喜欢将您的 WordPress 博客托管在 Windows 实例上，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[在您的 Amazon EC2 Windows 实例上部署 WordPress 博客](#)。如果您需要带分离数据库的高可用性解决方案，请参阅 AWS Elastic Beanstalk 开发人员指南 中的[部署高可用性 WordPress 网站](#)。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。本教程中的很多步骤对 Ubuntu 实例并不适用。有关在 Ubuntu 实例上安装 WordPress 的帮助，请参阅 Ubuntu 文档中的[WordPress](#)。

先决条件

本教程假定您已按照[教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)中的所有步骤，通过支持 PHP 和 MySQL 的功能性 Web 服务器启动了 Amazon Linux 实例。本教程还介绍了配置安全组以允许 HTTP 和 HTTPS 流量的步骤，以及用于确保为 Web 服务器正确设置文件权限的几个步骤。如果您尚未完成这些步骤，请参阅[教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)以满足这些先决条件，然后回到本教程安装 WordPress。有关添加规则到您安全组的信息，请参阅[向安全组添加规则 \(p. 359\)](#)。

强烈建议您将弹性 IP 地址 (EIP) 与您正用于托管 WordPress 博客的实例关联。这将防止您的实例的公有 DNS 地址更改和中断您的安装。如果您有一个域名且打算将其用于您的博客，则可更新该域名的 DNS 记录，使其指向您的 EIP 地址（如需帮助，请联系您的域名注册商）。您可以免费将一个 EIP 地址与正在运行的实例相关联。有关更多信息，请参阅[弹性 IP 地址 \(p. 467\)](#)。

如果您的博客还没有域名，则可使用 Amazon Route 53 注册一个域名并将您的实例的 EIP 地址与您的域名相关联。有关更多信息，请参阅 Amazon Route 53 开发人员指南 中的[使用 Amazon Route 53 注册域名](#)。

安装 WordPress

连接到您的实例，并下载 WordPress 安装包。

下载并解压 WordPress 安装包

1. 使用 wget 命令下载最新 WordPress 安装包。以下命令始终会下载最新版本。

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
--2013-08-09 17:19:01--  https://wordpress.org/latest.tar.gz
Resolving wordpress.org (wordpress.org)... 66.155.40.249, 66.155.40.250
Connecting to wordpress.org (wordpress.org)|66.155.40.249|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4028740 (3.8M) [application/x-gzip]
Saving to: latest.tar.gz

100%[=====] 4,028,740   20.1MB/s   in 0.2s

2013-08-09 17:19:02 (20.1 MB/s) - latest.tar.gz saved [4028740/4028740]
```

2. 解压并解档安装包。将安装文件夹解压到名为 `wordpress` 的文件夹。

```
[ec2-user ~]$ tar -xzf latest.tar.gz
[ec2-user ~]$ ls
latest.tar.gz  wordpress
```

创建 MySQL 用户和数据库以安装 WordPress

安装 WordPress 需要存储信息，例如数据库中的博客文章和用户评论。此步骤将帮助您为自己的博客创建一个数据库，并创建一个有权读取该数据库的信息并将信息保存到该数据库的用户。

1. 启动 MySQL 服务器。

```
[ec2-user ~]$ sudo service mysqld start
```

2. 以 `root` 用户身份登录到 MySQL 服务器。在系统提示时输入您的 MySQL `root` 密码，这可能与您的 `root` 系统密码不同，如果您尚未给您的 MySQL 服务器加密，它甚至可能是空的。

Important

如果您尚未给您的 MySQL 服务器加密，则必须执行这项操作。有关更多信息，请参阅[保障 MySQL 服务器的安全 \(p. 31\)](#)。

```
[ec2-user ~]$ mysql -u root -p  
Enter password:
```

3. 为您的 MySQL 数据库创建用户和密码。安装 WordPress 的过程将使用这些值与您的 MySQL 数据库通信。输入以下命令，以替换唯一的用户名和密码。

```
mysql> CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';  
Query OK, 0 rows affected (0.00 sec)
```

确保为您的用户创建强密码。请勿在您的密码中使用单引号字符 ('), 因为这将中断前面的命令。有关创建安全密码的更多信息，请转至 <http://www.pctools.com/guides/password/>。请勿重复使用现有密码，并确保将密码保存在安全的位置。

4. 创建数据库。为数据库提供一个有意义的描述性名称，例如 wordpress-db。

Note

以下命令中数据库名称两边的标点符号称为反引号。在标准键盘上，反引号 (`) 键通常位于 Tab 键的上方。并不总是需要反引号，但是它们允许您在数据库名称中使用其他的非法字符，例如 连字符。

```
mysql> CREATE DATABASE `wordpress-db`;  
Query OK, 1 row affected (0.01 sec)
```

5. 对您之前创建的 WordPress 用户授予您数据库的完全访问权限。

```
mysql> GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";  
Query OK, 0 rows affected (0.00 sec)
```

6. 刷新 MySQL 权限以接受您的所有更改。

```
mysql> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0.01 sec)
```

7. 退出 mysql 客户端。

```
mysql> exit  
Bye
```

创建和编辑 wp-config.php 文件

WordPress 安装文件夹包含名为 wp-config-sample.php 的示例配置文件。在本步骤中，您将复制此文件并进行编辑以适合您的具体配置。

1. 将 wp-config-sample.php 文件复制到名为 wp-config.php 的文件。这样做会创建新的配置文件并将原先的示例配置文件原样保留作为备份。

```
[ec2-user ~]$ cd wordpress/  
[ec2-user wordpress]$ cp wp-config-sample.php wp-config.php
```

2. 使用常用文本编辑器 (如 nano 或 vim) 来编辑 wp-config.php 文件，然后输入安装的值。如果您没有喜欢的文本编辑器，nano 对于初学者来说比较容易使用。

```
[ec2-user wordpress]$ nano wp-config.php
```

- a. 查找定义 DB_NAME 的行并将 database_name_here 更改为您在 [创建 MySQL 用户和数据库以安装 WordPress \(p. 36\)](#) 的 Step 4 (p. 37) 中创建的数据库名称。

```
define('DB_NAME', 'wordpress-db');
```

- b. 查找定义 DB_USER 的行并将 username_here 更改为您在 [创建 MySQL 用户和数据库以安装 WordPress \(p. 36\)](#) 的 Step 3 (p. 37) 中创建的数据库用户。

```
define('DB_USER', 'wordpress-user');
```

- c. 查找定义 DB_PASSWORD 的行并将 password_here 更改为您在 [创建 MySQL 用户和数据库以安装 WordPress \(p. 36\)](#) 的 Step 3 (p. 37) 中创建的强密码。

```
define('DB_PASSWORD', 'your_strong_password');
```

- d. 查找名为 Authentication Unique Keys and Salts 的一节。这些 KEY 和 SALT 值为 WordPress 用户存储在其本地计算机上的浏览器 Cookie 提供了加密层。总而言之，添加长的随机值将使您的站点更安全。访问 <https://api.wordpress.org/secret-key/1.1/salt/> 随机生成一组密钥值，您可以将这些密钥值复制并粘贴到 wp-config.php 文件中。要粘贴文本到 PuTTY 终端，请将光标放在您要粘贴文本的地方，并在 PuTTY 终端内部右键单击鼠标。

有关安全密钥的更多信息，请转至 http://codex.wordpress.org/Editing_wp-config.php#Security_Keys。

Note

以下值仅用作示例；请勿使用以下值进行安装。

```
define('AUTH_KEY', '#U$$+[RXN8:b^-L_0(WU+_c+WFkI~c]o]-bHw+/'
Aj[wTwSiz<Qb[mghEXcRh-']);
define('SECURE_AUTH_KEY', 'zsz._P=l/|y.Lq)Xjlkws1y5NJ76E6EJ.AVOpCKZZB,*~r ?6OP
$eJ@;+(ndLg');
define('LOGGED_IN_KEY', 'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY', 'P(g62HeZxEes/LnI^i=H,[XwK9I&[2s]:?ON)VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT', 'C$DpB4Hj[JK:{ql`sRVa{:7yShy(9A@5wg+`JJVb1fk%-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#)+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKV');
define('LOGGED_IN_SALT', 'j{00P*owZf)kVD+FVLn-->. /Y%Ug4#I^*LVd9QeZ^&XmK/e(76miC
+&W&+^OP/');
define('NONCE_SALT', '-97r*V/cgxLmp?Zy4zUU4r99QO_rGs2LTd%P;/
_e1tS)8_B/, .6[=UK<J_y9?JWG');
```

- e. 保存文件并退出您的文本编辑器。

移动 WordPress 安装至 Apache 文档根目录

现在，您已解压了安装文件夹、创建了 MySQL 数据库与用户并自定义了 WordPress 配置文件，那么也就准备好移动您的安装文件至 Web 服务器文档根目录，以便可以运行安装脚本完成安装。这些文件的位置取决于您是希望 WordPress 博客位于 Web 服务器的根目录（例如，<my.public.dns.amazonaws.com>）还是位于某个子目录或文件夹（例如，<my.public.dns.amazonaws.com/blog>）中。

- 选择要在其中提供博客的位置，仅运行与该位置关联的 mv。

Important

如果同时运行以下两组命令，则在运行第二个 mv 命令时，您会收到一条错误消息，因为您尝试移动的文件已不存在。

- 要在 [my.public.dns.amazonaws.com](#) 中提供博客，请将 wordpress 文件夹中的文件（而不是该文件夹本身）移动到 Apache 文档根目录中（Amazon Linux 实例上的 /var/www/html）。

```
[ec2-user wordpress]$ mv * /var/www/html/
```

- 或者，要在 [my.public.dns.amazonaws.com/blog](#) 提供博客，请在 Apache 文档根目录中创建名为 blog 的新文件夹，然后将 wordpress 文件夹中的文件（而不是该文件夹本身）移到新的 blog 文件夹中。

```
[ec2-user wordpress]$ mkdir /var/www/html/blog
[ec2-user wordpress]$ mv * /var/www/html/blog
```

Important

出于安全原因，如果您不打算立即进入到下一个过程，请立即停止 Apache Web 服务器（httpd）。将安装文件移动到 Apache 文档根目录后，WordPress 安装脚本将不受保护，如果 Apache Web 服务器运行，攻击者可能会获得访问您博客的权限。要停止 Apache Web 服务器，请输入命令 sudo service httpd stop。如果您即将继续到下一个步骤，则不需要终止 Apache Web 服务器。

允许 WordPress 使用 permalink

WordPress permalink 需要使用 Apache .htaccess 文件才能正常工作，但默认情况下这些文件在 Amazon Linux 上处于禁用状态。使用此过程可允许 Apache 文档根目录中的所有覆盖。

- 使用您常用的文本编辑器（如 nano 或 vim）打开 httpd.conf 文件。如果您没有喜欢的文本编辑器，nano 对于初学者来说比较容易使用。

```
[ec2-user wordpress]$ sudo vim /etc/httpd/conf/httpd.conf
```

- 找到以 <Directory "/var/www/html"> 开头的部分。

```
<Directory "/var/www/html">
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksIfOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
#
Options Indexes FollowSymLinks

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride None

#
```

```
# Controls who can get stuff from this server.  
#  
Require all granted  
</Directory>
```

- 在以上部分中将 AllowOverride None 行改为读取 AllowOverride All。

Note

此文件中有多个 AllowOverride 行；请确保更改 <Directory "/var/www/html"> 部分中的行。

```
AllowOverride All
```

- 保存文件并退出您的文本编辑器。

修复 Apache Web 服务器的文件权限

WordPress 中的某些可用功能要求具有对 Apache 文档根目录的写入权限（例如通过“Administration（管理）”屏幕上传媒体）。Web 服务器以 apache 用户身份运行，因此，您需要将该用户添加至在 wwwLAMP Web 服务器教程中创建的（p. 26）组。

- 将 apache 用户添加到 www 组。

```
[ec2-user wordpress]$ sudo usermod -a -G www apache
```

- 将 /var/www 及其内容的文件所有权更改到 apache 用户。

```
[ec2-user wordpress]$ sudo chown -R apache /var/www
```

- 将 /var/ 及其内容的组所有权更改到 www 组。

```
[ec2-user wordpress]$ sudo chgrp -R www /var/www
```

- 更改 /var/www 及其子目录的目录权限，以添加组写入权限和设置未来子目录上的组 ID。

```
[ec2-user wordpress]$ sudo chmod 2775 /var/www  
[ec2-user wordpress]$ find /var/www -type d -exec sudo chmod 2775 {} \;
```

- 递归更改 /var/www 及其子目录的文件权限，以添加组写入权限。

```
[ec2-user wordpress]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

- 重启 Apache Web 服务器，让新组和权限生效。

```
[ec2-user wordpress]$ sudo service httpd restart  
Stopping httpd: [OK]  
Starting httpd: [OK]
```

运行 WordPress 安装脚本

- 使用 chkconfig 命令确保 httpd 和 mysqld 服务在每次系统启动时启动。

```
[ec2-user wordpress]$ sudo chkconfig httpd on  
[ec2-user wordpress]$ sudo chkconfig mysqld on
```

- 验证 MySQL 服务器（mysqld）正在运行。

```
[ec2-user wordpress]$ sudo service mysqld status
mysqld (pid 4746) is running...
```

如果 mysqld 服务未运行，请启动。

```
[ec2-user wordpress]$ sudo service mysqld start
Starting mysqld: [ OK ]
```

- 验证您的 Apache Web 服务器 (httpd) 正在运行。

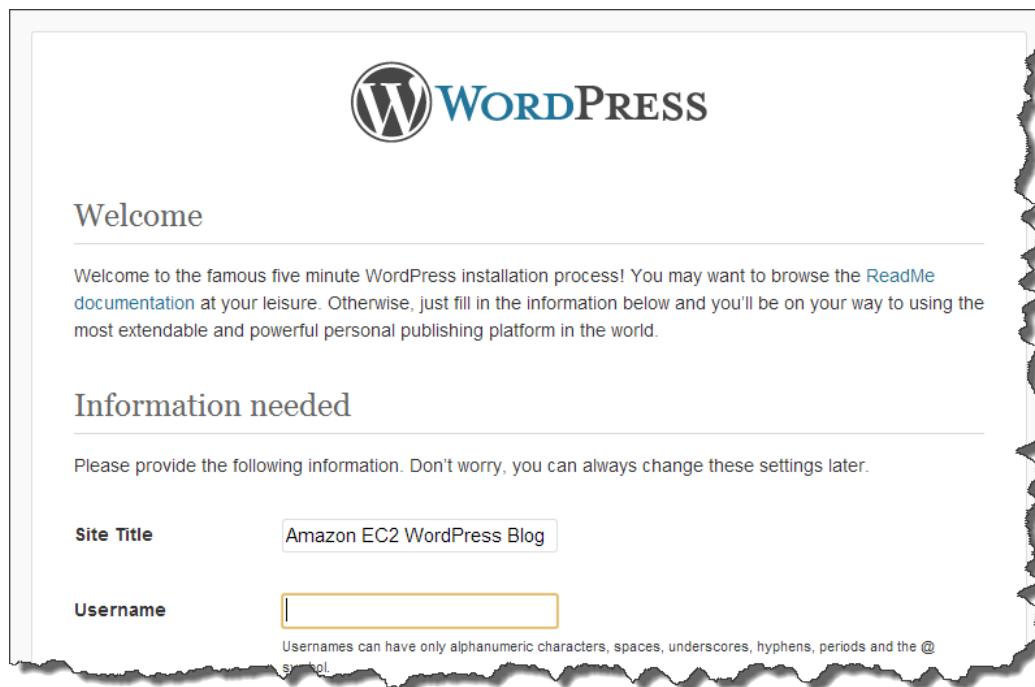
```
[ec2-user wordpress]$ sudo service httpd status
httpd (pid 502) is running...
```

如果 httpd 服务未运行，请启动。

```
[ec2-user wordpress]$ sudo service httpd start
Starting httpd: [ OK ]
```

- 在 Web 浏览器中，输入您 WordPress 博客的 URL (您实例的公有 DNS 地址，或者该地址后跟 blog 文件夹)。您应该可以看到 WordPress 安装屏幕。

```
http://my.public.dns.amazonaws.com
```



- 将其余安装信息输入 WordPress 安装向导。

| 字段 | 值 |
|-------------------|-----------------------|
| Site Title (网站标题) | 为您的 WordPress 网站输入名称。 |

| 字段 | 值 |
|----------------------|--|
| Username | 为您的 WordPress 管理员输入名称。出于安全原因，您应为此用户选择一个唯一名称，因为与默认用户名 admin 相比，该名称更难破解。 |
| 密码 | 输入强密码，然后再次输入进行确认。请勿重复使用现有密码，并确保将密码保存在安全的位置。 |
| Your E-mail (您的电子邮件) | 输入您用于接收通知的电子邮件地址。 |

6. 单击 Install WordPress (安装 WordPress) 完成安装。

恭喜您，您现在应该可以登录您的 WordPress 博客并开始发布博客文章。

后续步骤

在测试初始 WordPress 博客后，请考虑更新其配置。

使用自定义域名

如果您有一个与您的 EC2 实例的 EIP 地址关联的域名，则可将您的博客配置为使用该域名而不是 EC2 公有 DNS 地址。有关更多信息，请参阅 http://codex.wordpress.org/Changing_The_Site_URL。

配置您的博客

您可以将您的博客配置为使用不同的主题和插件，从而向您的读者提供更具个性化的体验。但是，有时安装过程可能事与愿违，从而导致您丢失您的整个博客。强烈建议您在尝试安装任何主题或插件之前，为您的实例创建一个备份 Amazon 系统映像 (AMI)，以便在安装过程中出现任何问题时，您还可以还原您的博客。有关更多信息，请参阅 [创建您自己的 AMI \(p. 58\)](#)。

添加容量

如果您的 WordPress 博客变得受关注并且您需要更多计算能力或存储，请考虑以下步骤：

- 对实例扩展存储空间。有关更多信息，请参阅 [在 Linux 上修改 EBS 卷的大小、IOPS 或类型 \(p. 543\)](#)。
- 将您的 MySQL 数据库移动到 [Amazon RDS](#) 以利用服务的自动扩展功能。
- 迁移到更大的实例类型。有关更多信息，请参阅 [调整您的实例大小 \(p. 156\)](#)。
- 添加额外实例。有关更多信息，请参阅 [教程：提高应用程序在 Amazon EC2 上的可用性 \(p. 51\)](#)。

了解有关 WordPress 的更多信息

有关 WordPress 的信息，请参阅 <http://codex.wordpress.org/> 上的 WordPress Codex 帮助文档。有关排除安装故障的更多信息，请转至 http://codex.wordpress.org/Installing_WordPress#Common_Installation_Problems。有关如何使您的 WordPress 博客更安全的信息，请转至 http://codex.wordpress.org/Hardening_WordPress。有关如何让您的 WordPress 博客保持最新的信息，请转至 http://codex.wordpress.org/Updating_WordPress。

帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪

已使用您的 EC2 实例的公有 DNS 地址自动配置您的 WordPress 安装。如果您停止并重启实例，公有 DNS 地址将发生更改（除非它与弹性 IP 地址相关联），并且您的博客将不会再运行，因为您的博客引用了不再存在的地址（或已分配给另一个 EC2 实例的地址）上的资源。http://codex.wordpress.org/Changing_The_Site_URL 中概括了有关该问题的更多详细和几个可能的解决方案。

如果您的 WordPress 安装发生了此问题，您可以使用以下过程恢复您的博客，该过程使用了适用于 WordPress 的 wp-cli 命令行界面。

使用 wp-cli 更改您的 WordPress 站点 URL

1. 使用 SSH 连接到您的 EC2 实例。
2. 请记下您的实例的旧站点 URL 和新站点 URL。安装了 WordPress 之后，旧站点 URL 可能是您的 EC2 实例的公有 DNS 名称。新站点 URL 是您的 EC2 实例的当前公有 DNS 名称。如果您不确定您的旧站点 URL，则可通过以下命令使用 curl 来查找它。

```
[ec2-user ~]$ curl localhost | grep wp-content
```

您应该会在输出中看到对您的旧公有 DNS 名称的引用，如下所示（旧站点 URL 用红色表示）：

```
<script type='text/javascript' src='http://ec2-52-8-139-223.us-west-1.compute.amazonaws.com/wp-content/themes/twentyfifteen/js/functions.js?ver=20150330'></script>
```

3. 使用以下命令下载 wp-cli。

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

4. 使用以下命令在 WordPress 安装中搜索并替换旧站点 URL。替换您的 EC2 实例的旧站点 URL 和新站点 URL 和到您的 WordPress 安装的路径（通常为 /var/www/html 或 /var/www/html/blog）。

```
[ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/path/to/wordpress/installation --skip-columns=guid
```

5. 在 Web 浏览器中，输入您的 WordPress 博客的新站点 URL 以验证站点是否再次正常运行。如果未正常运行，有关更多信息，请参阅 http://codex.wordpress.org/Changing_The_Site_URL 和 http://codex.wordpress.org/Installing_WordPress#Common_Installation_Problems。

教程：将 Amazon Linux 上的 Apache Web 服务器配置为使用 SSL/TLS

安全套接字层/传输层安全性 (SSL/TLS) 可在 Web 服务器和 Web 客户端之间创建一个加密通道，以防止数据在传输过程中被窃听。本教程介绍如何在运行 Apache Web 服务器的单个 Amazon Linux 实例上手动添加对 SSL/TLS 的支持。[AWS Certificate Manager](#)（本文未作介绍）也是一个不错的选择，尤其适合管理多个域或需要提供商业级服务的情况。

Note

由于历史原因，Web 加密通常简称为 SSL。虽然 Web 浏览器仍支持 SSL，但其后继者协议 TLS 被视为不易受攻击。默认情况下，Amazon Linux 将禁用 SSL 版本 2，本教程还建议禁用 SSL 版本 3，如下所述。有关建议的更新后加密标准的更多信息，请转至 [RFC7568](#)。

Important

这些过程适用于 Amazon Linux。如果您尝试在其他分配的实例上设置 LAMP Web 服务器，则本教程不适合您。有关 Ubuntu 上的 LAMP Web 服务器的信息，请转到 Ubuntu 社区文档 [ApacheMySQLPHP](#) 主题。有关 Red Hat Enterprise Linux 的信息，请转至客户门户网站主题 [Web 服务器](#)。

主题

- [先决条件 \(p. 44\)](#)

- 步骤 1：在服务器上启用 SSL/TLS (p. 44)
- 步骤 2：获取 CA 签名的证书 (p. 45)
- 步骤 3：测试和强化安全配置 (p. 48)
- 故障排除 (p. 50)

先决条件

在开始本教程之前，请完成以下步骤：

- 启动 Amazon Linux 实例。有关更多信息，请参阅 [步骤 1：启动实例 \(p. 21\)](#)。
- 将安全组配置为允许 SSH(端口 22)、HTTP(端口 80) 和 HTTPS(端口 443) 连接。有关更多信息，请参阅 [Amazon EC2 的设置 \(p. 15\)](#)。
- 安装 Apache Web 服务器。有关分步说明，请参阅 [教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)。仅需要 httpd 包及其依赖项；可以忽略涉及 PHP 和 MySQL 的说明。
- SSL/TLS 公钥基础设施 (PKI) 依赖域名系统 (DNS) 来识别和验证网站。如果您计划使用 EC2 实例来托管公共网站，您需要为 Web 服务器注册域名或将现有域名传输给您的 Amazon EC2 主机。可通过许多第三方域注册和 DNS 托管服务来执行此操作，也可以使用 [Amazon Route 53](#) 执行此操作。

步骤 1：在服务器上启用 SSL/TLS

此过程将指导您完成在 Amazon Linux 上使用自签名的数字证书设置 SSL/TLS 的流程。

在服务器上启用 SSL/TLS

1. [连接到您的实例 \(p. 22\)](#) 并确认 Apache 正在运行。

```
[ec2-user ~]$ sudo service httpd status
```

如有必要，启动 Apache。

```
[ec2-user ~]$ sudo service httpd start
```

2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

Note

-y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略此选项。

```
[ec2-user ~]$ sudo yum update -y
```

3. 您的实例现在处于最新状态，可通过安装 Apache 模块 mod_ssl 来添加 SSL/TLS 支持：

```
[ec2-user ~]$ sudo yum install -y mod24_ssl
```

在本教程的后面，您将使用已安装的三个重要文件：

- /etc/httpd/conf.d/ssl.conf

mod_ssl 的配置文件。它包含告知 Apache 以下信息的“指令”：在何处查找加密密钥和证书、允许哪些 SSL/TLS 协议、要使用哪种加密算法。

- /etc/pki/tls/private/localhost.key

针对 Amazon EC2 主机的自动生成的 2048 位 RSA 私有密钥。安装期间，OpenSSL 已使用此密钥生成自签名主机证书，您稍后也可使用此密钥生成证书签名请求 (CSR) 以提交给证书颁发机构 (CA)。

• /etc/pki/tls/certs/localhost.crt

针对服务器主机的自动生成的自签名 X.509 证书。此证书对于测试是否已将 Apache 正确设置为使用 SSL/TLS 来说很有用。

.key 和 .crt 文件均为 PEM 格式，其中包含采用 Base64 编码的 ASCII 字符，并用“BEGIN”和“END”行框起来，如下面的简短证书示例所示：

```
-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDALTb21lU3RhGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bmlOMRkwFwYDVQODDBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZoowZpNWTXjkQ3uFYH6s/
sBwtHpKKZMzOvDedREjNKAvk4ws6F0
WanXWehT6FiSzvB4sTEXXJN2jdw8g
+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSzvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUH0d0BQE8sBJxg==
-----END CERTIFICATE-----
```

文件名和扩展名只是为了提供便利，对功能没有影响；只要 ssl.conf 文件中的相关指令使用相同的名称，您可以将证书命名为 cert.crt、cert.pem 或 certificate.pem。

Note

使用自定义文件替换默认的 SSL 文件时，请确保它们采用 PEM 格式。

4. 重启 Apache。

```
[ec2-user ~]$ sudo service httpd restart
```

5. 现在，您的 Apache Web 服务器应通过端口 443 支持 HTTPS (安全 HTTP)。通过将您的 EC2 实例的 IP 地址或完全限定域名与前缀 https:// 一起键入浏览器 URL 栏中来对其进行测试。由于您正在使用自签名的不可信证书连接到站点，因此您的浏览器可能会显示一系列警告。

忽视这些警告并继续连接站点。如果默认 Apache 欢迎页面打开，则意味着您已在服务器上成功配置 SSL/TLS。现在，浏览器和服务器之间传递的所有数据均已进行安全加密，这可通过浏览器的 URL 栏中的锁定图标反映出来。

为了防止站点访问者遇到警告屏幕，您需要获取一个证书，该证书不仅用于加密，而且还用于公开验证您的站点所有者身份。

步骤 2：获取 CA 签名的证书

本部分介绍了以下流程：从私有密钥生成证书签名请求 (CSR)、将 CSR 提交给证书颁发机构 (CA)、获取签名证书并配置 Apache 以使用该证书。

从加密上来说，自签名 SSL/TLS X.509 证书与 CA 签名的证书相同。二者之间的区别在于社交层面，而非数学层面；CA 承诺，在向申请者颁发证书之前，至少验证域的所有权。每个 Web 浏览器均包含一个 CA 的列表，浏览器供应商信任这些 CA 来执行此操作。X.509 证书主要包含一个与您的私有服务器密钥对应的公有

密钥和一个以加密方式与该公有密钥关联的 CA 的签名。当浏览器通过 HTTPS 连接到 Web 服务器时，服务器将提供证书以便浏览器检查其可信 CA 的列表。如果签署人位于列表上，或可通过一系列其他的可信签署人访问，则浏览器将与服务器协商一个快速加密数据通道并加载页面。

由于验证请求需要投入人力，证书通常会产生费用，因此应货比三家。在 [dmoz.org](#) 上可找到知名 CA 的列表。一些 CA (例如 [StartCom](#)) 免费提供基础级别 (“1 级”) 证书。

密钥是证书的基础。自 2013 年起，[政府](#)和[行业](#)团体建议对 RSA 密钥使用最小密钥 (系数) 大小 2048 位。OpenSSL 在 Amazon Linux 中生成的默认系数大小为 2048 位，意味着现有的自动生成的密钥适用于 CA 签名的证书。下面介绍了适合需要自定义密钥的人员的替代过程，例如，具有较大系数或使用不同加密方法的过程。

获取 CA 签名的证书

1. [连接到您的实例 \(p. 22\)](#)并导航到 /etc/pki/tls/private/。这是存储适用于 SSL/TLS 的服务器私有密钥的目录。如果您希望使用现有主机密钥来生成 CSR，请跳至步骤 3。
2. (可选) 生成新的私有密钥。下面是一些示例密钥配置。任何生成的密钥都将用于 Web 服务器，但它们实施安全的方式和程度有所不同。

1. 以下命令可作为起点，用来创建与实例上默认主机密钥类似的 RSA 密钥：

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 2048
```

生成的文件 `custom.key` 是一个 2048 位 RSA 私有密钥。

2. 要创建系数更大的更严格的 RSA 密钥，请使用以下命令：

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
```

生成的文件 `custom.key` 是一个 4096 位 RSA 私有密钥。

3. 要创建具有密码保护的 4096 位加密的 RSA 密钥，请使用以下命令：

```
[ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key 4096
```

这将生成一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

Important

加密可增强安全性，但由于加密的密钥需要密码，因此依赖于加密密钥的服务无法自动启动。每当您使用此密钥时，都需要通过 SSH 连接提供密码“abcde12345”。

4. RSA 密码术可能相对较慢，因为其安全性依赖于对两个较大质数的乘积进行因子分解的难度。不过，可以为 SSL/TLS 创建使用非 RSA 密码的密钥。在交付同等级别的安全性时，基于椭圆曲线的数学运算的密钥更小更快。示例如下：

```
[ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
```

此示例中的输出为一个使用 prime256v1 (OpenSSL 支持的“命名曲线”) 的 256 位椭圆曲线私有密钥。根据 [NIST](#)，其加密强度略高于 2048 位 RSA 密钥。

Note

并非所有 CA 对基于椭圆曲线的密钥的支持级别与对 RSA 密钥的支持级别相同。

请确保新的私有密钥具有高度限制的权限 (所有者根权限、组根权限、仅面向所有者的读取/写入权限)。命令如下：

```
[ec2-user ~]$ sudo chown root.root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

上述命令应生成以下结果：

```
-rw----- root root custom.key
```

在创建并配置满意的密钥后，可以创建 CSR。

- 使用您首选的密钥创建 CSR；下面的示例将使用 **private.key**：

```
[ec2-user ~]$ sudo openssl req -new -key private.key -out csr.pem
```

OpenSSL 将打开一个对话框，并提示您输入下表中显示的信息。对于基本的经域验证的证书来说，除 Common Name 以外的所有字段都是可选字段。

| 名称 | 说明 | 示例 |
|---------|--|----------------------------------|
| 国家/地区名称 | 代表国家/地区的两个字母 ISO 缩写。 | US (=美国) |
| 州或省名称 | 组织所在州或省的名称。此名称不可使用缩写。 | Washington |
| 所在地名称 | 您的组织所在的位置，例如城市。 | Seattle |
| 组织名称 | 组织的法定全称。请勿缩写组织名称。 | Example Corp |
| 组织部门名称 | 额外的组织信息 (如果有)。 | 示例部门 |
| 公用名 | 此值必须与您希望用户键入浏览器中的 Web 地址完全匹配。通常，这表示以主机名称为前缀的域名或采用 <code>www.example.com</code> 格式的别名。在使用自签名证书且无 DNS 解析的测试中，公用名可能只包含主机名。CA 还提供费用更高的证书，这些证书接受通配符名称 (例如 <code>*.example.com</code>)。 | <code>www.example.com</code> |
| 电子邮件地址 | 服务器管理员的电子邮件地址。 | <code>someone@example.com</code> |

最后，OpenSSL 将提示您输入可选的质询密码。此密码仅适用于 CSR 和您与 CA 之间的事务，因此请遵循 CA 提供的有关此密码以及其他可选字段、可选公司名的建议。CSR 质询密码不会影响服务器操作。

生成的文件 `csr.pem` 包含您的公有密钥、您的公有密钥的数字签名以及您输入的元数据。

- 将 CSR 提交给 CA。这通常包括在文本编辑器中打开 CSR 文件并将内容复制到 Web 表格中。此时，您可能需要提供一个或多个主题备用名称 (SAN) 以放置到证书上。如果 `www.example.com` 是公用名，则 `example.com` 将是一个很好的 SAN，反之亦然。键入列出的任一名称的用户将看到一个无误连接。如果您的 CA Web 表格允许该连接，请在 SAN 列表中包含公用名。(一些 CA 会自动包含公用名。)

在您的请求获得批准后，您将收到一个由 CA 签署的新主机证书。此外，系统可能会指示您下载中间证书文件，该文件包含完成 CA 的信任链所需的其他证书。

- 从 `/etc/pki/tls/certs` 目录删除旧的自签名主机证书 `localhost.crt` 并将新的 CA 签署的证书 (以及任何中间证书) 放置到该目录中。

Note

有多种方法可以将新证书上传到 EC2 实例，但最直接、最有益的方法是在本地计算机及 EC2 实例上各打开一个文本编辑器（如 vi、nano、记事本等），然后在这两者之间复制、粘贴文件内容。这样，一旦有任何权限或路径问题，您会立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

从 /etc/pki/tls/certs 目录内部，检查文件所有权、组和权限设置是否与高度限制的 Amazon Linux 默认权限（所有者根权限、组根权限、仅面向所有者的读取/写入权限）匹配。命令如下：

```
[ec2-user certs]$ sudo chown root.root custom.crt
[ec2-user certs]$ sudo chmod 600 custom.crt
[ec2-user certs]$ ls -al custom.crt
```

上述命令应生成以下结果：

```
-rw----- root root custom.crt
```

中间证书文件的权限并不严格（所有者根权限、组根权限、所有者可写权限、任何人可读权限）。命令如下：

```
[ec2-user certs]$ sudo chown root.root intermediate.crt
[ec2-user certs]$ sudo chmod 644 intermediate.crt
[ec2-user certs]$ ls -al intermediate.crt
```

上述命令应生成以下结果：

```
-rw-r--r-- root root intermediate.crt
```

- 新的 CA 签署的证书的文件名（此示例中为 `custom.crt`）可能与旧证书的不同。使用 Apache 的 `SSLCertificateFile` 指令编辑 `/etc/httpd/conf.d/ssl.conf` 并提供正确的路径和文件名。

```
SSLCertificateFile /etc/pki/tls/certs/custom.crt
```

如果您收到一个中间证书文件（此示例中为 `intermediate.crt`），请使用 Apache 的 `SSLCACertificateFile` 指令提供其路径和文件名。

```
SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
```

- 保存 `/etc/httpd/conf.d/ssl.conf` 并重启 Apache。

```
[ec2-user ~]$ sudo service httpd restart
```

步骤 3：测试和强化安全配置

在 SSL/TLS 可操作且公开发布后，应测试其实际安全性。使用在线服务（例如 [Qualys SSL Labs](#)，该服务可对您的安全设置执行免费的全面分析）可轻松执行此操作。根据结果，您可以决定通过控制接受的协议、首选的密码和排除的密码来强化默认安全配置。有关更多信息，请参阅 [Qualys 如何用公式表示其分数](#)。

Important

实际测试对服务器的安全性非常重要。少量配置错误可能导致严重的安全漏洞和数据丢失。由于建议的安全实践会不断变化以响应调查和新兴威胁，因此定期安全审核对于良好的服务器管理来说是必不可少的。

在 Qualys SSL Labs 站点上，用 www.example.com 格式键入服务器的完全限定域名。约两分钟后，您将收到您站点的评级（从 A 到 F）和结果的详细信息。下表汇总了具有与 Amazon Linux 上的默认 Apache 配置相同的设置的域的报告：

| | |
|------|------|
| 总评 | C |
| 证书 | 100% |
| 协议支持 | 90% |
| 密钥交换 | 90% |
| 密码强度 | 90% |

该报告显示，配置通常是合理的，并且对证书、协议支持、密钥交换和密码强度问题的评级可接受。但该报告还标记了三个漏洞，这些漏洞会导致总体评级降低，应予以修复：

- POODLE 漏洞：2014 年发现的 [POODLE 攻击](#)利用了 SSL 版本 3 中允许攻击者假冒网站的弱点。修复方法很简单：在服务器上禁用 SSL 版本 3 支持。在配置文件 /etc/httpd/conf.d/ssl.conf 中，通过在行的开头键入 "#" 来注释掉以下内容：

```
SSLProtocol all -SSLv2
```

然后，添加以下指令：

```
SSLProtocol -SSLv2 -SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2
```

除了显式禁用 SSL 版本 2 之外，此命令还禁用 SSL 版本 3（安全审核标记的版本）并显式允许 TLS 的所有当前现有版本。现在，服务器将拒绝接受与使用 TLS 之外的任何协议的客户端进行加密连接。指令中冗长的文字可更清楚地告知人类读者服务器的作用。

- RC4 密码支持：密码是加密算法的数学核心。众所周知，用于加密 SSL/TLS 数据流的快速密码 RC4 具有多个[重大弱点](#)。修复方法是在 ssl.conf 中禁用 RC4 支持，此操作将是下一示例中的修复方法的一部分。
- 缺少对前向保密性的支持：[前向保密性](#)是协议的一种功能，该功能使用派生自私有密钥的临时（暂时）会话密钥进行加密。这意味着，在实践中，攻击者无法解密 HTTPS 数据，即使他们拥有 Web 服务器的长期私有密钥。Qualys 的“参考浏览器”列表中的 Web 浏览器都支持前向保密性。

修复 RC4 和前向保密性问题的方法是，自定义 Apache 的允许的密码和禁止的密码的列表，并强制实施强密码优先于弱密码的策略。这需要更改两个配置。

在配置文件 /etc/httpd/conf.d/ssl.conf 中，找到包含用于配置 **sslcipherSuite** 的注释掉示例的部分，注释掉（但保留）当前列表，并添加以下指令：

Note

此处为方便阅读将指令显示为几行，但整个指令必须在一行上且密码名称之间不能有空格。

```
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:  
AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES:!aNULL:!eNULL:  
EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:  
!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
```

这些密码是 OpenSSL 中更长的受支持密码列表的子集。根据以下标准选择这些密码并对其进行排序：

1. 对向前保密性的支持
2. 强度
3. 速度
4. 具体密码位于密码系列之前
5. 允许的密码位于拒绝的密码之前

请注意，高级密码的名称中具有 ECDHE (表示 Elliptic Curve Diffie-Hellman Ephemeral)；ephemeral 表示向前保密性。此外，RC4 现在位于禁止的密码中的结尾处。

建议您使用密码的明确列表，而不依赖于内容不可见的默认值或简短指令。

Important

此处显示的密码列表只是许多可能的列表之一；例如，您可能希望优化列表以加快速度而不是向前保密性。

如果您预计需要支持较旧的客户端，则可以允许 DES-CBC3-SHA 密码套件。

最后，对 OpenSSL 的每次更新将引入新密码并弃用旧密码。使 EC2 Amazon Linux 实例保持最新，关注来自 [OpenSSL](#) 的安全公告，并留意技术出版物中对新安全漏洞的报告。有关更多信息，请参阅 Elastic Load Balancing 用户指南 中的 [Elastic Load Balancing 的预定义 SSL 安全策略](#)。

通过删除“#”取消对以下行的注释：

```
#SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384
```

此命令强制服务器优先选择高级密码，包括（在此示例中）支持向前保密性的密码。启用此指令后，服务器会在回滚到允许的安全性较低的密码之前尝试建立高度安全的连接。

保存编辑后的配置文件后，重启 Apache。

如果您在 [Qualys SSL Labs](#) 上再次测试域，应会发现漏洞已修复，且摘要如下所示：

| | |
|------|------|
| 总评 | A |
| 证书 | 100% |
| 协议支持 | 95% |
| 密钥交换 | 90% |
| 密码强度 | 90% |

故障排除

- 除非我提供密码，否则我的 Apache Web 服务器不会启动。

如果您安装了受密码保护的加密的私有服务器密钥，这是预期行为。

您可以从此密钥上去除加密功能和密码。假设在默认目录中具有一个称为 `custom.key` 的加密的私有 RSA 密钥，并且此密钥上的密码是 `abcde12345`，对 EC2 实例运行以下命令可生成此密钥的未加密版本：

```
[ec2-user ~]$ cd /etc/pki/tls/private/
[ec2-user private]$ sudo cp custom.key custom.key.bak
```

```
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out  
custom.key.nocrypt  
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key  
[ec2-user private]$ sudo chown root.root custom.key  
[ec2-user private]$ sudo chmod 600 custom.key  
[ec2-user private]$ sudo service httpd restart
```

Apache 现在启动时应该不会提示您提供密码。

教程：提高应用程序在 Amazon EC2 上的可用性

假设您一开始在单个 EC2 实例上运行应用程序或网站，随着时间的推移，流量会增加到需要多个实例才能满足需求的数量。您可以从 AMI 启动多个 EC2 实例，然后使用 Elastic Load Balancing 来跨这些 EC2 实例为应用程序分配传入流量。这将提高应用程序的可用性。将实例放置在多个可用区中还可提高应用程序的容错能力。如果一个可用区发生中断，流量将路由到另一个可用区。

您可以使用 Auto Scaling 将您的应用程序的运行中的实例始终保持在最低数量。Auto Scaling 可检测您的实例或应用程序在何时运行状况不佳并自动替换它，从而保持应用程序的可用性。您还可以使用 Auto Scaling，通过您指定的条件来基于需求自动向上或向下扩展 Amazon EC2 容量。

在本教程中，我们将 Auto Scaling 与 Elastic Load Balancing 结合使用，以确保您在负载均衡器后保持指定数量的正常运行的 EC2 实例。请注意，这些实例不需要公有 IP 地址，因为流量会流入负载均衡器，然后再路由到这些实例。有关更多信息，请参阅 [Auto Scaling](#) 和 [Elastic Load Balancing](#)。

内容

- [先决条件 \(p. 51\)](#)
- [对应用程序进行扩展和负载均衡 \(p. 51\)](#)
- [测试负载均衡器 \(p. 53\)](#)

先决条件

本教程假定您已执行以下操作：

1. 如果您没有默认的 Virtual Private Cloud (VPC)，请在两个或更多可用区中利用公有子网创建一个 VPC。有关更多信息，请参阅 [创建 Virtual Private Cloud \(VPC\) \(p. 18\)](#)。
2. 在 VPC 中启动实例。
3. 连接到实例并对其进行自定义。例如，您可以安装软件和应用程序、复制数据和连接更多的 EBS 卷。有关在实例上设置 Web 服务器的信息，请参阅 [教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)。
4. 测试您的实例上的应用程序以确保您的实例配置正确。
5. 从您的实例创建自定义 Amazon 系统映像 (AMI)。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 或 [创建由实例存储支持的 Linux AMI \(p. 78\)](#)。
6. (可选) 如果您不再需要实例，请终止它。
7. 创建一个 IAM 角色，该角色将为您的应用程序授予对所需的 AWS 的访问权限。有关更多信息，请参阅 [使用 IAM 控制台创建 IAM 角色 \(p. 424\)](#)。

对应用程序进行扩展和负载均衡

使用以下过程创建负载均衡器、为您的实例创建启动配置、使用两个或更多实例创建 Auto Scaling 组以及将负载均衡器与 Auto Scaling 组关联。

对应用程序进行扩展和负载均衡

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Create Load Balancer。
4. 选择 Application Load Balancer，然后选择 Continue。
5. 在 Configure Load Balancer 页面上，执行以下操作：
 - a. 对于 Name，键入负载均衡器的名称。例如，`my-lb`。
 - b. 对于 Scheme，保留默认值 internet-facing。
 - c. 对于 Listeners，保留默认值，默认侦听器负责接收端口 80 上的 HTTP 流量。
 - d. 对于 Availability Zones，选择用于实例的 VPC。选择一个可用区，然后选择该可用区的公有子集。针对另一可用区重复这一步骤。
 - e. 选择 Next: Configure Security Settings。
6. 在本教程中，您不使用安全侦听器。选择 Next: Configure Security Groups。
7. 在 Configure Security Groups 页面上，执行以下操作：
 - a. 选择 Create a new security group。
 - b. 为安全组键入名称和描述，或者保留默认名称和描述。这个新的安全组包含一个规则，该规则允许为侦听器配置的流量流入端口。
 - c. 选择 Next: Configure Routing。
8. 在 Configure Routing 页面上，执行以下操作：
 - a. 对于 Target group，保留默认值 New target group。
 - b. 对于 Name，键入目标组的名称。
 - c. 将 Protocol 保留为 HTTP，将 Port 保留为 80。
 - d. 对于 Health checks，保留默认协议和路径。
 - e. 选择 Next: Register Targets。
9. 在 Register Targets 页面上，选择 Next: Review 可继续到下一页，我们将使用 Auto Scaling 向目标组添加 EC2 实例。
10. 在 Review 页面上，选择 Create。创建负载均衡器之后，选择 Close。
11. 在导航窗格中的 AUTO SCALING 上，选择 Launch Configurations。
 - 如果您是首次接触 Auto Scaling，您将看到欢迎页面。选择 Create Auto Scaling group 以启动“Create Auto Scaling Group”向导，然后选择 Create launch configuration。
 - 否则，请选择 Create launch configuration。
12. 在 Choose AMI (选择 AMI) 页面上，选择 My AMIs (我的 AMI) 选项卡，然后选择在先决条件 (p. 51) 中创建的 AMI。
13. 在 Choose Instance Type 页面上，选择实例类型，然后选择 Next: Configure details。
14. 在 Configure details 页面上，执行以下操作：
 - a. 对于 Name，为您的启动配置键入一个名称 (例如，`my-launch-config`)。
 - b. 对于 IAM role，选择您在先决条件 (p. 51) 中创建的 IAM 角色。
 - c. (可选) 如果您需要运行一个启动脚本，请展开 Advanced Details 并在 User data 中键入该脚本。
 - d. 选择 Skip to review。
15. 在 Review 页面上，选择 Edit security groups。您可以选择现有安全组或创建新安全组。此安全组必须允许来自负载均衡器的 HTTP 流量和运行状况检查。如果您的实例将拥有公有 IP 地址，您也可以选择允许 SSH 流量 (前提是您需要连接到该实例)。完成后，请选择 Review。
16. 在 Review 页上选择 Create launch configuration。
17. 在系统提示时，请选择一个现有密钥对、创建一个新的密钥对或在没有密钥对的情况下继续。选中确认复选框，然后选择 Create launch configuration。

18. 创建启动配置后，您必须创建 Auto Scaling 组。
 - 如果您是初次使用 Auto Scaling 并且正在使用“Create Auto Scaling group”向导，则会自动进入下一步。
 - 否则，请选择 Create an Auto Scaling group using this launch configuration。
19. 在 Configure Auto Scaling group details (配置 Auto Scaling 组详细信息) 页面上，执行以下操作：
 - a. 对于 Group name，键入 Auto Scaling 组的名称。例如，`my-asg`。
 - b. 对于 Group size，键入实例数量（例如，`2`）。请注意，建议您在每个可用区中保留数量大致相同的实例。
 - c. 从 Network 中选择您的 VPC，然后从 Subnet 中选择您的两个公有子网。
 - d. 在 Advanced Details 下方，选择 Receive traffic from one or more load balancers。从 Target Groups 中选择您的目标组。
 - e. 选择 Next: Configure scaling policies。
20. 在 Configure scaling policies 页面上，选择 Review，因为我们打算让 Auto Scaling 将组保持在指定大小。请注意，您稍后可以手动扩展此 Auto Scaling 组、根据计划配置要扩展的组或根据需求配置要扩展的组。
21. 在 Review 页面上，选择 Create Auto Scaling group。
22. 创建组后，选择 Close。

测试负载均衡器

当客户端将请求发送到您的负载均衡器时，负载均衡器会将请求路由到已注册实例之一。

测试负载均衡器

1. 验证您的实例已准备就绪。从 Auto Scaling Groups 页面中选择 Auto Scaling 组，然后选择 Instances 选项卡。最初，您的实例处于 Pending 状态。如果状态为 InService，则表示相应实例已就绪。
2. 验证您已向负载均衡器注册您的实例。从 Target Groups 页面中选择目标组，然后选择 Targets 选项卡。如果实例的状态是 initial，可能表示它们仍在注册过程中。当实例状态为 healthy 时，即可供使用。实例就绪后，您可通过以下步骤测试负载均衡器。
3. 从 Load Balancers (负载均衡器) 页面选择您的负载均衡器。
4. 在 Description (描述) 选项卡上，找到 DNS 名称。此名称具有以下形式：

`my-lb-xxxxxxxxxx.us-west-2.elb.amazonaws.com`

5. 在 Web 浏览器中，将负载均衡器的 DNS 名称粘贴到地址栏并按 Enter。您将看到您的网站。

教程：远程管理您的 Amazon EC2 实例

本教程介绍如何从您的本地计算机使用 Systems Manager Run Command 远程管理 Amazon EC2 实例。本教程包含使用 Amazon EC2 控制台、适用于 Windows PowerShell 的 AWS 工具和 AWS Command Line Interface 执行命令的过程。

Note

借助 Run Command，您还可以在本地环境或其他云提供商提供的环境中管理您的服务器和虚拟机 (VM)。有关更多信息，请参阅[在混合环境中设置 Systems Manager](#)。

开始前的准备工作

您必须为 Systems Manager 配置 AWS Identity and Access Management (IAM) 实例配置文件。将 AmazonEC2RoleforSSM 角色附加到 Amazon EC2 实例。借助该角色，实例能够与 Systems Manager API 通信。有关如何将角色附加到现有实例的更多信息，请参阅[将 IAM 角色连接到实例 \(p. 427\)](#)。

您还必须为 Systems Manager 配置您的 IAM 用户账户，如下一节中所述。

向您的用户账户授予对 Systems Manager 的访问权限

必须对您的用户账户进行配置，以便与 SSM API 进行通信。使用下面的过程将托管 AWS Identity and Access Management (IAM) 策略附加到您的用户账户，以便向您授予对 SSM API 操作的完全访问权。

为您的用户账户创建 IAM 策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在导航窗格中，选择 Policies。(如果这是您首次使用 IAM，请选择 Get Started，然后选择 Create Policy。)
3. 在 Filter 字段中，键入 **AmazonSSMFullAccess** 并按 Enter。
4. 选中 AmazonSSMFullAccess 旁边的复选框，然后依次选择 Policy Actions 和 Attach。
5. 在 Attach Policy 页面上，选择您的用户账户，然后选择 Attach Policy。

安装 SSM 代理 (Linux)

SSM 代理处理 Run Command 请求并配置在该请求中指定的实例。默认情况下，此代理将安装在 Windows 实例上。不过，您必须在 Linux 上手动安装此代理。以下过程介绍如何在 Red Hat Enterprise Linux (RHEL) 上安装代理。有关如何在 Ubuntu、Amazon Linux 或 CentOS 上安装代理的信息，请参阅[在 Linux 上安装 SSM 代理](#)。

在 Red Hat Enterprise Linux 上安装 SSM 代理

1. 连接到您的 RHEL 实例并在该实例上创建临时目录。

```
mkdir /tmp/ssm
```

2. 使用以下命令之一将 SSM 安装程序下载到临时目录中。

64 位

```
curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm -o /tmp/ssm/amazon-ssm-agent.rpm
```

32 位

```
curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_386/amazon-ssm-agent.rpm -o /tmp/ssm/amazon-ssm-agent.rpm
```

3. 运行 SSM 安装程序。

```
sudo yum install -y /tmp/ssm/amazon-ssm-agent.rpm
```

4. 运行以下命令之一，确定 SSM 代理是否在运行。该命令应返回“amazon-ssm-agent is running”。

RHEL 7.x

```
sudo systemctl status amazon-ssm-agent
```

RHEL 6.x

```
sudo status amazon-ssm-agent
```

5. 如果上一个命令返回“amazon-ssm-agent is stopped”，则执行以下命令。

- a. 启动服务。

RHEL 7.x

```
sudo systemctl start amazon-ssm-agent
```

RHEL 6.x

```
sudo start amazon-ssm-agent
```

- b. 检查代理的状态。

RHEL 7.x

```
sudo systemctl status amazon-ssm-agent
```

RHEL 6.x

```
sudo status amazon-ssm-agent
```

使用 EC2 控制台发送命令

使用下面的过程，列出通过从 Amazon EC2 控制台使用 Run Command 在实例上运行的所有服务。

从控制台使用 Run Command 执行命令

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Run Command。
3. 选择 Run a command。
4. 对于 Command document，选择 AWS-RunPowerShellScript (针对 Windows 实例) 和 AWS-RunShellScript (针对 Linux 实例)。
5. 对于 Target instances，选择您创建的实例。如果您没有看到该实例，请确保您当前位于创建实例时使用的区域。另外，按照前文所述，确保您已配置 IAM 角色和信任策略。
6. 对于 Commands，键入 **Get-Service** (针对 Windows) 或 **ps -aux | less** (针对 Linux)。
7. (可选) 对于 Working Directory，指定要将命令运行于的 EC2 实例上的文件夹的路径。
8. (可选) 对于 Execution Timeout，指定 EC2Config 服务或 SSM 代理在超时和失败前将尝试运行命令的秒数。
9. 对于 Comment，我们建议提供将帮助您在命令列表中标识此命令的信息。
10. 对于 Timeout (seconds)，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。
11. 选择 Run 执行命令。Run Command 将显示一个状态屏幕。选择 View result。
12. 要查看输出，请选择适用于该命令的命令调用，选择 Output 选项卡，然后选择 View Output。

有关如何使用 Run Command 执行命令的更多示例，请参阅[使用 Systems Manager Run Command 执行命令](#)。

使用适用于 Windows PowerShell 的 AWS 工具 发送命令

使用下面的过程，列出通过从 适用于 Windows PowerShell 的 AWS 工具 使用 Run Command 在实例上运行的所有服务。

执行命令

1. 在本地计算机上，下载最新版本的 [适用于 Windows PowerShell 的 AWS 工具](#)。
2. 在本地计算机上打开 适用于 Windows PowerShell 的 AWS 工具 并执行以下命令来指定凭证。

```
Set-AWSCredentials -AccessKey key -SecretKey key
```

3. 执行以下命令设置 PowerShell 会话的区域。指定您在前面的步骤中创建实例时使用的区域。此示例使用 us-west-2 区域。

```
Set-DefaultAWSRegion -Region us-west-2
```

4. 执行以下命令来检索在实例上运行的服务。

```
Send-SSMCommand -InstanceId 'Instance-ID' -DocumentName AWS-RunPowerShellScript -  
Comment 'listing services on the instance' -Parameter @{'commands'=@('Get-Service')}
```

命令将返回一个命令 ID，您将使用该 ID 来查看结果。

5. 以下命令返回原始实例 Send-SSMCommand 的输出。输出在 2500 个字符后被截断。要查看完整服务列表，请在命令中使用 -OutputS3BucketName *bucket_name* 参数指定 Amazon S3 存储桶。

```
Get-SSMCommandInvocation -CommandId Command-ID -Details $true | select -ExpandProperty  
CommandPlugins
```

有关如何将 Run Command 与 Windows PowerShell 工具 结合使用来执行命令的更多示例，请参阅[使用 适用于 Windows PowerShell 的 AWS 工具 的 Systems Manager Run Command 演练](#)。

使用 AWS CLI 发送命令

使用下面的过程，列出通过从 AWS CLI 使用 Run Command 在实例上运行的所有服务。

执行命令

1. 在您的本地计算机上，下载最新版本的 [AWS Command Line Interface \(AWS CLI\)](#)。
2. 在本地计算机上打开 AWS CLI 并执行以下命令来指定凭证和区域。

```
aws configure
```

3. 系统将提示您指定以下内容。

```
AWS Access Key ID [None]: key  
AWS Secret Access Key [None]: key  
Default region name [None]: region, for example us-east-1  
Default output format [None]: ENTER
```

4. 执行以下命令来检索在实例上运行的服务。

```
aws ssm send-command --document-name "AWS-RunShellScript" --comment "listing services"
--instance-ids "Instance-ID" --parameters commands="service --status-all" --region us-
west-2 --output text
```

命令将返回一个命令 ID，您将使用该 ID 来查看结果。

5. 以下命令返回原始实例 Send-SSMCommand 的输出。输出在 2500 个字符后被截断。要查看完整服务列表，您需要在命令中使用 --output-s3-bucket-name *bucket_name* 参数指定 Amazon S3 存储桶。

```
aws ssm list-command-invocations --command-id "command ID" --details
```

有关如何使用 AWS CLI 通过 Run Command 执行命令的更多示例，请参阅[使用 AWS CLI 的 Systems Manager Run Command 演练](#)。

相关内容

有关 Run Command 和 Systems Manager 的更多信息，请参阅以下主题和参考资料。

- [Amazon EC2 Systems Manager 用户指南](#)
- [Amazon EC2 Systems Manager API Reference](#)
- [Systems Manager 适用于 Windows PowerShell 的 AWS 工具 Reference](#)
- [Systems Manager AWS Command Line Interface Reference](#)
- [AWS 软件开发工具包](#)

有关视频，请参阅[AWS 说明视频和实验室](#)。

Amazon 系统映像 (AMI)

Amazon 系统映像 (AMI) 提供启动实例 (云中的虚拟服务器) 所需的信息。您在启动实例时指定 AMI，可以从该 AMI 启动所需任意数量的实例。您还可以根据需要从任意多个不同 AMI 启动实例。

AMI 包括以下内容：

- 一个用于实例 (例如，操作系统、应用程序服务器和应用程序) 根卷的模板
- 控制可以使用 AMI 启动实例的 AWS 账户的启动许可
- 一个指定在实例启动时要附加到实例的卷的块储存设备映射。

使用 AMI

下图总结了 AMI 生命周期。创建并注册一个 AMI 之后，您可以将其用于启动新实例。(如果 AMI 拥有者向您授予启动许可，则您也可以从 AMI 启动实例。)您可以将 AMI 复制到同一区域或不同区域。当您完成从 AMI 启动实例时，可以取消注册 AMI。

您可以搜索符合您实例条件的 AMI。您可以搜索 AWS 提供的 AMI 或社区提供的 AMI。有关更多信息，请参阅 [AMI 类型 \(p. 59\)](#) 和 [查找 Linux AMI \(p. 62\)](#)。

连接到某个实例之后，您可以像使用任何其他服务器那样使用该实例。有关启动、连接和使用实例的信息，请参阅 [Amazon EC2 实例 \(p. 135\)](#)。

创建您自己的 AMI

可以自定义从公用 AMI 启动的实例，然后将配置保存为自定义 AMI 以供自己使用。从 AMI 启动的实例使用您的所有自定义项。

实例的根存储设备确定创建 AMI 所遵循的过程。实例的根卷是 Amazon EBS 卷或实例存储卷。有关信息，请参阅 [Amazon EC2 根设备卷 \(p. 11\)](#)。

要创建由 Amazon EBS 支持的 AMI，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。要创建由实例存储支持的 AMI，请参阅[创建由实例存储支持的 Linux AMI \(p. 78\)](#)。

您可以为 AMI 分配自定义标签，以帮助您对 AMI 进行分类和管理。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 626\)](#)。

购买、共享和出售 AMI

创建 AMI 之后，您可以将其设为私有，这样只有您才能使用它，也可以与指定的 AWS 账户列表进行共享。您还可以选择公开您的自定义 AMI，以供社区使用。如果遵循一些简单的指导，为公共使用构建安全、可靠、可用的 AMI 的过程可以很简单。有关如何创建和使用共享 AMI 的信息，请参阅[共享 AMI \(p. 64\)](#)。

您可以从第三方购买 AMI，包括具有 Red Hat 等组织的服务合同的 AMI。您还可以创建 AMI 并将其出售给其他 Amazon EC2 用户。有关购买或出售 AMI 的更多信息，请参阅[付费 AMI \(p. 72\)](#)。

取消注册您的 AMI

使用完 AMI 之后，可以取消注册它。取消注册 AMI 之后，便无法将其用于启动新实例。有关更多信息，请参阅[取消注册您的 AMI \(p. 121\)](#)。

Amazon Linux

Amazon Linux AMI 是 AWS 提供、支持和维护的 Linux 映像。以下是一些 Amazon Linux 功能：

- 稳定、安全和高性能的执行环境，适用于 Amazon EC2 上运行的应用程序。
- 对于 Amazon EC2 用户没有额外费用。
- 对多个版本的 MySQL、PostgreSQL、Python、Ruby、Tomcat 及许多常见软件包的存储库访问权限。
- 定期更新以包括最新组件，这些更新也可在 yum 存储库中使用，适用于安装在运行中的实例上。
- 包括可与 AWS 服务轻松集成的软件包，如 AWS CLI、Amazon EC2 API 和 AMI 工具、适用于 Python 的 Boto 库以及 Elastic Load Balancing 工具。

有关更多信息，请参阅[Amazon Linux \(p. 123\)](#)。

AMI 类型

可以基于以下特性选择要使用的 AMI：

- 区域 (请参阅[地区和可用区域 \(p. 7\)](#))
- 操作系统
- 架构 (32 位或 64 位)
- 启动许可 (p. 59)
- 根设备存储 (p. 60)

启动许可

AMI 的拥有者通过指定启动许可来确定其可用性。启动许可分为以下类别。

| 启动许可 | 说明 |
|------|----------------------|
| 公有 | 拥有者向所有 AWS 账户授予启动许可。 |
| 显式 | 拥有者向特定 AWS 账户授予启动许可。 |

| 启动许可 | 说明 |
|------|--------------------|
| 隐式 | 拥有者拥有 AMI 的隐式启动许可。 |

Amazon 和 Amazon EC2 社区提供了大量的公用 AMI。有关更多信息，请参阅 [共享 AMI \(p. 64\)](#)。开发人员可以为其 AMI 收费。有关更多信息，请参阅 [付费 AMI \(p. 72\)](#)。

根设备存储

所有 AMI 均可归类为由 Amazon EBS 支持或由实例存储支持。前者是指从 AMI 启动的实例的根设备是从 Amazon EBS 快照创建的 Amazon EBS 卷。后者是指从 AMI 启动的实例的根设备是从存储在 Amazon S3 中的模板创建的实例存储卷。有关更多信息，请参阅 [Amazon EC2 根设备卷 \(p. 11\)](#)。

本节总结了两种类型的 AMI 之间的重要区别。下表简要总结了这些区别。

| 性能 | 由 Amazon EBS 支持 | 由 Amazon 实例存储支持 |
|-----------|---|--|
| 启动时间 | 通常不到 1 分钟 | 通常不到 5 分钟 |
| 大小限制 | 16 TiB | 10 GiB |
| 根设备卷 | Amazon EBS 卷 | 实例存储卷 |
| 数据持久性 | 默认情况下，当实例终止时，将删除根卷。 [*] 默认情况下，实例终止后，任何其他 Amazon EBS 卷上的数据将会保留。任意实例存储卷上的数据仅在实例的生命周期内保留。 | 任意实例存储卷上的数据仅在实例的生命周期内保留。默认情况下，实例终止后，任何 Amazon EBS 卷上的数据将会保留。 |
| 升级 | 实例停止后，实例类型、内核、RAM 磁盘和用户数据仍可更改。 | 实例存在期间，实例属性是稳定不变的。 |
| 收费 | 您需要为实例使用、Amazon EBS 卷 使用以及将 AMI 存储为 Amazon EBS 快照付费。 | 您需要为实例使用以及在 Amazon S3 中存储 AMI 付费。 |
| AMI 创建/捆绑 | 使用单一命令/调用 | 需要安装和使用 AMI 工具 |
| 停止状态 | 可置于停止状态，在该状态下，实例不运行，但是根卷可在 Amazon EBS 中保留 | 不可置于停止状态；实例正在运行或已终止 |

* 默认情况下，Amazon EBS 支持的实例根卷的 `DeleteOnTermination` 标志设置为 `true`。有关如何更改此标志以便卷在终止之后保留的信息，请参阅 [将根设备卷更改为持久保留 \(p. 13\)](#)。

确定 AMI 的根设备类型

使用控制台确定 AMI 的根设备类型

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，单击 AMI，然后选择 AMI。
3. 在 Details (详细信息) 选项卡中检查 Root Device Type 的值，如下所示：
 - 如果值是 `ebs`，则是 Amazon EBS 支持的 AMI。
 - 如果值是 `instance store`，则是实例存储支持的 AMI。

使用命令行确定 AMI 的根设备类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

停止状态

您可以停止由 Amazon EBS 支持的实例，但不能停止由 Amazon EC2 实例存储支持的实例。停止操作会导致实例停止运行（它的状态会由 `running` 变成 `stopping` 再到 `stopped`）。停止的实例保留在 Amazon EBS 中，这样就可重新启动。停止与终止不同；您无法重新启动一个已终止的实例。因为由 Amazon EC2 实例存储支持的 AMI 不能被停止，所以这些 AMI 要么在运行要么已经终止。有关实例停止可能会发生情况及您可以执行哪些操作的更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

默认数据存储和持久性

使用实例存储卷作为根设备的实例自动具有可用的实例存储（根卷包含根分区并且您可以存储其他数据）。如果实例失败或终止，实例存储卷上的所有数据将被删除（根设备上的数据除外）。您可以通过附加一个或多个 Amazon EBS 卷向您的实例添加持久性存储。

使用 Amazon EBS 作为根设备的实例自动附加 Amazon EBS 卷。该卷像其他卷一样显示在您的卷列表中。默认情况下，实例不使用任何可用的实例存储卷。您可以使用块储存设备映射添加实例存储或其他 Amazon EBS 卷。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。有关停止实例时实例存储卷可能发生的状况的信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

启动时间

比起由 Amazon EC2 实例存储支持的 AMI，由 Amazon EBS 支持的 AMI 的启动速度更快。当您启动由 Amazon EC2 实例存储支持的 AMI 时，必须先从 Amazon S3 中检索所有部件才能使用该实例。使用由 Amazon EBS 支持的 AMI 时，仅需从快照中检索启动实例所需的分段，然后即可使用该实例。但是，使用 Amazon EBS 卷作为根设备的实例在从快照中检索剩余分段并加载到卷中的这一小段时间内会运行地较为缓慢。当您停止和重新启动实例时，实例可快速启动，因为实例状态已存储在 Amazon EBS 卷中。

AMI 创建

要创建由实例存储支持的 Linux AMI，您必须使用 Amazon EC2 AMI 工具在您的实例上创建来自实例的 AMI。

AMI 创建对于由 Amazon EBS 支持的 AMI 来说要容易得多。`CreateImage` API 操作创建由 Amazon EBS 支持的 AMI 并为其注册。AWS 管理控制台中还有一个按钮能让您从正在运行的实例中创建 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。

如何向您收费

如果您使用由实例存储支持的 AMI，您需要为 AMI 存储和实例使用付费。如果您使用由 Amazon EBS 支持的 AMI，除了 AMI 和实例使用费用之外，您还需要为卷的存储和使用付费。

如果您使用由 Amazon EC2 实例存储支持的 AMI，当您每次自定义以及新建一个 AMI 时，所有分段都存储在每个 AMI 的 Amazon S3 中。因此，每个定制 AMI 的存储占用空间都是 AMI 的完整大小。对于由 Amazon EBS 支持的 AMI，当您每次自定义以及新建 AMI 时，将仅存储更改内容。因此，您之后自定义的 AMI 的存储占用空间比首次自定义的 AMI 要小得多，从而降低 AMI 存储费用。

当由 Amazon EBS 支持的实例停止时，您无需再为实例使用付费；但是，您仍需为卷存储付费。每次从停止状态转换到运行状态，即使您在一小时内进行多次状态转换，我们都按一个完整实例小时收费。例如，假设您的实例每小时的实例收费为 0.10 USD。如果您要运行该实例一小时，中途不停止，您将被收取

0.10 USD。如果您在一小时内停止并重新启动该实例两次，您将因该使用小时被收取 0.30 USD (最初 0.10 USD，加上 2 x 每次重新启动 0.10 USD)。

Linux AMI 虚拟化类型

Linux Amazon 系统映像 使用两种虚拟化类型之一：半虚拟化 (PV) 或硬件虚拟机 (HVM)。半虚拟化和 HVM AMI 之间的主要区别在于它们的启动方式，以及它们能否使用特定硬件扩展 (CPU、网络和存储) 实现更好的性能。

为获得最佳性能，建议您在启动您的实例时使用最新一代的实例类型和 HVM AMI。有关最新一代实例类型的更多信息，请参阅 [Amazon EC2 实例](#) 详细信息页面。如果您正在使用上一代实例类型并且想升级，请参阅 [升级路径](#)。

有关建议的针对每个实例类型的 Amazon Linux AMI 的类型的信息，请参阅 [Amazon Linux AMI 实例类型](#) 详细信息页面。

HVM AMI

硬件虚拟机 AMI 配有一组完全虚拟化的硬件，通过执行映像根块储存设备的主启动记录来启动。通过此虚拟化类型可以直接在虚拟机上运行操作系统而不进行任何修改 (如同它在裸机硬件上运行一样)。Amazon EC2 主机系统可模拟向客户机提供的部分或所有底层硬件。

与半虚拟化客户机不同，硬件虚拟机客户机可以利用硬件扩展快速访问主机系统上的底层硬件。有关 Amazon EC2 中可用的 CPU 虚拟化扩展的更多信息，请参阅 Intel 网站上的 [英特尔虚拟化技术](#)。硬件虚拟机 AMI 需要利用增强联网和 GPU 处理。要将指令传递给专用网络和 GPU 设备，操作系统需要能够访问本机硬件平台；HVM 虚拟化提供这种访问。有关更多信息，请参阅 [增强联网 \(p. 492\)](#) 和 [Linux 加速计算实例 \(p. 150\)](#)。

当前一代的所有实例类型都支持 HVM AMI。CC2、CR1、HI1 和 HS1 上一代实例类型支持 HVM AMI。

要查找 HVM AMI，请使用控制台或 [describe-images](#) 命令验证 AMI 的虚拟化类型是否已设置为 `hvm`。

PV AMI

PV AMI 使用名为 PV-GRUB 的特殊启动加载程序启动，该加载程序开始启动循环，然后对您的映像链式加载 `menu.lst` 文件中指定的内核。半虚拟化来宾可以在没有显式虚拟化支持的主机硬件上运行，但无法利用特殊硬件扩展 (如增强联网或 GPU 处理)。以往，半虚拟化来宾在许多情况下的性能优于 HVM 来宾，但是由于硬件虚拟机虚拟化的功能增强以及 HVM AMI 可使用半虚拟化驱动程序，情况发生了改变。有关 PV-GRUB 及其在 Amazon EC2 中的使用情况的更多信息，请参阅 [用户提供的内核 \(p. 129\)](#)。

C3 和 M3 最新一代实例类型支持 PV AMI。C1、HI1、HS1、M1、M2 和 T1 上一代实例类型支持 PV AMI。

要查找 PV AMI，请使用控制台或 [describe-images](#) 命令验证 AMI 的虚拟化类型是否已设置为 `paravirtual`。

硬件虚拟机上的半虚拟化

以往，半虚拟化客户机在存储和网络操作方面的性能要优于硬件虚拟机客户机，因为它们可以对 I/O 使用特殊驱动程序，从而避免模拟网络和磁盘硬件的开销，而硬件虚拟机客户机必须将这些指令转换为模拟的硬件。现在，这些半虚拟化驱动程序可用于硬件虚拟机客户机，因此无法移植到半虚拟化环境中运行的操作系统 (如 Windows) 仍可以使用它们获取存储和网络 I/O 方面的性能优势。借助这些硬件虚拟机驱动程序上的半虚拟化，硬件虚拟机客户机可以获得与半虚拟化客户机相同甚至更佳的性能。

查找 Linux AMI

启动实例之前，必须选择要使用的 AMI。选择 AMI 时，对于将启动的实例，可能需要考虑以下要求：

- 区域

- 操作系统
- 架构 : 32 位 (i386) 或 64 位 (x86_64)
- 根设备类型 : Amazon EBS 或实例存储
- 提供商 : Amazon Web Services、Oracle、IBM、Microsoft 或社区

如果您需要查找 Windows AMI，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[查找 Windows AMI](#)。

内容

- [使用 Amazon EC2 控制台查找 Linux AMI \(p. 63\)](#)
- [使用 AWS CLI 查找 AMI \(p. 63\)](#)

使用 Amazon EC2 控制台查找 Linux AMI

您可以使用 Amazon EC2 控制台查找 Linux AMI。您可以使用 Images (映像) 页面搜索所有可用 AMI，或者，在使用控制台启动实例时，使用 Quick Launch (快速启动) 选项卡在常用 AMI 中选择。

使用“Images (映像)”页面查找 Linux AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择区域。您可以选择向您提供的任何区域，无需理会您身处的位置。这是您将在其中启动实例的区域。
3. 在导航窗格中，选择 AMIs。
4. (可选) 使用 Filter (筛选条件) 选项将显示的 AMI 列表范围确定为仅限您关注的 AMI。例如，要列出 AWS 提供的所有 Linux AMI，请选择 Public images (公有映像)。选择搜索栏，从菜单中选择 Owner，然后选择 Amazon images。再次选择搜索栏以选择 Platform，然后从提供的列表中选择操作系统。
5. (可选) 选择 Show/Hide Columns 图标以选择要显示的映像属性，例如根设备类型。或者，可以从列表中选择 AMI，然后在 Details (详细信息) 选项卡中查看其属性。
6. 选择 AMI 之前，请确认它是由实例存储支持还是由 Amazon EBS 支持并了解此差异的影响，这十分重要。有关更多信息，请参阅[根设备存储 \(p. 60\)](#)。
7. 要从此 AMI 启动实例，请选择该实例，然后选择 Launch。有关使用控制台启动实例的更多信息，请参阅[从 AMI 启动实例 \(p. 245\)](#)。如果您没有准备好立即启动实例，请记下 AMI ID (ami-xxxxxxxx) 以供将来使用。

在您启动实例时查找 Linux AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从控制台控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面的 Quick Start (快速启动) 选项卡上，从列表中选择一个常用的 AMI。如果您没有看到所需的 AMI，请选择 AWS Marketplace 或 Community AMIs (社区 AMI) 选项卡来查找其他 AMI。

使用 AWS CLI 查找 AMI

您可以使用命令行参数仅列出感兴趣的 AMI 类型。例如，您可以按如下所示使用 `describe-images` 命令查找由您或者 Amazon 拥有的公用 AMI。

```
$ aws ec2 describe-images --owners self amazon
```

将以下筛选条件添加到上一个命令以便仅显示 Amazon EBS 支持的 AMI：

```
--filters "Name=root-device-type,Values=ebs"
```

找到满足您需要的 AMI 之后，记下其 ID (ami-xxxxxxxx)。您可以使用此 AMI 启动实例。有关更多信息，请参阅 AWS Command Line Interface 用户指南 中的[使用 AWS CLI 启动实例](#)。

共享 AMI

共享 AMI 是开发人员创建并可供其他开发人员使用的 AMI。要开始使用 Amazon EC2，最简单的方法之一是使用共享 AMI，您可以从中获得所需的组件，然后添加自定义内容。您还可以创建自己的 AMI 并与他人共享。

使用共享 AMI 需自行承担风险。Amazon 不保证其他 Amazon EC2 用户共享的 AMI 的完整性或安全性。因此，您应该像处理其他您可能会考虑在自己的数据中心部署的外来代码一样处理共享 AMI，对其执行适当的功能调查。我们建议您从可靠来源获取 AMI。如果您对某个共享 AMI 有任何问题或意见，请访问[AWS 论坛](#)。

Amazon 的公有映像的拥有者有一个别名，在账户字段中显示为 amazon。这使您可以轻松地从 Amazon 查找 AMI。其他用户不能对其 AMI 使用别名。

有关创建 AMI 的信息，请参阅[创建实例存储支持的 Linux AMI](#) 或[创建 Amazon EBS 支持的 Linux AMI](#)。有关在 AWS Marketplace 中构建、交付和维护应用程序的更多信息，请参阅[AWS Marketplace 用户指南](#) 和[AWS Marketplace 卖方指南](#)。

内容

- [查找共享 AMI \(p. 64\)](#)
- [将 AMI 设为公用 \(p. 66\)](#)
- [将 AMI 与特定 AWS 账户共享 \(p. 67\)](#)
- [使用书签 \(p. 68\)](#)
- [共享 Linux AMI 指导原则 \(p. 68\)](#)

查找共享 AMI

可以使用 Amazon EC2 控制台或命令行查找共享 AMI。

查找共享 AMI (控制台)

使用控制台查找共享的私有 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 AMIs。
3. 在第一个筛选条件中，选择 Private images。将列出已与您共享的所有 AMI。要细化您的搜索，可选择搜索栏并使用菜单中提供的筛选条件选项。

使用控制台查找共享的公用 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 AMIs。
3. 在第一个筛选条件中，选择 Public images。要细化您的搜索，可选择搜索栏并使用菜单中提供的筛选条件选项。
4. 使用筛选条件仅列出您需要的 AMI 类型。例如，依次选择 Owner : 和 Amazon images 可仅显示 Amazon 的公有映像。

查找共享 AMI (命令行)

使用命令行工具查找共享的公用 AMI

使用 [describe-images](#) 命令 (AWS CLI) 可以列出 AMI。可以将该列表范围确定为所需的 AMI 类型，如以下示例所示。

以下命令使用 `--executable-users` 选项列出所有公用 AMI。此列表包括您拥有的所有公用 AMI。

```
$ aws ec2 describe-images --executable-users all
```

以下命令列出您对其拥有显式启动许可的 AMI。此列表不包括您拥有的任何此类 AMI。

```
$ aws ec2 describe-images --executable-users self
```

以下命令列出 Amazon 拥有的 AMI。Amazon 的公用 AMI 的拥有者有一个别名，在账户字段中显示为 `amazon`。这使您可以轻松地从 Amazon 查找 AMI。其他用户不能对其 AMI 使用别名。

```
$ aws ec2 describe-images --owners amazon
```

以下命令列出指定 AWS 账户拥有的 AMI。

```
$ aws ec2 describe-images --owners 123456789012
```

要减少显示的 AMI 数量，请使用筛选条件只列出您感兴趣的 AMI 类型。例如，使用以下筛选条件可以只显示 EBS 支持的 AMI。

```
--filters "Name=root-device-type,Values=ebs"
```

或者，您可以使用以下适用于 Windows PowerShell 的 AWS 工具命令：[Get-EC2Image](#)。

使用共享 AMI

使用共享 AMI 之前，应执行以下步骤以确认没有预安装证书允许第三方对您的实例进行不希望的访问，并且没有可能将敏感数据传输给第三方的预配置远程登录。查看 AMI 使用的 Linux 发行版的文档以了解有关提高系统安全性 的信息。

为了确保您不会在无意中丢失对您实例的访问，我们建议您启动两个 SSH 会话并将第二个会话保持为打开状态，直到您删除了无法识别的证书并确认您仍可以使用 SSH 登录您的实例。

1. 标识并禁用任何未经授权的公有 SSH 密钥。该文件中的唯一密钥应是您用于启动 AMI 的密钥。以下命令查找 `authorized_keys` 文件：

```
$ sudo find / -name "authorized_keys" -print -exec cat {} \;
```

2. 对根用户禁用基于密码的身份验证。打开 `ssh_config` 文件并编辑 `PermitRootLogin` 行，如下所示：

```
PermitRootLogin without-password
```

或者，您可以禁用以根身份登录实例的功能：

```
PermitRootLogin No
```

重启 `sshd` 服务。

3. 检查是否有任何其他用户账户能够登录您的实例。具有超级用户权限的账户尤为危险。删除或锁定任何未知账户的密码。
4. 检查打开的端口以确认您未在使用和运行侦听传入连接的网络服务。
5. 要防止预配置的远程登录，应删除现有配置文件并重启 rsyslog 服务。例如：

```
$ sudo rm /etc/  
rsyslog.config  
$ sudo service rsyslog restart
```

6. 确认所有 cron 任务是合法的。

如果您发现了认为存在安全风险的公用 AMI，请联系 AWS 安全团队。有关更多信息，请参阅 [AWS 安全中心](#)。

将 AMI 设为公用

Amazon EC2 使您能与其他 AWS 账户共享您的 AMI。您可以允许所有 AWS 账户启动 AMI (将 AMI 设置为公用)，也可以仅允许几个特定的账户启动 AMI (请参阅[将 AMI 与特定 AWS 账户共享 \(p. 67\)](#))。当其他 AWS 账户启动您的 AMI 时，不会向您收费；只会向启动 AMI 的账户收取费用。

AMI 是一种区域性资源。因此，共享 AMI 可使其能够在其他区域使用。要使 AMI 能够在其他区域使用，请将该 AMI 复制到目标区域并共享。有关更多信息，请参阅[复制 AMI \(p. 117\)](#)。

要避免在共享 AMI 时泄露敏感数据，请阅读[共享 Linux AMI 指导原则 \(p. 68\)](#)中的安全注意事项并遵循建议的操作。

Note

如果 AMI 有产品代码，则不能将其设为公用。只能将 AMI 与特定 AWS 账户共享。

与所有 AWS 账户分享 AMI (控制台)

将 AMI 设置为公用后，当您使用控制台在相同区域启动实例时，Community AMIs 中会出现该 AMI。请注意，将某个 AMI 设置为公用之后，可能需要一点时间 Community AMIs 中才会显示该 AMI。将某个 AMI 再次设置为私有后，也可能需要一点时间才能将它从 Community AMIs 中删除。

使用控制台共享公用 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 AMIs。
3. 从列表中选择您的 AMI，然后选择 Actions、Modify Image Permissions。
4. 选择 Public，然后选择 Save。

与所有 AWS 账户共享 AMI (命令行)

每个 AMI 都有一个 `launchPermission` 属性，用于控制允许哪些 AWS 账户 (除拥有者账户外) 使用该 AMI 启动实例。通过修改 AMI 的 `launchPermission` 属性，可以将 AMI 设为公用 (这会向所有 AWS 账户授予启动权限) 或仅将其与指定的 AWS 账户共享。

您可以在具有 AMI 启动权限的账户的列表中添加或从中删除账户 ID。要将 AMI 设为公用，请指定 `all` 组。公用和显式启动许可都可以指定。

将 AMI 设为公用

使用 [modify-image-attribute](#) 命令 (AWS CLI) 可以将 `all` 组添加到指定 AMI 的 `launchPermission` 列表中，如下所示。

```
$ aws ec2 modify-image-attribute --image-id ami-12345678 --launch-permission "{\"Add\": [{\"Group\": \"all\"}]}"
```

要验证 AMI 的启动许可，请使用以下 [describe-image-attribute](#) 命令。

```
$ aws ec2 describe-image-attribute --image-id ami-12345678 --attribute launchPermission
```

(可选) 要再次将 AMI 设为私有，请从其启动许可中删除 all 组。请注意，AMI 的拥有者始终具有启动许可，因此不受此命令影响。

```
$ aws ec2 modify-image-attribute --image-id ami-12345678 --launch-permission "{\"Remove\": [{\"Group\": \"all\"}]}"
```

或者，您可以使用以下适用于 Windows PowerShell 的 AWS 工具命令：[Edit-EC2ImageAttribute](#) 和 [Get-EC2ImageAttribute](#)。

将 AMI 与特定 AWS 账户共享

您可以在不将 AMI 设为公用的情况下，与特定 AWS 账户共享 AMI。您只需要 AWS 账户 ID 即可。

AMI 是一种区域性资源。因此，共享 AMI 可使其能够在其他区域使用。要使 AMI 能够在其他区域使用，请将该 AMI 复制到目标区域并共享。有关更多信息，请参阅 [复制 AMI \(p. 117\)](#)。

共享 AMI (控制台)

使用控制台授予显式启动许可

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 AMIs。
3. 在列表中选择您的 AMI，然后选择 Actions、Modify Image Permissions。
4. 在 AWS Account Number 字段中指定您想与之共享 AMI 的用户的 AWS 账号，然后选择 Add Permission。

要与多个用户共享此 AMI，请重复上述步骤，直至您添加完所需全部用户。

5. 要允许创建快照的卷权限，请选择 Add "create volume" permissions to the following associated snapshots when creating permissions。

Note

您不需要为了共享 AMI 而共享 AMI 引用的 Amazon EBS 快照。只需共享 AMI 本身；系统自动为实例提供访问所引用 Amazon EBS 快照的权限以便启动。

6. 完成后选择 Save。

共享 AMI (命令行)

使用 [modify-image-attribute](#) 命令 (AWS CLI) 可以共享 AMI，如以下示例所示。

要授予显式启动许可

以下命令向指定 AWS 账户授予指定 AMI 的启动许可。

```
$ aws ec2 modify-image-attribute --image-id ami-12345678 --launch-permission "{\"Add\": [{\"UserId\": \"123456789012\"}]}"
```

以下命令为快照授予创建卷的权限。

```
$ aws ec2 modify-snapshot-attribute --snapshot-id snap-1234567890abcdef0 --attribute createVolumePermission --operation-type add --user-ids 123456789012
```

要删除账户的启动许可

以下命令从指定 AWS 账户中删除指定 AMI 的启动许可：

```
$ aws ec2 modify-image-attribute --image-id ami-12345678 --launch-permission "{\"Remove\": [{\"UserId\": \"123456789012\"}]}"
```

以下命令为快照授予删除卷的权限。

```
$ aws ec2 modify-snapshot-attribute --snapshot-id snap-1234567890abcdef0 --attribute createVolumePermission --operation-type remove --user-ids 123456789012
```

要删除所有的启动许可

以下命令从指定 AMI 中删除所有公用和显式启动许可。请注意，AMI 的拥有者始终具有启动许可，因此不受此命令影响。

```
$ aws ec2 reset-image-attribute --image-id ami-12345678 --attribute launchPermission
```

或者，您可以使用以下适用于 Windows PowerShell 的 AWS 工具 命令：[Edit-EC2ImageAttribute](#)。

使用书签

如果您创建了公用 AMI，或与其他 AWS 用户共享了 AMI，您可以创建一个书签来允许用户访问您的 AMI 并允许他们立即在自己的账户中启动一个实例。这是共享 AMI 引用的一种简单方法，借助这种方法，用户无需花时间来查找您的 AMI 即可使用。

请注意，您的 AMI 必须为公用，否则必须与您要向其发送书签的用户共享它。

为您的 AMI 创建书签

1. 在 URL 中键入以下信息，其中 <region> 是您的 AMI 所属的区域，<ami_id> 是 AMI 的 ID：

```
https://console.aws.amazon.com/ec2/v2/home?  
region=<region>#LaunchInstanceWizard:ami=<ami_id>
```

举例来说，该 URL 从 us-east-1 区域的 ami-12345678 AMI 启动实例：

```
https://console.aws.amazon.com/ec2/v2/home?region=us-  
east-1#LaunchInstanceWizard:ami=ami-12345678
```

2. 将链接分发给那些想要使用您的 AMI 的用户。
3. 要使用书签，请选择链接或将其复制并粘贴到您的浏览器中。启动向导打开，同时 AMI 已被选定。

共享 Linux AMI 指导原则

使用以下指南可缩小攻击面并提高您创建的 AMI 的可靠性。

Note

任何安全指南都不是详尽无遗的。请仔细构建您的共享 AMI，并花时间考虑可能导致暴露敏感数据的位置。

主题

- 在启动时更新 AMI 工具 (p. 69)
- 对根禁用基于密码的远程登录 (p. 69)
- 禁用本地根访问 (p. 70)
- 删除 SSH 主机密钥对 (p. 70)
- 安装公有密钥证书 (p. 70)
- 禁用 sshd DNS 检查 (可选) (p. 71)
- 标识您的身份 (p. 71)
- 保护自己 (p. 71)

如果为 AWS Marketplace 构建 AMI，请参阅[为 AWS Marketplace 构建 AMI](#)，以了解指导原则、策略和最佳实践。

有关安全共享 AMI 的更多信息，请参阅以下文章：

- [How To Share and Use Public AMIs in A Secure Manner](#)
- [Public AMI Publishing: Hardening and Clean-up Requirements](#)

在启动时更新 AMI 工具

对于实例存储支持型 AMI，我们建议您的 AMI 在启动期间下载和更新 Amazon EC2 AMI 创建工具。这可确保基于您的共享 AMI 的新 AMI 拥有最新的 AMI 工具。

对于 [Amazon Linux](#)，请将以下内容添加到 `/etc/rc.local`：

```
# Update the Amazon EC2 AMI tools
echo " + Updating EC2 AMI tools"
yum update -y aws-amitools-ec2
echo " + Updated EC2 AMI tools"
```

使用此方法自动更新您映像上的其他软件。

Note

确定自动更新何种软件时，要考虑到此更新将产生的 WAN 流量 (您的用户将为此付费)，以及更新破坏 AMI 上其他软件的风险。

对于其他分配，请确保您拥有最新的 AMI 工具。

对根禁用基于密码的远程登录

为公用 AMI 使用固定的根密码是一种很快为人知晓的安全风险。甚至于用户在第一次登录后更改密码都会给可能的滥用以可乘之机。

要解决此问题，请对根用户禁用基于密码的远程登录。

对根禁用基于密码的远程登录

1. 用文字编辑器打开 `/etc/ssh/sshd_config` 文件并查找以下行：

```
#PermitRootLogin yes
```

2. 将行更改为：

```
PermitRootLogin without-password
```

若您的分配不同或您不在运行 OpenSSH，此配置文件的位置可能也会不同。若情况如此，请咨询相关文档。

禁用本地根访问

在使用共享 AMI 时，最佳做法是禁用直接根登录。为此，请登录到您正在运行的实例并发出以下命令：

```
[ec2-user ~]$ sudo passwd -l root
```

Note

此命令不影响 sudo 的使用。

删除 SSH 主机密钥对

如果您计划共享源自公用 AMI 的 AMI，请删除 /etc/ssh 中的现有 SSH 主机密钥对。这会促使 SSH 在有人使用您的 AMI 启动实例时生成新的独特 SSH 密钥对，从而提高安全性并降低“中间人”攻击可能性。

删除系统上存在的以下所有密钥文件。

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

您可以使用以下命令安全地删除所有这些文件。

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

Warning

安全删除实用工具（例如 `shred`）可能不会删除存储介质中某个文件的所有副本。文件的隐藏副本可能是由日志文件系统（包括 Amazon Linux 默认 ext4）、快照、备份、RAID 和临时缓存创建的。有关更多信息，请参阅 [shred 文档](#)。

Important

如果您忘记从您的公用 AMI 中删除现有 SSH 主机密钥对，我们的例行审核过程会通知您和所有运行您的 AMI 实例的客户存在潜在安全风险。短暂的宽限期过后，我们会将 AMI 标记为私有。

安装公用密钥证书

配置 AMI 以防止使用密码进行登录后，您必须确保用户能用另一种机制登录。

Amazon EC2 允许用户在启动实例时指定公用–私有密钥对名称。向 `RunInstances` API 调用提供有效的密钥对名称后（或通过命令行 API 工具），公用密钥（Amazon EC2 在至 `CreateKeyPair` 或 `ImportKeyPair` 的调用后在服务器上保留的密钥对的部分）通过针对实例元数据的 HTTP 查询供实例使用。

要通过 SSH 登录，您的 AMI 必须在启动时检索密钥值并将该值附加到 `/root/.ssh/authorized_keys` (或 AMI 上任何其他用户账户的等效密钥)。用户可使用密钥对启动您的 AMI 的实例，并在不需要根密码的情况下进行登录。

许多发布版 (包括 Amazon Linux 和 Ubuntu) 使用 `cloud-init` 软件包为配置的用户插入公有密钥证书。如果您的分发版本不支持 `cloud-init`，则可以将以下代码添加到系统启动脚本 (如 `/etc/rc.local`)，以提取您在启动时为 `root` 用户指定的公有密钥。

```
if [ ! -d /root/.ssh ] ; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 700 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

这一点适用于任何用户账户；您不需要将其限制为 `root`。

Note

根据此 AMI 进行的实例重新捆绑包括启动时所用的密钥。要防止密钥被包含，您必须清除 (或删除) `authorized_keys` 文件或将此文件排除在重新捆绑之外。

禁用 sshd DNS 检查 (可选)

禁用 sshd DNS 检查会稍微减弱您的 `sshd` 安全性。但是，如果 DNS 解析失败，SSH 的登录仍然有效。如果您未禁用 `sshd` 检查，DNS 解析失败后会阻止所有的登录。

要禁用 sshd DNS 检查

1. 用文字编辑器打开 `/etc/ssh/sshd_config` 文件并查找以下行：

```
#UseDNS yes
```

2. 将行更改为：

```
UseDNS no
```

Note

若您的分配不同或您不在运行 OpenSSH，此配置文件的位置也会不同。若情况如此，请咨询相关文档。

标识您的身份

目前，没有简单的方法来了解谁提供了共享 AMI，因为每个 AMI 都由账户 ID 代表。

我们建议您将您的 AMI 描述和 AMI ID 发布在 [Amazon EC2 forum](#) 中。这可为有兴趣尝试新的共享 AMI 的用户提供方便的中心位置。您还可以将 AMI 发布到[Amazon 系统映像 \(AMI\)](#) 页面。

保护自己

前述各节介绍如何使您的共享 AMI 成为安全、有保障的可用 AMI，以供启动它们的用户使用。本节描述了保护您不受您的 AMI 用户影响的指南。

我们不建议您将敏感数据或软件存储在您共享的任何 AMI 上。启动共享 AMI 的用户可能能够重新捆绑 AMI 并能自行注册 AMI。遵循上述指南可助您避免一些容易被忽视的安全风险：

- 我们建议对 `ec2-bundle-vol` 使用 `--exclude directory` 选项，以跳过包含您不想在捆绑中包含的机密信息的所有目录和子目录。具体而言，在捆绑映像时，排除所有用户拥有的 SSH 公有/私有密钥对和 SSH `authorized_keys` 文件。Amazon 公用 AMI 会将它们存储在 `/root/.ssh`（对于 `root` 账户）和 `/home/user_name/.ssh/`（对于常规用户账户）中。有关更多信息，请参阅 [ec2-bundle-vol \(p. 85\)](#)。
- 务必在捆绑前删除外壳程序历史记录。如果您在同一 AMI 中多次尝试捆绑上传，外壳程序历史中会包含您的秘密访问密钥。以下示例应为从实例内部捆绑前执行的最后一个命令。

```
[ec2-user ~]$ shred -u ~/.history
```

Warning

以上警告中描述的 `shred` 的限制在此处也适用。

请注意，`bash` 在退出时会将当前会话的历史记录写入磁盘。如果您在删除 `~/.bash_history` 后注销您的实例，然后重新登录，您将发现 `~/.bash_history` 已重新创建且包含上一会话期间执行的所有命令。

`Bash` 以外的其他程序也会将历史记录写入磁盘，请谨慎使用并删除或排除不必要的点文件和点目录。

- 捆绑正在运行的实例需要您的私有密钥和 X.509 证书。将上述密钥和证书以及其他证书放置到未予捆绑的位置（如实例存储）。

付费 AMI

付费 AMI 是可以从开发人员处购买的 AMI。

Amazon EC2 与 AWS Marketplace 集成，使开发人员能够向使用其 AMI 的其他 Amazon EC2 用户收取费用或提供实例支持。

AWS Marketplace 是一个在线商店，您可以从中购买在 AWS 上运行的软件，包括可用来启动 EC2 实例的 AMI。AWS Marketplace AMI 分为各种类别（如开发人员工具），您可以根据自己的要求查找产品。有关 AWS Marketplace 的更多信息，请参阅 [AWS Marketplace](#) 站点。

从付费 AMI 启动实例与从任何其他 AMI 启动实例的方式相同。不需要额外参数。实例根据 AMI 拥有者设置的费率以及相关 Web 服务的标准使用费（例如，在 Amazon EC2 中运行 `m1.small` 实例类型的小时费率）来收费。还可能需要支付其他税款。付费 AMI 拥有者可以确认是否使用该付费 AMI 启动特定实例。

Important

Amazon DevPay 不再接受新的卖家或产品。AWS Marketplace 现在是通过 AWS 销售软件和服务的统一电子商务平台。有关如何从 AWS Marketplace 部署和销售软件的信息，请参阅[在 AWS Marketplace 上出售](#)。AWS Marketplace 支持受 Amazon EBS 支持的 AMI。

主题

- [出售 AMI \(p. 73\)](#)
- [查找付费 AMI \(p. 73\)](#)
- [购买付费 AMI \(p. 73\)](#)
- [获取实例的产品代码 \(p. 74\)](#)
- [使用付费支持 \(p. 74\)](#)
- [付费和支持 AMI 的账单 \(p. 75\)](#)
- [管理 AWS Marketplace 订阅 \(p. 75\)](#)

出售 AMI

您可以使用 AWS Marketplace 销售 AMI。AWS Marketplace 提供组织有序的购物体验。此外，AWS Marketplace 还支持 AWS 功能，如 Amazon EBS 支持的 AMI、预留实例和竞价型实例。

有关如何在 AWS Marketplace 上出售 AMI 的信息，请参阅[在 AWS Marketplace 上出售](#)。

查找付费 AMI

有几种方法可查找可供您购买的 AMI。例如，您可以使用 [AWS Marketplace](#)、Amazon EC2 控制台或命令行。开发人员自己也可能向您介绍付费 AMI。

使用控制台查找付费 AMI

使用控制台查找付费 AMI

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，单击 AMIs。
3. 从第一个 Filter (筛选条件) 列表中选择 Public images (公有映像)。单击搜索栏并选择 Product Code (产品代码)，然后选择 Marketplace (市场)。再次单击搜索栏并选择 Platform，然后从列表中选择操作系统。

使用 AWS Marketplace 查找付费 AMI

使用 AWS Marketplace 查找付费 AMI

1. 打开 [AWS Marketplace](#)。
2. 在搜索框中输入操作系统的名称，然后单击 Go (开始)。
3. 要进一步确定结果范围，请使用一种类别或筛选条件。
4. 每个产品都使用其产品类型进行标记：AMI 或 Software as a Service。

使用命令行查找付费 AMI

您可以使用 `describe-images` 命令 (AWS CLI) 查找付费 AMI，如下所示。

```
$ aws ec2 describe-images --owners aws-marketplace
```

此命令返回描述每个 AMI 的大量详细信息，包括付费 AMI 的产品代码。`describe-images` 的输出包含一个用于产品代码的条目，如下所示：

```
"ProductCodes": [  
    {  
        "ProductCodeId": "product_code",  
        "ProductCodeType": "marketplace"  
    }  
,
```

或者，您可以使用以下适用于 Windows PowerShell 的 AWS 工具命令：[Get-EC2Image](#)。

购买付费 AMI

必须先注册 (购买) 付费 AMI，然后才能使用该 AMI 启动实例。

通常情况下，付费 AMI 的卖方会为您提供 AMI 的相关信息，包括其价格以及购买网站链接。单击该链接时，首先会提示您登录 AWS，然后可以购买 AMI。

使用控制台购买付费 AMI

可以使用 Amazon EC2 启动向导购买付费 AMI。有关更多信息，请参阅 [启动 AWS Marketplace 实例 \(p. 250\)](#)。

使用 AWS Marketplace 订阅产品

要使用 AWS Marketplace，必须拥有 AWS 账户。要从 AWS Marketplace 产品启动实例，必须注册以使用 Amazon EC2 服务，并且必须订阅从中启动实例的产品。可通过两种方式在 AWS Marketplace 中订阅产品：

- AWS Marketplace 网站：您可以使用一键部署功能快速启动预配置的软件。
- Amazon EC2 启动向导：您可以直接从向导搜索 AMI 并启动实例。有关更多信息，请参阅 [启动 AWS Marketplace 实例 \(p. 250\)](#)。

从开发人员处购买付费 AMI

通过付费 AMI 的开发人员，可以购买 AWS Marketplace 中未列出的付费 AMI。开发人员为您提供用于通过 Amazon 购买产品的链接。您可以使用 Amazon.com 证书登录，选择存储在您的 Amazon.com 账户中的信用卡以在购买 AMI 时使用。

获取实例的产品代码

可以使用实例元数据检索实例的 AWS Marketplace 产品代码。有关检索元数据的更多信息，请参阅 [实例元数据和用户数据 \(p. 295\)](#)。

要检索产品代码，请使用以下查询：

```
$ GET http://169.254.169.254/latest/meta-data/product-codes
```

如果实例具有产品代码，则 Amazon EC2 将返回产品代码。例如：

```
774F4FF8
```

使用付费支持

Amazon EC2 还使开发人员可以为软件（或派生 AMI）提供支持。开发人员可以创建您可注册使用的支持产品。在注册支持产品的过程中，开发人员会为您提供产品代码，您必须将该代码与您自己的 AMI 关联起来。这样，开发人员就能确认您的实例有获取支持的权限。此外，还能确保您在运行产品实例时，按照开发人员指定的产品使用条款付费。

Important

不能将支持产品用于预留实例。通常情况下，您需按支持产品卖方指定的价格付费。

要将产品代码与您的 AMI 相关联，请使用以下命令之一，其中，`ami_id` 是 AMI 的 ID，`product_code` 是产品代码：

- [modify-image-attribute \(AWS CLI\)](#)

```
$ aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- [Edit-EC2ImageAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

您设置产品代码属性后，该属性不能被更改或删除。

付费和支持 AMI 的账单

在每个月月底，您会收到一封电子邮件，邮件里注明了该月因使用任何付费和受支持的 AMI 所产生的信用卡付费金额情况。这个账单与您的常规 Amazon EC2 账单是分开的。有关更多信息，请参阅[为 AWS Marketplace 产品付费](#)。

管理 AWS Marketplace 订阅

在 AWS Marketplace 网站上，您可以检查订阅详细信息，查看供应商的使用说明，管理订阅等。

检查订阅详细信息

1. 登录 [AWS Marketplace](#)。
2. 单击 Your Account (我的账户)。
3. 单击 Manage Your Software Subscriptions (管理软件订阅)。
4. 会列出当前所有订阅。单击 Usage Instructions (使用说明) 查看使用产品的特定说明，例如，用于连接到运行中的实例的用户名称。

取消 AWS Marketplace 订阅

1. 确保您终止了从订阅运行的所有实例。
 - a. 打开 Amazon EC2 控制台。
 - b. 在导航窗格中，单击 Instances。
 - c. 选择实例，单击 Actions (操作)，选择 Instance State (实例状态)，然后选择 Terminate (终止)。出现提示时，单击 Yes, Terminate (是，终止)。
2. 登录 [AWS Marketplace](#)，单击 Your Account (我的账户)，然后单击 Manage Your Software Subscriptions (管理软件订阅)。
3. 单击 Cancel subscription (取消订阅)。会提示您确认取消。

Note

取消了订阅之后，您无法再从该 AMI 启动任何实例。要再次使用该 AMI，需要在 AWS Marketplace 网站上或通过 Amazon EC2 控制台中的启动向导重新订阅它。

创建 Amazon EBS 支持的 Linux AMI

要创建 Amazon EBS 支持的 Linux AMI，请通过从 Amazon EBS 支持的现有 Linux AMI 启动的实例开始进行。这可能是您从 AWS Marketplace 获取的 AMI，使用 [AWS Server Migration Service](#) 或 [VM Import/Export](#) 创建的 AMI，或您可访问的任何其他 AMI。根据您自己的需要自定义该实例之后，请创建和注册新 AMI，您可以使用它来启动具有这些自定义项的新实例。有关创建 Amazon EBS 支持的 Windows AMI 的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[创建 Amazon EBS 支持的 Windows AMI](#)。

下述过程适用于由加密的 Amazon EBS 卷（包括根卷）支持的 Amazon EC2 实例，也适用于未加密卷。

用于由实例存储支持的 AMI 的 AMI 创建过程有些不同。有关 Amazon EBS 支持的实例和实例存储支持的实例之间的差别以及如何确定实例的根设备类型的更多信息，请参阅[根设备存储 \(p. 60\)](#)。有关创建实例存储支持的 Linux AMI 的更多信息，请参阅[创建由实例存储支持的 Linux AMI \(p. 78\)](#)。

创建 Amazon EBS 支持的 AMI 的概述

首先，从类似于您要创建的 AMI 的 AMI 启动实例。您可以连接到您的实例并进行自定义。正确配置实例后，通过在创建 AMI 和映像之前停止实例来确保数据完整性。当您创建 Amazon EBS 支持的 AMI 时，我们会自动为您注册它。

Amazon EC2 先切断实例的电源再创建 AMI，以确保创建过程中实例上的所有内容均停止并保持一致状态。如果您确信您的实例处于适合 AMI 创建的一致状态，则可以告知 Amazon EC2 不断电和重启实例。一些文件系统（例如 XFS）可以冻结和解冻活动，因此能在不重启实例的情况下安全创建映像。

在 AMI 创建过程中，Amazon EC2 会创建您实例的根卷和附加到您实例的任何其他 EBS 卷的快照。如果有任何附加到实例的卷进行了加密，则新 AMI 只会在支持 Amazon EBS 加密的实例上成功启动。有关更多信息，请参阅[Amazon EBS Encryption \(p. 568\)](#)。

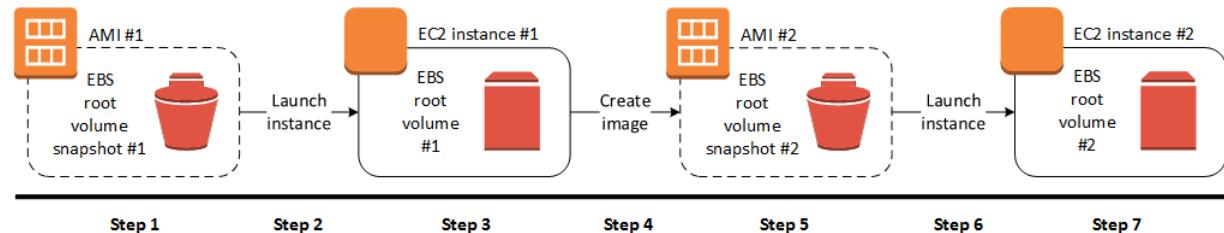
根据卷的大小，可能需要几分钟才能完成 AMI 创建过程（有时长达 24 小时）。您可能发现在创建 AMI 之前创建卷快照更有效。这样，创建 AMI 时就只需创建小的增量快照，且创建过程完成得更快（快照创建的总时间保持不变）。有关更多信息，请参阅[创建 Amazon EBS 快照 \(p. 559\)](#)。

该过程完成之后，您便具有从实例的根卷创建的新 AMI 和快照。当您使用新 AMI 启动实例时，我们会使用快照为其根卷创建新 EBS 卷。AMI 和快照都会对您的账户产生费用，直至您删除它们。有关更多信息，请参阅[取消注册您的 AMI \(p. 121\)](#)。

如果除了根设备卷之外，您还向实例添加了实例存储卷或 EBS 卷，则新 AMI 的块储存设备映射包含这些卷的信息，并且您从新 AMI 启动的实例的块储存设备映射自动包含这些卷的信息。新实例的块储存设备映射中指定的实例存储卷是新的，不包含用于创建 AMI 的实例的实例存储卷中的任何数据。EBS 卷上的数据会持久保留。有关更多信息，请参阅[块储存设备映射 \(p. 609\)](#)。

从实例创建 Linux AMI

可以使用 AWS 管理控制台或命令行创建 AMI。下图总结了从正在运行的 EC2 实例创建 Amazon EBS 支持的 AMI 的过程。从现有 AMI 开始，启动一个实例，自定义该实例，从该实例创建新 AMI，并最终启动新 AMI 的实例。下图中的步骤与下面的过程中的步骤匹配。



使用控制台从实例创建 AMI

- 选择适当的由 EBS 支持的 AMI 作为新 AMI 的起始点，并在启动前根据需要对其进行配置。有关更多信息，请参阅[启动实例 \(p. 244\)](#)。
- 选择 Launch 以启动您选择的由 EBS 支持的 AMI 实例。接受默认值，以按向导逐步操作。有关更多信息，请参阅[启动实例 \(p. 244\)](#)。
- 在实例运行时连接到该实例。

您可以对您的实例执行以下任何操作，以便根据您的需求自定义该实例：

- 安装软件和应用程序
- 复制数据

- 通过删除临时文件、对您的硬盘进行碎片整理以及将可用空间清零来缩短启动时间
- 连接其他 Amazon EBS 卷

(可选) 创建所有附加到您实例的卷的快照。有关创建快照的更多信息，请参阅[创建 Amazon EBS 快照 \(p. 559\)](#)。

在导航窗格中，选择 Instances，然后选择您的实例。依次选择 Actions、Image 和 Create Image。

Tip

如果此选项处于禁用状态，则表明您的实例不是 Amazon EBS 支持的实例。

4. 在 Create Image 对话框中，指定以下字段的值，然后选择 Create Image。

名称

映像的唯一名称。

说明

(可选) 映像的描述 (最多 255 个字符)。

默认情况下，Amazon EC2 将关闭实例，为附加的任意卷拍摄快照，创建和注册 AMI，然后重新启动实例。如果不希望关闭实例，请选择 No reboot。

Warning

如果您选择 No reboot 选项，则我们无法保证所创建映像的文件系统完整性。

您可以修改根卷、Amazon EBS 卷和实例存储卷，方法如下：

- 要更改根卷的大小，请在 Type (类型) 列中找到 Root (根) 卷，然后填写 Size (大小) 字段。
 - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的 Amazon EBS 卷，请在列表中找到该 EBS 卷，然后选择 Delete。
 - 要添加 Amazon EBS 卷，请依次选择 Add New Volume、Type 和 EBS，然后填写字段。然后，当您从新 AMI 启动实例时，这些额外的卷会自动附加到该实例。您必须格式化并安装空卷。您必须安装基于快照的卷。
 - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的实例存储卷，请在列表中找到卷，然后选择 Delete。
 - 要添加实例存储卷，请依次选择 Add New Volume、Type 和 Instance Store，然后从 Device 列表中选择设备名称。当您从新 AMI 启动实例时，这些额外的卷会自动初始化并挂载。这些卷不包含您的 AMI 所基于的运行实例的实例存储卷上的数据。
5. 在创建 AMI 时，您可以选择导航窗格中的 AMIs 以查看其状态。最初，状态将为 pending。几分钟后，状态应更改为 available。
 - (可选) 选择导航窗格中的 Snapshots 以查看为新 AMI 创建的快照。您从此 AMI 启动实例时，我们使用此快照创建其根设备卷。
 6. 从新 AMI 启动实例。有关更多信息，请参阅[启动实例 \(p. 244\)](#)。
 7. 正在运行的新实例包含您在之前的步骤中应用的所有自定义项。

使用命令行从实例创建 AMI

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [create-image](#) (AWS CLI)
- [New-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

从快照创建 Linux AMI

如果您有实例的根设备卷的快照，则可以使用 AWS 管理控制台或命令行从此快照创建 AMI。

Important

某些 Linux 分配 (如 Red Hat Enterprise Linux (RHEL) 和 SUSE Linux Enterprise Server (SLES)) 使用与 AMI 关联的 Amazon EC2 `billingProduct` 代码来验证程序包更新的订阅状态。从 EBS 快照创建 AMI 不会保留此账单代码，并且从此类 AMI 启动的后续实例不能连接到程序包更新基础设施。

同样，虽然您可以从快照中创建一个 Windows AMI，但是您不能从该 AMI 中成功启动实例。

一般来说，AWS 不建议从快照手动创建 AMI。

有关创建 Windows AMI 或创建必须保持 AMI 账单代码正常工作的适用于 Linux 操作系统的 AMI 的更多信息，请参阅[从实例创建 Linux AMI \(p. 76\)](#)。

使用控制台从快照创建 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 Elastic Block Store 下，选择 Snapshots。
3. 依次选择快照、Actions 和 Create Image。
4. 在 Create Image from EBS Snapshot 对话框中，填写与创建 AMI 相关的字段，然后选择 Create。如果要重新创建父实例，请选择与父实例相同的选项。
 - Architecture：对 32 位选择 i386，对 64 位选择 x86_64。
 - Root device name：输入相应的根卷名称。有关更多信息，请参阅[Linux 实例上的设备命名 \(p. 608\)](#)。
 - Virtualization type：选择是从此 AMI 使用半虚拟化 (PV) 还是硬件虚拟机 (HVM) 虚拟化启动实例。有关更多信息，请参阅[Linux AMI 虚拟化类型 \(p. 62\)](#)。
 - (仅限 PV 虚拟化类型) Kernel ID 和 RAM disk ID：从列表中选择 AKI 和 ARI。如果选择默认 AKI 或不选择 AKI，则每次使用此 AMI 启动实例时系统都会要求您指定 AKI。此外，如果默认 AKI 与实例不兼容，对您的实例进行的运行状况检查可能会失败。
 - (可选) Block Device Mappings：添加卷或扩展 AMI 根卷的默认大小。有关调整实例上的文件系统大小以扩展卷的更多信息，请参阅[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。

使用命令行从快照创建 AMI

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `register-image` (AWS CLI)
- `Register-EC2Image` (适用于 Windows PowerShell 的 AWS 工具)

创建由实例存储支持的 Linux AMI

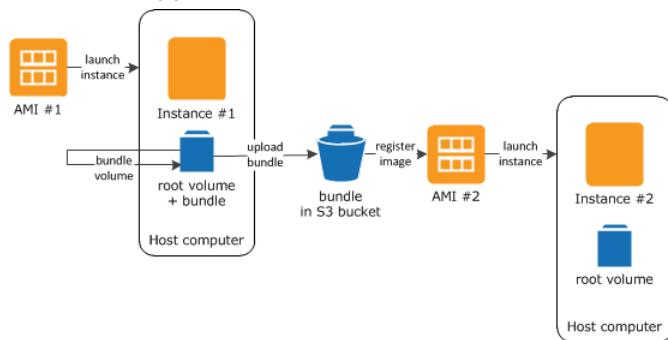
要创建由实例存储支持的 Linux AMI，请通过从由实例存储支持的现有 Linux AMI 启动的实例开始进行。根据您自己的需要自定义该实例之后，请捆绑卷并注册新 AMI，您可以使用该 AMI 启动具有这些自定义项的新实例。

如果您需要创建实例存储支持的 Windows AMI，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[创建实例存储支持的 Windows AMI](#)。

用于由实例存储支持的 AMI 的 AMI 创建过程有些不同。有关 Amazon EBS 支持的实例和实例存储支持的实例之间的差别，以及如何确定实例的根设备类型的更多信息，请参阅[根设备存储 \(p. 60\)](#)。如果您需要创建 Amazon EBS 支持的 Linux AMI，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。

由实例存储支持的 AMI 的创建过程概述

下图总结了从由实例存储支持的实例创建 AMI 的过程。



首先，从类似于您要创建的 AMI 的 AMI 启动实例。您可以连接到您的实例并进行自定义。根据您的需要设置好实例后，您可以捆绑它。完成捆绑过程需要几分钟的时间。该过程完成后，会有一个捆绑，由映像清单 (`image.manifest.xml`) 和文件 (`image.part.xx`) 组成，文件中包含根卷模板。接下来，将该捆绑上传到 Amazon S3 存储桶，然后注册您的 AMI。

当您使用新 AMI 启动实例时，我们会使用您上传到 Amazon S3 的捆绑为实例创建根卷。Amazon S3 中的捆绑使用的存储空间会使您的账户产生费用，直到将其删除。有关更多信息，请参阅 [取消注册您的 AMI \(p. 121\)](#)。

如果除了根设备卷之外，您还向实例添加实例存储卷，则新 AMI 的块储存设备映射包含这些卷的信息，并且您从新 AMI 启动的实例的块储存设备映射自动包含这些卷的信息。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。

先决条件

必须先完成以下任务才能创建 AMI：

- 安装 AMI 工具。有关更多信息，请参阅 [设置 AMI 工具 \(p. 80\)](#)。
- 安装 AWS CLI。有关更多信息，请参阅 [开始设置 AWS Command Line Interface](#)。
- 确保您具有用于捆绑的 Amazon S3 存储桶。要创建 Amazon S3 存储桶，请打开 Amazon S3 控制台，然后单击 Create Bucket (创建存储桶)。或者，您可以使用 AWS CLI `mb` 命令。
- 确保您拥有您的 AWS 账户 ID。有关更多信息，请参阅 AWS General Reference 中的 [AWS 账户标识符](#)。
- 确保您拥有您的访问密钥 ID 和私有访问密钥。有关更多信息，请参阅 AWS General Reference 中的 [访问密钥](#)。
- 确保您拥有 X.509 证书以及相应的私有密钥。
 - 如果您需要创建 X.509 证书，请参阅 [管理签名证书 \(p. 100\)](#)。X.509 证书和私有密钥用于加密和解密您的 AMI。
 - [中国 (北京)] 使用 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem` 证书。
 - [AWS GovCloud (US)] 使用 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` 证书。
- 连接到您的实例并进行自定义。例如，您可以安装软件和应用程序、复制数据、删除临时文件及修改 Linux 配置。

主题

- [设置 AMI 工具 \(p. 80\)](#)
- [通过实例存储支持的 Amazon Linux 实例创建 AMI \(p. 104\)](#)
- [通过实例存储支持的 Ubuntu 实例创建 AMI \(p. 108\)](#)
- [将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI \(p. 113\)](#)

设置 AMI 工具

您可以使用 AMI 工具创建和管理实例存储支持的 Linux AMI。要使用这些工具，必须在您的 Linux 实例上安装它们。AMI 工具可作为 RPM 提供，也为不支持 RPM 的 Linux 发行版提供 .zip 格式的文件。有关更多信息，请参阅 [Amazon EC2 AMI 工具](#)。

Note

仅实例存储支持的 Linux 实例支持 AMI 工具。要创建 Amazon EBS 支持的 AMI，请改为使用 [create-image](#) AWS CLI 命令。要创建实例存储支持的 Windows AMI，请参阅[创建实例存储支持的 Windows AMI](#)。

使用 RPM 设置 AMI 工具

1. 使用您的 Linux 发行版的程序包管理器(如 yum)安装 Ruby。例如：

```
$ sudo yum install -y ruby
```

2. 使用 wget 或 curl 等工具下载 RPM 文件。例如：

```
$ sudo wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. 使用以下命令安装 RPM：

```
$ sudo yum install ec2-ami-tools.noarch.rpm
```

4. 使用以下命令验证您的 AMI 工具安装。

```
$ ec2-ami-tools-version
```

Note

如果您收到加载错误，例如 `cannot load such file -- ec2/amitools/version` (`LoadError`)，请完成下一步将您的 AMI 工具的安装位置添加到您的 `RUBYLIB` 路径中。

5. (可选) 如果您在上一步中收到了错误，则将您的 AMI 工具的安装位置添加到您的 `RUBYLIB` 路径中。

- a. 运行以下命令以确定要添加的路径：

```
$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

在以上示例中，前面的加载错误提示的缺失文件位于 `/usr/lib/ruby/site_ruby` 和 `/usr/lib64/ruby/site_ruby` 位置。

- b. 将上一步的位置添加到您的 `RUBYLIB` 路径中。

```
$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
```

- c. 使用以下命令验证您的 AMI 工具安装。

```
$ ec2-ami-tools-version
```

使用 .zip 文件设置 AMI 工具

1. 使用您的 Linux 发行版的程序包管理器安装 Ruby 并解压缩，例如 apt-get。例如：

```
$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. 使用 wget 或 curl 等工具下载 .zip 文件。例如：

```
$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. 将文件解压缩到合适的安装目录，如 /usr/local/ec2。

```
$ sudo mkdir -p /usr/local/ec2  
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

请注意，该 .zip 文件包含一个文件夹 ec2-ami-tools-**xx.x.x**，其中 **xx.x.x** 是工具的版本号（例如，ec2-ami-tools-1.5.7）。

4. 将 EC2_AMITOOL_HOME 环境变量设置为工具的安装目录。例如：

```
$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-xx.x.x
```

5. 将工具添加到您的 PATH 环境变量。例如：

```
$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. 您可以使用以下命令验证您的 AMI 工具安装。

```
$ ec2-ami-tools-version
```

AMI 工具命令

您可以使用以下命令通过 AMI 工具创建和管理实例存储支持的 Linux AMI。要设置工具，请参阅[设置 AMI 工具 \(p. 80\)](#)。

主题

- [ec2-ami-tools-version \(p. 81\)](#)
- [ec2-bundle-image \(p. 82\)](#)
- [ec2-bundle-vol \(p. 85\)](#)
- [ec2-delete-bundle \(p. 89\)](#)
- [ec2-download-bundle \(p. 91\)](#)
- [ec2-migrate-manifest \(p. 94\)](#)
- [ec2-unbundle \(p. 96\)](#)
- [ec2-upload-bundle \(p. 97\)](#)
- [AMI 工具的常用选项 \(p. 100\)](#)

ec2-ami-tools-version

说明

描述 AMI 工具的版本。

语法

ec2-ami-tools-version

选项

此命令没有参数。

输出

版本信息。

示例

此示例命令显示所用 AMI 工具的版本信息。

```
$ ec2-ami-tools-version  
1.5.2 20071010
```

ec2-bundle-image

说明

通过回环文件中创建的操作系统映像创建实例存储支持的 Linux AMI。

语法

```
ec2-bundle-image -c path -k path -u account -i path [-d path] [--ec2cert path] [-r architecture] [--productcodes code1,code2,...] [-B mapping] [-p prefix]
```

选项

| 选项 | 说明 |
|-------------------------------|---|
| -c, --cert <i>path</i> | 用户的 PEM 编码 RSA 公有密钥证书文件。 必需：是 示例： <code>-c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem</code> |
| -k, --privatekey <i>path</i> | 指向 PEM 编码 RSA 密钥文件的路径。您需要指定此密钥解开此捆绑包，因此，请将其保存在安全的地方。注意，该密钥不需要注册到您的 AWS 账户。 必需：是 示例： <code>-k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem</code> |
| -u, --user <i>account</i> | 用户的 AWS 账户 ID (不包含破折号)。 必需：是 示例： <code>-u 111122223333</code> |
| -i, --image <i>path</i> | 指向待捆绑映像的路径。 必需：是 示例： <code>-i /var/spool/my-image/version-2/debian.img</code> |
| -d, --destination <i>path</i> | 要在其中创建捆绑的目录。 默认： <code>/tmp</code> 必需：否 |

| 选项 | 说明 |
|------------------------------------|--|
| | 示例 : -d /media/ephemeral0 |
| --ec2cert path | 用于加密映像清单的 Amazon EC2 X.509 公有密钥证书的路径。 us-gov-west-1 和 cn-north-1 区域使用非默认公有密钥证书，必须随此选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 /opt/aws/amitools/ec2/etc/ec2/amitools/。如果您在 设置 AMI 工具 (p. 80) 中通过 RPM 或 ZIP 文件安装了 AMI 工具，则证书位于 \$EC2_AMITOOL_HOME/etc/ec2/amitools/。 |
| | 默认 ：因工具而异 必需 ：仅对 us-gov-west-1 和 cn-north-1 区域是必需的。 示例 : --ec2cert \$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2.pem |
| -r, --arch architecture | 映像架构。如果您不在命令行上提供架构，则会在绑定开始时提示您输入架构。 有效值 ：i386 x86_64 必需 ：否 示例 ： -r x86_64 |
| --productcodes code1,code2,... | 在注册时挂载到映像的产品代码，用逗号隔开。 必需 ：否 示例 ：--productcodes 1234abcd |
| -B, --block-device-mapping mapping | 定义块储存设备向此 AMI 的实例公开的方式 (如果其实例类型支持指定的设备)。 指定键值对的逗号分隔列表，每个键是虚拟名称，每个值是相应的设备名称。虚拟名称包括： <ul style="list-style-type: none"> • ami—实例所看到的根文件系统设备 • root—内核所看到的根文件系统设备 • swap—实例所看到的交换设备 • ephemeralN—第 n 个实例存储卷 必需 ：否 示例 ：--block-device-mapping ami=sda1,root=/dev/sda1,ephemeral0=sda2,swap=sda3 示例 ：--block-device-mapping ami=0,root=/dev/dsk/c0d0s0,ephemeral0=1 |

| 选项 | 说明 |
|-----------------------------------|---|
| <code>-p, --prefix prefix</code> | <p>捆绑的 AMI 文件的文件名前缀。</p> <p>默认：映像文件的名称。例如，如果映像路径为 <code>/var/spool/my-image/version-2/debian.img</code>，则默认前缀为 <code>debian.img</code>。</p> <p>必需：否</p> <p>示例：<code>-p my-image-is-special</code></p> |
| <code>--kernel kernel_id</code> | <p>已淘汰。使用 register-image 设置内核。</p> <p>必需：否</p> <p>示例：<code>--kernel aki-ba3adfd3</code></p> |
| <code>--ramdisk ramdisk_id</code> | <p>已淘汰。使用 register-image 设置 RAM 磁盘（若需要）。</p> <p>必需：否</p> <p>示例：<code>--ramdisk ari-badbad00</code></p> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

描述捆绑过程的阶段和状态的状态消息。

示例

此示例从回环文件中所创建的操作系统映像创建捆绑的 AMI。

```
$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

说明

通过对实例根设备卷的副本进行压缩、加密和签名来创建实例存储支持的 Linux AMI。

Amazon EC2 将尝试从实例继承产品代码、内核设置、RAM 磁盘设置和块储存设备映射。

默认情况下，捆绑过程不包括可能包含敏感信息的文件。这些文件包括

.sw、.swo、*.swp、*.pem、*.priv、*id_rsa*、*id_dsa* *.gpg、*.jks、*/.ssh/authorized_keys 和 */.bash_history。要包括所有这些文件，请使用 --no-filter 选项。要包括其中部分文件，请使用 --include 选项。

有关更多信息，请参阅 [创建实例存储支持的 Linux AMI](#)。

语法

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-r architecture]
[--productcodes code1,code2,...] [-B mapping] [--all] [-e directory1,directory2,...] [-i
file1,file2,...] [--no-filter] [-p prefix] [-s size] [--[no-]inherit] [-v volume] [-P type]
[-S script] [--fstab path] [--generate-fstab] [--grub-config path]
```

选项

| 选项 | 说明 |
|-------------------------------|--|
| -c, --cert path | 用户的 PEM 编码 RSA 公有密钥证书文件。 必需：是 示例：-c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem |
| -k, --privatekey path | 用户的 PEM 编码 RSA 密钥文件的路径。 必需：是 示例：-k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem |
| -u, --user account | 用户的 AWS 账户 ID (不包含破折号)。 必需：是 示例：-u 111122223333 |
| -d, --destination destination | 要在其中创建捆绑的目录。 默认：/tmp 必需：否 示例：-d /var/run/my-bundle |
| --ec2cert path | 用于加密映像清单的 Amazon EC2 X.509 公有密钥证书的路径。 us-gov-west-1 和 cn-north-1 区域使用非默认公有密钥证书，必须随此选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 /opt/ aws/amitools/ec2/etc/ec2/amitools/。如果您在 设置 AMI 工具 (p. 80) 中通过 RPM 或 ZIP 文件安装了 AMI 工具，则证书位于 \$EC2_AMITOOL_HOME/etc/ec2/amitools/。 |

| 选项 | 说明 |
|--|--|
| | <p>默认：因工具而异</p> <p>必需：仅对 us-gov-west-1 和 cn-north-1 区域是必需的。</p> <p>示例: <code>--ec2cert \$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2.pem</code></p> |
| <code>-r, --arch architecture</code> | <p>映像架构。如果您不在命令行上提供架构，则会在绑定开始时提示您提供架构。</p> <p>有效值：i386 x86_64</p> <p>必需：否</p> <p>示例： <code>-r x86_64</code></p> |
| <code>--productcodes code1,code2,...</code> | <p>在注册时挂载到映像的产品代码，用逗号隔开。</p> <p>必需：否</p> <p>示例： <code>--productcodes 1234abcd</code></p> |
| <code>-B, --block-device-mapping mapping</code> | <p>定义块储存设备向此 AMI 的实例公开的方式 (如果其实例类型支持指定的设备)。</p> <p>指定键值对的逗号分隔列表，每个键是虚拟名称，每个值是相应的设备名称。虚拟名称包括：</p> <ul style="list-style-type: none"> • ami—实例所看到的根文件系统设备 • root—内核所看到的根文件系统设备 • swap—实例所看到的交换设备 • ephemeralN—第 n 个实例存储卷 <p>必需：否</p> <p>示例： <code>--block-device-mapping ami=sda1,root=/dev/sda1,ephemeral0=sda2,swap=sda3</code></p> <p>示例： <code>--block-device-mapping ami=0,root=/dev/dsk/c0d0s0,ephemeral0=1</code></p> |
| <code>-a, --all</code> | <p>捆绑所有目录，包括远程加载的文件系统上的目录。</p> <p>必需：否</p> <p>示例： <code>-a</code></p> |
| <code>-e, --exclude directory1,directory2,...</code> | <p>要从捆绑操作中排除的绝对目录路径和文件的列表。此参数覆盖 <code>--all</code> 选项。指定排除时，随此参数列出的目录和子目录将不会随卷捆绑。</p> <p>必需：否</p> <p>示例：假设卷的安装点为 <code>-v /foo</code>，而您希望排除目录 <code>/foo/bar</code> 和 <code>/foo/baz</code>，则指定 <code>-e /bar,/baz</code>。</p> |

| 选项 | 说明 |
|--|---|
| <code>-i, --include file1,file2,...</code> | <p>要在捆绑操作中包含的文件的列表。因为指定的文件可能包含敏感信息，若不指定则会从 AMI 中排除。</p> <p>必需：否</p> <p>示例：如果卷安装点为 <code>/mnt/myvol/</code>，而您希望包含文件 <code>/mnt/myvol/foo/bar.pem</code>，则指定 <code>-i /foo/bar.pem</code>。</p> |
| <code>--no-filter</code> | <p>如果指定，则我们不会因为文件可能包含敏感信息而将其从 AMI 排除。</p> <p>必需：否</p> <p>示例：<code>--no-filter</code></p> |
| <code>-p, --prefix prefix</code> | <p>捆绑的 AMI 文件的文件名前缀。</p> <p>默认：<code>image</code></p> <p>必需：否</p> <p>示例：<code>-p my-image-is-special</code></p> |
| <code>-s, --size size</code> | <p>要创建的映像文件的大小，以 MB (1024 * 1024 字节)为单位。 最大大小为 10240 MB。</p> <p>默认：10240</p> <p>必需：否</p> <p>示例：<code>-s 2048</code></p> |
| <code>--[no-]inherit</code> | <p>指示映像是否应当继承实例的元数据 (默认为继承)。如果启用 <code>--inherit</code> 但实例元数据不可访问，则捆绑将失败。</p> <p>必需：否</p> <p>示例：<code>--inherit</code></p> |
| <code>-v, --volume volume</code> | <p>要从中创建捆绑的安装卷的绝对路径。</p> <p>默认：根目录 (<code>/</code>)</p> <p>必需：否</p> <p>示例：<code>-v /mnt/my-customized-ami</code></p> |
| <code>-P, --partition type</code> | <p>指示磁盘映像是否应使用分区表。如果不指定分区表类型，则默认使用卷的父块储存设备上使用的类型 (如果适用)，否则默认为 <code>gpt</code>。</p> <p>有效值：<code>mbr gpt none</code></p> <p>必需：否</p> <p>示例：<code>--partition gpt</code></p> |

| 选项 | 说明 |
|-----------------------------------|---|
| <code>-S, --script script</code> | 将在捆绑前运行的自定义脚本。该脚本必须获得一个参数，即卷的安装点。 必需：否 |
| <code>--fstab path</code> | 要捆绑到映像中的 fstab 的路径。如果未指定，Amazon EC2 将捆绑 /etc/fstab。 必需：否 示例： <code>--fstab /etc/fstab</code> |
| <code>--generate-fstab</code> | 使用 Amazon EC2 提供的 fstab 捆绑卷。 必需：否 示例： <code>--generate-fstab</code> |
| <code>--grub-config</code> | 将捆绑到映像中的备用 GRUB 配置文件的路径。默认情况下， <code>ec2-bundle-vol</code> 要求克隆映像上存在 <code>/boot/grub/menu.lst</code> 或 <code>/boot/grub/grub.conf</code> 。此选项可让您指定备用 GRUB 配置文件的路径，将会复制该文件以覆盖默认值（若存在）。 必需：否 示例： <code>--grub-config /path/to/grub.conf</code> |
| <code>--kernel kernel_id</code> | 已淘汰。使用 register-image 设置内核。 必需：否 示例： <code>--kernel aki-ba3adfd3</code> |
| <code>--ramdisk ramdisk_id</code> | 已淘汰。使用 register-image 设置 RAM 磁盘（若需要）。 必需：否 示例： <code>--ramdisk ari-badbado0</code> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

描述捆绑的阶段和状态的状态消息。

示例

此示例通过对本机根文件系统进行压缩、加密和签名创建捆绑的 AMI。

```
$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
Copying / into the image file /mnt/image...
Excluding:
  sys
  dev/shm
  proc
```

```
dev/pts
proc/sys/fs/binfmt_misc
dev
media
mnt
proc
sys
tmp/image
mnt/img-mnt
1+0 records in
1+0 records out
mke2fs 1.38 (30-Jun-2005)
warning: 256 blocks unused.

Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

说明

从 Amazon S3 存储中删除指定的捆绑。删除捆绑后，您不能从相应的 AMI 启动实例。

语法

```
ec2-delete-bundle -b bucket -a access_key_id -s secret_access_key [-t token] [--url url]
[--region region] [--sigv version] [-m path] [-p prefix] [--clear] [--retry] [-y]
```

选项

| 选项 | 说明 |
|---|---|
| -b, --bucket <i>bucket</i> | 包含捆绑的 AMI 的 Amazon S3 存储桶的名称，后跟可选的以“/”分隔的路径前缀 必需：是 示例：-b myawsbucket/ami-001 |
| -a, --access-key <i>access_key_id</i> | AWS 访问密钥 ID。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需：是 示例：-a AKIAIOSFODNN7EXAMPLE |
| -s, --secret-key <i>secret_access_key</i> | AWS 秘密访问密钥。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需：是 示例：-s wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY |

| 选项 | 说明 |
|---|---|
| <code>-t, --delegation-token token</code> | <p>传递到 AWS 请求的委托令牌。有关更多信息，请参阅 使用临时安全凭证。</p> <p>必需：仅当使用临时安全凭证时是必需的。</p> <p>默认：<code>AWS_DELEGATION_TOKEN</code> 环境变量的值 (若已设置)。</p> <p>示例：<code>-t AQtDYXdzEJr...<remainder of security token></code></p> |
| <code>--region region</code> | <p>要在请求签名中使用的区域。</p> <p>默认：<code>us-east-1</code></p> <p>必需：有条件</p> <p>条件：使用签名版本 4 时必需</p> <p>示例：<code>--region eu-west-1</code></p> |
| <code>--sigv version</code> | <p>对请求进行签名时要使用的签名版本。</p> <p>有效值：<code>2 4</code></p> <p>默认：<code>4</code></p> <p>必需：否</p> <p>示例：<code>--sigv 2</code></p> |
| <code>-m, --manifest path</code> | <p>清单文件的路径。</p> <p>必需：有条件</p> <p>条件：必须指定 <code>--prefix</code> 或 <code>--manifest</code>。</p> <p>示例：<code>-m /var/spool/my-first-bundle/image.manifest.xml</code></p> |
| <code>-p, --prefix prefix</code> | <p>捆绑的 AMI 文件名前缀。请提供完整前缀。例如，如果前缀是 <code>image.img</code>，请使用 <code>-p image.img</code> 而不是 <code>-p image</code>。</p> <p>必需：有条件</p> <p>条件：必须指定 <code>--prefix</code> 或 <code>--manifest</code>。</p> <p>示例：<code>-p image.img</code></p> |
| <code>--clear</code> | <p>删除指定的捆绑之后删除 Amazon S3 存储桶 (若为空)。</p> <p>必需：否</p> <p>示例：<code>--clear</code></p> |
| <code>--retry</code> | <p>在所有 Amazon S3 错误后自动重试，每个操作最多五次。</p> <p>必需：否</p> <p>示例：<code>--retry</code></p> |

| 选项 | 说明 |
|-----------|--|
| -y, --yes | 自动假定所有提示的回复为 yes。 必需：否 示例：-y |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

Amazon EC2 显示状态消息以指示删除过程的阶段和状态。

示例

此示例从 Amazon S3 删除捆绑。

```
$ ec2-delete-bundle -b myawsbucket -a your_access_key_id -s your_secret_access_key
Deleting files:
myawsbucket/image.manifest.xml
myawsbucket/image.part.00
myawsbucket/image.part.01
myawsbucket/image.part.02
myawsbucket/image.part.03
myawsbucket/image.part.04
myawsbucket/image.part.05
myawsbucket/image.part.06
Continue? [y/n]
y
Deleted myawsbucket/image.manifest.xml
Deleted myawsbucket/image.part.00
Deleted myawsbucket/image.part.01
Deleted myawsbucket/image.part.02
Deleted myawsbucket/image.part.03
Deleted myawsbucket/image.part.04
Deleted myawsbucket/image.part.05
Deleted myawsbucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

说明

从 Amazon S3 存储下载指定的实例存储支持的 Linux AMI。

语法

```
ec2-download-bundle -b bucket -a access_key_id -s secret_access_key -k path [--url url] [--region region] [--sigv version] [-m file] [-p prefix] [-d directory] [--retry]
```

选项

| 选项 | 说明 |
|---------------------|--|
| -b, --bucket bucket | 捆绑所在的 Amazon S3 存储桶的名称，后跟可选的以"/"分隔的路径前缀。 必需：是 |

| 选项 | 说明 |
|---|--|
| | 示例： <code>-b myawsbucket/ami-001</code> |
| <code>-a, --access-key access_key_id</code> | AWS 访问密钥 ID。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需：是 示例： <code>-a AKIAIOSFODNN7EXAMPLE</code> |
| <code>-s, --secret-key secret_access_key</code> | AWS 秘密访问密钥。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需：是 示例： <code>-s wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY</code> |
| <code>-k, --privatekey path</code> | 用于解密清单的私有密钥。 必需：是 示例： <code>-k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem</code> |
| <code>--url url</code> | Amazon S3 服务 URL。 默认： <code>https://s3.amazonaws.com/</code> 必需：否 示例： <code>--url https://s3.example.com</code> |
| <code>--region region</code> | 要在请求签名中使用的区域。 默认： <code>us-east-1</code> 必需：有条件 条件：使用签名版本 4 时必需 示例： <code>--region eu-west-1</code> |
| <code>--sigv version</code> | 对请求进行签名时要使用的签名版本。 有效值： <code>2 4</code> 默认： <code>4</code> 必需：否 示例： <code>--sigv 2</code> |
| <code>-m, --manifest file</code> | 清单文件的名称 (无路径)。我们建议您指定清单 (<code>-m</code>) 或前缀 (<code>-p</code>)。 必需：否 示例： <code>-m my-image.manifest.xml</code> |

| 选项 | 说明 |
|--|---|
| <code>-p, --prefix prefix</code> | 捆绑的 AMI 文件的文件名前缀。 默认 : image 必需 : 否 示例 : <code>-p my-image</code> |
| <code>-d, --directory directory</code> | 保存下载的捆绑的目录。该目录必须存在。 默认 : 当前工作目录。 必需 : 否 示例 : <code>-d /tmp/my-downloaded-bundle</code> |
| <code>--retry</code> | 在所有 Amazon S3 错误后自动重试，每个操作最多五次。 必需 : 否 示例 : <code>--retry</code> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

将显示指示下载过程各个阶段的状态消息。

示例

此示例创建 `bundled` 目录 (使用 Linux `mkdir` 命令) 并从 `myawsbucket` Amazon S3 存储桶下载捆绑。

```
$ mkdir bundled
$ ec2-download-bundle -b myawsbucket/bundles/bundle_name -m image.manifest.xml -
a your_access_key_id -s your_secret_access_key -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -
d mybundle
Downloading manifest image.manifest.xml from myawsbucket to mybundle/image.manifest.xml ...
Downloading part image.part.00 from myawsbucket/bundles/bundle_name to mybundle/
image.part.00 ...
Downloaded image.part.00 from myawsbucket
Downloading part image.part.01 from myawsbucket/bundles/bundle_name to mybundle/
image.part.01 ...
Downloaded image.part.01 from myawsbucket
Downloading part image.part.02 from myawsbucket/bundles/bundle_name to mybundle/
image.part.02 ...
Downloaded image.part.02 from myawsbucket
Downloading part image.part.03 from myawsbucket/bundles/bundle_name to mybundle/
image.part.03 ...
Downloaded image.part.03 from myawsbucket
Downloading part image.part.04 from myawsbucket/bundles/bundle_name to mybundle/
image.part.04 ...
Downloaded image.part.04 from myawsbucket
Downloading part image.part.05 from myawsbucket/bundles/bundle_name to mybundle/
image.part.05 ...
Downloaded image.part.05 from myawsbucket
Downloading part image.part.06 from myawsbucket/bundles/bundle_name to mybundle/
image.part.06 ...
Downloaded image.part.06 from myawsbucket
```

ec2-migrate-manifest

说明

修改实例存储支持的 Linux AMI (例如，其证书、内核和 RAM 磁盘)以使其支持其他区域。

语法

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -s secret_access_key --region region) | (--no-mapping)} [--ec2cert ec2_cert_path] [--kernel kernel-id] [--ramdisk ramdisk_id]
```

选项

| 选项 | 说明 |
|------------------------------------|--|
| -c, --cert path | 用户的 PEM 编码 RSA 公有密钥证书文件。 必需 ：是 示例 ：-c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem |
| -k, --privatekey path | 用户的 PEM 编码 RSA 密钥文件的路径。 必需 ：是 示例 ：-k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem |
| --manifest path | 清单文件的路径。 必需 ：是 示例 ：--manifest my-ami.manifest.xml |
| -a, --access-key access_key_id | AWS 访问密钥 ID。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需 ：有条件 条件 ：若使用自动映射则必需。 示例 ：-a AKIAIOSFODNN7EXAMPLE |
| -s, --secret-key secret_access_key | AWS 秘密访问密钥。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 必需 ：有条件 条件 ：若使用自动映射则必需。 示例 ：-s wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY |
| --region region | 要在映射文件中查找的区域。 条件 ：若使用自动映射则必需。 必需 ：有条件 示例 ：--region eu-west-1 |
| --no-mapping | 禁用内核和 RAM 磁盘的自动映射。 |

| 选项 | 说明 |
|-----------------------------------|---|
| | <p>迁移期间，Amazon EC2 会将清单文件中的内核和 RAM 磁盘替换为为目标区域指定的内核和 RAM 磁盘。除非提供了 <code>--no-mapping</code> 参数，否则 <code>ec2-migrate-bundle</code> 便可能使用 <code>DescribeRegions</code> 和 <code>DescribeImages</code> 操作执行自动映射。</p> <p>必需：有条件</p> <p>条件：未提供 <code>-a</code>、<code>-s</code> 和 <code>--region</code> 选项（用于自动映射）时为必需。</p> |
| <code>--ec2cert path</code> | <p>用于加密映像清单的 Amazon EC2 X.509 公有密钥证书的路径。</p> <p><code>us-gov-west-1</code> 和 <code>cn-north-1</code> 区域使用非默认公有密钥证书，必须随此选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 <code>/opt/aws/amitools/ec2/etc/ec2/amitools/</code>。如果您在设置 AMI 工具 (p. 80)中通过 ZIP 文件安装了 AMI 工具，则证书位于 <code>\$EC2_AMITOOL_HOME/etc/ec2/amitools/</code>。</p> <p>默认：因工具而异</p> <p>必需：仅对 <code>us-gov-west-1</code> 和 <code>cn-north-1</code> 区域是必需的。</p> <p>示例：<code>--ec2cert \$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2.pem</code></p> |
| <code>--kernel kernel_id</code> | <p>要选择的内核的 ID。</p> <p>Important</p> <p>我们建议您使用 PV-GRUB 而不是内核和 RAM 磁盘。有关更多信息，请参阅 PV-GRUB。</p> <p>必需：否</p> <p>示例：<code>--kernel aki-ba3adfd3</code></p> |
| <code>--ramdisk ramdisk_id</code> | <p>供选择的 RAM 磁盘的 ID。</p> <p>Important</p> <p>我们建议您使用 PV-GRUB 而不是内核和 RAM 磁盘。有关更多信息，请参阅 PV-GRUB。</p> <p>必需：否</p> <p>示例：<code>--ramdisk ari-badbado0</code></p> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

描述捆绑过程的阶段和状态的消息。

示例

此示例将 `my-ami.manifest.xml` 清单中指定的 AMI 从美国复制到欧洲。

```
$ ec2-migrate-manifest --manifest my-ami.manifest.xml --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

说明

从实例存储支持的 Linux AMI 重新创建捆绑。

语法

```
ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]
```

选项

| 选项 | 说明 |
|--|---|
| -k, --privatekey <i>path</i> | 您的 PEM 编码 RSA 密钥文件的路径。 必需：是 示例： <code>-k \$HOME/pk-234242example.pem</code> |
| -m, --manifest <i>path</i> | 清单文件的路径。 必需：是 示例： <code>-m /var/spool/my-first-bundle/Manifest</code> |
| -s, --source <i>source_directory</i> | 包含捆绑的目录。 默认：当前目录。 必需：否 示例： <code>-s /tmp/my-bundled-image</code> |
| -d, --destination <i>destination_directory</i> | 将 AMI 解绑到的目录。目标目录必须存在。 默认：当前目录。 必需：否 示例： <code>-d /tmp/my-image</code> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

示例

此 Linux 和 UNIX 示例解绑 `image.manifest.xml` 文件中指定的 AMI。

```
$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
```

```
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

输出

将显示指示解绑过程各个阶段的状态消息。

ec2-upload-bundle

说明

将实例存储支持的 Linux AMI 的捆绑上传到 Amazon S3，并在上传的对象上设置相应的 ACL。有关更多信息，请参阅[创建实例存储支持的 Linux AMI](#)。

语法

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t token] -m path [--url url] [--region region] [--sigv version] [--acl acl] [-d directory] [--part part] [--retry] [--skipmanifest]
```

选项

| 选项 | 说明 |
|---|--|
| <code>-b, --bucket bucket</code> | 用于存储捆绑的 Amazon S3 存储桶的名称，后跟可选的以“/”分隔的路径前缀。如果存储桶不存在，则创建一个（若存储桶名称可用）。 |
| | 必需：是 |
| | 示例： <code>-b myawsbucket/bundles/ami-001</code> |
| <code>-a, --access-key access_key_id</code> | 您的 AWS 访问密钥 ID。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 |
| | 必需：是 |
| | 示例： <code>-a AKIAIOSFODNN7EXAMPLE</code> |
| <code>-s, --secret-key secret_access_key</code> | 您的 AWS 秘密访问密钥。为此选项指定值之前，请查看并遵循 有关管理 AWS 访问密钥的最佳实践 中的指导。 |
| | 必需：是 |
| | 示例： <code>-s wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY</code> |
| <code>-t, --delegation-token token</code> | 传递到 AWS 请求的委托令牌。有关更多信息，请参阅 使用临时安全凭证 。 |
| | 必需：仅当使用临时安全凭证时是必需的。 |
| | 默认： <code>AWS_DELEGATION_TOKEN</code> 环境变量的值（若已设置）。 |
| | 示例： <code>-t AQoDYXdzEJr...<remainder of security token></code> |
| <code>-m, --manifest path</code> | 清单文件的路径。清单文件是在捆绑过程中创建的，可以在包含捆绑的目录中找到。 |
| | 必需：是 |
| | 示例： <code>-m image.manifest.xml</code> |

| 选项 | 说明 |
|-----------------|--|
| --url url | <p>已淘汰。请使用 <code>--region</code> 选项，除非您的存储桶被约束到 EU 位置 (且不是 <code>eu-west-1</code>)。<code>--location</code> 标记是确定该特定位置约束的唯一途径。</p> <p>Amazon S3 终端节点服务 URL。</p> <p>默认：<code>https://s3.amazonaws.com/</code></p> <p>必需：否</p> <p>示例：<code>--url https://s3.example.com</code></p> |
| --region region | <p>要在请求签名中为目标 Amazon S3 存储桶使用的区域。</p> <ul style="list-style-type: none"> 如果存储桶不存在，您也没有指定区域，则该工具将创建无位置约束的存储桶 (在 <code>us-east-1</code> 中)。 如果存储桶不存在，而您指定了区域，则该工具将在指定区域创建存储桶。 如果存储桶存在，而您没有指定区域，则该工具将使用存储桶的位置。 如果存储桶存在，并且您指定 <code>us-east-1</code> 为区域，则该工具将使用存储桶的实际位置而不会显示任何错误消息，并将覆盖任何现有的匹配文件。 如果存储桶存在，并且您指定与存储桶的实际位置不符的区域 (非 <code>us-east-1</code>)，则该工具将报错退出。 <p>如果您的存储桶被约束到 EU 位置 (不是 <code>eu-west-1</code>)，请改用 <code>--location</code> 标记。<code>--location</code> 标记是确定该特定位置约束的唯一途径。</p> <p>默认：<code>us-east-1</code></p> <p>必需：有条件</p> <p>条件：使用签名版本 4 时必需</p> <p>示例：<code>--region eu-west-1</code></p> |
| --sigv version | <p>对请求进行签名时要使用的签名版本。</p> <p>有效值：<code>2 4</code></p> <p>默认：<code>4</code></p> <p>必需：否</p> <p>示例：<code>--sigv 2</code></p> |

| 选项 | 说明 |
|---------------------------|---|
| --acl acl | <p>捆绑的映像的访问控制列表策略。</p> <p>有效值 : public-read aws-exec-read</p> <p>默认 : aws-exec-read</p> <p>必需 : 否</p> <p>示例 : --acl public-read</p> |
| -d, --directory directory | <p>包含捆绑的 AMI 段的目录。</p> <p>默认 : 包含清单文件的目录 (参阅 -m 选项)。</p> <p>必需 : 否</p> <p>示例 : -d /var/run/my-bundle</p> |
| --part part | <p>开始上传指定的段及所有后续段。</p> <p>必需 : 否</p> <p>示例 : --part 04</p> |
| --retry | <p>在所有 Amazon S3 错误后自动重试，每个操作最多五次。</p> <p>必需 : 否</p> <p>示例 : --retry</p> |
| --skipmanifest | <p>不上传清单。</p> <p>必需 : 否</p> <p>示例 : --skipmanifest</p> |
| --location location | <p>已淘汰。请使用 --region 选项，除非您的存储桶被约束到 EU 位置 (且不是 eu-west-1)。--location 标记是确定该特定位置约束的唯一途径。</p> <p>目标 Amazon S3 存储桶的位置约束。如果存储桶存在，而您指定的位置与存储桶的实际位置不符，则该工具将报错退出。如果存储桶存在，而您没有指定位置，则该工具将使用存储桶的位置。如果存储桶不存在，而您指定了位置，则该工具将在指定位置创建存储桶。如果存储桶不存在，您也没有指定位置，则该工具将创建无位置约束的存储桶 (在 us-east-1 中)。</p> <p>默认 : 如果指定 --region，则将位置设置为该指定区域。如果未指定 --region，则位置默认为 us-east-1。</p> <p>必需 : 否</p> <p>示例 : --location eu-west-1</p> |
| 常用选项 | 有关大多数 AMI 工具的常用选项信息，请参阅 AMI 工具的常用选项 (p. 100) 。 |

输出

Amazon EC2 显示状态消息以指示上传过程的阶段的状态。

示例

此示例上传 `image.manifest.xml` 清单所指定的捆绑。

```
$ ec2-upload-bundle -b myawsbucket/bundles/bundle_name -m image.manifest.xml -  
a your_access_key_id -s your_secret_access_key  
Creating bucket...  
Uploading bundled image parts to the S3 bucket myawsbucket ...  
Uploaded image.part.00  
Uploaded image.part.01  
Uploaded image.part.02  
Uploaded image.part.03  
Uploaded image.part.04  
Uploaded image.part.05  
Uploaded image.part.06  
Uploaded image.part.07  
Uploaded image.part.08  
Uploaded image.part.09  
Uploaded image.part.10  
Uploaded image.part.11  
Uploaded image.part.12  
Uploaded image.part.13  
Uploaded image.part.14  
Uploading manifest ...  
Uploaded manifest.  
Bundle upload completed.
```

AMI 工具的常用选项

此部分介绍的大多数命令都接受下表中描述的可选参数集合。

| 选项 | 说明 |
|------------|--------------------|
| --help, -h | 显示帮助消息。 |
| --version | 显示版本和版权声明。 |
| --manual | 显示手动输入。 |
| --batch | 以批处理模式运行，不显示交互提示。 |
| --debug | 显示对故障排除可能有帮助的调试信息。 |

管理签名证书

本节介绍如何创建和管理签名证书（也称为 X.509 证书）。这些证书对于某些 AMI 工具命令而言是必需的。

Important

Amazon EC2 最初支持 SOAP 协议用于执行服务调用，基于 SOAP 的调用使用签名证书，以便数字化签署请求。但是，Amazon EC2 中的 SOAP 支持已遭弃用（请参阅 [SOAP 请求](#)），您应改用 HTTP 查询请求。有关更多信息，请参阅 [创建 API 请求](#)。

每个用户可拥有两个证书，以供证书交替之用。

Note

您可授予用户列出和管理自有证书的许可。有关更多信息，请参阅 IAM 用户指南 中的[允许用户管理自己的密码、访问密钥和签名证书](#)。

主题

- [创建用户签名证书 \(p. 101\)](#)
- [管理用户签名证书 \(p. 103\)](#)

创建用户签名证书

如果需要签名证书，您首先必须获取一个签名证书，然后将其上传到 AWS。没有 Amazon EC2 API 操作可用于创建签名证书，因此，您必须使用第三方工具（如 OpenSSL）创建用户签名证书。

Note

尽管您可以使用 AWS 管理控制台中的安全凭证页面创建 X.509 证书，但这种方法仅适用于 AWS 账户根凭证。您无法为各个 Amazon EC2 用户上传使用控制台生成的证书。正确的做法是使用下面几节介绍的流程。

要创建签名证书，您必须执行以下操作：

- 安装和配置 OpenSSL。
- 创建私有密钥。
- 使用私有密钥创建证书。
- 将证书上传到 AWS。

安装和配置 OpenSSL

创建和上传证书时要求使用支持 SSL 和 TLS 协议的工具。OpenSSL 是一种开源工具，提供创建 RSA 令牌以及使用私有密钥进行签名所需的基本加密功能。若您尚未安装 OpenSSL，请遵循下列说明。

要在 Linux 和 UNIX 系统上安装 OpenSSL

1. 请转到 [OpenSSL: Source, Tarballs](http://www.openssl.org/source/) (<http://www.openssl.org/source/>)。
2. 下载最新的源代码和构建数据包。

要在 Windows 系统上安装 OpenSSL

1. 转到 [Binaries](https://wiki.openssl.org/index.php/Binaries) (<https://wiki.openssl.org/index.php/Binaries>)。
2. 选择适当的 OpenSSL for Windows 选项。

新页面显示了到 Windows 下载的链接。

3. 若您的系统尚未安装 OpenSSL，请选择适用于您的操作环境的 Microsoft Visual C++ 2008 Redistributables 链接，然后单击 Download。请遵循 Microsoft Visual C++ 2008 Redistributable Setup Wizard 提供的说明。

Note

如果您不确定您的系统是否安装有 Microsoft Visual C++ 2008 Redistributable 软件包，您可以先尝试安装 OpenSSL。如果尚未安装 Microsoft Visual C++ 2008 Redistributable 软件包，OpenSSL 安装程序将显示错误。确保您安装的架构（32 位或 64 位）与您所安装的 OpenSSL 版本相匹配。

4. 在您安装 Microsoft Visual C++ 2008 Redistributable 软件包之后，请选择适用于您的操作环境的 OpenSSL 二进制文件的版本，然后将文件存入本地。启动 OpenSSL Setup Wizard（OpenSSL 设置向导）。

5. 请按照 OpenSSL Setup Wizard (OpenSSL 设置向导) 中所述的说明进行操作。

在使用 OpenSSL 命令之前，您必须对操作系统进行配置，使其获得有关 OpenSSL 安装位置的信息。

在 Linux 或 Unix 上配置 OpenSSL

1. 在命令行处，将 `openssl_HOME` 变量设置到 OpenSSL 的安装位置：

```
export OpenSSL_HOME=path_to_your_OpenSSL_installation
```

2. 设置包含 OpenSSL 安装文件的路径：

```
export PATH=$PATH:$OpenSSL_HOME/bin
```

Note

您使用 `export` 命令对环境变量做出的任何更改仅对当前会话有效。通过使用 Shell 配置文件设置环境变量，您可对其进行持久性更改。有关更多信息，请参阅您的操作系统文档。

如要在 Windows 系统上配置 OpenSSL

1. 打开 Command Prompt 窗口。
2. 将 `openssl_HOME` 变量设置到 OpenSSL 的安装位置：

```
set OpenSSL_HOME=path_to_your_OpenSSL_installation
```

3. 将 `openssl_CONF` 变量设置为 OpenSSL 安装中配置文件的位置：

```
set OpenSSL_CONF=path_to_your_OpenSSL_installation\bin\openssl.cfg
```

4. 设置包含 OpenSSL 安装文件的路径：

```
set Path=%Path%;%OpenSSL_HOME%\bin
```

Note

您在 Command Prompt (命令提示符) 窗口中对 Windows 环境变量所做的任何更改只对当前的命令行会话有效。通过将环境变量设置为系统属性，您可对其执行永久性更改。具体流程取决于您使用的 Windows 版本。有关更多信息，请参阅 Windows 文档。

创建私有密钥

您需要一个独一无二的私有密钥，以便在生成用户签名证书时使用。

创建私有密钥

1. 在命令行处，按照下列句法使用 `openssl genrsa` 命令：

```
openssl genrsa 2048 > private-key.pem
```

对于 `private-key.pem`，请指定您自己的文件名。在示例中，2048 代表 2048 位加密。AWS 还支持 1024 位和 4096 位加密。我们建议您创建 2048 位或 4096 位 RSA 密钥。

2. 如果您将使用证书来验证用于 Auto Scaling、CloudWatch 或 Elastic Load Balancing 的 CLI 命令，则使用以下命令生成 PKCS8 格式的证书：

```
openssl pkcs8 -topk8 -nocrypt -inform PEM -in private-key.pem -out private-key-in-PKCS8-format.pem
```

创建用户签名证书

现在，您可以创建用户签名证书了。

如要创建用户签名证书

- 按照以下语法使用 `openssl req` 命令：

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -out certificate.pem
```

对于 `private-key.pem`，请使用您在上一步中生成的 .pem 文件。对于 `certificate.pem`，使用生成证书的目标文件名称。证书必须采用 .pem 格式。出于安全考虑，我们建议使用 SHA-256 (如本例) 或 SHA-512 哈希算法。

在此示例中，`-days 365` 开关指定证书的有效期为 365 天。有关其他开关的信息，请在命令行处输入 `openssl req -h`。

OpenSSL 显示的消息与下列内容类似：

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank.  
For some fields there will be a default value.  
If you enter '.', the field will be left blank.
```

由于您创建的是用户签名证书 (而非服务器证书)，因此，在提示您时，您可将所有值留空。证书管理机构 (CA) 将使用这些值来帮助验证服务器证书。不过，由于在经验证的会话内上传用户签名证书，因此，AWS 不要求在证书内包含任何信息来执行进一步验证，而只要求提供公有和私有密钥对。

您可在随后进行的上传期间复制和粘贴 .pem 文件中包含的证书值。

上传用户签名证书

您可以使用 `upload-signing-certificate` AWS CLI 命令上传签名证书。指定您要为其上传证书的用户的名称，以及包含证书值的 .pem 文件的路径。

```
aws iam upload-signing-certificate --user-name user-name --certificate-body file://path/to/certificate.pem
```

或者，您可以使用 `UploadSigningCertificate` IAM API 操作。

Note

由于证书的大小问题，在上传签名证书时使用 POST 请求。

用户拥有的签名证书数量不得超过两个。

管理用户签名证书

您可以使用 AWS CLI 管理签名证书。

正如访问密钥一样，每个证书也可有 Active 或 Inactive 两种状态。在默认情况下，当您上传证书时，状态为 Active。当您上传证书时，将返回证书 ID，您可保存此 ID 以供备用。您可以列出用户证书的 ID。您可以随时删除证书。

要列出用户的证书，请使用 [list-signing-certificates](#) AWS CLI 命令：

```
aws iam list-signing-certificates --user-name user-name
```

要禁用或重新启用用户的签名证书，请使用 [update-signing-certificate](#) AWS CLI 命令。以下命令可禁用证书：

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --  
status Inactive --user-name user-name
```

要删除证书，请使用 [delete-signing-certificate](#) AWS CLI 命令：

```
aws iam delete-signing-certificate --user-name user-name --certificate-  
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

或者，您可以使用以下 IAM API 操作：

- [ListSigningCertificates](#)
- [UpdateSigningCertificate](#)
- [DeleteSigningCertificate](#)

通过实例存储支持的 实例创建 AMI

下列步骤用于从实例存储支持的实例创建实例存储支持的 AMI。在开始之前，请您务必阅读[先决条件 \(p. 79\)](#)。

主题

- [通过实例存储支持的 Amazon Linux 实例创建 AMI \(p. 104\)](#)
- [通过实例存储支持的 Ubuntu 实例创建 AMI \(p. 108\)](#)

通过实例存储支持的 Amazon Linux 实例创建 AMI

本节介绍如何通过 Amazon Linux 实例创建 AMI。以下过程可能不适用于运行其他 Linux 分配的实例。有关特定于 Ubuntu 的过程，请参阅[通过实例存储支持的 Ubuntu 实例创建 AMI \(p. 108\)](#)。

准备使用 Amazon EC2 AMI 工具 (仅限 HVM 实例)

1. Amazon EC2 AMI 工具需要正确启动传统 GRUB。使用以下命令安装 GRUB：

```
[ec2-user ~]$ sudo yum install -y grub
```

2. 使用以下命令安装分区管理程序包：

```
[ec2-user ~]$ sudo yum install -y gdisk kpartx parted
```

通过实例存储支持的 Linux 实例创建 AMI

此过程假设您满足[先决条件 \(p. 79\)](#)中的先决条件。

1. 将您的证书上传到您的实例。我们使用这些证书确保只有您和 Amazon EC2 才能访问您的 AMI。

- a. 在您的实例上为证书创建临时目录，如下所示：

```
[ec2-user ~]$ mkdir /tmp/cert
```

这使您可以从创建的映像中排除您的证书。

- b. 使用安全复制工具（如 [scp \(p. 254\)](#)）将 X.509 证书和对应的私有密钥从您的计算机复制到实例上的 `/tmp/cert` 目录中。以下 `scp` 命令中的 `-i my-private-key.pem` 选项是用来通过 SSH 连接到实例的私有密钥，而不是 X.509 私有密钥。例如：

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /  
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00  
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

此外，由于这些是纯文本文件，所以您可以在文本编辑器中打开证书和密钥，并将其内容复制到 `/tmp/cert` 中的新文件。

2. 通过从您的实例内部运行 [ec2-bundle-vol \(p. 85\)](#) 命令，准备捆绑包以便上传到 Amazon S3。请务必指定 `-e` 选项以排除用于存储您的证书的目录。默认情况下，捆绑过程不包括可能包含敏感信息的文件。这些文件包括 `*.sw`、`*.swo`、`*.swp`、`*.pem`、`*.priv`、`*id_rsa*`、`*id_dsa*`、`*.gpg`、`*.jks`、`*/.ssh/authorized_keys` 和 `*/.bash_history`。要包括所有这些文件，请使用 `--no-filter` 选项。要包括其中部分文件，请使用 `--include` 选项。

Important

默认情况下，AMI 捆绑过程在表示根卷的 `/tmp` 目录中创建经过压缩和加密的文件集合。如果 `/tmp` 中没有足够的可用磁盘空间来存储捆绑，则需要使用 `-d /path/to/bundle/storage` 选项指定其他捆绑存储位置。某些实例在 `/mnt` 或 `/media/ephemeral0` 上安装您可以使用的短暂存储，您也可以[创建 \(p. 527\)](#)、[连接 \(p. 530\)](#)和[安装 \(p. 531\)](#)新的 Amazon EBS 卷来存储捆绑。

- a. `ec2-bundle-vol` 命令需要作为 `root` 运行。对于大多数命令，您可以使用 `sudo` 获取提升的权限，但在这种情况下，您应运行 `sudo -E su` 以保留环境变量。

```
[ec2-user ~]$ sudo -E su
```

请注意，在 bash 提示符下现在将您标识为根用户，并且美元符号已替换为哈希标签，表示您现在处于 root shell 中：

```
[root ec2-user]#
```

- b. 要创建 AMI 捆绑，请运行带有以下参数的 [ec2-bundle-vol \(p. 85\)](#) 命令：

-c

RSA 证书的路径和文件名

-k

RSA 证书私有密钥的路径和文件名

--分区

分区类型：`mbr`、`gpt` 或 `none`。HVM 实例中的 AMI 在没有此分区类型的情况下将不启动。

-r

CPU 架构 : i386 或 x86_64。您可以通过运行 arch 命令检查此架构。

-u

您的 AWS 用户账户 ID

-v

要从已创建映像中排除的目录的逗号分隔列表。

-d

如果默认目录 /tmp 的空间不足以存放捆绑包，可以在此提供具有足够空间的目录的路径。

--ec2cert

仅以下区域需要此参数：中国（北京）和 AWS GovCloud (US)。对于这些区域，您必须指定一个区域特定的公有密钥证书。

有关此命令及其可用选项的更多信息，请参阅 [ec2-bundle-vol \(p. 85\)](#)。

下面是一个示例命令：

```
[root ec2-user]# $EC2_AMITOOL_HOME/bin/ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/cert --partition gpt
```

创建映像可能需要几分钟时间。此命令执行完后，/tmp (或非默认) 目录中包含捆绑包 (image.manifest.xml 以及多个 image.part.xx 文件)。

- c. 从 root shell 退出。

```
[root ec2-user]# exit
```

3. (可选) 编辑 image.manifest.xml 文件中您的 AMI 所对应的块储存设备映射。对于实例存储支持的 AMI，只能在创建 AMI 时在块储存设备映射中指定实例存储卷，这些映射是在 image.manifest.xml 文件中指定的。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。

Note

只有当您希望在 AMI 上添加一个或多个其他实例存储卷时，才需要执行此步骤。

- a. 创建 image.manifest.xml 文件的备份。

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. 重新设置 image.manifest.xml 文件的格式，使其更易于阅读和编辑。

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > sudo /tmp/image.manifest.xml
```

- c. 使用文本编辑器编辑 image.manifest.xml 中的块储存设备映射。以下示例显示了 *ephemeral1* 实例存储卷的一个新条目。

```
<block_device_mapping>
  <mapping>
    <virtual>ami</virtual>
    <device>sda</device>
  </mapping>
```

```
<mapping>
    <virtual>ephemeral0</virtual>
    <device>sdb</device>
</mapping>
<mapping>
    <virtual>ephemeral1</virtual>
    <device>sdc</device>
</mapping>
<mapping>
    <virtual>root</virtual>
    <device>/dev/sda1</device>
</mapping>
</block_device_mapping>
```

- d. 保存 `image.manifest.xml` 文件并退出文本编辑器。
4. 要将捆绑上传到 Amazon S3 , 请运行带有以下参数的 [ec2-upload-bundle \(p. 97\)](#) 命令。

-b

S3 存储桶位置 : `my-s3-bucket/bundle_folder/bundle_name`。请注意 , 如果存储桶和文件夹路径不存在 , 此命令将会创建。

-m

`image.manifest.xml` 的路径。如果您在 [Step 2 \(p. 105\)](#) 中使用 `-d /path/to/bundle/storage` 指定了路径 , 那么请在此参数中使用同一路经。

-a

您的 AWS 账户访问密钥 ID

-s

您的 AWS 账户秘密访问密钥

--region

如果您打算在美国东部 (弗吉尼亚北部) 之外的区域中注册 AMI , 则必须指定带 `--region` 选项的目标区域和目标区域中已存在的存储桶路径或可在目标区域中创建的唯一存储桶路径。

有关此命令及其可用选项的更多信息 , 请参阅 [ec2-upload-bundle \(p. 97\)](#)。

下面是一个示例命令 :

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

5. (可选) 将捆绑上传到 Amazon S3 之后 , 可以使用以下 `rm` 命令从实例上的 `/tmp` 目录删除捆绑 :

Note

如果在 [Step 2 \(p. 105\)](#) 中使用 `-d /path/to/bundle/storage` 选项指定了路径 , 请在下面使用该路径 , 而不使用 `/tmp`。

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

6. 要注册 AMI , 请运行带有以下参数的 `register-image` AWS CLI 命令。
- `--image-location`

`my-s3-bucket/bundle_folder/bundle_name/image.manifest.xml`

--name

AMI 的名称

--virtualization-type

可能的值为 hvm 和 paravirtual。

--region

如果您先前为 [ec2-upload-bundle \(p. 97\)](#) 命令指定了某个区域，请为此命令再次指定该区域。

有关此命令及其可用选项的更多信息，请参阅 AWS Command Line Interface Reference 中的 [register-image](#)。

下面是一个示例命令：

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-type hvm
```

通过实例存储支持的 Ubuntu 实例创建 AMI

本节介绍如何通过 Ubuntu Linux 实例创建 AMI。以下过程可能不适用于运行其他 Linux 分配的实例。有关特定于 Amazon Linux 的过程，请参阅 [通过实例存储支持的 Amazon Linux 实例创建 AMI \(p. 104\)](#)。

准备使用 Amazon EC2 AMI 工具 (仅限 HVM 实例)

Amazon EC2 AMI 工具需要正确启动传统 GRUB。不过，Ubuntu 配置为使用 GRUB 2。您必须检查您的实例是否使用传统 GRUB，如果未使用，您需要安装并配置它。

HVM 实例还需要安装分区工具，以便 AMI 工具可以正常工作。

1. GRUB Legacy (版本 0.9x 或更早版本) 必须安装在您的实例上。检查传统 GRUB 是否存在，并根据需要安装它。

a. 检查您的 GRUB 安装版本。

```
ubuntu:~$ grub-install --version
grub-install (GRUB) 1.99-21ubuntu3.10
```

在该示例中，GRUB 版本高于 0.9x，因此必须安装传统 GRUB。继续执行[Step 1.b \(p. 108\)](#)。如果传统 GRUB 已存在，您可以跳到[Step 2 \(p. 108\)](#)。

b. 使用以下命令安装 grub 程序包。

```
ubuntu:~$ sudo apt-get install -y grub
```

验证您的实例是否正在使用 GRUB Legacy。

```
ubuntu:~$ grub --version
grub (GNU GRUB 0.97)
```

2. 使用您发布版的软件包管理器安装以下分区管理软件包。

- gdisk (此软件包在某些发布版可能名为 gptfdisk)
- kpartx

- parted

使用以下命令。

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. 检查您实例的内核参数。

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

请注意内核和根设备参数之后的选项：ro、console=ttyS0 和 xen_emul_unplug=unnecessary。您的选项可能有所不同。

4. 检查 /boot/grub/menu.lst 中的内核条目。

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel  /boot/memtest86+.bin
```

请注意，console 参数指向 hvc0 而不是 ttyS0，并且缺少 xen_emul_unplug=unnecessary 参数。同样，您的选项可能有所不同。

5. 使用常用文本编辑器（如 vim 或 nano）编辑 /boot/grub/menu.lst 文件以更改控制台并将之前标识的参数添加到启动条目中。

```
title      Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root      (hd0)
kernel    /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
ro console=ttyS0 xen_emul_unplug=unnecessary
initrd   /boot/initrd.img-3.2.0-54-virtual

title      Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root      (hd0)
kernel    /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
single console=ttyS0 xen_emul_unplug=unnecessary
initrd   /boot/initrd.img-3.2.0-54-virtual

title      Ubuntu 12.04.3 LTS, memtest86+
root      (hd0)
kernel    /boot/memtest86+.bin
```

6. 验证您的内核条目现在是否包含正确参数。

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7.（仅适用于 Ubuntu 14.04 及更高版本）从 Ubuntu 14.04 开始，实例存储支持的 Ubuntu AMI 使用 GPT 分区表和挂载在 /boot/efi 中的单独 EFI 分区。ec2-bundle-vol 命令不会捆绑此启动分区，因此您需要为 EFI 分区的 /etc/fstab 条目添加注释，如下所示。

```
LABEL=cloudimg-rootfs  /          ext4  defaults        0 0
#LABEL=UEFI            /boot/efi    vfat   defaults        0 0
```

| | | | | |
|-----------|------|------|---|---|
| /dev/xvdb | /mnt | auto | defaults,nobootwait,comment=cloudconfig 0 | 2 |
|-----------|------|------|---|---|

通过实例存储支持的 Linux 实例创建 AMI

此过程假设您满足 [先决条件 \(p. 79\)](#) 中的先决条件。

1. 将您的证书上传到您的实例。我们使用这些证书确保只有您和 Amazon EC2 才能访问您的 AMI。
 - a. 在您的实例上为证书创建临时目录，如下所示：

```
ubuntu:~$ mkdir /tmp/cert
```

这使您可以从创建的映像中排除您的证书。

- b. 使用安全复制工具（如 [scp \(p. 254\)](#)）将 X.509 证书和私有密钥从您的计算机复制到实例上的 /tmp/cert 目录。以下 scp 命令中的 -i *my-private-key.pem* 选项是用来通过 SSH 连接到实例的私有密钥，而不是 X.509 私有密钥。例如：

```
you@your_computer:~ $ scp -i my-private-key.pem /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00  
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

此外，由于这些是纯文本文件，所以您可以在文本编辑器中打开证书和密钥，并将其内容复制到 /tmp/cert 中的新文件。

2. 通过从您的实例内部运行 [ec2-bundle-vol \(p. 85\)](#) 命令，准备捆绑包以便上传到 Amazon S3。请务必指定 -e 选项以排除用于存储您的证书的目录。默认情况下，捆绑过程不包括可能包含敏感信息的文件。这些文件包括 *.sw、*.swo、*.swp、*.pem、*.priv、*id_rsa*、*id_dsa*、*.gpg、*.jks、*/.ssh/authorized_keys 和 */.bash_history。要包括所有这些文件，请使用 --no-filter 选项。要包括其中部分文件，请使用 --include 选项。

Important

默认情况下，AMI 捆绑过程在表示根卷的 /tmp 目录中创建经过压缩和加密的文件集合。如果 /tmp 中没有足够的可用磁盘空间来存储捆绑，则需要使用 -d */path/to/bundle/storage* 选项指定其他捆绑存储位置。某些实例在 /mnt 或 /media/ephemeral0 上安装您可以使用的短暂存储，您也可以 [创建 \(p. 527\)](#)、[连接 \(p. 530\)](#) 和 [安装 \(p. 531\)](#) 新的 Amazon EBS 卷来存储捆绑。

- a. ec2-bundle-vol 命令需要作为 root 运行。对于大多数命令，您可以使用 sudo 获取提升的权限，但在这种情况下，您应运行 sudo -E su 以保留环境变量。

```
ubuntu:~$ sudo -E su
```

请注意，在 bash 提示符下现在将您标识为根用户，并且美元符号已替换为哈希标签，表示您现在处于 root shell 中：

```
root@ubuntu:#
```

- b. 要创建 AMI 捆绑，请运行带有以下参数的 [ec2-bundle-vol \(p. 85\)](#) 命令。

-C

RSA 证书的路径和文件名

-k

RSA 证书私有密钥的路径和文件名

--分区

分区类型 : mbr、gpt 或 none。对于 Ubuntu 14.04 及更高版本的 HVM 实例 , 请添加 --partition mbr 标志以正确捆绑启动指令 ; 否则 , 新创建的 AMI 不会启动。

-r

CPU 架构 : i386 或 x86_64。您可以通过运行 arch 命令检查此架构。

-u

您的 AWS 用户账户 ID

-环

要从已创建映像中排除的目录的逗号分隔列表。

-d

如果默认目录 /tmp 的空间不足以存放捆绑包 , 可以在此提供具有足够空间的目录的路径。

有关此命令及其可用选项的更多信息 , 请参阅 [ec2-bundle-vol \(p. 85\)](#)。

下面是一个示例命令 :

```
root@ubuntu:# $EC2_AMITOOL_HOME/bin/ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/cert --partition gpt
```

创建映像可能需要几分钟时间。此命令执行完后 , tmp 目录包含捆绑 (image.manifest.xml 以及多个 image.part.xx 文件)。

- c. 从 root shell 退出。

```
root@ubuntu:# exit
```

3. (可选) 编辑 image.manifest.xml 文件中您的 AMI 所对应的块储存设备映射。对于实例存储支持的 AMI , 只能在创建 AMI 时在块储存设备映射中指定实例存储卷 , 这些映射是在 image.manifest.xml 文件中指定的。有关更多信息 , 请参阅 [块储存设备映射 \(p. 609\)](#)。

Note

只有当您希望在 AMI 上添加一个或多个其他实例存储卷时 , 才需要执行此步骤。

- a. 创建 image.manifest.xml 文件的备份。

```
ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. 重新设置 image.manifest.xml 文件的格式 , 使其更易于阅读和编辑。

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/image.manifest.xml
```

- c. 使用文本编辑器编辑 image.manifest.xml 中的块储存设备映射。以下示例显示了 ephemeral1 实例存储卷的一个新条目。

```
<mapping>
  <virtual>ami</virtual>
  <device>sda</device>
</mapping>
<mapping>
  <virtual>ephemeral0</virtual>
  <device>sdb</device>
</mapping>
<mapping>
  <virtual>ephemeral1</virtual>
  <device>sdc</device>
</mapping>
<mapping>
  <virtual>root</virtual>
  <device>/dev/sda1</device>
</mapping>
</block_device_mapping>
```

- d. 保存 `image.manifest.xml` 文件并退出文本编辑器。
4. 要将捆绑上传到 Amazon S3 , 请运行带有以下参数的 [ec2-upload-bundle \(p. 97\)](#) 命令。

-b

S3 存储桶位置 : `my-s3-bucket/bundle_folder/bundle_name`。请注意 , 如果存储桶和文件夹路径不存在 , 此命令将会创建。

-m

`image.manifest.xml` 的路径。如果您在 [Step 2 \(p. 110\)](#) 中使用 `-d /path/to/bundle/storage` 指定了路径 , 那么请在此参数中使用同一路径。

-a

您的 AWS 账户访问密钥 ID

-s

您的 AWS 账户秘密访问密钥

--region

如果您打算在美国东部 (弗吉尼亚北部) 之外的区域中注册 AMI , 则必须指定带 `--region` 选项的目标区域和目标区域中已存在的存储桶路径或可在目标区域中创建的唯一存储桶路径。

有关此命令及其可用选项的更多信息 , 请参阅 [ec2-upload-bundle \(p. 97\)](#)。

下面是一个示例命令 :

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

5. (可选) 将捆绑上传到 Amazon S3 之后 , 可以使用以下 `rm` 命令从实例上的 `/tmp` 目录删除捆绑 :

Note

如果在 [Step 2 \(p. 110\)](#) 中使用 `-d /path/to/bundle/storage` 选项指定了路径 , 请在下面使用该路径 , 而不使用 `/tmp`。

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

6. 要注册 AMI , 请运行带有以下参数的 `register-image` AWS CLI 命令。

清单路径

```
my-s3-bucket/bundle_folder/bundle_name/image.manifest.xml  
-n  
AMI 的名称  
--virtualization-type  
可能的值为 hvm 和 paravirtual。  
--region  
如果您先前为 ec2-upload-bundle \(p. 97\) 命令指定了某个区域，请为此命令再次指定该区域。
```

有关此命令及其可用选项的更多信息，请参阅 AWS Command Line Interface Reference 中的 [register-image](#)。

下面是一个示例命令：

```
ubuntu:~$ aws ec2 register-image my-s3-bucket/bundle_folder/bundle_name/  
image.manifest.xml --name AMI_name --virtualization-type hvm
```

7. (仅适用于 Ubuntu 14.04 及更高版本) 在 /etc/fstab 中取消对 EFI 条目的注释；否则，正在运行的实例不会重启。

将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI

您可以将拥有的实例存储支持的 Linux AMI 转换为 Amazon EBS 支持的 Linux AMI。

Important

您无法将实例存储支持的 Windows AMI 转换为 Amazon EBS 支持的 Windows AMI，并且无法转换您不拥有的 AMI。

将由实例存储支持的 AMI 转换为由 Amazon EBS 支持的 AMI

1. 从 Amazon EBS 支持的 AMI 启动 Amazon Linux 实例。有关更多信息，请参阅 [启动实例 \(p. 244\)](#)。Amazon Linux 实例预装了 AWS CLI 和 AMI 工具。
2. 上传您用于将实例存储支持的 AMI 捆绑到实例的 X.509 私有密钥。我们使用此密钥确保只有您和 Amazon EC2 才能访问您的 AMI。
 - a. 在您的实例上为 X.509 私有密钥创建临时目录，如下所示：

```
[ec2-user ~]$ mkdir /tmp/cert
```

- b. 使用安全复制工具（如 [scp \(p. 254\)](#)）将 X.509 私有密钥从您的计算机复制到实例上的 /tmp/cert 目录。以下命令中的 `my-private-key` 参数是您用于通过 SSH 连接到实例的私有密钥。例如：

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00
```

3. 为您的 AWS 访问密钥和私有密钥设置环境变量。

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
```

4. 为新 AMI 准备 Amazon EBS 卷。

- 使用 [create-volume](#) 命令在您的实例所在的同一可用区中创建空 Amazon EBS 卷。记下命令输出中的卷 ID。

Important

此 Amazon EBS 卷不小于原始实例存储根卷。

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --availability-zone us-west-2b
```

- 使用 [attach-volume](#) 命令将该卷挂载到 Amazon EBS 支持的实例。

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-id instance_id --device /dev/sdb --region us-west-2
```

5. 创建用于捆绑的文件夹。

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. 使用 [##### AMI ##### /tmp/bundle](#)[ec2-download-bundle](#) (p. 91)。

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m image.manifest.xml -a $AWS_ACCESS_KEY -s $AWS_SECRET_KEY --privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. 使用 [ec2-unbundle](#) (p. 96) 命令从捆绑重新构建映像文件。

- 将目录更改为捆绑文件夹。

```
[ec2-user ~]$ cd /tmp/bundle/
```

- 运行 [ec2-unbundle](#) (p. 96) 命令。

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. 将文件从未捆绑的映像复制到新 Amazon EBS 卷。

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. 探测所有未捆绑的新分区的卷。

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. 列出块储存设备以查找要挂载的设备名称。

```
[ec2-user bundle]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

在此示例中，要挂载的分区是 /dev/sdb1，但您的设备名称可能有所不同。如果您的卷未分区，则要挂载的设备类似于 /dev/sdb (没有设备分区尾部数字)。

11. 为新 Amazon EBS 卷创建安装点并安装该卷。

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. 使用常用文本编辑器 (如 vim 或 nano) 打开 EBS 卷上的 /etc/fstab 文件，并删除任何实例存储 (短暂) 卷条目。由于 Amazon EBS 卷安装在 /mnt/ebs 上，fstab 文件位于 /mnt/ebs/etc/fstab 中。

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/      /          ext4    defaults,noatime  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/sdb     /media/ephemeral0 auto    defaults,comment=cloudconfig  0
2
```

在本示例中，应删除最后一行。

13. 从实例中卸载和分离该卷。

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. 按如下所示从新 Amazon EBS 卷创建 AMI。

- a. 创建新 Amazon EBS 卷的快照。

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
"your_snapshot_description" --volume-id volume_id
```

- b. 检查快照是否完整。

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

- c. 使用 describe-images 命令标识在原始 AMI 上使用的处理器架构、虚拟化类型和内核映像 (aki)。对于此步骤，您需要实例存储支持的原始 AMI 的 AMI ID。

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami_id --
output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon available
public machine aki-fc8f11cc instance-store paravirtual xen
```

在此示例中，架构是 x86_64，内核映像 ID 是 aki-fc8f11cc。在以下步骤中使用这些值。如果上面命令的输出还列出 ari ID，请记下该 ID。

- d. 使用新 Amazon EBS 卷的快照 ID 和上一步中得到的值注册新 AMI。如果前一命令输出列出了 ari ID，请通过 --ramdisk-id **ari_id** 将其包括在后续命令中。

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings Ebs={SnapshotId=snapshot_id} --
virtualization-type hvm --architecture x86_64 --kernel-id aki-fc8f11cc
```

15. (可选) 测试了您可以从新 AMI 启动实例之后，您可以删除为此过程创建的 Amazon EBS 卷。

```
$ aws ec2 delete-volume --volume-id volume_id
```

带加密快照的 AMI

由 Amazon EBS 快照支持的 AMI 可以利用 Amazon EBS 加密。可以将数据和根卷的快照加密并附加到 AMI。

带加密卷的 EC2 实例从 AMI 中启动的方式与其他实例的相同。

`CopyImage` 操作可用于从带未加密快照的 AMI 创建带加密快照的 AMI。默认情况下，在创建目标副本时，`CopyImage` 会保留源快照的加密状态。但是，您也可以配置复制过程的参数来加密目标快照。

可使用您的默认 AWS Key Management Service 客户主密钥 (CMK)，或您指定的自定义密钥加密快照。在所有情况下，您都必须拥有使用所选密钥的权限。如果您拥有带加密快照的 AMI，则可以选择使用其他加密密钥对其进行重新加密以作为 `CopyImage` 操作的一部分。`copyImage` 一次只接受一个密钥并且会将映像的所有快照（无论是根还是数据）加密到该密钥。但是，无法使用加密到多个密钥的快照手动构建 AMI。

对创建带加密快照的 AMI 的支持可通过 Amazon EC2 控制台、Amazon EC2 API 或 AWS CLI 获得。

`CopyImage` 的加密参数在 AWS KMS 可用的所有区域中都可用。

涉及加密的 EBS 快照的 AMI 情景

您可以使用 AWS 管理控制台或命令行复制 AMI 并同时对与其关联的 EBS 快照进行加密。

复制带加密数据快照的 AMI

在此方案中，EBS 支持的 AMI 拥有未加密的根快照和加密的数据快照，如步骤 1 所示。在步骤 2 中，`CopyImage` 操作在没有加密参数的情况下调用。因此，将保留每个快照的加密状态，以便让目标 AMI（如步骤 3 所示）也由未加密的根快照和加密的数据快照提供支持。尽管这两种快照包含相同的数据，但两者是截然不同的，两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。

您可以使用 Amazon EC2 控制台或命令行执行简单复制（如上述复制）。有关更多信息，请参阅 [复制 AMI \(p. 117\)](#)。

复制由加密的根快照支持的 AMI

在此方案中，Amazon EBS 支持的 AMI 拥有加密的根快照，如步骤 1 所示。在步骤 2 中，`CopyImage` 操作在没有加密参数的情况下调用。因此，将保留快照的加密状态，以便让目标 AMI（如步骤 3 所示）也由加密的根快照支持。尽管这两种根快照包含相同的系统数据，但两者是截然不同的，两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。

您可以使用 Amazon EC2 控制台或命令行执行简单复制（如上述复制）。有关更多信息，请参阅 [复制 AMI \(p. 117\)](#)。

从未加密的 AMI 创建带加密的根快照的 AMI

在此方案中，Amazon EBS 支持的 AMI 拥有未加密的根快照（如步骤 1 所示），将创建带加密的根快照的 AMI（如步骤 3 所示）。步骤 2 中的 `CopyImage` 操作将通过两个加密参数（包括选择 CMK）调用。因此，根快照的加密状态将更改，以便让目标 AMI 由包含与源快照相同的数据但使用指定密钥进行加密的根快照提供支持。两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。

您可以使用 Amazon EC2 控制台或命令行执行复制和加密操作 (如上述操作)。有关更多信息，请参阅 [复制 AMI \(p. 117\)](#)。

从正在运行的实例创建带加密的根快照的 AMI

在此方案中，将从正在运行的 EC2 实例创建 AMI。步骤 1 中的正在运行的实例拥有加密的根卷，步骤 3 中创建的 AMI 拥有加密到与源卷相同的密钥的根快照。无论加密是否存在，`createImage` 操作都具有完全相同的行为。

您可以使用 Amazon EC2 控制台或命令行从正在运行的 Amazon EC2 实例 (带或不带加密卷) 创建 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。

使用每个加密快照的唯一 CMK 创建 AMI

此方案最初有一个由根卷快照 (加密到密钥 #1) 支持的 AMI，最终得到一个附加了 2 个额外数据卷快照 (加密到密钥 #2 和密钥 #3) 的 AMI。`CopyImage` 操作无法将多个加密密钥应用于单个操作。但是，您可以从拥有加密到不同密钥的多个附加卷的实例创建 AMI。生成的 AMI 拥有加密到这些密钥的快照，且从此新 AMI 启动的任何实例也拥有加密到这些密钥的卷。

本示例过程的步骤对应于下图。

1. 从 vol. #1 (根) 快照支持的源 AMI 开始，该快照使用密钥 #1 进行加密。
2. 从源 AMI 启动 EC2 实例。
3. 创建 EBS 卷 vol.#2 (数据) 和 vol.#3 (数据)，它们分别加密到密钥 #2 和密钥 #3。
4. 将加密的数据卷附加到 EC2 实例。
5. EC2 实例现在拥有 1 个加密的根卷以及 2 个加密的数据卷，这些卷都使用不同的密钥。
6. 对 EC2 实例执行 `createImage` 操作。
7. 生成的目标 AMI 包含三个 EBS 卷的加密快照，这些卷都使用不同的密钥。

您可以使用 Amazon EC2 控制台或命令行执行此过程。有关更多信息，请参阅以下主题：

- [启动实例 \(p. 243\)](#)
- [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。
- [Amazon EBS 卷 \(p. 517\)](#)
- AWS Key Management Service Developer Guide 中的 [AWS 密钥管理](#)

复制 AMI

您可以使用 AWS 管理控制台、AWS 命令行工具或开发工具包，或 Amazon EC2 API (三者都支持 `copyImage` 操作) 在 AWS 区域内或跨 AWS 区域复制 Amazon 系统映像 (AMI)。您可以复制由 Amazon EBS 支持的 AMI 和由实例存储支持的 AMI。您可以复制带有加密快照的 AMI 和加密的 AMI。

复制源 AMI 将生成完全相同但独立的目标 AMI (具有自己的唯一标识符)。对于 Amazon EBS 支持的 AMI，默认情况下其每个支持快照将会复制到完全相同但独立的目标快照。(一个例外是您选择加密快照时。)您可以更改或取消注册源 AMI，这不会对目标 AMI 产生任何影响。反之亦然。

复制 AMI 没有任何费用。但要收取标准存储和数据传输费。

AWS 不会将启动许可、用户定义的标签或 Amazon S3 存储桶许可从源 AMI 复制到新 AMI。复制操作完成之后，可以将启动许可、用户定义的标签和 Amazon S3 存储桶权限应用于新 AMI。

权限

如果您使用一个 IAM 用户复制由实例存储支持的 AMI，该用户必须具有以下 Amazon S3 权限：
s3:CreateBucket、s3:GetBucketAcl、s3>ListAllMyBuckets、s3:GetObject、s3:PutObject 和
s3:PutObjectAcl。

以下示例策略允许该用户将指定存储桶中的 AMI 源复制到指定区域。

```
{  
    "Version": "2016-12-09",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListAllMyBuckets",  
            "Resource": [  
                "arn:aws:s3::::*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": "s3:GetObject",  
            "Resource": [  
                "arn:aws:s3:::ami-source-bucket/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3>CreateBucket",  
                "s3:GetBucketAcl",  
                "s3:PutObjectAcl",  
                "s3:PutObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::amis-for-123456789012-in-us-east-1*"  
            ]  
        }  
    ]  
}
```

跨区域 AMI 复制

跨不同地理位置复制 AMI 具有以下优势：

- **一致的全球部署**：通过将 AMI 从一个区域复制到另一个区域，使您能够在不同的区域启动基于相同 AMI 的一致实例。
- **可扩展性**：无论用户身处何处，您都可以更轻松地设计和构建能满足他们需求的全球范围应用程序。
- **性能**：您可以通过分发您的应用程序以及找到较接近您用户的应用程序的关键组件来提高性能。您还可以利用区域特定的功能，例如实例类型或其他 AWS 服务。
- **高可用性**：您可以跨 AWS 区域设计和部署应用程序以提高可用性。

下图显示源 AMI 和不同区域中的两个复制 AMI 以及从三者启动的 EC2 实例之间的关系。当您从 AMI 启动一个实例时，该实例将驻留在 AMI 所在的区域。如果您更改源 AMI，并希望这些更改反映到目标区域的 AMI 中，则必须将源 AMI 重新复制到目标区域。

当您首次将实例存储支持的 AMI 复制到一个区域时，我们会为复制到该区域的 AMI 创建一个 Amazon S3 存储桶。复制到该区域的所有实例存储支持的 AMI 都将存储在此存储桶中。存储桶名称具有以下格式：amis-for-**account-in-region-hash**。例如：amis-for-123456789012-in-us-west-2-yhjmxvp6。

先决条件

复制 AMI 前，您必须确保源 AMI 的内容得到更新，以支持在另一个区域运行。例如，您应更新任何数据库连接字符串或相似的应用程序配置数据，以指向适当的资源。否则，从目标区域的新 AMI 启动的实例可能会继续使用来自源区域的资源，这可能会影响性能和成本。

Limit

目标区域限制为一次 50 个并发 AMI 副本，并且来自一个源区域的不能超过 25 个。要请求提高此限制，请参阅 [Amazon EC2 服务限制 \(p. 633\)](#)。

跨账户 AMI 复制

您可以与其他 AWS 账户共享 AMI。共享 AMI 不影响 AMI 的所有权。拥有的账户需要支付区域中的存储费用。有关更多信息，请参阅 [将 AMI 与特定 AWS 账户共享 \(p. 67\)](#)。

如果您复制已与您的账户共享的 AMI，则您是您的账户中的目标 AMI 的所有者。源 AMI 的所有者需要支付标准 Amazon EBS 或 Amazon S3 传输费，您需要支付目标区域中目标 AMI 的存储费用。

资源权限

要从另一个账户复制已与您共享的 AMI，源 AMI 的所有者必须向您授予对支持该 AMI 的存储（对于由 Amazon EBS 支持的 AMI，为关联的 EBS 快照；对于由实例存储支持的 AMI，为关联的 S3 存储桶）的读取权限。

限制

- 不能从另一个账户复制已与您共享的加密的 AMI。相反，如果已与您共享基础快照和加密密钥，则您可以在复制该快照的同时使用您自己的密钥对其进行重新加密。您拥有已复制的快照，并且可以将其注册为新的 AMI。
- 不能从另一个账户复制已与您共享的带关联 `billingProduct` 代码的 AMI。这包括 Windows AMI 和来自 AWS Marketplace 的 AMI。要复制带 `billingProduct` 代码的已共享 AMI，请使用已共享 AMI 启动您的账户中的 EC2 实例，然后从该实例创建 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。

加密和 AMI 复制

在 AMI 复制期间加密仅适用于 Amazon EBS 支持的 AMI。由于实例存储支持的 AMI 不依赖快照，因此无法使用 AMI 复制来更改其加密状态。

您可以使用 AMI 复制创建由加密 Amazon EBS 快照支持的新 AMI。如果您在复制 AMI 时调用加密，将使用您指定的密钥对为其关联的 Amazon EBS 卷（包括根卷）拍摄的每个快照进行加密。有关使用具有加密快照的 AMI 的更多信息，请参阅 [带加密快照的 AMI \(p. 116\)](#)。

默认情况下，将复制 AMI 的备份快照并保持其原始加密状态。复制未加密快照支持的 AMI 将生成完全相同、也未加密的目标快照。如果源 AMI 受加密快照支持，则复制它将生成一个加密到指定密钥的目标快照。复制多个快照支持的 AMI 将保留其在每个目标快照中的源加密状态。有关复制具有多个快照的 AMI 的更多信息，请参阅 [带加密快照的 AMI \(p. 116\)](#)。

下表显示了各种场景的加密支持。请注意，尽管可以复制未加密快照来生成加密快照，但是不能复制加密快照来生成未加密快照。

| 场景 | 说明 | 支持服务 |
|----|---------|------|
| 1 | 未加密到未加密 | 是 |
| 2 | 加密到加密 | 是 |
| 3 | 未加密到加密 | 是 |
| 4 | 加密到未加密 | 否 |

将未加密的源 AMI 复制到未加密的目标 AMI

在此场景中，具有单个未加密支持快照的 AMI 副本是在指定地理区域（未显示）中创建的。尽管此图显示了具有单一支持快照的 AMI，您也可以使用多个快照复制 AMI。将保留每个快照的加密状态。因此，源 AMI 中的未加密快照将在目标 AMI 中生成未加密快照，源 AMI 中的加密快照将在目标 AMI 中生成加密快照。

将加密源 AMI 复制到加密目标 AMI

尽管此场景涉及加密快照，但它在功能上等效于前一场景。如果您在复制多快照 AMI 时应用加密，则将使用指定密钥（如果未指定密钥，则使用默认密钥）来加密所有目标快照。

将未加密的源 AMI 复制到加密目标 AMI

在此场景中，复制 AMI 将更改目标映像的加密状态，例如，对未加密快照进行加密，或使用不同密钥对加密快照进行重新加密。要在复制期间应用加密，您必须提供一个加密标志和一个密钥。只能使用此密钥访问从目标快照创建的卷。

复制 AMI

您可以按如下方式复制 AMI。

先决条件

创建或获取 Amazon EBS 快照支持的 AMI。请注意，您可以使用 Amazon EC2 控制台搜索 AWS 提供的各种 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)和[查找 Linux AMI \(p. 62\)](#)。

使用控制台复制 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从控制台导航栏中，选择包含 AMI 的区域。在导航窗格中，选择 Images 和 AMIs 以显示区域中可供您使用的 AMI 的列表。
3. 选择要复制的 AMI，然后选择 Actions 和 Copy AMI。
4. 在 AMI Copy 页面上，指定以下信息，然后选择 Copy AMI：
 - Destination region：要将 AMI 复制到的区域。
 - Name：新 AMI 的名称。您可以在名称中包含操作系统信息，因为我们在显示有关 AMI 的详情时不提供该信息。
 - Description：默认情况下，描述包括源 AMI 的相关信息，以便您能区分副本和原本。您可以按需更改此描述。
 - Encryption：选择此字段可加密目标快照，或使用不同的密钥对它们进行重新加密。
 - Master Key：用于加密目标快照的 KMS 密钥。
5. 我们将显示一个确认页面，以告知您复制操作已启动，并为您提供新 AMI 的 ID。

若要立即查看复制操作的进度，请访问提供的链接。若要稍后查看进度，请选择 Done，然后在您准备就绪时使用导航栏切换到目标区域（如果适用）并在 AMI 列表中找到您的 AMI。

目标 AMI 的初始状态为 pending，当状态为 available 时，此操作完成。

使用命令行复制 AMI

使用命令行复制 AMI 需要您同时指定源区域和目标区域。可使用 `--source-region` 参数指定源区域。对于目标区域，您有两种选择：

- 使用 `--region` 参数。
- 设置环境变量。有关更多信息，请参阅[配置 AWS 命令行界面](#)。

在复制期间加密目标快照时，您必须指定这些额外参数：

- 一个布尔值，`--encrypted`
- 一个字符串，`--kms-key-id`，提供主加密密钥 ID

您可以使用以下命令之一复制 AMI。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `copy-image` (AWS CLI)
- `Copy-EC2Image` (适用于 Windows PowerShell 的 AWS 工具)

停止待处理的 AMI 复制操作

您可以按如下方式停止待处理的 AMI 复制。

使用控制台停止 AMI 复制操作

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中，在区域选择器中选择目标区域。
3. 在导航窗格中，选择 AMIs。
4. 选择要停止复制的 AMI 并选择 Actions 和 Deregister。
5. 当系统要求确认时，请选择 Continue。

使用命令行停止 AMI 复制操作

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `deregister-image` (AWS CLI)
- `Unregister-EC2Image` (适用于 Windows PowerShell 的 AWS 工具)

取消注册您的 AMI

使用完 AMI 之后，可以取消注册它。取消注册 AMI 之后，便无法将其用于启动新实例。

取消注册某个 AMI 时，不会影响您已从该 AMI 启动的任何实例。这些实例将继续对您产生使用费用。因此，如果您使用完这些实例，应终止它们。

用于清除 AMI 的过程取决于它是由 Amazon EBS 还是由实例存储支持。（请注意，只有用于 Windows Server 2003 的 Windows AMI 可由实例存储支持。）

内容

- 清除由 Amazon EBS 支持的 AMI (p. 122)
- 清除由实例存储支持的 AMI (p. 122)

清除由 Amazon EBS 支持的 AMI

在取消注册 Amazon EBS 支持的 AMI 时，不会影响在创建 AMI 的过程中为实例的根卷创建的快照。此快照将继续对您产生存储费用。因此，如果您使用完该快照，应删除它。

下图说明清除由 Amazon EBS 支持的 AMI 的过程。

清除由 Amazon EBS 支持的 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 AMIs。选择 AMI 并记下其 ID — 这可帮助您在下一步骤中找到正确的快照。选择 Actions，然后选择 Deregister。当系统提示进行确认时，请选择 Continue。

AMI 状态现在变为 unavailable。

Note

可能要用几分钟时间，控制台才会将状态 available 变为 unavailable 或者从列表中完全删除该 AMI。选择 Refresh 以刷新状态。

3. 在导航窗格中，选择 Snapshots，然后选择快照 (在 Description 列中查找 AMI ID)。选择 Actions，然后选择 Delete Snapshot。当系统提示进行确认时，选择 Yes, Delete。
4. (可选) 如果您使用完从 AMI 启动的实例，请终止该实例。在导航窗格中，选择 Instances。选择实例，然后依次选择 Actions、Instance State 和 Terminate。当系统提示您确认时，选择 Yes, Terminate。

清除由实例存储支持的 AMI

取消注册某个由实例存储支持的 AMI 时，不会影响您在创建该 AMI 时上传到 Amazon S3 的文件。这些文件将继续在 Amazon S3 中对您产生使用费用。因此，如果您使用完这些文件，应删除它们。

下图说明清除由实例存储支持的 AMI 的过程。

清除由实例存储支持的 AMI

1. 使用 `deregister-image` 命令取消注册 AMI，如下所示。

```
aws ec2 deregister-image --image-id ami_id
```

AMI 状态现在变为 unavailable。

2. 使用 `ec2-delete-bundle` (p. 89) (AMI 工具) 命令删除 Amazon S3 中的源包，如下所示。

```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -s your_secret_access_key  
-p image
```

3. (可选) 如果您使用完从 AMI 启动的实例，则可以使用 `terminate-instances` 命令终止该实例，如下所示。

```
aws ec2 terminate-instances --instance-ids instance_id
```

4. (可选) 如果您使用完将捆绑上传到的 Amazon S3 存储桶，则可以删除该存储桶。要删除 Amazon S3 存储桶，请打开 Amazon S3 控制台，选择存储桶，再选择 Actions，然后选择 Delete。

Amazon Linux

Amazon Linux 由 Amazon Web Services (AWS) 提供。它旨在为 Amazon EC2 上运行的应用程序提供稳定、安全和高性能的执行环境。此外，它还包括让您能够与 AWS 轻松集成的软件包，包括启动配置工具和许多常见的 AWS 库及工具。AWS 为运行 Amazon Linux 的所有实例提供持续的安全性和维护更新。

Note

对 Amazon Linux AMI 存储库结构进行了配置以提供不间断的更新，可让您从一个版本的 Amazon Linux AMI 更新到下一版本。要将现有实例锁定到当前版本，请参阅 [存储库配置 \(p. 126\)](#)。

要启动 Amazon Linux 实例，请使用 Amazon Linux AMI。AWS 向 Amazon EC2 用户提供 Amazon Linux AMI，无需额外费用。

主题

- [查找 Amazon Linux AMI \(p. 123\)](#)
- [启动并连接到 Amazon Linux 实例 \(p. 123\)](#)
- [识别 Amazon Linux AMI 映像 \(p. 123\)](#)
- [包含的 AWS 命令行工具 \(p. 124\)](#)
- [cloud-init \(p. 125\)](#)
- [存储库配置 \(p. 126\)](#)
- [添加软件包 \(p. 127\)](#)
- [访问源软件包获取参考信息 \(p. 127\)](#)
- [开发应用程序 \(p. 127\)](#)
- [实例存储访问 \(p. 128\)](#)
- [产品生命周期 \(p. 128\)](#)
- [安全更新 \(p. 128\)](#)
- [支持 \(p. 128\)](#)

查找 Amazon Linux AMI

有关最新 Amazon Linux AMI 的列表，请参阅 [Amazon Linux AMI](#)。

启动并连接到 Amazon Linux 实例

找到您需要的 AMI 后，记下 AMI ID。您可以使用 AMI ID 来启动，然后连接到您的实例。

默认情况下，Amazon Linux 不支持远程根 SSH。此外，密码验证已禁用，以防止强力 (brute-force) 密码攻击。要在 Amazon Linux 实例上启用 SSH 登录，您必须在实例启动时为其提供密钥对。您还必须设置用于启动实例的安全组以允许 SSH 访问。默认情况下，唯一可以使用 SSH 进行远程登录的账户是 `ec2-user`；此账户还拥有 `sudo` 特权。如果您希望启动远程根登录，请注意，其安全性不及依赖密钥对和二级用户。

有关启动和使用 Amazon Linux 实例的信息，请参阅 [启动实例 \(p. 243\)](#)。有关连接到 Amazon Linux 实例的更多信息，请参阅 [连接到 Linux 实例 \(p. 253\)](#)。

识别 Amazon Linux AMI 映像

每个映像都包含唯一的 `/etc/image-id`，用于识别 AMI。此文件包含有关映像的信息。

下面是 /etc/image-id 文件示例：

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn-ami-hvm"
image_version="2017.03"
image_arch="x86_64"
image_file="amzn-ami-hvm-2017.03.0.20170401-x86_64.ext4.gpt"
image_stamp="26a3-ed31"
image_date="20170402053945"
recipe_name="amzn ami"
recipe_id="47cfa924-413c-d460-f4f2-2af7-feb6-9e37-7c9f1d2b"
```

image_name、image_version 和 image_arch 项目来自 Amazon 用于构建映像的构建配方。image_stamp 只是映像创建期间随机生成的唯一十六进制值。image_date 项目的格式为 YYYYMMDDhhmmss，是映像创建时的 UTC 时间。recipe_name 和 recipe_id 是 Amazon 用于构建映像的构建配方的名称和 ID，用于识别当前运行的 Amazon Linux 的版本。当您从 yum 存储库安装更新时，此文件不会更改。

Amazon Linux 包含 /etc/system-release 文件，用于指定当前安装的版本。此文件通过 yum 进行更新，是 system-release RPM 的一部分。

下面是 /etc/system-release 文件示例：

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux AMI release 2017.03
```

Amazon Linux 还包含 /etc/system-release 文件（在 /etc/system-release-cpe 中）的计算机可读版本，遵循 MITRE 的 CPE 规范（[CPE](#)）。

包含的 AWS 命令行工具

以下常用 AWS 集成命令行工具及使用方法已包含在 Amazon Linux 或默认存储库中：

- aws-amitools-ec2
- aws-apitools-as
- aws-apitools-cfn
- aws-apitools-ec2
- aws-apitools-elb
- aws-apitools-iam
- aws-apitools-mon
- aws-apitools-rds
- aws-cfn-bootstrap
- aws-cli
- aws-scripts-ses

Note

最低版本 Amazon Linux (amzn-ami-minimal-*) 不包含以上包；但您可以在默认 yum 存储库中找到它们并使用以下命令安装：

```
[ec2-user ~]$ sudo yum install -y package_name
```

虽然每个 Amazon Linux 版本都包含 aws-apitools-* 命令行工具，但是 aws-cli 命令行工具可在所有 Amazon Web Services 间提供标准体验，将最终替代特定于服务的工具集。

对于使用 IAM 角色启动的实例，提供了一个简单脚本，用于在安装证书文件后准备 AWS_CREDENTIAL_FILE、JAVA_HOME、AWS_PATH、PATH 和产品特定的环境变量，以简化这些工具的配置。

此外，为了支持安装多个版本的 API 和 AMI 工具，我们还在 /opt/aws 中提供了指向所需工具版本的符号链接，如下所述：

/opt/aws/bin

指向每个已安装工具目录中的 /bin 目录的符号链接。

/opt/aws/{apitools|amitools}

产品安装在形式为 *name--version* 的目录中，符号链接 *name* 附加到最近安装的版本。

/opt/aws/{apitools|amitools}/*name*/environment.sh

/etc/profile.d/aws-apitools-common.sh 用于设置产品特定的环境变量，如 EC2_HOME。

cloud-init

cloud-init 软件包是由 Canonical 构建的开源应用程序，用于在云计算环境（例如 Amazon EC2）中引导启动 Linux 映像。Amazon Linux 包含自定义版 cloud-init。它使您能够指定实例启动时应执行的操作。启动实例时，您可以通过用户数据字段将需要的操作传递到 cloud-init。这意味着，您可以在许多用例中使用普通 AMI，并在启动时进行动态配置。Amazon Linux 还使用 cloud-init 来执行 ec2-user 账户的初始配置。

有关 cloud-init 的更多信息，请参阅 <http://cloudinit.readthedocs.org/en/latest/>。

Amazon Linux 使用以下 cloud-init 操作（可在 /etc/sysconfig/cloudinit 中配置）：

- 操作：INIT (始终运行)
 - 设置默认区域设置
 - 设置主机名
 - 解析并处理用户数据
- 动作：CONFIG_SSH
 - 生成主机私有 SSH 密钥
 - 将用户的公有 SSH 密钥添加到 ssh/authorized_keys，以便于登录和管理
- 动作：PACKAGE_SETUP
 - 准备 yum 存储库
 - 处理用户数据中定义的软件包操作
- 动作：RUNCMD
 - 运行 shell 命令
- 动作：RUN_USER_SCRIPTS
 - 执行在用户数据中找到的脚本
- 动作：CONFIG_MOUNTS
 - 装载暂存驱动器
- 动作：CONFIG_LOCALE
 - 根据用户数据，在区域设置配置文件中配置区域设置

支持的用户数据格式

cloud-init 软件包可处理多种格式的用户数据：

- Gzip
 - 如果用户数据是经过 gzip 压缩过的，cloud-init 可解压缩数据，并进行适当处理。

- **MIME 多部分内容型**
 - 使用 MIME 多部分内容型文件，您可以指定多种数据类型。例如，您可以指定用户数据脚本和云配置类型。如果分段文件是受支持的格式，则 `cloud-init` 可以处理其每个段。
- **Base64 解码**
 - 如果用户数据使用 base64 编码，`cloud-init` 可确定它能否将解码后的数据理解为一种受支持的类型。如果它能理解解码后的数据，则会解码数据，并进行适当处理。如果不能，它将完整地返回 base64 数据。
- **用户数据脚本**
 - 开头为 `#!` 或 `Content-Type: text/x-shellscript`。
 - 该脚本由 `/etc/init.d/cloud-init-user-scripts` 在首轮启动过程中执行。此操作会在启动过程的后期发生（即执行初始配置操作后）。
- **包含文件**
 - 开头为 `#include` 或 `Content-Type: text/x-include-url`。
 - 此内容是一个包含文件。该文件包含一个 URL 列表，每行一个 URL。系统会读取每个 URL，其内容会通过此相同规则集验证。从 URL 读取的内容可使用 `gzip` 进行压缩、采用 MIME 分段处理或存储为纯文本。
- **云配置数据**
 - 开头为 `#cloud-config` 或 `Content-Type: text/cloud-config`。
 - 此内容是云配置数据。查看示例以了解受支持配置格式的带有注释的示例。
- **Cloud Boothook**
 - 开头为 `#cloud-boothook` 或 `Content-Type: text/cloud-boothook`。
 - 此内容为 boothook 数据。它存储在 `/var/lib/cloud` 下的文件中，然后立即执行。
 - 这是最早可用的 "hook"。请注意，尚无仅供运行一次的机制。boothook 必须自行解决此问题。它的环境变量 `INSTANCE_ID` 中包含实例 ID。可使用此变量来提供一组一个实例可用一次的 boothook 数据。

存储库配置

从 2011.09 版 Amazon Linux 开始，Amazon Linux AMI 被当作时间快照处理，因此当您运行 `yum update -y` 时，存储库和更新结构可始终为您提供最新的软件包。

存储库结构进行了配置以提供不间断的更新流，可让您从一个版本的 Amazon Linux 滚动到下一版本。举例来说，如果从较旧版本的 Amazon Linux AMI（如 2016.09 或更低版本）启动实例并运行 `yum update -y`，则会得到最新程序包。

您可通过启用 `lock-on-launch` 功能禁用 Amazon Linux 滚动更新。`lock-on-launch` 功能会锁定您最近启动的实例，使其仅接收来自指定版本的 AMI 的更新。举例来说，您可以启动 2016.09 AMI，使其仅接收早于 2017.03 AMI 发布的更新，直至您准备好迁移到 2017.03 AMI 为止。要在新实例中启用 `lock-on-launch` 功能，请使用 Amazon EC2 控制台或带有 `cloud-init` 标志的 `ec2-run-instances` 命令启动它，同时将以下用户数据传递到 `-f`。

Important

如果将 AMI 锁定到并非 `latest` 的存储库版本，则您不会收到任何后续更新。接收 Amazon Linux AMI 的连续更新流的唯一方式是使用最新的 AMI，或持续更新您的旧 AMI，使存储库指向 `latest`。

```
#cloud-config
repo_releasever: 2016.09
```

将现有实例锁定在当前 AMI 版本

1. 编辑 `/etc/yum.conf`。
2. 评论 `releasever=latest`。

3. 运行 `yum clean all`，以清除缓存。

添加软件包

Amazon Linux 可与每个 Amazon EC2 区域中托管的在线软件包存储库结合使用。这些存储库为 Amazon Linux AMI 中的软件包提供持续更新，并可再访问数百个常见的开源服务器应用程序。所有区域都提供这些存储库，可使用 yum 更新工具访问，[Amazon Linux AMI 软件包站点](#) 也有提供。通过在每个地区托管存储库，我们可以快速部署更新，不会产生任何数据传输费。通过发出 yum 命令可安装软件包，如下例所示：

```
[ec2-user ~]$ sudo yum install httpd
```

系统配置了对 Extra Packages for Enterprise Linux (EPEL) 存储库的访问权限，但默认情况下没有启用。除了 Amazon Linux 存储库中的软件包以外，EPEL 还提供了第三方软件包。AWS 不支持第三方软件包。

如果您发现 Amazon Linux 中没有您需要的应用程序，可以直接在 Amazon Linux 实例上安装该应用程序。Amazon Linux 使用 RPM 和 yum 进行软件包管理，这可能是最简单的新应用程序安装方式。您始终应该首先查看我们的中央 Amazon Linux 存储库，确定其中是否有您需要应用程序，因为许多应用程序在那里都可以找到。您可以轻松地将这些应用程序添加到 Amazon Linux 实例。

要将应用程序上传到正在运行的 Amazon Linux 实例，请使用 `scp` 或 `sftp`，然后通过登录实例来配置应用程序。您还可以使用内置 `PACKAGE_SETUP` 软件包中的 `cloud-init` 操作，在实例启动期间上传应用程序。有关更多信息，请参阅 [cloud-init \(p. 125\)](#)。

Important

如果您的实例在 Virtual Private Cloud (VPC) 中运行，则必须将 Internet 网关连接到 VPC，才能连接您的 yum 存储库。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [Internet 网关](#)。

访问源软件包获取参考信息

您可以使用 Amazon Linux 中提供的工具，查看您已在实例上安装的软件包的源，获取参考信息。您可以查看 Amazon Linux 和在线软件包存储库中包含的全部软件包的源软件包。只需确定您要安装的源软件包的名称，并使用 `get_reference_source` 命令在您正在运行的实例中查看源。例如：

```
[ec2-user ~]$ get_reference_source -p bash
```

以下为示例响应：

```
Requested package: bash Found package from local RPM database:  
bash-4.2.46-20.36.amzn1.x86_64 Corresponding source RPM to found package :  
bash-4.2.46-20.36.amzn1.src.rpm Are these parameters correct? Please type  
'yes' to continue: yes Source RPM downloaded to: /usr/src/srpm/debug/  
bash-4.2.46-20.36.amzn1.src.rpm
```

源 RPM 在实例的 `/usr/src/srpm/debug` 目录中。您可以在那里进行解压缩，并可以使用标准 RPM 工具查看源树进行参考。完成调试之后，该软件包可供使用。

Important

如果您的实例在 Virtual Private Cloud (VPC) 中运行，则必须将 Internet 网关连接到 VPC，才能连接您的 yum 存储库。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [Internet 网关](#)。

开发应用程序

Amazon Linux 的 yum 存储库中提供了一套完整的 Linux 开发工具。要在 Amazon Linux 上开发应用程序，请通过 yum 选择所需的开发工具。另外，许多在 CentOS 和其他类似发行版上开发的应用程序应该可以在 Amazon Linux 上运行。

实例存储访问

实例存储驱动器 `ephemeral0` 只能安装在 Amazon 实例存储支持的 AMI 上的 `/media/ephemeral0` 中。这与在 `/mnt` 下安装实例存储驱动器的许多其他映像不同。

产品生命周期

Amazon Linux AMI 定期进行更新，增强了安全性及功能。如果您不需要在 Amazon Linux 实例上保留数据或自定义项，只需用最新 Amazon Linux AMI 重新启动新实例即可。如果您需要保留 Amazon Linux 实例的数据或自定义项，可以通过 Amazon Linux yum 存储库维护这些实例。yum 存储库包含所有已更新软件包。您可以选择将这些更新应用到正在运行的实例中。

即使新版本发布后，旧版的 AMI 和更新软件包仍继续可用。在某些情况下，如果您需要针对旧版 Amazon Linux 的支持，则通过 AWS Support，作为支持流程的一部分，我们可能会要求您迁移到较新的版本。

安全更新

安全更新通过 Amazon Linux AMI yum 存储库及更新的 Amazon Linux AMI 提供。[Amazon Linux AMI 安全中心](#)会发布安全警报。有关 AWS 安全策略的更多信息，或要报告安全问题，请访问 [AWS 安全中心](#)。

Amazon Linux AMI 已配置为在启动时下载和安装安全更新。此操作是通过名为 `cloud-init` 的 `repo_upgrade` 设置控制的。以下 `cloud-init` 配置片段显示如何修改传递到实例初始化的用户数据文本中的设置：

```
#cloud-config
repo_upgrade: security
```

`repo_upgrade` 设置可能会有以下值：

`security`

应用 Amazon 标记为安全更新的重要更新。

`bugfix`

应用 Amazon 标记为缺陷修正的更新。缺陷修正是一组较大的更新，其中包括安全更新和针对各种其他小漏洞的修正更新。

`all`

应用全部适用更新 (不论类别)。

`none`

实例启动时不应用任何更新。

`repo_upgrade` 的默认设置是安全的。也就是说，如果您不在用户数据中指定其他值，在默认情况下，Amazon Linux AMI 在启动时执行适用于当时所有已安装软件包的安全升级。在您使用 `/etc/motd` 文件登录时，Amazon Linux AMI 还会通过列出可用更新的数量，通知您已安装程序包的所有更新。要安装这些更新，您需要在实例上运行 `sudo yum upgrade`。

Important

如果您的实例在 Virtual Private Cloud (VPC) 中运行，则必须将 Internet 网关连接到 VPC，才能连接您的 yum 存储库。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [Internet 网关](#)。

支持

AWS Support 订阅包含对安装和使用基础 Amazon Linux AMI 的支持。有关更多信息，请参阅 [AWS Support](#)。

建议您将有关 Amazon Linux 的任何问题发布到 [Amazon EC2 forum](#)。

用户提供的内核

如果您的Amazon EC2实例上需要自定义内核，您可以从与您所需最接近的AMI开始，在您的实例上编译自定义内核，并修改 `menu.lst` 文件以指向新内核。该过程根据您的AMI所使用的虚拟化类型而异。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。

内容

- [HVM AMI \(GRUB\) \(p. 129\)](#)
- [半虚拟化 AMI \(PV-GRUB\) \(p. 130\)](#)

HVM AMI (GRUB)

HVM 实例卷就像是物理磁盘。启动过程类似于具有分区磁盘和启动加载程序的裸金属操作系统，使它能够与当前支持的所有 Linux 分发配合使用。最常见的启动加载程序是 GRUB，以下部分对配置 GRUB 以使用自定义内核进行了说明。

针对 HVM AMI 配置 GRUB

以下是针对 HVM AMI 的 `menu.lst` 配置文件的示例。在该示例中，可以选择两个内核条目：Amazon Linux 2017.03 (该 AMI 的原始内核)，和 Vanilla Linux 4.7.4 (来自 <https://www.kernel.org/> 的较新版 Vanilla Linux 内核)。Vanilla 条目是从此 AMI 的原始条目复制的，`kernel` 和 `initrd` 路径已更新为新位置。`default 0` 参数将引导加载器指向其发现的第一个条目 (在此例中为 Vanilla 条目)，`fallback 1` 参数在引导第一个条目的过程中发生问题时，将引导加载器指向下一个条目。

默认情况下，GRUB 不会将其输出发送到实例控制台，因为它会造成额外启动延迟。有关更多信息，请参阅 [实例控制台输出 \(p. 671\)](#)。如果您安装自定义内核，您应该考虑通过删除 `hiddenmenu` 行并将 `serial` 和 `terminal` 行添加到 `/boot/grub/menu.lst` 启用 GRUB 输出，如下例中所示。

Important

避免在启动过程打印大量调试信息；连续控制台不支持高速数据传输。

```
default=0
fallback=1
timeout=5
serial --unit=0 --speed=9600
terminal --dumb --timeout=5 serial console

title Vanilla Linux 4.7.4
root (hd0)
kernel /boot/vmlinuz-4.7.4 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initrd.img-4.7.4

title Amazon Linux 2017.03 (4.9.17-8.31.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-4.9.17-8.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initramfs-4.9.17-8.31.amzn1.x86_64.img
```

无需在 `menu.lst` 文件中指定后备内核，但是我们建议您在测试新内核时准备好后备内核。如果新内核发生故障时，GRUB 可以退回其他内核。如果有后备内核，实例即使没有找到新内核也能进行引导。

如果您的新 vanilla Linux 内核发生故障，则输出类似于以下示例。

```
^M Entry 0 will be booted automatically in 3 seconds. ^M Entry 0 will be booted
automatically in 2 seconds. ^M Entry 0 will be booted automatically in 1 seconds.
```

```
Error 13: Invalid or unsupported executable format  
[ 0.000000] Initializing cgroup subsys cpuset
```

半虚拟化 AMI (PV-GRUB)

使用半虚拟化 (PV) 的 Amazon 系统映像 会在启动过程中使用名为 PV-GRUB 的系统。PV-GRUB 是半虚拟化启动加载器，运行经过修补的 GNU GRUB 0.97 版本。当您启动实例时，PV-GRUB 会开始启动过程，然后链式加载映像的 `menu.lst` 文件指定的内核。

PV-GRUB 理解标准 `grub.conf` 或 `menu.lst` 命令，可与当前支持的所有 Linux 分发版本配合使用。较旧发布版 (如 Ubuntu 10.04 LTS、Oracle Enterprise Linux 或 CentOS 5.x) 需要特殊的“`ec2`”或“`xen`”内核软件包，而较新发布版在默认内核软件包中包含所需驱动程序。

大多数新半虚拟化 AMI 在默认情况下使用 PV-GRUB AKI (包括 Amazon EC2 启动向导快速启动菜单中提供的所有半虚拟化 Linux AMI)，无需执行附加步骤即可在实例上使用不同的内核，前提是使用的内核与您的发布版兼容。在实例上运行自定义内核的最佳方式是从接近于您所需内容的 AMI 开始，然后在实例上编译自定义内核并修改 `menu.lst` 文件 (如为半虚拟化 AMI 配置 GRUB (p. 130) 所示) 以使用该内核启动。

可以通过使用 Amazon EC2 命令行工具执行以下 `describe-images` 命令 (换入要检查的内核映像 ID)，验证 AMI 的内核映像是否为 PV-GRUB AKI：

```
$ aws ec2 describe-images --filters Name=image-id,Values=aki-880531cd
```

检查 `Name` 字段是否以 `pv-grub` 开头。

主题

- [PV-GRUB 的限制 \(p. 130\)](#)
- [为半虚拟化 AMI 配置 GRUB \(p. 130\)](#)
- [Amazon PV-GRUB Kernel Image ID \(p. 131\)](#)
- [更新 PV-GRUB \(p. 133\)](#)

PV-GRUB 的限制

PV-GRUB 具有以下限制：

- 您不能使用 64 位版本的 PV-GRUB 来启动 32 位的内核，反之亦然。
- 当您使用 PV-GRUB AKI 时，不能指定 Amazon Ramdisk Image (ARI)。
- AWS 经测试确认 PV-GRUB 可与以下文件系统格式配合使用：EXT2、EXT3、EXT4、JFS、XFS 和 ReiserFS。其他文件系统格式可能不适用。
- PV-GRUB 可以引导使用 gzip、bzip2、lzo 和 xz 压缩格式压缩的内核。
- 群集 AMI 不支持也不需要 PV-GRUB，因为它们使用完全硬件虚拟化 (HVM)。当半虚拟化实例使用 PV-GRUB 来启动时，HVM 实例卷用作实际磁盘，并且启动过程与带已分区磁盘和启动加载程序的裸金属操作系统的类似。
- PV-GRUB 版本 1.03 及更低版本不支持 GPT 分区；它们仅支持 MBR 分区。
- 如果您计划通过 Amazon EBS 卷使用逻辑卷管理 (LVM)，则需要在 LVM 外有一个独立的启动分区。然后，您可以通过 LVM 创建逻辑卷。

为半虚拟化 AMI 配置 GRUB

要启动 PV-GRUB，GRUB `menu.lst` 文件必须存在于映像中；此文件的最常见位置是 `/boot/grub/menu.lst`。

以下是用于启动带 PV-GRUB AKI 的 AMI 的 menu.lst 配置文件示例。在该示例中，可在两个内核条目中进行选择：Amazon Linux 2017.03 (此 AMI 的原始内核)，以及 Vanilla Linux 4.7.4 (来自 <https://www.kernel.org/> 的较新 Vanilla Linux 内核版本)。Vanilla 条目是从此 AMI 的原始条目复制的，kernel 和 initrd 路径已更新为新位置。default 0 参数将引导加载器指向其发现的第一个条目 (在此例中为 Vanilla 条目)，fallback 1 参数在引导第一个条目的过程中发生问题时，将引导加载器指向下一个条目。

```
default 0
fallback 1
timeout 0
hiddenmenu

title Vanilla Linux 4.7.4
root (hd0)
kernel /boot/vmlinuz-4.7.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.7.4

title Amazon Linux 2017.03 (4.9.17-8.31.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.9.17-8.31.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.9.17-8.31.amzn1.x86_64.img
```

无需在 menu.lst 文件中指定后备内核，但是我们建议您在测试新内核时准备好后备内核。如果新内核发生故障，PV-GRUB 可以回退到其他内核。如果有后备内核，实例即使没有找到新内核也能进行引导。

PV-GRUB 检查以下位置是否存在 menu.lst，使用找到的第一项：

- (hd0)/boot/grub
- (hd0,0)/boot/grub
- (hd0,0)/grub
- (hd0,1)/boot/grub
- (hd0,1)/grub
- (hd0,2)/boot/grub
- (hd0,2)/grub
- (hd0,3)/boot/grub
- (hd0,3)/grub

请注意，PV-GRUB 1.03 及更低版本仅检查此列表中的前两个位置。

Amazon PV-GRUB Kernel Image ID

PV-GRUB AKI 在所有 Amazon EC2 区域中都可用。同时存在适用于 32 位和 64 位架构类型的 AKI。大多数新 AMI 在默认情况下使用 PV-GRUB AKI。

我们建议您始终使用最新版本的 PV-GRUB AKI，因为并不是所有的 PV-GRUB AKI 版本都能与全部实例类型兼容。使用以下 `describe-images` 命令可获取当前区域的 PV-GRUB AKI 列表：

```
$ aws ec2 describe-images --owners amazon --filters Name=name,Values=pv-grub-* .gz
```

请注意，PV-GRUB 是 ap-southeast-2 区域中唯一可用的 AKI。您应验证要复制到此区域的任何 AMI 是否使用此区域中可用的 PV-GRUB 版本。

以下是每个区域的当前 AKI ID。使用 hd0 AKI 注册新 AMI。

Note

在之前提供 hd0 AKI 的地区，我们将继续提供，以实现向后兼容性。

ap-northeast-1 , 亚太区域 (东京)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-f975a998 | pv-grub-hd0_1.05-i386.gz |
| aki-7077ab11 | pv-grub-hd0_1.05-x86_64.gz |

ap-southeast-1、亚太区域 (新加坡)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-17a40074 | pv-grub-hd0_1.05-i386.gz |
| aki-73a50110 | pv-grub-hd0_1.05-x86_64.gz |

ap-southeast-2、亚太区域 (悉尼)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-ba5665d9 | pv-grub-hd0_1.05-i386.gz |
| aki-66506305 | pv-grub-hd0_1.05-x86_64.gz |

eu-central-1、欧洲 (法兰克福)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-1419e57b | pv-grub-hd0_1.05-i386.gz |
| aki-931fe3fc | pv-grub-hd0_1.05-x86_64.gz |

eu-west-1、欧洲 (爱尔兰)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-1c9fd86f | pv-grub-hd0_1.05-i386.gz |
| aki-dc9ed9af | pv-grub-hd0_1.05-x86_64.gz |

sa-east-1、南美洲 (圣保罗)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-7cd34110 | pv-grub-hd0_1.05-i386.gz |
| aki-912fbcf9 | pv-grub-hd0_1.05-x86_64.gz |

us-east-1、美国东部 (弗吉尼亚北部)

| 映像 ID | 映像名称 |
|--------------|--------------------------|
| aki-04206613 | pv-grub-hd0_1.05-i386.gz |

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-5c21674b | pv-grub-hd0_1.05-x86_64.gz |

us-gov-west-1、AWS GovCloud (US)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-5ee9573f | pv-grub-hd0_1.05-i386.gz |
| aki-9ee55bff | pv-grub-hd0_1.05-x86_64.gz |

us-west-1、美国西部 (加利福尼亚北部)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-43cf8123 | pv-grub-hd0_1.05-i386.gz |
| aki-59cc8239 | pv-grub-hd0_1.05-x86_64.gz |

us-west-2、美国西部 (俄勒冈)

| 映像 ID | 映像名称 |
|--------------|----------------------------|
| aki-7a69931a | pv-grub-hd0_1.05-i386.gz |
| aki-70cb0e10 | pv-grub-hd0_1.05-x86_64.gz |

更新 PV-GRUB

我们建议您始终使用最新版本的 PV-GRUB AKI，因为并不是所有的 PV-GRUB AKI 版本都能与全部实例类型兼容。较旧版本的 PV-GRUB 也并非在所有区域都可用，因此如果您将使用较旧版本的 AMI 复制到不支持该版本的区域，则无法引导从该 AMI 启动的实例，直至您更新内核映像。使用以下过程可检查您的实例的 PV-GRUB 版本并在必要时更新它。

检查您的 PV-GRUB 版本

1. 查找您实例的内核 ID。

```
$ aws ec2 describe-instance-attribute --instance-id instance_id --attribute kernel --region region

{
    "InstanceId": "instance_id",
    "KernelId": "aki-70cb0e10"
}
```

此实例的内核 ID 是 aki-70cb0e10。

2. 查看该内核 ID 的版本信息。

```
$ aws ec2 describe-images --image-ids aki-70cb0e10 --region region

{
    "Images": [
```

```
{  
    "VirtualizationType": "paravirtual",  
    "Name": "pv-grub-hd0_1.05-x86_64.gz",  
    ...  
    "Description": "PV-GRUB release 1.05, 64-bit"  
}  
]  
}
```

该内核映像是 PV-GRUB 1.05。如果您的 PV-GRUB 版本不是最新版本 (如 [Amazon PV-GRUB Kernel Image ID \(p. 131\)](#) 所示) , 则应使用以下过程更新它。

更新您的 PV-GRUB 版本

如果您的实例使用较旧版本的 PV-GRUB , 则您应将它更新为最新版本。

1. 通过 [Amazon PV-GRUB Kernel Image ID \(p. 131\)](#) 确定您区域和处理器架构的最新 PV-GRUB AKI。
2. 停止您的实例。您的实例必须停止才能修改所使用的内核映像。

```
$ aws ec2 stop-instances --instance-ids instance_id --region region
```

3. 修改用于您实例的内核映像。

```
$ aws ec2 modify-instance-attribute --instance-id instance_id --kernel kernel_id --  
region region
```

4. 重新启动您的实例。

```
$ aws ec2 start-instances --instance-ids instance_id --region region
```

Amazon EC2 实例

如果您是首次接触 Amazon EC2，请参阅以下主题了解其用法：

- [什么是 Amazon EC2？\(p. 1\)](#)
- [Amazon EC2 的设置 \(p. 15\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 20\)](#)
- [实例生命周期 \(p. 241\)](#)

您需先回答以下问题，然后才能启动生产环境。

Q. 什么样的实例类型最能满足我的需求？

Amazon EC2 提供不同的实例类型，以便您可以选择需要的 CPU、内存、存储和网络容量来运行您的应用程序。有关更多信息，请参阅 [实例类型 \(p. 135\)](#)。

Q. 什么样的购买选项最能满足我的需求？

Amazon EC2 支持按需实例（默认设置）、竞价型实例和预留实例。有关更多信息，请参阅 [实例购买选项 \(p. 160\)](#)。

Q. 哪种类型的根卷能满足我的需求？

由 Amazon EBS 或实例存储支持的每一个实例。根据您需要的根卷类型选择 AMI。有关更多信息，请参阅 [根设备存储 \(p. 60\)](#)。

Q. 我能否从使用 Virtual Private Cloud 中获益？

如果您可以在 EC2-Classic 或 EC2-VPC 中启动实例，您将需要确定哪个平台能满足您的需求。有关更多信息，请参阅 [支持的平台 \(p. 435\)](#) 和 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 431\)](#)。

问：我能否在混合环境中远程管理 EC2 实例以及 设备的队列？

您可以使用 Amazon Elastic Compute Cloud (Amazon EC2) 安全地远程管理混合环境中您的 Amazon EC2 实例、虚拟机 (VM) 和服务器的配置，或者来自其他云提供商的虚拟机的配置。有关更多信息，请参阅 [Systems Manager 远程管理 \(Run Command\)](#)。

实例类型

启动实例时，您指定的实例类型 决定了用于您的实例的主机硬件。每个实例类型提供不同的计算、内存和存储功能，并按照这些功能分组到实例系列。选择一种基于您打算在实例上运行的应用程序或软件的需求的实例类型。

Amazon EC2 为每个实例提供一致且可预计的 CPU 容量，无论实际的底层硬件是什么。

CPU、内存和实例存储这类主机资源是 Amazon EC2 专用的。但 Amazon EC2 也会在实例间共享主机的另一些资源，例如网络和磁盘子系统。如果一台主机上的每个实例都试图尽可能多地使用这些共享的资源，那么每个实例都将获得该资源相等份额。然而，当某个资源未被充分利用时，实例往往可以在它可用时获取该资源的更高份额。

每种实例类型均从共享资源提供更高或更低的起始性能。例如，高 I/O 性能的实例类型能获取共享资源的更高份额。分配更大份额的共享资源也降低了 I/O 性能的方差。对于大多数应用程序，中等 I/O 是绰绰有余的。然而，对于需要更大或一致性更高的 I/O 性能的应用程序，可考虑使用更高 I/O 性能的实例类型。

内容

- [可用实例类型 \(p. 136\)](#)
- [硬件规格 \(p. 137\)](#)
- [虚拟化类型 \(p. 137\)](#)
- [联网和存储功能 \(p. 137\)](#)
- [实例限量 \(p. 139\)](#)

可用实例类型

Amazon EC2 提供了以下各表中列出的实例类型。

当前一代实例

为获得最佳性能，我们建议您在启动新实例时使用当前一代实例类型。有关当前一代实例类型的更多信息，请参阅 [Amazon EC2 实例](#)。

| 实例系列 | 当前一代实例类型 |
|-------|--|
| 通用型 | t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge m3.medium m3.large m3.xlarge m3.2xlarge |
| 计算优化 | c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge |
| 内存优化 | r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge r4.large r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge x1.16xlarge x1.32xlarge |
| 存储优化 | d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge i3.large i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge |
| 加速的计算 | p2.xlarge p2.8xlarge p2.16xlarge g2.2xlarge g2.8xlarge |

上一代实例

Amazon Web Services 为根据上一代实例优化了应用程序，但尚未升级的用户提供了上一代实例。我们鼓励您使用最新一代的实例以获得最佳性能，但我们将继续支持这些上一代数据库实例。如果您目前使用的是上一代实例，您可以查看哪个当前一代实例是合适的升级。有关更多信息，请参阅 [上一代实例](#)。

| 实例系列 | 上一代实例类型 |
|-------|---|
| 通用型 | m1.small m1.medium m1.large m1.xlarge |
| 计算优化 | c1.medium c1.xlarge cc2.8xlarge |
| 内存优化 | m2.xlarge m2.2xlarge m2.4xlarge cr1.8xlarge |
| 存储优化 | hi1.4xlarge hs1.8xlarge |
| 加速的计算 | cg1.4xlarge |
| 微型实例 | t1.micro |

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

要确定最适合您需求的实例类型，我们建议启动一个实例，并使用自己的基准测试应用程序。由于是按实例小时数付费，因而您能够在做出决策前方便而经济地测试不同的实例类型。

在做出决策后，如果您的需求有变化，则可以在稍后调整您的实例的大小。有关更多信息，请参阅 [调整您的实例大小 \(p. 156\)](#)。

Note

Amazon EC2 实例运行在 64 位虚拟 Intel 处理器上，如实例类型产品页面上所指定。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。然而，64 位 CPU 的命名约定可能会导致混淆。芯片制造商 Advanced Micro Devices (AMD) 成功引入了第一款基于 Intel x86 指令集的商用 64 位架构。因此，不论芯片制造商是谁，这一架构被普遍称为 AMD64。Windows 和多个 Linux 发行版遵循这一实践。这说明了为什么实例即使运行在 Intel 硬件上，但 Ubuntu 或 Windows EC2 实例上的内部系统信息仍将 CPU 架构显示为 AMD64。

虚拟化类型

每个实例类型支持以下虚拟化类型中的一种或两种：半虚拟 (PV) 或硬件虚拟机 (HVM)。实例的虚拟化类型由用于启动该实例的 AMI 决定。

为获得最佳性能，我们建议您使用 HVM AMI。此外，HVM AMI 还需要利用增强联网。HVM 虚拟化使用 AWS 平台提供的硬件辅助技术。借助 HVM 虚拟化，客户虚拟机如同在本地硬件平台上运行一样，除了仍然使用半虚拟 (PV) 网络和存储驱动程序以提高性能。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。

联网和存储功能

当您选择实例类型时，您同时选择了可用的联网和存储功能。

联网功能

- 某些实例类型在 EC2-Classic 中不可用，因此您必须在 VPC 中启动它们。在 VPC 中启动实例可以让您获得 EC2-Classic 不支持的功能，例如增强联网、将多个私有 IPv4 地址分配给实例、将 IPv6 地址分配给实例，以及更改分配给实例的安全组。有关更多信息，请参阅 [实例类型仅在 VPC 中可用 \(p. 434\)](#)。
- 为了最大程度提高您的实例类型的联网和带宽性能，您可以执行以下操作：
 - 在置放群组中启动受支持的实例类型可以面向高性能计算 (HPC) 应用程序优化实例。通用置放群组中的实例可以受益于高带宽 (10 Gbps)、低延迟的联网。有关更多信息，请参阅 [置放群组 \(p. 487\)](#)。支持 10 Gbps 网络速度的实例类型只有在置放群组中启动时才能利用这些网络速度。

- 为受支持的当前一代实例类型启用增强联网，从而显著提高每秒数据包数 (PPS) 性能、减弱网络抖动和减少网络延迟。有关更多信息，请参阅 [Linux 上的增强联网 \(p. 492\)](#)。
- 支持的最大 MTU 因实例类型而异。所有 Amazon EC2 实例类型都支持标准以太网 V2 1500 MTU 框架。所有当前一代实例都支持 9001 MTU (超大框架)，某些上一代实例也支持它们。有关更多信息，请参阅 [EC2 实例的网络最大传输单位 \(MTU\) \(p. 489\)](#)。

存储功能

- 一些实例类型支持 EBS 卷和实例存储卷，而另一些实例类型仅支持 EBS 卷。某些支持实例存储卷的实例使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。有关更多信息，请参阅 [存储 \(p. 515\)](#)。
- 若要获得 Amazon EBS I/O 的额外专用容量，您可以将某些实例类型作为 EBS 优化实例启动。某些实例类型在默认情况下会进行 EBS 优化。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。

下表总结了当前一代实例类型支持的联网和存储功能。

| | 仅限 VPC | 仅限于 EBS | SSD 卷 | 置放群组 | 仅限 HVM | 增强联网 | IPv6 支持 (仅限 VPC) |
|-----|--------|---------|-------|------|--------|---|------------------|
| C3 | | | 是 | 是 | | Intel 82599 VF | 是 |
| C4 | 是 | 是 | | 是 | 是 | Intel 82599 VF | 是 |
| D2 | | | | 是 | 是 | Intel 82599 VF | 是 |
| G2 | | | 是 | 是 | 是 | | |
| I2 | | | 是 | 是 | 是 | Intel 82599 VF | 是 |
| I3 | 是 | | 是 * | 是 | 是 | ENA | 是 |
| M3 | | | 是 | | | | |
| M4 | 是 | 是 | | 是 | 是 | m4.16xlarge: ENA 所有其他尺寸：Intel 82599 VF | 是 |
| P2 | 是 | 是 | | 是 | 是 | ENA | 是 |
| R3 | | | 是 | 是 | 是 | Intel 82599 VF | 是 |
| R4 | 是 | 是 | | 是 | 是 | ENA | 是 |
| T2 | 是 | 是 | | | 是 | | 是 |
| X 1 | 是 | | 是 | 是 | 是 | ENA | 是 |

* I3 实例的根设备卷必须是 Amazon EBS 卷。

实例限量

在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。

有关默认限制的更多信息，请参阅[我在 Amazon EC2 中运行多少个实例？](#)

有关查看当前限制或请求提高当前限制的更多信息，请参阅[Amazon EC2 服务限制 \(p. 633\)](#)。

T2 实例

T2 实例旨在提供适度的基准性能，并能够根据您工作负载的需要实现性能的显著突增。它们旨在用于不经常或不持续使用完整 CPU、但偶尔需要突增性能的工作负载。T2 实例非常适合于通用工作负载，如 Web 服务器、开发人员环境和小型数据库。有关 T2 实例定价的更多信息和其他硬件详细信息，请参阅[Amazon EC2 实例](#)。

如果您的账户不到 12 个月，您可以在特定使用限制下免费使用 t2.micro 实例。有关更多信息，请参阅[AWS 免费套餐](#)。

内容

- [硬件规格 \(p. 139\)](#)
- [T2 实例要求 \(p. 139\)](#)
- [CPU 积分 \(p. 139\)](#)
- [监控 CPU 积分 \(p. 141\)](#)

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅[Amazon EC2 实例](#)。

T2 实例要求

以下是 T2 实例的要求：

- 必须在 Virtual Private Cloud (VPC) 中启动 T2 实例；EC2-Classic 平台不支持 T2 实例。Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。您无法将 EC2-Classic 中的现有实例的实例类型更改为 T2 实例类型。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 435\)](#)。有关启动仅限 VPC 的实例的更多信息，请参阅[实例类型仅在 VPC 中可用 \(p. 434\)](#)。
- 您必须使用 HVM AMI 启动 T2 实例。有关更多信息，请参阅[Linux AMI 虚拟化类型 \(p. 62\)](#)。
- 您必须使用 EBS 卷作为根设备来启动 T2 实例。有关更多信息，请参阅[Amazon EC2 根设备卷 \(p. 11\)](#)。
- T2 实例可用作按需实例和预留实例，但它们不能用作竞价型实例、计划实例或专用实例。此外，它们在专用主机上不受支持。有关这些选项的详细信息，请参阅[实例购买选项 \(p. 160\)](#)。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。默认情况下，您最多可同时运行 20 个 T2 实例。如果您需要更多 T2 实例，可以使用[Amazon EC2 实例请求表](#)请求实例。
- 确保您选择的 T2 实例大小达到您的操作系统和应用程序的最低内存要求。在许多使用案例中，带有消耗大量内存和 CPU 资源的图形用户界面的操作系统（例如，Windows）可能需要 t2.micro 或更大的实例大小。随着您的工作负载对内存和 CPU 的需求随着时间增加，您可以扩展到更大的 T2 实例或其他 EC2 实例类型。

CPU 积分

一个 CPU 积分可以持续一分钟提供完整的 CPU 核心性能。传统 Amazon EC2 实例类型提供固定性能，而 T2 实例提供基准水平的 CPU 性能并能够突增到基准水平之上。基准性能和突增能力由 CPU 积分控制。

什么是 CPU 积分？

一个 CPU 积分等于一个 vCPU 按 100% 利用率运行一分钟。vCPU、利用率和时间的其他组合也等于一个 CPU 积分；例如，一个 vCPU 按 50% 利用率运行两分钟，或是两个 vCPU 按 25% 利用率运行两分钟。

如何赢取 CPU 积分？

每个 T2 实例开始都附带适量的初始 CPU 积分余额，随后每小时都以固定的数额持续（以毫秒级精度）接收 CPU 积分（具体取决于实例大小）。用于加减积分的核算过程也以毫秒级精度进行，因此您不必担心 CPU 积分超支；CPU 的短时间突增只消耗少部分的 CPU 积分。

当 T2 实例使用的 CPU 资源少于其基本性能水平资源限量时（如空闲时），未使用的 CPU 积分（或积分赢取与花费之间的差异）将存入积分余额且最多保留 24 小时，从而积累 CPU 积分以应对性能突增。当您的 T2 实例需要的 CPU 资源超过其基本性能水平资源限量时，它将占用 CPU 积分余额中的积分突增到最大 100% 的使用率。T2 实例拥有的 CPU 资源积分越多，它在需要更佳性能时可以超过其基本性能水平的突增时间就越长。

下表列出启动时收到的初始 CPU 积分分配、收到 CPU 积分的速率、采用完整核心性能百分比形式（利用单个 vCPU）的基本性能水平，以及实例可以累积获得的最大 CPU 积分余额。

| 实例类型 | 初始 CPU 积分* | 每小时获得的 CPU 积分 | vCPU | 基本性能（CPU 使用率） | 获得的最大 CPU 积分余额*** |
|------------|------------|---------------|------|-----------------|-------------------|
| t2.nano | 30 | 3 | 1 | 5% | 72 |
| t2.micro | 30 | 6 | 1 | 10% | 144 |
| t2.small | 30 | 12 | 1 | 20% | 288 |
| t2.medium | 60 | 24 | 2 | 40%（最大 200%）** | 576 |
| t2.large | 60 | 36 | 2 | 60%（最大 200%）** | 864 |
| t2.xlarge | 120 | 54 | 4 | 90%（最大 400%）** | 1296 |
| t2.2xlarge | 240 | 81 | 8 | 135%（最大 800%）** | 1944 |

* 可使用初始 CPU 积分启动的 T2 实例数量存在限制；默认情况下，该限制被设置为每个区域中每个账户的任何 T2 实例每 24 小时可启动 100 次。如果您要提高此限制，则可以使用[基于 Amazon EC2 积分的实例启动积分表](#)提出客户支持限制提高请求。如果您的账户在 24 小时内不会启动 100 个以上 T2 实例，则此限制对您没有影响。

** t2.medium 和更大的实例都拥有多个 vCPU。表中的基本性能使用一个 vCPU 的百分比（您可以将性能拆分到多个 vCPU 上）。要计算实例的基本 CPU 使用率，则用 vCPU 百分比总和除以 vCPU 数量。例如，t2.large 的基本性能为 1 个 vCPU 的 60%。一个 t2.large 实例有 2 个 vCPU，因此以基本性能运行的 t2.large 实例的 CPU 使用率在 CloudWatch CPU 指标中显示为 30%。

*** 此最大值不包括初始 CPU 积分，初始积分将最先使用，并且不会过期。例如，启动后保持空闲长达 24 小时以上的 t2.micro 实例可达到高达 174 个积分余额（30 个初始 CPU 积分 + 获得的 144 个积分）。但是，在此实例使用初始 30 个 CPU 积分后，积分余额绝对不会超过 144 个，除非通过停止并启动此实例来产生了新的初始 CPU 积分余额。

此初始积分余额旨在提供良好的启动体验。实例的获得的最大积分余额等于每小时收到的 CPU 积分数乘以 24 小时。例如，一个 t2.micro 实例每小时获得 6 个 CPU 积分，可以积累获得的最大 CPU 积分余额为 144 个 CPU 积分。

CPU 积分是否会过期？

初始 CPU 积分不会过期，但将在实例使用 CPU 积分时最先使用它们。以指定的 5 分钟时间为间隔，未使用的获得的积分将在获得后 24 小时过期，届时，在添加任何新获得的积分之前，将从 CPU 积分余额中删除过期的任何积分。此外，实例的 CPU 积分余额不会在实例停止与启动之间保留；停止实例会导致它丢失其全部积分余额，但是当它重新启动时会再次收到初始积分余额。

例如，如果 t2.small 实例在某个小时的 CPU 使用率为 5%，则它会使用 3 个 CPU 积分（60 分钟的 5%），但它在该小时赢得 12 个 CPU 积分，因此相差的 9 个 CPU 积分会添加到 CPU 积分余额。若在这个小时内，余额中有任何 CPU 积分达到其 24 小时的过期时间，这些积分（如果实例在 24 小时前完全空闲，则会有多达 12 个积分）也会从余额中扣除。如果过期的积分量大于赢得的积分量，则积分余额会减少；相反，如果过期的积分量小于赢得的积分量，则积分余额会增多。

如果我用掉了所有积分，会发生什么情况？

如果您的实例使用其所有 CPU 积分余额，则性能会保持在基准性能水平。如果您的实例在积分较少的情况下运行，则实例的 CPU 积分消耗（因此还有 CPU 性能）会在 15 分钟间隔内逐渐降低到基本性能水平，因此您在 CPU 积分耗尽时不会遇到急剧的性能下降。如果您的实例经常用完所有 CPU 积分余额，建议您使用更大的 T2 大小，或使用固定性能实例类型（如 M3 或 C3）。

监控 CPU 积分

您可以查看 CloudWatch 控制台 Amazon EC2 每个实例的指标中提供的每个 T2 实例积分余额。T2 实例有两个指标：CPUCreditUsage 和 CPUCreditBalance。CPUCreditUsage 指标指示在测量期内使用的 CPU 积分数。CPUCreditBalance 指标指示 T2 实例获得的未使用 CPU 积分数。此余额会在突增期间耗尽，因为花费 CPU 积分的速度比获得积分的速度更快。

下表介绍新提供的 CloudWatch 指标。有关如何在 CloudWatch 中使用这些指标的更多信息，请参阅[列出实例的可用 CloudWatch 指标 \(p. 322\)](#)。

| 指标 | 说明 |
|------------------|---|
| CPUCreditUsage | <p>[T2 实例] 实例使用的 CPU 积分数。一个 CPU 积分等于一个 vCPU 按 100% 利用率运行一分钟，或者 vCPU、利用率和时间的等效组合（例如，一个 vCPU 按 50% 利用率运行两分钟，或者两个 vCPU 按 25% 利用率运行两分钟）。</p> <p>CPU 积分指标每 5 分钟仅可用一次。如果您指定一个大于五分钟的时间段，请使用 Sum 统计数据，而非 Average 统计数据。</p> <p>单位：计数</p> |
| CPUCreditBalance | <p>[T2 实例] 可供实例用于突增至超出基础 CPU 使用率的 CPU 积分数。获得积分后，积分便存储在积分余额中，到期后便会从积分余额中删除。积分在获得后 24 小时到期。</p> <p>CPU 积分指标每 5 分钟仅可用一次。</p> <p>单位：计数</p> |

计算优化型实例

计算优化型实例是受益于高性能处理器的受计算限制的应用程序的理想选择。它们非常适合用于下列应用场合：

- 批处理工作负载
- 媒体转码
- 高流量 Web 服务器、大型多人联机 (MMO) 游戏服务器和广告服务引擎

- 高性能计算 (HPC) 以及其他计算密集型应用程序

内容

- [硬件规格 \(p. 142\)](#)
- [计算实例性能 \(p. 142\)](#)
- [计算实例功能 \(p. 142\)](#)
- [支持 36 个 vCPU \(p. 142\)](#)
- [实例限量 \(p. 143\)](#)

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

计算实例性能

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。默认情况下，C4 实例会进行 EBS 优化，这不会产生额外的费用。您可以额外的较低每小时费用为您的 C3 实例启用 EBS 优化。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。

您可以启用增强联网功能。通过增强联网功能，您可以显著提高每秒数据包数 (PPS) 性能，降低网络抖动，并减少延迟。有关更多信息，请参阅 [Linux 上的增强联网 \(p. 492\)](#)。

`c4.8xlarge` 实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅 [您的 EC2 实例的处理器状态控制 \(p. 282\)](#)。

计算实例功能

计算优化型实例的功能汇总如下：

| | 仅限 VPC | 仅限于 EBS | SSD 卷 | 置放群组 | 仅限 HVM | 增强联网 |
|----|--------|---------|-------|------|--------|----------------|
| C3 | | | 是 | 是 | | Intel 82599 VF |
| C4 | 是 | 是 | | 是 | 是 | Intel 82599 VF |

有关更多信息，请参阅下列内容：

- [实例类型仅在 VPC 中可用 \(p. 434\)](#)
- [Amazon EBS 优化实例 \(p. 564\)](#)
- [Amazon EC2 实例存储 \(p. 591\)](#)
- [置放群组 \(p. 487\)](#)
- [Linux 上的增强联网 \(p. 492\)](#)

支持 36 个 vCPU

`c4.8xlarge` 实例类型提供了 36 个 vCPU，在某些 vCPU 数量限制为 32 个的 Linux 操作系统中可能会导致启动问题。强烈建议您在启动 `c4.8xlarge` 实例时，使用最新的 AMI。

以下 AMI 支持启动具有 36 个虚拟 CPU 的 `c4.8xlarge` 实例：

- Amazon Linux AMI 2017.03 (HVM)
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 (HVM)

如果必须为您的应用程序使用其他 AMI，并且您的 `c4.8xlarge` 实例启动未成功完成（例如，如果您的实例状态在启动过程中因 `Client.InstanceInitiatedShutdown` 状态转换原因而更改为 `stopped`），则请修改您的实例（如以下过程所述）以支持 32 个以上的 vCPU，以便能够使用 `c4.8xlarge` 实例类型。

更新实例以支持 32 个以上的 vCPU

1. 通过选择除 `c4.8xlarge` 以外的任何其他 C4 实例类型来使用您的 AMI 启动 C4 实例。
2. 遵照特定于操作系统的说明，将内核更新到最新版本。例如，对于 RHEL 6，使用以下命令。

```
sudo yum update -y kernel
```

3. 停止实例。
4. （可选）从可用于启动其他任何您将来所需的 `c4.8xlarge` 实例的实例创建 AMI。
5. 将已停止实例的实例类型更改为 `c4.8xlarge`（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。
6. 启动实例。如果实例正确启动，则您已完成操作。如果实例仍未正确启动，请继续执行下一个步骤。
7. （可选）如果实例仍未正确启动，则实例上的内核可能不支持 32 个以上的 vCPU。但是，如果您限制 vCPU 的数量，则可能可以启动实例。
 - a. 将已停止实例的实例类型更改为 `c4.8xlarge` 之外的任何 C4 实例类型（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。
 - b. 遵照特定于操作系统的说明，将 `maxcpus=32` 选项添加到您的启动内核参数。例如，对于 RHEL 6，编辑 `/boot/grub/menu.lst` 文件，并将以下选项添加到最近处于活动状态的 `kernel` 条目：

```
default=0
timeout=1
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-504.3.3.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-504.3.3.el6.x86_64 maxcpus=32 console=ttyS0 ro
    root=UUID=9996863e-b964-47d3-a33b-3920974fdbd9 rd_NO_LUKS KEYBOARDTYPE=pc
    KEYTABLE=us LANG=en_US.UTF-8 xen_blkfront.sda_is_xvda=1 console=ttyS0,115200n8
    console=tty0 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto rd_NO_LVM
    rd_NO_DM
initrd /boot/initramfs-2.6.32-504.3.3.el6.x86_64.img
```

- c. 停止实例。
- d. （可选）从可用于启动其他任何您将来所需的 `c4.8xlarge` 实例的实例创建 AMI。
- e. 将已停止实例的实例类型更改为 `c4.8xlarge`（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。
- f. 启动实例。

实例限量

- C4 实例需要 64 位 HVM AMI。它们具有大容量内存（RAM 最高可达 60 GiB），需要 64 位操作系统才能充分利用该容量。与内存增强型实例类型上的半虚拟化（PV）AMI 相比，HVM AMI 可提供卓越的性能。此外，您必须使用 HVM AMI 才能利用增强联网功能。

- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅[我可以在 Amazon EC2 中运行多少个实例？](#)。要申请提高限制，请使用[Amazon EC2 实例申请表](#)。

内存优化型实例

内存优化型实例旨在让处理内存中的大型数据集的工作负载实现快速性能。

R4 实例

R4 实例也适用于以下应用程序：

- 高性能关系 (MySQL) 数据库和 NoSQL (MongoDB、Cassandra) 数据库。
- 提供键值型数据内存缓存功能的分布式 Web 级缓存存储 (Memcached 和 Redis)。
- 使用用于商业智能的优化型数据存储格式与分析的内存数据库 (例如 SAP HANA)。
- 实时处理大型非结构化数据的应用程序 (金融服务、Hadoop/Spark 集群)。
- 高性能计算 (HPC) 和电子设计自动化 (EDA) 应用程序。

X1 实例

X1 实例也适用于以下应用程序：

- 内存数据库，如 SAP HANA，包含针对 Business Suite S/4HANA、Business Suite on HANA (SoH)、Business Warehouse on HANA (BW) 和 Data Mart Solutions on HANA 的 SAP 认证支持。有关更多信息，请参阅[AWS 云上的 SAP HANA](#)。
- 大数据处理引擎 (如 Apache Spark 或 Presto)。
- 高性能计算 (HPC) 应用程序。

R3 实例

R3 实例也适用于以下应用程序：

- 高性能关系 (MySQL) 数据库和 NoSQL (MongoDB、Cassandra) 数据库。
- 内存分析。
- 基因组排序和分析。
- 企业应用程序 (例如 Microsoft SharePoint)。

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅[Amazon EC2 实例](#)。

内存性能

R4 实例可以支持高达 488GiB 的 RAM。

X1 实例包括 Intel 可扩展内存缓冲区，从而提供了 300 GiB/s 的可持续内存读取带宽和 140 GiB/s 的可持续内存写入带宽。

R3 实例可以支持高达 244GiB 的 RAM。

内存优化型实例拥有增强型内存，并且需要 64 位 HVM AMI 才能利用这一容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。有关更多信息，请参阅[Linux AMI 虚拟化类型 \(p. 62\)](#)。

计算性能

R4 实例具备多达 64 个虚拟 CPU，采用两个基于 E5-2686v4 的 AWS 定制 Intel Xeon 处理器（具备内存增强型带宽和更大的 L3 缓存），可以提升内存应用程序的性能。

X1 实例具备高达 128 的 vCPU 并且由 4 个 Intel Xeon E7-8880 v3 处理器（具备内存增强型带宽和更大的 L3 缓存）提供动力来提升内存应用程序的性能。

内存优化型实例还通过最新的 Intel AES-NI 功能实现更高的加密性能，支持 Intel 事务性同步扩展 (TSX) 以提升内存事务性数据处理的性能，并支持高级矢量扩展 2 (Intel AVX2) 处理器指令以将大部分整数命令扩展为 256 位。

一些内存优化型实例提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处于非活动状态时可以进入的睡眠级别，而 P 状态控制核心所需的性能（通过 CPU 频率来测量）。有关更多信息，请参阅 [您的 EC2 实例的处理器状态控制 \(p. 282\)](#)。

网络性能

要提高内存优化型实例的网络性能，请启用增强联网功能。有关更多信息，请参阅 [Linux 上的增强联网 \(p. 492\)](#)。

R4 实例可以通过 Elastic Network Adapter (ENA) 实现较高的每秒数据包数性能同时保证稳定的低延迟。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。R4 实例的规模更小，可以实现 10Gbps 的高峰吞吐量。这些实例使用一种网络 I/O 积分机制，根据平均带宽利用率为不同实例分配网络带宽。实例在网络吞吐量低于其基线限制时会积累积分，并能够在执行网络数据传输时使用这些积分。对于需要持续使用 10Gbps 或更高带宽的工作负载，我们建议使用 r4.8xlarge 和 r4.16xlarge 实例，这两种实例分别可以使用高达 10Gbps 和 20Gbps 的网络带宽。

实例功能

内存优化型实例的功能汇总如下。

| | 仅限 VPC | 仅限于 EBS | SSD 卷 | 置放群组 | 增强联网 |
|-----|--------|---------|-------|------|----------------|
| R3 | | | 是 | 是 | Intel 82599 VF |
| R4 | 是 | 是 | | 是 | ENA |
| X 1 | 是 | | 是 | 是 | ENA |

有关更多信息，请参阅下列内容：

- [实例类型仅在 VPC 中可用 \(p. 434\)](#)
- [Amazon EBS 优化实例 \(p. 564\)](#)
- [Amazon EC2 实例存储 \(p. 591\)](#)
- [置放群组 \(p. 487\)](#)
- [Linux 上的增强联网 \(p. 492\)](#)

支持 个 vCPU

内存优化型实例具有大量虚拟 CPU，可能会在虚拟 CPU 数量上限较低的操作系统上导致启动问题。我们强烈建议您在启动内存优化型实例时使用最新的 AMI。

以下 AMI 支持启动内存优化型实例：

- Amazon Linux AMI 2016.03 (HVM) 或更高版本
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 SP1 (HVM)
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 64 位
- Windows Server 2008 SP2 64 位
- Windows Server 2003 R2 64 位

实例限量

- 您不能使用 Windows Server 2008 R2 64 位 AMI 启动 `r4.large` 和 `r4.4xlarge` 实例。
- 您不能使用 Windows Server 2008 SP2 64 位 AMI 或 Windows Server 2003 R2 64 位 AMI 启动 X1 实例，但 `x1.16xlarge` 实例外。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅[我可以在 Amazon EC2 中运行多少个实例？](#)。要申请提高限制，请使用 [Amazon EC2 实例申请表](#)。

存储优化型实例

存储优化型实例适用于需要对本地存储上的极大型数据集进行高性能顺序读写访问的工作负载。它们经过了优化，可以向应用程序提供每秒上万次低延迟性随机 I/O 操作 (IOPS)。

D2 实例

D2 实例也适用于以下应用程序：

- 大规模并行处理 (MPP) 数据仓库
- MapReduce 和 Hadoop 分布式计算
- 日志或数据处理应用程序

I2 实例

I2 实例也适用于以下应用程序：

- NoSQL 数据库
- 群集化数据库
- 联机事务处理 (OLTP) 系统

I3 实例

I3 实例也适用于以下应用程序：

- 高频率联机事务处理 (OLTP) 系统
- 关系数据库
- NoSQL 数据库
- 内存内数据库 (例如，Redis) 的缓存

- 数据仓库应用程序
- 低延迟广告技术服务应用程序

内容

- 硬件规格 (p. 147)
- 存储性能 (p. 147)
- SSD I/O 性能 (p. 147)
- 存储实例功能 (p. 148)
- 支持 个 vCPU (p. 149)
- 实例限量 (p. 150)

硬件规格

D2 实例的主要数据存储是 HDD 实例存储卷。I2 实例的主要数据存储是 SATA SSD 实例存储卷。I3 实例的主要数据存储是非易失性存储规范 (NVMe) SSD 实例存储卷。

实例存储卷仅在实例生命周期内保留。当您停止或终止实例时，将擦除其实例存储卷中的应用程序和数据。我们建议您定期备份或复制实例存储卷中的重要数据。有关更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#) 和 [SSD 实例存储卷 \(p. 597\)](#)。

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

存储性能

要确保 Linux 上的实例实现最佳磁盘吞吐量性能，建议您使用最新版本的 Amazon Linux AMI。

对于具有 NVMe 实例存储卷的实例，您必须使用内核版本为 4.4 或更高版本的 Linux AMI。否则，您的实例将无法实现可用的最大 IOPS 性能。

如果使用可支持持久授予 (可显著提高磁盘吞吐量和可扩展性的 Xen 数据块环协议的扩展) 的 Linux 内核，D2 实例可提供最佳磁盘性能。有关持久授予的更多信息，请参阅 Xen 项目博客中的[文章](#)。

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。默认情况下，D2 实例会进行 EBS 优化，这不会产生额外的费用。您可以额外的较低每小时费用为您的 I2 实例启用 EBS 优化。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。

您可以启用增强联网功能。通过增强联网功能，您可以显著提高每秒数据包数 (PPS) 性能，降低网络抖动，并减少延迟。有关更多信息，请参阅 [Linux 上的增强联网 \(p. 492\)](#)。

`d2.8xlarge` 和 `i3.16xlarge` 实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅 [您的 EC2 实例的处理器状态控制 \(p. 282\)](#)。

SSD I/O 性能

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您可以获取下表所列的 IOPS (4,096 字节的数据块大小) 性能 (在队列深度饱和时)。否则，您将获得较低的 IOPS 性能。

| 实例大小 | 100% 随机读取 IOPS | 首次写入 IOPS |
|------------------------|----------------|-----------|
| <code>i2.xlarge</code> | 35000 | 35000 |

| 实例大小 | 100% 随机读取 IOPS | 首次写入 IOPS |
|-------------|----------------|-----------|
| i2.2xlarge | 75000 | 75000 |
| i2.4xlarge | 175000 | 155000 |
| i2.8xlarge | 365000 | 315000 |
| i3.large * | 100,125 | 9,375 |
| i3.xlarge * | 206,250 | 18,750 |
| i3.2xlarge | 412,500 | 37,500 |
| i3.4xlarge | 825,000 | 75000 |
| i3.8xlarge | 1.65 百万 | 150,000 |
| i3.16xlarge | 3.3 百万 | 300,000 |

* 对于 i3.large 和 i3.xlarge 实例，您最多可获得指定的性能。

随着您不断在您的实例的基于 SSD 的实例存储卷中填充数据，您可以达到的写入 IOPS 将不断减少。这是因为，SSD 控制器必须执行额外的工作，即查找可用空间、重写现有数据，以及擦除未使用的空间以使之可供重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为实例提供的基于 SSD 的实例存储卷不会为超额配置预留空间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。(您可以使用 hdparm 实用程序来超额预置您的 SSD 卷。)虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅 [实例存储卷 TRIM 支持 \(p. 598\)](#)。

存储实例功能

存储优化型实例的功能汇总如下：

| | 仅限 VPC | SSD 卷 | 置放群组 | 增强联网 |
|----|--------|-------|------|----------------|
| D2 | | | 是 | Intel 82599 VF |
| I2 | | SATA | 是 | Intel 82599 VF |
| I3 | 是 | NVMe | 是 | ENAs |

有关更多信息，请参阅下列内容：

- [实例类型仅在 VPC 中可用 \(p. 434\)](#)
- [Amazon EBS 优化实例 \(p. 564\)](#)
- [Amazon EC2 实例存储 \(p. 591\)](#)
- [置放群组 \(p. 487\)](#)

- [Linux 上的增强联网 \(p. 492\)](#)

支持 36 个 vCPU

d2.8xlarge 实例类型提供了 36 个 vCPU，在某些 vCPU 数量限制为 32 个的 Linux 操作系统中可能会导致启动问题。强烈建议您在启动 d2.8xlarge 实例时，使用最新的 AMI。

以下 Linux AMI 支持启动具有 36 个虚拟 CPU 的 d2.8xlarge 实例：

- Amazon Linux AMI 2017.03 (HVM)
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 (HVM)

如果必须为您的应用程序使用其他 AMI，并且您的 d2.8xlarge 实例启动未成功完成（例如，如果您的实例状态在启动过程中因 `Client.InstanceInitiatedShutdown` 状态转换原因而更改为 `stopped`），则请修改您的实例（如以下过程所述）以支持 32 个以上的 vCPU，以便能够使用 d2.8xlarge 实例类型。

更新实例以支持 32 个以上的 vCPU

1. 通过选择除 d2.8xlarge 以外的任何其他 D2 实例类型来使用您的 AMI 启动 D2 实例。
2. 遵照特定于操作系统的说明，将内核更新到最新版本。例如，对于 RHEL 6，使用以下命令：

```
sudo yum update -y kernel
```

3. 停止实例。
4. (可选) 从可用于启动其他任何您将来所需的 d2.8xlarge 实例的实例创建 AMI。
5. 将已停止实例的实例类型更改为 d2.8xlarge（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。
6. 启动实例。如果实例正确启动，则您已完成操作。如果实例仍未正确启动，请继续执行下一个步骤。
7. (可选) 如果实例仍未正确启动，则实例上的内核可能不支持 32 个以上的 vCPU。但是，如果您限制 vCPU 的数量，则可能可以启动实例。
 - a. 将已停止实例的实例类型更改为 d2.8xlarge 之外的任何 D2 实例类型（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。
 - b. 遵照特定于操作系统的说明，将 `maxcpus=32` 选项添加到您的启动内核参数。例如，对于 RHEL 6，编辑 `/boot/grub/menu.lst` 文件，并将以下选项添加到最近处于活动状态的 `kernel` 条目：

```
default=0
timeout=1
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-504.3.3.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-504.3.3.el6.x86_64 maxcpus=32 console=ttyS0 ro
    root=UUID=9996863e-b964-47d3-a33b-3920974fdbd9 rd_NO_LUKS KEYBOARDTYPE=pc
    KEYTABLE=us LANG=en_US.UTF-8 xen_blkfront.sda_is_xvda=1 console=ttyS0,115200n8
    console=tty0 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto rd_NO_LVM
    rd_NO_DM
initrd /boot/initramfs-2.6.32-504.3.3.el6.x86_64.img
```

- c. 停止实例。
- d. (可选) 从可用于启动其他任何您将来所需的 d2.8xlarge 实例的实例创建 AMI。
- e. 将已停止实例的实例类型更改为 d2.8xlarge（依次选择 Actions、Instance Settings、Change Instance Type，然后按照说明进行操作）。

- f. 启动实例。

实例限量

- 您必须使用 HVM AMI 启动存储优化型实例。有关更多信息，请参阅[Linux AMI 虚拟化类型 \(p. 62\)](#)。
- 您必须使用由 Amazon EBS 支持的 AMI 启动 I3 实例。
- d2.8xlarge 实例类型具有 36 个 vCPU，在某些 vCPU 数量限制为 32 个的 Linux 操作系统中可能会导致启动问题。有关更多信息，请参阅[支持 个 vCPU \(p. 149\)](#)。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅[我可以在 Amazon EC2 中运行多少个实例？](#)。要申请提高限制，请使用[Amazon EC2 实例申请表](#)。

Linux 加速计算实例

如果需要高并行处理能力，您将受益于使用加速计算实例，这些实例提供对 NVIDIA GPU 的访问。可以通过加速计算实例来利用 CUDA 或开放计算语言 (OpenCL) 并行计算框架，从而为很多科学、工程和绘制应用加速。还可以将这些实例用于图形应用程序，包括游戏流式处理、3-D 应用流式处理和其他图形工作负载。

加速计算实例作为基于 HVM 的实例运行。硬件虚拟机 (HVM) 虚拟化使用 AWS 平台提供的硬件辅助技术。凭借 HVM 虚拟化，访客 VM 就像是在本机硬件平台上运行，这使得 Amazon EC2 提供对每个加速计算实例中的一个或多个离散 GPU 的专用访问。

可以将群集加速计算实例放入置放群组中。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅[置放群组 \(p. 487\)](#)。

内容

- [加速计算实例系列 \(p. 150\)](#)
- [硬件规格 \(p. 151\)](#)
- [加速计算实例限制 \(p. 151\)](#)
- [加速计算实例的 AMI \(p. 151\)](#)
- [在 Amazon Linux 上安装 NVIDIA 驱动程序 \(p. 151\)](#)
- [优化 GPU 设置 \(仅限 P2 实例\) \(p. 153\)](#)

有关 Windows 加速计算实例的信息，请参见 Amazon EC2 用户指南（适用于 Windows 实例）中的[Windows 加速计算实例](#)。

加速计算实例系列

加速计算实例系列使用硬件加速器（或协处理器）来执行一些功能，如浮点数计算和图形处理，比可能在 CPU 上运行的软件更有效。以下加速计算实例系列可供您在 Amazon EC2 中启动。

P2 实例

P2 实例使用 NVIDIA Tesla GPU K80 和适用于使用 CUDA 和 OpenCL 编程模型的通用 GPU 计算设计。P2 实例提供了高带宽网络、强大的单双精度浮点功能以及每个 GPU 12 GiB 的内存，非常适合深度学习、图形数据库、高性能数据库、计算流体动力学、计算金融、地震分析、分子建模、基因组学、渲染和其他服务器端 GPU 计算工作负载。

- P2 实例支持使用 Elastic Network Adapter 实现增强联网。有关更多信息，请参阅[在 VPC 中的 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 501\)](#)。
- P2 实例在默认情况下会进行 EBS 优化。有关更多信息，请参阅[Amazon EBS 优化实例 \(p. 564\)](#)。

- P2 实例支持 NVIDIA GPUDirect 对等传输。有关更多信息，请参阅 [NVIDIA GPUDirect](#)。
- 您可以执行多个 GPU 设置优化，以实现 P2 实例的最佳性能。有关更多信息，请参阅 [优化 GPU 设置（仅限 P2 实例）\(p. 153\)](#)。
- p2.16xlarge 实例类型为操作系统提供了控制处理器 C 状态和 P 状态的能力。有关更多信息，请参阅 [您的 EC2 实例的处理器状态控制 \(p. 282\)](#)。

G2 实例

G2 实例使用 NVIDIA GRID K520 GPU，并为使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。NVIDIA GRID GPU 还支持 NVIDIA 的快速捕获和编码 API 操作。示例应用程序包括视频创建服务、3D 可视化、流图形密集型应用程序，以及其他服务器端图形工作负载。

CG1 实例

CG1 实例使用 NVIDIA Tesla GPU M2050 和适用于使用 CUDA 和 OpenCL 编程模型的通用 GPU 计算设计。CG1 实例为客户提供高带宽网络、双精度浮点功能和纠错码 (ECC) 内存，使其成为高性能计算 (HPC) 应用的理想选择。

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

加速计算实例限制

加速计算实例具有以下限制：

- 您必须使用 HVM AMI 启动实例。
- 除非安装了 NVIDIA 驱动程序，否则实例无法访问 GPU。
- 您可运行的实例数存在限制。有关更多信息，请参阅 Amazon EC2 常见问题中的 [我可以在 Amazon EC2 中运行多少个实例？](#)。要请求增大这些限制，请使用以下表格：[增大 Amazon EC2 实例限制请求](#)。

加速计算实例的 AMI

为了帮助您开始使用，NVIDIA 为加速计算实例提供了 AMI。这些参考 AMI 包含 NVIDIA 驱动程序，可实现 NVIDIA GPU 的完整功能和性能。

有关具有 NVIDIA 驱动程序的 AMI 的列表，请参阅 [AWS Marketplace \(NVIDIA GRID\)](#)。

您可以使用任意 HVM AMI 启动加速计算实例。

在 Amazon Linux 上安装 NVIDIA 驱动程序

加速计算实例必须具有相应 NVIDIA 驱动程序。必须针对您计划在实例上运行的内核编译您安装的 NVIDIA 驱动程序。

Amazon 在 AWS Marketplace 中针对每次官方内核升级向 AMI 提供 NVIDIA 内核驱动程序的兼容更新版本。如果您决定使用与 Amazon 提供的版本不同的 NVIDIA 驱动程序，或决定使用非 Amazon 官方版本的内核，则须从您的系统中卸载 Amazon 提供的 NVIDIA 软件包，以避免与您将要安装的驱动程序版本相冲突。

使用此命令卸载 Amazon 提供的 NVIDIA 软件包：

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Amazon 提供的 CUDA 工具包安装包对 NVIDIA 驱动程序有依赖性。卸载 NVIDIA 软件包也会删除 CUDA 工具包。必须在安装 NVIDIA 驱动程序之后重新安装 CUDA 工具包。

您可以从 <http://www.nvidia.com/Download/Find.aspx> 下载 NVIDIA 驱动程序。为实例选择适当的驱动程序：

P2 实例

| | |
|-------|------------|
| 产品类型 | Tesla |
| 产品系列 | E 系列 |
| 产品 | K-80 |
| 操作系统 | Linux 64 位 |
| 建议/测试 | 建议/认证 |

G2 实例

| | |
|-------|------------|
| 产品类型 | GRID |
| 产品系列 | GRID 系列 |
| 产品 | GRID K520 |
| 操作系统 | Linux 64 位 |
| 建议/测试 | 建议/认证 |

CG1 实例

| | |
|-------|------------|
| 产品类型 | Tesla |
| 产品系列 | M-Class |
| 产品 | M2050 |
| 操作系统 | Linux 64 位 |
| 建议/测试 | 建议/认证 |

有关安装和配置驱动程序的更多信息，请在 NVIDIA 网站上选择驱动程序下载页面上的 ADDITIONAL INFORMATION (附加信息) 选项卡，然后选择“README (自述文件)”链接。

手动安装 NVIDIA 驱动程序

安装 Amazon Linux AMI 的驱动程序

- 运行 yum update 命令以获取用于您实例的包的最新版本。

```
[ec2-user ~]$ sudo yum update -y
```

- 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

- 重启之后重新连接到实例。

4. 为您当前运行的内核版本安装 gcc 编译器和 kernel-devel 包。

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-`uname -r`
```

5. 下载之前确定的驱动程序包。例如，以下命令为 P2 实例下载 NVIDIA 驱动程序的 352.99 版本。

```
[ec2-user ~]$ wget http://us.download.nvidia.com/XFree86/Linux-x86_64/352.99/NVIDIA-Linux-x86_64-352.99.run
```

6. 运行自安装脚本以安装 NVIDIA 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/bash ./NVIDIA-Linux-x86_64-352.99.run
```

7. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

8. 确认驱动程序正常运行。以下命令的响应会列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

Note

该命令可能需要几分钟才能运行。

```
[ec2-user ~]$ nvidia-smi -q | head  
=====NVSMI LOG=====  
Timestamp : Thu Aug 25 04:59:03 2016  
Driver Version : 352.99  
  
Attached GPUs : 8  
GPU 0000:00:04.0 : Tesla K80  
Product Name : Tesla  
Product Brand : Tesla
```

9. (仅限 P2 实例) 如果您使用的是 P2 实例，请完成下一节中的优化步骤以实现 GPU 的最佳性能。

优化 GPU 设置 (仅限 P2 实例)

您可以执行多个 GPU 设置优化，以实现 P2 实例的最佳性能。默认情况下，NVIDIA 驱动程序使用 autoboot 功能，这会改变 GPU 时钟速度。通过禁用 autoboot 功能并将 GPU 时钟速度设置为其最大频率，您可以始终实现 P2 实例的最大性能。以下过程可帮助您将 GPU 设置配置为永久，禁用 autoboot 功能，并将 GPU 时钟速度设置为其最大频率。

要优化 P2 GPU 设置

1. 将 GPU 设置配置为永久。

Note

该命令可能需要几分钟才能运行。

```
[ec2-user ~]$ sudo nvidia-smi -pm 1  
Enabled persistence mode for GPU 0000:00:0F.0.  
Enabled persistence mode for GPU 0000:00:10.0.  
Enabled persistence mode for GPU 0000:00:11.0.  
Enabled persistence mode for GPU 0000:00:12.0.  
Enabled persistence mode for GPU 0000:00:13.0.
```

```
Enabled persistence mode for GPU 0000:00:14.0.  
Enabled persistence mode for GPU 0000:00:15.0.  
Enabled persistence mode for GPU 0000:00:16.0.  
Enabled persistence mode for GPU 0000:00:17.0.  
Enabled persistence mode for GPU 0000:00:18.0.  
Enabled persistence mode for GPU 0000:00:19.0.  
Enabled persistence mode for GPU 0000:00:1A.0.  
Enabled persistence mode for GPU 0000:00:1B.0.  
Enabled persistence mode for GPU 0000:00:1C.0.  
Enabled persistence mode for GPU 0000:00:1D.0.  
Enabled persistence mode for GPU 0000:00:1E.0.  
All done.
```

- 禁用实例上所有 GPU 的 autoboot 功能。

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0  
All done.
```

- 将所有 GPU 时钟速度设置为其最大频率。

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:0F.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:10.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:11.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:12.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:13.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:14.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:15.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:16.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:17.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:18.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:19.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:1A.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:1B.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:1C.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:1D.0  
Applications clocks set to "(MEM 2505, SM 875)" for GPU 0000:00:1E.0  
All done.
```

T1 微型实例

T1 微型实例 (`t1.micro`) 提供了少量一致性 CPU 资源，可在存在更多周期时在短时间内突增 CPU 容量。这种实例非常适合需要定期增加计算周期的低吞吐量应用程序和网站。

Note

`t1.micro` 是上一代实例，已被 `t2.micro` 取代，后者具有更好的性能配置。我们建议使用 `t2.micro` 实例类型而不是 `t1.micro`。有关更多信息，请参阅 [T2 实例 \(p. 139\)](#)。

`t1.micro` 实例只可作为 Amazon EBS 支持的实例使用。

本文档介绍了 `t1.micro` 实例的运行方式，以便您了解如何对其进行应用。我们的目的不在于指定确切的行为，而是让您了解实例的工作行为，从而了解其性能。

主题

- [硬件规格 \(p. 155\)](#)
- [T1 微型实例的最佳应用程序 \(p. 155\)](#)
- [峰值期间的可用 CPU 资源 \(p. 155\)](#)
- [当实例用其分配到的资源时 \(p. 155\)](#)

- [与 m1.small 实例类型的比较 \(p. 156\)](#)
- [微型实例的 AMI 优化 \(p. 156\)](#)

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

T1 微型实例的最佳应用程序

针对 CPU 占用状态与下图所示类似的工作负载，`t1.micro` 实例可为其在短时间内突增 CPU 资源。

该实例设计为基本只在两个水平上用其 CPU 占用进行运行：普通的低背景水平和比背景水平高的简短峰值水平。我们允许实例在最高为 2 个 EC2 计算单位 (ECU) 的情况下运行（一个 ECU 提供相当于一个 1.0-1.2 GHz 2007 Opteron 或 2007 Xeon 处理器的 CPU 容量）。最大层面与背景层面之间的比率被设定为大值。我们对 `t1.micro` 实例的设计使其可以支持您的应用程序上每分钟产生的数十个请求。但是，根据您的应用程序上的每个请求所需 CPU 资源量的不同，实际性能也会大有不同。

您的应用程序 CPU 占用状态可能会不同于前述章节中的描述。下图显示了一个不适合使用 `t1.micro` 实例的应用程序的 CPU 占用状态。该应用程序针对每个请求都需要连续的数据处理 CPU 资源，从而带来 `t1.micro` 实例无法处理的 CPU 占用停滞期。

下图显示了另一个不适合使用 `t1.micro` 实例的 CPU 占用情况。此处的 CPU 占用峰值简短，但它们的产生频率太高，以使微型实例不能处理。

下图显示了另一个不适合使用 `t1.micro` 实例的 CPU 占用情况。此图中峰值的产生频率不高，但峰值之间的背景水平太高，导致 `t1.micro` 实例不能处理。

在上述每一个不适合使用 `t1.micro` 实例的工作负载案例中，我们建议您考虑使用其他实例类型。有关实例类型的信息，请参阅 [实例类型 \(p. 135\)](#)。

峰值期间的可用 CPU 资源

当您的实例 bursts 按需调节峰值以计算资源时，该实例会使用主机上的未用资源。可用量的多少取决于峰值产生时争用量的多少。无论主机上的其他实例是否处于峰值状态，实例的可用 CPU 资源永远不会为零。

当实例用其分配到的资源时

我们希望您的应用程序在一段时间内只消耗一定量的 CPU 资源。如果应用程序消耗的资源超过您的实例分配到的资源，则我们会暂时限制实例，以使其在较低的 CPU 水平下运行。如果您的实例继续使用其分配到的所有资源，则其性能会下降。我们会增加对其 CPU 水平的限制时间，从而延长实例被允许再次进行突增前的等待时间。

如果您针对您的 `t1.micro` 实例启用 CloudWatch 监控，则您可以使用 AWS 管理控制台中的“Avg CPU Utilization (CPU 平均利用率)”图表来判断您的实例是否在定期使用其分配到的所有 CPU 资源。我们建议您在每个给定的期间查看达到的最大值。如果最大值为 100%，我们建议您使用 Auto Scaling 来横向扩展（使用其他 `t1.micro` 实例和负载均衡器），或迁移到更大的实例类型。有关更多信息，请参阅 [Auto Scaling 用户指南](#)。

下图显示了前述章节中所述的三个非最优配置文件，以及它在实例消耗所分配到的资源且我们不得不限制实例 CPU 水平时可能出现的样子。如果实例消耗了其分配到的资源，我们会将其限制到低背景水平。

下图显示了数据处理 CPU 占用长时间停滞的状况。CPU 达到最大允许水平，且在实例所分配到的资源在此期间消耗完之前停留在此水平。此时，我们限制实例在低背景水平下运行，且在我们允许其在该水平之上再

次迸发之前都到在此水平运行。在分配到的资源被消耗完与我们再次对其限制之前，实例会再次停留在此水平(图形中未予显示)。

下图显示了请求太频繁的状况。实例在仅有几个请求后使用其分配到的资源，所以我们对其进行限制。我们取消限制后，实例的 CPU 占用达到了最高限制并试图紧跟请求，我们对其再次进行了限制。

下图显示了背景水平太高的情况。请注意，实例不必在最大的 CPU 水平下运行，因为我们会对其进行限制。当实例在正常背景水平之上运行且在给定期间消耗完了分配给其的资源时，我们会对实例进行限制。在此情况下(与前述情况相同)，实例无法跟进工作，于是我们会再次对其进行限制。

与 m1.small 实例类型的比较

`t1.micro` 实例在不同时间提供不同水平的 CPU 资源(最高为 2 个 ECU)。相比而言，`m1.small` 实例类型始终提供 1 个 ECU 的 CPU 资源。下图阐明了两者间的不同。

下列各图所示为前述章节所讨论的各种情况下，`t1.micro` 实例与 `m1.small` 实例的 CPU 占用情况对比。

以下第一幅图显示了对 `t1.micro` 实例而言的最佳情况(左图)，并且显示了 `m1.small` 实例的可能情况(右图)。在此情况下，我们不需要限制 `t1.micro` 实例。与 `m1.small` 实例相比，`t1.micro` 实例对每次 CPU 需求峰值的处理时间要更长。

下一幅图所示为数据处理请求用尽了 `t1.micro` 实例所分配到的资源的情况，并且显示了使用 `m1.small` 实例时的可能情况。

下一幅图所示为频繁的请求用尽了 `t1.micro` 实例所分配到的资源的情况，并且显示了使用 `m1.small` 实例时的可能情况。

下一幅图所示为背景水平用尽了 `t1.micro` 实例分配到的资源的情况，并且显示了使用 `m1.small` 实例时的可能情况。

微型实例的 AMI 优化

在为 `t1.micro` 实例类型优化 AMI 时，我们建议您遵循以下最佳做法：

- 将 AMI 设计为在 600 MB 的 RAM 上运行
- 限制使用 CPU 时间的重复出现的进程(例如，Cron 作业、守护程序)的数量

您可以使用交换空间和虚拟内存优化性能(例如，通过在独立于根文件系统的分区上设置交换空间)。

调整您的实例大小

随着您的需求变化，您可能会发现您的实例过度使用(实例类型过小)或利用不足(实例类型过大)。如果出现这种情况，您可更改您的实例大小。例如，如果您的 `t2.micro` 实例对于其工作负载过小，您可将其更改为 `m3.medium` 实例。

如果实例的根设备是 EBS 卷，您可以通过更改其实例类型来更改实例的大小，这称为调整大小。如果实例的根设备是实例存储卷，则必须将应用程序迁移到实例类型为您所需的新实例。有关根设备卷的更多信息，请参阅 [根设备存储 \(p. 60\)](#)。

在调整实例大小时，您必须选择与实例的配置兼容的实例类型。如果您所需的实例类型与您具有的实例配置不兼容，则必须将应用程序迁移到实例类型为您所需的新实例。

Important

在调整实例大小时，已调整大小的实例通常具有您在启动原始实例时指定的相同实例存储卷数。如果您要添加实例存储卷，则必须将应用程序迁移到实例类型和实例存储卷为您所需的全新实例。此规则的一个例外是：调整为存储密集型的实例类型时，默认包含更多数量的卷。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#)。

内容

- [调整大小的实例的兼容性 \(p. 157\)](#)
- [调整 Amazon EBS 支持实例的大小 \(p. 157\)](#)
- [迁移实例存储支持的实例 \(p. 158\)](#)
- [迁移到新的实例配置 \(p. 159\)](#)

调整大小的实例的兼容性

仅当实例的当前实例类型和您所需的新实例类型在下列方面兼容时，才能调整实例的大小：

- 虚拟化类型。Linux AMI 使用两种虚拟化之一：半虚拟化 (PV) 或硬件虚拟机 (HVM)。您不能调整实例大小从 PV AMI 启动的实例类型到 HVM 的实例类型。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。要查看实例的虚拟化类型，请查看 Amazon EC2 控制台中 Instances 屏幕的详细信息窗格中的 Virtualization 字段。
- 网络。EC2-Classic 中不支持某些实例类型，这些类型必须在 VPC 中启动。因此，您不能将 EC2-Classic 中的实例的大小调整为仅在 VPC 中可用的实例类型的大小，除非您有非默认 VPC。有关更多信息，请参阅 [实例类型仅在 VPC 中可用 \(p. 434\)](#)。要查看您的实例是否在 VPC 中，请查看 Amazon EC2 控制台中 Instances 屏幕的详细信息窗格中的 VPC ID 值。
- 平台。所有 Amazon EC2 实例类型都支持 64 位 AMI，但只有以下实例类型支持 32 位 AMI：t2.nano、t2.micro、t2.small、t2.medium、c3.large、t1.micro、m1.small、m1.medium 和 c1.medium。如果您要调整 32 位实例的大小，将限于这些实例类型。要查看实例的平台，请转到 Amazon EC2 控制台中的 Instances 屏幕，并选择 Show/Hide Columns、Architecture。

例如，EC2-Classic 中不支持 T2 实例，这些实例仅限 HVM。因此，您不能将 T1 实例的大小调整为 T2 实例的大小，因为 T1 实例不支持 HVM 且必须从 PV AMI 启动。如果您要将 T2 实例的大小调整到更大的实例类型的大小，则可以选择任何当代实例类型（如 M3），因为所有当代实例类型都支持 HVM AMI。有关更多信息，请参阅 [可用实例类型 \(p. 136\)](#)。

调整 Amazon EBS 支持实例的大小

您必须先停止 Amazon EBS 支持实例，然后才能更改其实例类型。当您停止和启动实例时，需要注意以下事项：

- 我们将实例迁移到新硬件；但是，实例 ID 不会更改。
- 如果您的实例在 VPC 中运行并具有公有 IPv4 地址，则我们会释放该地址并向实例提供一个新的公有 IPv4 地址。实例会保留其私有 IPv4 地址、任何弹性 IP 地址以及任何 IPv6 地址。
- 如果实例在 EC2-Classic 中运行，则我们会为其提供新的公有和私有 IP 地址，并取消该实例与任何弹性 IP 地址的关联。因此，为确保您的用户可不间断地继续使用托管在您的实例上的应用程序，在重启实例后，您必须重新关联所有弹性 IP 地址。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。为防止出现此情况，您可以在调整实例大小时，为组暂停 Auto Scaling 流程。有关更多信息，请参阅 Auto Scaling 用户指南 中的 [暂停和恢复 Auto Scaling 流程](#)。
- 当实例停止时，请确保您已计划停机时间。停止实例并调整其大小可能需要几分钟时间，重新启动实例所用的时间则由应用程序的启动脚本决定。

有关更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

使用 AWS 管理控制台，通过以下过程调整 Amazon EBS 支持实例的大小。

调整 Amazon EBS 支持实例的大小

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. [EC2-Classic] 如果实例具有关联的弹性 IP 地址，则记录下详细信息窗格中显示的弹性 IP 地址和实例 ID。
4. 依次选择 Actions、Instance State 和 Stop。
5. 在确认对话框中，选择 Yes, Stop。停止实例可能需要几分钟时间。

[EC2-Classic] 当实例状态变为 stopped 时，详细信息窗格中的 Elastic IP、Public DNS (IPv4)、Private DNS 和 Private IPs 字段为空，表明旧值不再与实例关联。
6. 在实例仍处于选中状态的情况下，依次选择 Actions、Instance Settings 和 Change Instance Type。请注意，如果实例状态不是 stopped，则禁用此操作。
7. 在 Change Instance Type 对话框中，执行以下操作：
 - a. 从 Instance Type 中，选择您所需的实例类型。如果列表中未显示您所需的实例类型，则说明它与您的实例配置不兼容（例如，由于虚拟化类型）。
 - b. （可选）如果您选择的实例类型支持 EBS 优化，则选择 EBS-optimized 以启用 EBS 优化或取消选择 EBS-optimized 以禁用 EBS 优化。请注意，如果您选择的实例类型默认情况下已经过 EBS 优化，则 EBS-optimized 已选中，您无法取消选择。
 - c. 选择 Apply 以接受新设置。
8. 要重启已停止的实例，请选择该实例，然后依次选择 Actions、Instance State 和 Start。
9. 在确认对话框中，选择 Yes, Start。实例进入 running 状态可能需要几分钟时间。
10. [EC2-Classic] 当实例状态为 running 时，详细信息窗格中的 Public DNS (IPv4)、Private DNS 和 Private IPs 字段包含我们分配给实例的新值。如果您的实例具有关联的弹性 IP 地址，则必须按以下方式对其进行重新关联：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择您在停止实例前所记下的弹性 IP 地址。
 - c. 依次选择 Actions 和 Associate address。
 - d. 从 Instance 中，选择您在停止实例前所记下的实例 ID，然后选择 Associate。

迁移实例存储支持的实例

如果您要将应用程序从一个实例存储支持的实例移至另一个不同实例类型的实例存储支持的实例，则必须通过从您的实例创建映像来迁移它，然后从此映像启动实例类型为您所需的新实例。要确保您的用户可不间断地继续使用托管在您的实例上的应用程序，您必须使用已与您的原始实例关联的任何弹性 IP 地址，并将其与新实例关联。之后您可以终止原始实例。

迁移实例存储支持的实例

1. [EC2-Classic] 如果您迁移的实例具有关联的弹性 IP 地址，请立即记录该弹性 IP 地址，以便之后可将其与新实例关联。
2. 备份实例存储卷上所有您需要保留在持久性存储中的数据。要迁移 EBS 卷上您需要保留的数据，请拍摄这些卷的快照（请参阅 [创建 Amazon EBS 快照 \(p. 559\)](#)）或从实例中分离卷，以便您之后可以将其连接到新的实例（请参阅 [从实例断开 Amazon EBS 卷 \(p. 541\)](#)）。
3. 通过满足先决条件并按照[创建由实例存储支持的 Linux AMI \(p. 78\)](#)中的过程操作，从实例存储支持的实例创建 AMI。当您通过您的实例创建完 AMI 后，请返回到此过程。

4. 打开 Amazon EC2 控制台，在导航窗格中选择 AMIs。从筛选条件列表中，选择 Owned by me，然后选择您在上一步中创建的映像。请注意，AMI Name (AMI 名称) 是您在注册映像时指定的名称，而 Source (源) 是您的 Amazon S3 存储桶。

Note

如果您没有看到在上一步中创建的 AMI，请确保您已选择在其中创建了 AMI 的区域。

5. 选择 Launch。在您为实例指定选项时，务必选择您所需的新实例类型。如果无法选择您所需的实例类型，则说明它与您创建的 AMI 的配置不兼容（例如，由于虚拟化类型）。您还可以指定从原始实例中分离的任何 EBS 卷。

请注意，实例进入 running 状态可能需要几分钟时间。

6. [EC2-Classic] 如果您启动的实例具有关联的弹性 IP 地址，则必须将该地址与新实例关联，如下所示：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择您在此过程开始时记录的弹性 IP 地址。
 - c. 依次选择 Actions 和 Associate Address。
 - d. 从 Instance 中，选择新实例，然后选择 Associate。
7. (可选) 如果不再需要用以创建映像的原有实例，则您可将其终止。选择实例并确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间）。依次选择 Actions、Instance State 和 Terminate。

迁移到新的实例配置

如果您的实例的当前配置与您所需的新实例类型不兼容，则不能将该实例的大小调整为新实例类型的大小。您可以将应用程序迁移到其配置与您所需的新实例类型兼容的新实例。

如果您要将从 PV AMI 启动的实例变为仅限 HVM 的实例类型，一般过程如下：

1. 备份实例存储卷上所有您需要保留在持久性存储中的数据。要迁移 EBS 卷上您需要保留的数据，请创建这些卷的快照（请参阅 [创建 Amazon EBS 快照 \(p. 559\)](#)）或从实例中分离卷，以便您之后可以将其挂载到新实例（请参阅 [从实例断开 Amazon EBS 卷 \(p. 541\)](#)）。
2. 启动新实例，选择下列内容：
 - HVM AMI。
 - 仅限 HVM 的实例类型。
 - [EC2-VPC] 如果您正在使用弹性 IP 地址，请选择原始实例当前正在其中运行的 VPC。
 - 您从原始实例中分离并且要挂载到新实例的任何 EBS 卷，或者基于您创建的快照的新的 EBS 卷。
 - 如果您要允许相同的流量到达新实例，请选择与原始实例关联的安全组。
3. 在实例上安装应用程序和所有必需软件。
4. 还原您在原始实例的实例存储卷中备份的所有数据。
5. 如果您正在使用弹性 IP 地址，请按如下所示将其分配给新启动的实例：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择与原始实例关联的弹性 IP 地址，然后依次选择 Actions 和 Disassociate address。当系统提示进行确认时，选择 Disassociate address。
 - c. 在弹性 IP 地址仍处于选中状态的情况下，依次选择 Actions 和 Associate address。
 - d. 从 Instance 中，选择新实例，然后选择 Associate。
6. (可选) 如果不再需要原始实例，您可以将其终止。选择实例并确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间）。依次选择 Actions、Instance State 和 Terminate。

有关将应用程序从 EC2-Classic 中的实例迁移到 VPC 中的实例的信息，请参阅 [从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 \(p. 445\)](#)。

实例购买选项

Amazon EC2 提供了以下让您根据需求优化成本的购买选项：

- 按需实例 - 按小时为您启动的实例付费。
- 预留实例 - 以大幅折扣购买一年期到三年期的始终可用的实例。
- 计划实例 - 以一年为期限购买按指定重复计划始终可用的实例。
- 竞价型实例 - 对未使用的实例竞价，只要这些实例可用且您的出价高于现货价格，就可以以大幅折扣运行这些实例。
- 专用主机 - 为完全专用于运行您的实例的物理主机付费，通过您现有的按套接字、按内核或按 VM 的软件许可证来降低成本。
- 专用实例 - 按小时付费的在单一租户硬件上运行的实例。

如果您需要容量预留，请考虑预留实例或计划实例。如果您能灵活控制应用程序的运行时间并且应用程序可以中断，那么竞价型实例将是您的经济实惠之选。使用专用主机，既能在满足合规要求上助您一臂之力，又能通过使用现有服务器端绑定软件许可来节省费用。有关更多信息，请参阅 [Amazon EC2 实例购买选项](#)。

内容

- [实例生命周期 \(p. 160\)](#)
- [预留实例 \(p. 161\)](#)
- [计划的预留实例 \(p. 184\)](#)
- [竞价型实例 \(p. 187\)](#)
- [专用主机 \(p. 227\)](#)
- [专用实例 \(p. 237\)](#)

实例生命周期

实例的生命周期在运行时开始，在停止时结束。您所选择的购买选项会影响实例的生命周期。例如，按需实例，当您启动并结束，在您终止实例。只要竞价型实例的容量可用，并且您的出价高于现货价格，便可运行。在计划的时间周期内，您可以启动计划内的实例；Amazon EC2 会启动实例并在时间周期结束的前三分钟终止它们。

使用以下程序来确定实例的生命周期。

使用控制台确定实例的生命周期

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 在描述选项卡上，查找租期。如果值为 host，表示实例正在专用主机上运行。如果值为 dedicated，表示是实例专用实例。
5. 在 Description 选项卡上，查找 生命周期。如果值为 spot，表示实例是竞价型实例。如果值为 scheduled，表示实例是计划内的实例。如果值为 normal，此实例或者是按需实例，或者是预留实例。
6. (可选)，如果您购买了预留实例并要验证它是应用，您就可以检查Amazon EC2的使用报告。有关更多信息，请参阅 [预留实例使用率报告 \(p. 638\)](#)。

使用AWS CLI来确定实例的生命周期。

使用以下[描述实例](#)口令：

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

如果实例在专用主机上运行，那么输出内容包含以下信息：

```
"Tenancy": "host"
```

如果实例为专用实例，那么输出内容包含以下信息：

```
"Tenancy": "dedicated"
```

如果实例为竞价型实例，那么输出内容包含以下信息：

```
"InstanceLifecycle": "spot"
```

如果实例为计划内的实例，那么输出内容包含以下信息：

```
"InstanceLifecycle": "scheduled"
```

否则，输出内容包含以下信息：

```
"InstanceLifecycle": "normal"
```

预留实例

相比按需实例定价，预留实例可以提供大幅折扣。预留实例不是物理实例，而是对账户中使用的按需实例所应用的账单折扣。这些按需实例必须匹配特定属性才能享受账单折扣。

在购买特定可用区中的预留实例时，它们提供了容量预留。您可以选择通过购买特定区域中的预留实例（区域预留实例）来放弃此容量预留。这些区域预留实例提供了可用区和实例大小灵活性。借助可用区灵活性，区域中任何可用区内对预留实例的使用可享受预留实例折扣。借助实例大小灵活性，对预留实例系列中的实例的使用可享受预留实例折扣，无论实例大小如何。有关更多信息，请参阅 [应用预留实例 \(p. 164\)](#)。

当您购买预留实例时，请选择符合您需求的付款选项、期限和产品类别。一般而言，通过选择具有较高预付款的预留实例您可以节省更多资金。提供了三个付款选项（无预付、部分预付、全部预付）、两个期限长度（一年或三年）和两个产品类别（可转换预留实例和标准预留实例）。

- 无预付和部分预付的预留实例将根据使用情况按小时计费，无论这些实例是否正在被使用。全部预付的预留实例无额外的按小时计算的费用。
- 可转换预留实例可以在可转换预留实例期间进行交换，新属性包括实例类型。标准预留实例可以在该期间进行修改，但是，实例类型在整个期限内固定不变。

您还可以找到由第三方卖家提供的短期低价预留实例。有关更多信息，请参阅 [预留实例市场 \(p. 163\)](#)。

预留实例不会自动续签；当它们过期时，您可以继续使用 EC2 实例而不会中断，但要支付按需费率。新的预留实例可以具有与过期实例相同的参数，或者，您也可以购买具有不同参数的预留实例。

您可以使用 Auto Scaling 或其他 AWS 服务来启动使用预留实例优惠的按需实例。有关启动按需实例的信息，请参阅[启动实例](#)。有关使用 Auto Scaling 启动实例的信息，请参阅 [Auto Scaling 用户指南](#)。

有关产品定价信息的更多信息，请参阅以下内容：

- [AWS 服务定价概述](#)
- [Amazon EC2 按需实例定价](#)

- [Amazon EC2 预留实例定价](#)

有关预留实例定价套餐的信息，请参阅[了解预留实例折扣定价套餐 \(p. 167\)](#)。

主题

- [预留实例类型 \(p. 162\)](#)
- [预留实例如何运行 \(p. 162\)](#)
- [账单优惠和付款选项 \(p. 164\)](#)
- [购买预留实例 \(p. 169\)](#)
- [在预留实例市场中出售实例 \(p. 172\)](#)
- [修改您的标准预留实例 \(p. 178\)](#)
- [交换可转换预留实例 \(p. 182\)](#)
- [修改请求故障排除 \(p. 184\)](#)

预留实例类型

有两种类型的预留实例。标准预留实例可按一年或三年期购买并应用于该期限内的单个实例系列、平台、范围和租期。

可转换预留实例可以按三年期购买，并可以在该期限内交换具有不同实例系列、平台、租期或范围的可转换预留实例交换与。

可以购买标准和可转换预留实例应用于特定可用区域，或区域中的实例。针对特定可用区购买的标准预留实例可以进行修改以应用到区域，但这样做会移除相关容量预留。

可转换预留实例可用于交换具有完全不同配置的其他可转换预留实例，包括实例类型、平台、范围或租期。不可能以这种方式交换标准预留实例。一旦购买可转换预留实例，便无法修改其范围。有关更多信息，请参阅[修改您的标准预留实例 \(p. 178\)](#) 和 [交换可转换预留实例 \(p. 182\)](#)。

预留实例如何运行

Amazon EC2 预留实例和 预留实例市场 可为您的业务运行提供强大且节省成本的战略。但是，在您使用预留实例或预留实例市场之前，请确保满足购买和出售的要求。您还必须了解预留实例和预留实例市场中某些元素的详细信息和限制。这些限制可能包括卖家注册、银行、使用 AWS 免费套餐以及处理取消的实例，等等。使用本主题作为购买和出售预留实例以及在预留实例市场中购买和出售的核对清单。

Note

要购买并修改预留实例，请确保您的 IAM 用户账户具有适当的权限，例如描述可用区的能力。有关信息，请参阅[使用 AWS CLI 或 AWS SDK 的策略示例](#)和[用于 Amazon EC2 控制台的策略示例](#)。

入门

- AWS 账户 - 您必须拥有 AWS 账户才能购买预留实例。如果您没有 AWS 账户，请阅读[Amazon EC2 的设置 \(p. 15\)](#)中所述的说明（其中包括注册 Amazon EC2 账户和凭证的相关信息）并完成相应操作。
- AWS 免费套餐 - AWS 免费套餐可供新 AWS 账户使用。如果您正在用 AWS 免费套餐运行 Amazon EC2 实例，然后您购买了一个预留实例，那么您将按照标准定价指南付费。有关适用服务及使用量的信息，请参阅[AWS 免费套餐](#)。

购买预留实例

- 使用费 - 使用预留实例时，无论您是否使用，您都需为整个期限付费。
- 购买时的套餐折扣 - 预留实例定价套餐折扣仅适用于通过 AWS 进行的购买。这些折扣不适用于第三方预留实例购买。有关信息，请参阅[了解预留实例折扣定价套餐 \(p. 167\)](#)。

- 取消购买 – 在您确认购买前，请检查您计划购买的预留实例的详细信息，并确保所有参数都是准确的。在您购买预留实例（无论是从预留实例市场中的第三方卖家购买还是从 AWS 购买）之后，将无法取消您的购买。但是，如果您需要更改，则可出售预留实例。有关信息，请参阅 [列出您的预留实例 \(p. 175\)](#)。

预留实例出售与预留实例市场

- 可转换预留实例—仅 Amazon EC2 标准预留实例可以在 预留实例市场 上出售。可转换预留实例不能出售。
- 预留实例范围 - 仅针对可用区购买的标准预留实例可在预留实例市场上出售。针对区域购买的预留实例不能出售。
- 卖方要求 – 要成为 预留实例市场 中的卖方，必须注册为卖方。有关信息，请参阅 [列出您的预留实例 \(p. 175\)](#)。
- 银行要求 - 为了在您出售预留实例时支付收取的资金，AWS 必须获得您的银行信息。您指定的银行必须有一个美国地址。有关更多信息，请参阅 [银行账户 \(p. 173\)](#)。
- 税务要求 – 出于税务原因，交易次数达到 50 次或以上的卖方或是计划出售价值 20000 USD 或以上标准预留实例的卖方必须提供关于他们业务的额外信息。有关信息，请参阅 [税务信息 \(p. 174\)](#)。
- 最低售价 - 预留实例市场中允许的最低价格为 \$0.00。
- 何时可以出售标准预留实例 - 只有在 AWS 收到预付款且预留实例已激活（您已拥有）达到 30 天之后，标准预留实例才能出售。此外，您列出的标准预留实例的剩余期限必须至少为一个月。
- 修改您的实例出售清单 - 无法直接修改您在预留实例市场中的实例出售清单。然而，您可通过先取消它然后再用新参数创建另一个实例出售清单来改变您的实例出售清单。有关信息，请参阅 [给您的预留实例定价 \(p. 175\)](#)。您也可以在列出预留实例之前修改它们。有关信息，请参阅 [修改您的标准预留实例 \(p. 178\)](#)。
- 出售折扣标准预留实例 - 通过某个套餐折扣以较低成本购买的 Amazon EC2 标准预留实例不能在预留实例市场中出售。有关更多信息，请参阅 [预留实例市场 \(p. 163\)](#)。
- 服务费 - AWS 会向您收取您在预留实例市场中出售的每个标准预留实例的总预付价格 12% 的服务费。预付价格是卖方对标准预留实例收取的费用。
- 其他 AWS 预留实例 - 只有 Amazon EC2 标准预留实例可在预留实例市场中出售。其他 AWS 预留实例（如 Amazon RDS 和 Amazon ElastiCache 预留实例）不能在预留实例市场中出售。

在 VPC 中使用预留实例

您可以将实例启动进入 VPC 并从您的标准和可转换预留实例中获益。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [Amazon VPC 是什么？](#)

如果您有 EC2 经典账户，则可购买预留实例，通过选择名称内含有 Amazon VPC 的平台将其应用于启动进入非默认 VPC 的实例。有关更多信息，请参阅 [检测支持的平台以及是否具有默认 VPC](#)。

如果您的账户仅限于 EC2-VPC，由于所有平台都有默认子网，因此可用平台列表的名称中不包含 Amazon VPC。如果您启动与预留的容量具有相同配置的实例，则会在您的默认或非默认的 VPC 中启动该实例，并且容量预留和账单优惠也会自动应用于该实例。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [您的默认 VPC 和子网](#)。

您还可以通过将专用 指定为实例租赁，选择购买在主机硬件级别被物理隔离的预留实例。有关更多信息，请参阅 [专用实例 \(p. 237\)](#)。

预留实例市场

预留实例市场是一个支持销售第三方和 AWS 客户的未使用的标准预留实例的平台，这些实例的期限时间和定价选项各不相同。例如，某位 AWS 客户可能希望在将预留实例迁移到新的 AWS 区域、更换为新的实例类型或结束项目之后，在预留实例到期之前将其出售。

预留实例市场允许您满足特定的业务需求，提供了更多选择，更加灵活。搜索与您首选的实例类型、区域及持续时间组合最接近的预留实例。

Note

仅 Amazon EC2 标准预留实例可在预留实例市场中出售。其他类型实例 (如 Amazon RDS 和 Amazon ElastiCache 预留实例) 不能在预留实例市场中出售。

账单优惠和付款选项

相比按需定价，所有预留实例为您提供了折扣。分配给可用区的预留实例提供了容量预留。您可以选择通过购买特定区域中的预留实例 (区域预留实例) 来放弃此容量预留。区域预留实例提供了可用区和实例大小灵活性。此灵活性使您能够更轻松地享受预留实例的折扣费率。

应用预留实例

预留实例以相同的方式应用，而不管产品类型如何 (标准预留实例或可转换预留实例)，并且将自动应用于满足规范要求 (例如租期和平台) 的正在运行的按需实例。分配给特定可用区的预留实例可以为该可用区中符合条件的实例使用情况提供预留实例折扣。

所有区域预留实例都提供了可用区灵活性。除此之外，Linux/Unix 平台上具有默认租期的区域预留实例也提供了实例大小灵活性。借助可用区灵活性，该区域中任何可用区内对预留实例的使用可享受预留实例折扣。借助实例大小灵活性，对该实例类型中的实例的使用可享受预留实例折扣，无论实例大小如何。

Note

仅分配给区域的具有默认租期的 Linux/Unix 预留实例支持实例大小灵活性。实例大小灵活性不适用于 Windows、带 SQL Standard 的 Windows、带 SQL Server Enterprise 的 Windows、带 SQL Server Web 的 Windows、RHEL 和 SLES 预留实例。

如果您购买可用区 us-east-1a 中的两个 c4.xlarge 默认租期 Linux/Unix 标准预留实例，则可用区 us-east-1a 中最多两个正在运行的 c4.xlarge 默认租期 Linux/Unix 实例可享受预留实例折扣。正在运行的实例的规范 (租期、平台、可用区、实例类型和实例大小) 必须匹配预留实例的规范。

如果您购买 美国东部 (弗吉尼亚北部) 中的四个 c4.xlarge 默认租期 Amazon Linux/Unix 预留实例，则预留实例折扣权益将自动应用于您账户在美国东部 (弗吉尼亚北部) 区域中的任何可用区中的任何 c4 实例，无论其大小如何。必须匹配的规范仅为实例类型、租期和平台。

下表描述了实例类型中的各种大小以及相应的标准化因子。对于实例大小灵活性，此扩展用于将预留实例的折扣费率应用于实例类型的标准化使用。

在修改标准预留实例时，标准化因子也适用。有关更多信息，请参阅 [修改您的标准预留实例 \(p. 178\)](#)。

| 实例 size | 标准化因子 |
|---------|-------|
| nano | 0.25 |
| 微型 | 0.5 |
| small | 1 |
| medium | 2 |
| large | 4 |
| xlarge | 8 |
| 2xlarge | 16 |
| 4xlarge | 32 |
| 8xlarge | 64 |

| 实例 size | 标准化因子 |
|----------|-------|
| 10xlarge | 80 |
| 32xlarge | 256 |

了解预留实例的应用

以下方案涵盖了各种应用预留实例的方式。

方案一

客户在账户 A 中运行以下按需实例：

- 4 x m3.large Linux，可用区域 us-east-1a 中的默认租期实例
- 2 x m4.xlarge Amazon Linux，可用区 us-east-1b 中的默认租期实例
- 1 x c4.xlarge Amazon Linux，可用区 us-east-1c 中的默认租期实例

然后，客户购买账户 A 中的以下预留实例：

- 4 x m3.large Linux，可用区域 us-east-1a 中的默认租期预留实例 (容量为预留)
- 4 x m4.large Amazon Linux，us-east-1 中的默认租期预留实例
- 1 x c4.large Amazon Linux，us-east-1 中的默认租期预留实例

预留实例优势以下方式应用：

- 四个 m3.large 预留实例的折扣和容量预留将由四个 m3.large 实例使用，因为它们之间的属性 (实例大小、区域、平台、租期) 相匹配。
- m4.large 预留实例提供了可用区和实例大小灵活性，因为它们是带默认租期的 Amazon Linux 预留实例。m4.large 等效于 4 个标准化单位/小时。

客户已购买四个 m4.large 预留实例，它们一起等效于 16 个标准化单位/小时 (4x4)。账户 A 具有两个正在运行的 m4.xlarge 实例，等效于 16 个标准化单位/小时 (2x8)。在此情况下，四个 m4.large 预留实例提供了针对两个 m4.xlarge 实例的整个使用时间 (小时) 的账单优势。

- us-east-1 中的 c4.large 预留实例提供了可用区和实例大小灵活性，因为它是带默认租期的 Amazon Linux 预留实例，并且将应用于 c4.xlarge 实例。c4.large 实例等效于 4 个标准化单位/小时，c4.xlarge 等效于 8 个标准化单位/小时。

在此情况下，c4.large 预留实例提供了针对 c4.xlarge 用量的部分优势。这是因为 c4.large 预留实例等效于 4 个标准化单位/小时的用量，而 c4.xlarge 实例与 8 个标准化单位/小时对应。因此，c4.large 预留实例账单折扣应用于 50% 的 c4.xlarge 用量。剩余的 c4.xlarge 用量按照按需费率收费。

区域 Linux/Unix 预留实例应用于匹配实例系列中的区域、租期和平台的任何用量。预留实例先应用于购买账户中的用量，然后应用于组织的任何其他账户中符合条件的用量。对于提供大小灵活性的预留实例，预留实例应用于的系列中的实例大小没有优先级。预留实例折扣应用于 AWS 账单系统先检测到的合格用量。以下示例可能有助于您的理解。

方案二

客户在账户 A 中运行以下按需实例：

- 2 x m4.xlarge Linux，可用区域 us-east-1a 中的默认租期实例
- 1 x m4.2xlarge Linux，可用区域 us-east-1b 中的默认租期实例

- 2 x c4.xlarge Linux , 可用区域 us-east-1a 中的默认租期实例
- 1 x c4.2xlarge Linux , 可用区域 us-east-1b 中的默认租期实例

客户正在账户 B (关联账户) 中运行以下按需实例：

- 2 x m4.xlarge Linux , 可用区域 us-east-1a 中的默认租期实例

然后，客户购买账户 A 中的以下预留实例：

- 4 x m4.xlarge Linux , us-east-1 中的默认租期预留实例
- 2 x c4.xlarge Linux , us-east-1 中的默认租期预留实例

预留实例优势以以下方式应用：

- 四个 m4.xlarge 预留实例的折扣由账户 A 中的两个 m4.xlarge 实例和账户 A 中的 m4.2xlarge 实例使用。所有三个实例都匹配属性 (实例系列、区域、平台、租期)。没有容量预留。
- 两个 c4.xlarge 预留实例的折扣可应用于匹配属性 (实例系列、区域、平台、租期) 的两个 c4.xlarge 实例或 c4.2xlarge 实例，具体取决于账单系统首先检测到的用量。不为特定实例大小提供优先权。没有容量预留。

通常，一个账户拥有的预留实例将首先应用于该账户中的用量。不过，如果组织中其他账户中有合格的未使用区域预留实例，这些实例将先于账户拥有的区域预留实例应用于账户。这样做是为了确保实现最大预留实例使用率和较低的费用。出于记账目的，组织中的所有账户将被视为一个账户。以下示例可能有助于您的理解。

方案三

客户正在运行账户 A 中的以下实例

- 1 x m4.xlarge Linux , 可用区域 us-east-1a 中的默认租期实例

客户正在运行另一个关联账户 B 中的以下实例：

- 1 x m4.xlarge Linux , 可用区域 us-east-1b 中的默认租期实例

然后，客户购买账户 A 中的以下预留实例：

- 1 x m4.xlarge Linux , 可用区 us-east-1 中的默认租期预留实例

客户还购买账户 C 中的以下预留实例：

- 1 x m4.xlarge Linux , 可用区域 us-east-1a 中的默认租期预留实例

预留实例优势以以下方式应用：

- 账户 C 拥有的 m4.xlarge 预留实例的折扣应用于账户 A 中的 m4.xlarge 用量。
- 账户 A 拥有的 m4.xlarge 预留实例的折扣应用于账户 B 中的 m4.xlarge 用量。
- 如果账户 A 拥有的预留实例先应用于账户 A 中的用量，则账户 C 拥有的预留实例将保持未使用状态，而账户 B 中的用量将按照按需费率收费。

有关更多信息，请参阅 [Billing and Cost Management 报告中的预留实例](#)。

选择预留实例付款选项

预留实例有三种付款选项：

- 无预付 - 无论是否使用，您都将按照期限内的小时数，采用打折小时费率进行付费，无需任何预付款。此选项只能用于标准预留实例一年期预留和可转换预留实例三年期预留。

Note

在整个预留期限内，“无预付”预留实例需要根据合同义务每月支付费用。因此，在某个账户能够购买“无预付”预留实例前，该账户需要具有成功的账单历史记录。

- 部分预付 - 必须预付部分费用，期限内剩余的小时数无论是否使用，都将按照打折小时费率计费。
- 全部预付 - 所有款项于期限开始时支付，无论使用了多少个小时，剩余期限不会再产生其他任何费用。

了解按小时计费

在您选择的预留实例期限内，无论实例是否正在运行，预留实例均按小时进行计费。请务必了解实例状态之间的差异以及这些差异对计费小时数的影响。有关更多信息，请参阅 [实例生命周期 \(p. 241\)](#)。

预留实例的计费优惠仅适用于每小时内一个实例小时。实例小时从实例启动之时开始计时，持续 60 分钟或持续到实例停止或终止时，以时间较早者为准。将从午夜至次日午夜的标准 24 小时均分为 24 个小时，其中一个小时则定义为一个实例小时（例如，1:00: 00 到 1:59:59 为一小时）。

当实例持续运行 60 分钟时，或者实例停止又重新启动时，一个新的实例小时则开始计时。重启实例将不会重置运行实例小时。

例如，如果实例在一个小时内停止后重新启动，并持续运行了两个多小时，则第一个实例小时（重启前）按折扣后的预留实例费率收费。下一个实例小时（重启后）以按需费率收费，下两个实例小时按折扣后的预留实例费率收费。

[预留实例使用率报告 \(p. 638\)](#)部分包括示例报告，其中说明了针对正在运行的按需实例节省的成本。[预留实例常见问题](#)包括标价计算的示例。

了解预留实例折扣定价套餐

如果您的账户有资格获得折扣定价套餐，那么自您取得该资格时起，您在该套餐等级内购买的所有预留实例的预付费和每小时使用费均自动享受折扣。要取得折扣资格，您在该区域内的预留实例的标价必须达到 500000 美元或更高。

Note

折扣定价套餐当前不适用于可转换预留实例购买。

主题

- [计算预留实例定价折扣 \(p. 167\)](#)
- [定价套餐的整合账单 \(p. 168\)](#)
- [以折扣套餐价格购买 \(p. 168\)](#)
- [当前定价套餐限制 \(p. 168\)](#)
- [跨越定价套餐 \(p. 169\)](#)

计算预留实例定价折扣

通过计算您在区域中的所有预留实例的标价，可以确定您的账户所适用的定价套餐。将每个预留实例的每小时费用乘以每个期限的剩余小时数，加上购买时 [AWS 营销网站](#) 所列的未打折预付价格（称为固定价格）。由于标价基于未打折（公开）定价，您是否有资格获得总量折扣或者您购买预留实例后是否降价均不影响标价。

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

使用 AWS 管理控制台查看预留实例的固定价格

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 通过选择右上角的 Show/Hide 显示 Fixed Price 列。

使用命令行查看预留实例的固定价格

- 使用 AWS CLI , 请参阅 [describe-reserved-instances](#)
- 使用适用于 Windows PowerShell 的 AWS 工具 , 请参阅 [Get-EC2ReservedInstance](#)
- 使用 Amazon EC2 API , 请参阅 [DescribeReservedInstances](#)

定价套餐的整合账单

整合账单账户汇总了某个区域内所有成员账户的标价。当整合账单账户的所有活动预留实例的标价达到折扣定价套餐时，整合账单账户的任何账户成员在此后购买任何预留实例都将享受打折费率 (前提是整合账单账户的标价始终高于折扣定价套餐阈值)。有关更多信息，请参阅 [预留实例和整合账单 \(p. 169\)](#)。

以折扣套餐价格购买

当您购买预留实例时，Amazon EC2 会自动将所有折扣应用于购买中处于折扣定价套餐范围内的部分。您无需执行任何其他操作，而且可以使用任何 Amazon EC2 工具进行购买。有关更多信息，请参阅 [在预留实例市场中购买 \(p. 172\)](#)。

Note

预留实例购买是确定您的折扣定价套餐的唯一购买行为，这些折扣也仅适用于购买 Amazon EC2 预留实例。

您在某区域的活动预留实例的标价达到某一折扣定价套餐范围后，未来在该区域中购买任何预留实例都将按打折费率收费。如果在某区域的预留实例单项购买额超过了折扣套餐阈值，那么此项购买超出价格阈值的部分将按打折费率收费。有关在购买过程中创建的临时预留实例 ID 的更多信息，请参阅 [跨越定价套餐 \(p. 169\)](#)。

如果您的标价降至低于折扣定价套餐价格点 (例如，如果部分预留实例到期)，之后在该区域购买预留实例将不享受折扣。但是，原来在折扣定价套餐范围内购买的所有预留实例都将继续享受折扣。

当您购买预留实例时，可能出现以下四种情况之一：

- 没有折扣 - 您在某区域内的购买仍然低于折扣阈值。
- 部分折扣 - 您在某区域内的购买跨越了第一折扣套餐的阈值。没有折扣将应用于一个或多个预留，而折扣费率将应用于剩余的预留。
- 全部折扣 - 您在某区域内的购买全部在一个折扣套餐之内并且获得了相应的折扣。
- 两种折扣率 - 您在某区域内的购买从较低折扣套餐跨入较高的折扣套餐。您将按两种费率付费：一个或多个预留采用较低的折扣费率，剩余的预留采用较高的折扣费率。

当前定价套餐限制

以下限制当前适用于预留实例定价套餐：

- 预留实例定价套餐和相关折扣仅适用于购买Amazon EC2预留实例。
- 预留实例定价套餐不适用于带有 SQL Server Standard 的 Windows 或带有 SQL Server Web 的 Windows 的预留实例。

- 作为套餐折扣的一部分购买的 预留实例无法在预留实例市场上出售。有关更多信息，请参阅[预留实例市场 \(p. 163\)](#)页面。

跨越定价套餐

如果您的购买跨入某个折扣定价套餐范围，您将看到该项购买有多个条目：一个条目显示购买中将按常规价格收费的部分，另一个条目显示购买中将按适用的打折费率收费的部分。

预留实例服务会生成多个预留实例 ID，因为您的购买从未打折套餐跨入到打折套餐，或从一个打折套餐跨入到另一个打折套餐。套餐中的每组预留都有一个 ID。因此，由您的购买 CLI 命令或 API 操作返回的 ID 将不同于新预留实例的实际 ID。

预留实例和整合账单

当购买账户属于在一个整合账单付款人账户之下开具账单的一套账户的一部分时，预留实例的定价优惠可以共享。将所有子账户的小时使用量每月聚合到付款人账户。这通常对具有不同职能团队或团体的公司很有用；然后，将应用正常的预留实例逻辑来计算账单。有关更多信息，请参阅[AWS Billing and Cost Management 用户指南](#)中的整合账单。

有关预留实例定价套餐的折扣如何应用于整合账单账户的更多信息，请参阅[Amazon EC2 预留实例](#)。

阅读您的声明 (发票)

您可通过查看 AWS 管理控制台 中的 Billing & Cost Management 页面来查明您的账户的支出和费用状况。选择账户名旁的箭头可访问它。

- Dashboard 页面将显示您的账户的所有支出 - 例如预付费用、一次性费用及周期性费用。您可获得关于您的开支的汇总和详细清单。
- 您在预留实例市场中购买第三方预留实例而产生的预付费用将在 AWS Marketplace Charges 部分中列出，并在旁边显示卖方名称。这些预留实例的所有经常性费用或使用费将在 AWS Service Charges 部分列出。
- Detail 部分包含关于预留实例的信息 - 例如可用区域、实例类型、成本及实例的数量。

您可在线上查看开支，而且您还能下载一个关于开支信息 PDF 文件。

购买预留实例

您可搜索要购买的特定类型的预留实例，从而在找到您所寻找的完全匹配的实例之前调整参数。

购买任何预留实例时，一定要注意以下内容：

- 使用费 - 使用预留实例时，无论您是否实际使用了整个期限，都需要为该期限付费。
- 购买时的套餐折扣 - 定价套餐折扣仅适用于 AWS 标准预留实例购买。这些折扣不适用于第三方预留实例或可转换预留实例购买。有关更多信息，请参阅[了解预留实例折扣定价套餐 \(p. 167\)](#)。
- 取消购买 - 确认购买之后便无法取消。在确认之前，请检查您计划购买的预留实例的详细信息，并确保所有参数都是准确的。但是，如果您的需求发生更改并且您符合相应要求，则可以出售预留实例。有关更多信息，请参阅[在预留实例市场中出售实例 \(p. 172\)](#)。

在选择要购买的预留实例后，您将收到一个关于您选择的实例的总成本报价。当您决定购买后，AWS 将自动对购买价格设定一个限定价格。您的预留实例的总成本将不会超过对您报价的金额。

如果价格因任何原因而上升或发生变化，您将会返回至前一屏幕，并且购买将不会完成。如果在购买之时有与您的选择类似的低价位产品，AWS 将为您提供价格更低的产品。

使用 AWS 管理控制台购买标准预留实例

您可以购买带或不带容量预留的标准预留实例。

使用 AWS 管理控制台购买标准预留实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Reserved Instances 和 Purchase Reserved Instances。
3. 选择 Offering Class，再选择 Standard 以显示标准预留实例。
4. 要购买容量预留，请选择购买屏幕右上角中的 Only show offerings that reserve capacity。
5. 根据需要选择其他配置并选择 搜索。

Note

搜索结果中的 Seller 列显示卖方是否是第三方。如果是，则 Term 列会显示非标准期限。

6. 选择您要购买的预留实例，输入数量，然后选择 Add to Cart。
7. 要查看已选择的预留实例的汇总，请选择 View Cart。
8. 要完成订单，请选择 Purchase。

Note

如果在购买之时有与您的选择类似的低价位产品，AWS 将为您提供价格更低的产品。

要应用您的预留实例，请启动按需实例，确保匹配您已为您的预留实例指定的相同标准。AWS 将自动按较低的小时价格对您收费。您不必重启您的实例。

使用 AWS 管理控制台查看交易状态

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择预留实例页面。您的购买状态将在 State 列中列出。当您的订单完成时，State 值将从 payment-pending 变为 active。

使用 AWS 管理控制台购买可转换预留实例

您可以购买带或不带容量预留的可转换预留实例。

使用 AWS 管理控制台购买可转换预留实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Reserved Instances。
3. 在 Reserved Instances 页面上，选择 Purchase Reserved Instances。
4. 选择产品类别并选择 可转换以显示可转换预留实例。
5. 要购买容量预留，请选择购买屏幕右上角中的 Only show offerings that reserve capacity。
6. 根据需要选择其他配置并选择 搜索。
7. 选择您要购买的可转换预留实例，输入数量，然后选择 Add to Cart。
8. 要查看您的选择的摘要，请选择 View Cart"。
9. 要完成订单，请选择 Purchase。

Note

如果在购买之时有与您的选择类似的低价位产品，AWS 将为您提供价格更低的产品。

账单优势会自动应用到指定区域中具有匹配规范的匹配的按需实例。AWS 将自动按较低的小时价格对您收费。您不必重启您的实例。

使用 AWS 管理控制台查看交易状态

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择预留实例页面。您的购买状态将在 State 列中列出。当您的订单完成时，State 值将从 payment-pending 变为 active。

使用命令行界面或 API 购买预留实例

使用命令行或 API 购买预留实例

1. 使用 AWS CLI，请参阅 [purchase-reserved-instances-offering](#)
2. 使用适用于 Windows PowerShell 的 AWS 工具，请参阅 [New-EC2ReservedInstance](#)
3. 使用 Amazon EC2 API，请参阅 [PurchaseReservedInstancesOffering](#)

使用命令行或 API 查看交易状态

1. 使用 AWS CLI，请参阅 [describe-reserved-instances](#)
2. 使用适用于 Windows PowerShell 的 AWS 工具，请参阅 [Get-EC2ReservedInstance](#)
3. 使用 Amazon EC2 API，请参阅 [DescribeReservedInstances](#)

应用预留实例

预留实例将自动应用于正在运行的按需实例（前提是满足规范要求）。您可以使用 AWS 管理控制台、命令行工具或 Amazon EC2 API 执行这些任务。

Note

要购买并修改预留实例，请确保您的 IAM 用户账户具有适当的权限，例如描述可用区的能力。有关信息，请参阅[使用 AWS CLI 或 AWS SDK 的策略示例](#)和[用于 Amazon EC2 控制台的策略示例](#)。

购买 - 确定要预留的容量大小。指定以下条件：

- 平台（例如，Linux）。

Note

要在特定平台（例如 Windows、Linux/Unix）上使用您的预留实例，您必须在购买预留容量时确定该平台。然后，当您启动实例以使用购买的容量时，必须选择运行该特定平台的 Amazon 系统映像（AMI）以及在购买时确定的任何其他规格。

- 实例类型（例如，m1.small）。
- 预留的范围（地区或可用区域）。
- 预留容量的期限（时间段）。
- 租期。您可为实例预留容量，以便在单租户硬件（dedicated 租户，与 shared 相反）中运行。您选择的租期必须与正在或计划将预留实例应用于的按需实例的租期匹配。有关更多信息，请参阅[专用实例（p. 237）](#)。
- 产品类别（标准或可转换）。
- 服务（无预付、部分预付、全部预付）。

使用 - 要使用您的预留实例，请启动具有与购买的预留相同的规格的按需实例。定价优惠和容量预留自动适用于预留容量中尚未包含的所有匹配实例。

有关更多信息，请参阅[启动实例（p. 243）](#)。

预留实例状态

预留实例可以处于以下某种状态：

- **active** – 预留实例可供使用。
- **payment-pending** – AWS 正在处理您的预留实例付款。当状态变为 active 时，您可以使用预留实例。
- **retired** – 预留实例由于以下任何原因而终止：
 - AWS 没有收到您的付款。例如，信用卡交易没有完成。
 - 预留实例超出期限。

请务必注意，为 Reserved Instance 页面上的 State 列显示的状态信息与为 My Listings 选项卡上的 Listing State 显示的状态信息不同。

如果您是预留实例市场中的卖家，Listing State 将显示已在预留实例市场中列出的预留的状态。有关更多信息，请参阅 [预留实例出售清单状态 \(p. 177\)](#)。

在预留实例市场中购买

Note

可转换预留实例无法在预留实例市场中购买。

您可以购买 Amazon EC2 预留实例（从 AWS 购买或从拥有其不再需要的预留实例的第三方卖方购买）。

对于买方而言，预留实例市场提供了更多选择，更加灵活。您可以搜索与您首选的实例类型、区域及持续时间组合最接近的预留实例。

有关预留实例市场的更多信息，请参阅 [在预留实例市场中出售实例 \(p. 172\)](#)。

在预留实例市场中购买的预留实例与直接从 AWS 购买的预留实例有一些区别：

- **期限** – 从第三方卖方购买的预留实例拥有的剩余期限短于完整标准期限。从 AWS 获得的完整标准期限为一年或三年。
- **预付价格** – 第三方预留实例可以不同的预付价格出售。使用费或周期性费用与最初从 AWS 购买预留实例时设定的费用一致。

有关您的基本信息将与卖方进行共享，如您的邮政编码和国家/地区信息。

此信息使卖方能够计算他们必须向政府缴纳并且采用支付报告形式提供的任何必需的交易税（如销售税或增值税）。在极少数情况下，AWS 可能必须向卖方提供您的电子邮件地址，这样卖方才能就与销售相关的问题（例如税务问题）与您联系。

出于相似的原因，AWS 将在买方的购货发票上共享卖方的法律实体名称。如果您出于税务或相关原因需要关于卖方的额外信息，请联系 [AWS Support](#)。

在预留实例市场中出售实例

Note

可转换预留实例无法在预留实例市场中列出。

您在业务需求发生改变时或拥有不再需要的容量时，可以在预留实例市场中出售未使用的预留并迁移到新配置。

只要您在预留实例市场中列出您的预留实例，便可供潜在的买方找到。所有预留实例将会根据剩余期限及小时价格进行分组。

要满足买方的请求，AWS 首先出售指定群组中预付费用最低的预留实例。然后再出售下一个最低价格的预留实例，直到买方的整个订单完成为止。AWS 随后处理这些交易，并将预留实例的所有权转移给买方。

在您的预留实例出售之前，该实例将归您所有。出售之后，您便放弃了容量预留（如果已为可用区购买预留实例）和打折的周期性费用。如果继续使用您的实例，AWS 将从您的预留实例出售的时间开始以按需价格向您收费。

要注意以下重要限制：

- 预留实例可在 30 天之后出售 - 预留实例只能在您已拥有它们至少 30 天之后进行出售。此外，您列出的预留实例的剩余期限至少为一个月。
- 预留实例范围 — 在 预留实例市场 中只能销售具有容量预留的标准预留实例。不能销售具有地区优势的预留实例。
- 无法修改实例出售清单 - 您无法在预留实例市场中修改您的实例出售清单。然而，您可通过先取消它，然后再用新参数创建另一个实例出售清单来更改您的实例出售清单。有关信息，请参阅 [列出您的预留实例 \(p. 175\)](#)。您也可以在列出预留实例之前修改它们。有关信息，请参阅 [修改您的标准预留实例 \(p. 178\)](#)。
- 无法出售打折的预留实例 - 通过某个套餐折扣以较低价格购买的预留实例不能在预留实例市场中出售。有关更多信息，请参阅 [预留实例市场 \(p. 163\)](#)。

内容

- [注册为卖家 \(p. 173\)](#)
- [列出您的预留实例 \(p. 175\)](#)
- [实例出售清单的生命周期 \(p. 177\)](#)
- [在您的预留实例出售后 \(p. 178\)](#)

注册为卖家

为了能够在 预留实例市场 进行销售，您的第一个任务是注册为卖家。注册期间，您需要提供您的企业名称、关于您的银行的信息以及企业的税务标识号。

在 AWS 收到您已完成的卖家注册后，您将收到对您的注册进行确认并告知您可以开始在预留实例市场中出售实例的电子邮件。

主题

- [银行账户 \(p. 173\)](#)
- [税务信息 \(p. 174\)](#)
- [与买家共享信息 \(p. 174\)](#)
- [收款 \(p. 175\)](#)

银行账户

为了在您出售您的预留实例时支付收取的资金，AWS 必须获得您的银行信息。您指定的银行必须有一个美国地址。

注册付款的默认银行账户

1. 在 [预留实例市场 Seller Registration](#) 页面上登录。如果您没有 AWS 账户，也可通过此页面创建一个。
2. 在 Manage Bank Account 页面上，提供有关您的收款行的以下信息：

- 银行账户持有人姓名
- 路由号码

- 账号
- 银行账户类型

Note

如果您正在使用一个公司银行账户，则系统将提示您通过传真 (1-206-765-3424) 发送关于该银行账户的信息。

注册后，将提供的银行账户设置为默认账户，等待银行进行验证。验证新的银行账户可能需要两周时间，在此期间，您无法收到付款。对于已建立的账户，付款的完成通常需要两天左右的时间。

更改付款的默认银行账户

1. 在 [预留实例市场 Seller Registration](#) 页面上，使用您注册时所用的账户登录。
2. 在 Manage Bank Account 页面上，根据需要添加新的银行账户或修改默认银行账户。

[税务信息](#)

您出售预留实例可能需要交纳交易税，例如销售税或增值税。您应与您的企业的税务、法律、财务或会计部门沟通，以确定是否适用于基于交易的税种。您负责向相关税务机构收集并交纳基于交易的税款。

作为卖家注册的一部分，您可选择完成税务资料提供。如果以下事项之任一适用，那么我们鼓励您完成此过程：

- 您要 AWS 生成一个表 1099-K。
- 您期待在一个日历年内进行 50 次或更多次的交易，或者销售价值 20000 USD 或更多的预留实例。一项交易涉及一个或多个预留实例。如果您在注册时选择跳过此步骤，后来您的交易次数达到 49，那么您将收到一条消息“You have reached the transaction limit for pre-tax. Please complete the tax interview in the [Seller Registration Portal](#)”。一旦完成税务资料提供，便会自动添加账户限制。
- 您是非美国卖家。在这种情况下，您必须以电子手段完成表 W-8BEN。

有关 IRS 要求和表 1099-K 的详细信息，请参阅 [IRS website](#)。

根据您的企业是美国法律实体还是非美国法律实体，您在提供税务资料时输入的税务信息将有所不同。当您填写税务资料时，请记住以下事项：

- AWS 提供的信息（包括本主题中的信息）不构成税务、法律或其他专业建议。查明 IRS 报告要求将如何影响您的企业，或者如果您有其他问题，请联系您的税务、法律或其他专业顾问。
- 为了尽可能高效地满足 IRS 报告要求，在会见过程中回答所有的问题并输入所有要求的信息。
- 检查您的回答。避免拼写错误或输入了不正确的税务识别号，它们会导致纳税申报表格无效。

在您完成税务注册过程后，AWS 将表 1099-K 归档。您将在您的税务账户达到阈值水平的年份的后一年的 1 月 31 日收到通过美国邮政发来的 1099-K 副本。例如，如果您的税务账户于 2016 年达到阈值，则您将于 2017 年收到该表。

[与买家共享信息](#)

当您在预留实例市场中出售时，AWS 将按照美国的规章在买方声明上分享您的公司法律名称。此外，如果买家因发票或其他税务相关的原因需要联系您而致电 AWS Support，那么 AWS 可能需要向买家提供您的电子邮件地址，这样买家就能与您直接联系。

出于同样的原因，买方的邮政编码和国家/地区信息将在支付报告中提供给卖方。作为卖家，您可能需要在汇给政府任何必要的交易税（例如销售税和增值税）时附带此信息。

AWS 不能提供税务建议，但如果您的税务专家确定您另外需要特定的信息，请[联系 AWS Support](#)。

收款

AWS 从买方收到资金后，会向已售预留实例的拥有者注册账户发送一封电子邮件。

AWS 将自动清算所 (ACH) 电汇发送至您的指定银行账户。通常，此电汇在您的预留实例已售出后的一天到三天内发生。您可通过查看预留实例支付报告来查看此支付的状态。支付每天只发生一次。请记住，在 AWS 从您的银行那里收到确认信息之前，您无法接收付款。此期间可能最多需要两个星期。

您售出的预留实例将继续出现在您的 `DescribeReservedInstances` 调用的结果中。

您将直接从您的银行账户通过电汇转账收到您的预留实例的现金付款。AWS 会向您收取您在预留实例市场中出售的每个预留实例的总预付价格 12% 的服务费。

Note

仅 Amazon EC2 预留实例可在预留实例市场中出售。其他类型实例 (如 Amazon RDS 和 Amazon ElastiCache 预留实例) 不能在预留实例市场中出售。

列出您的预留实例

作为注册卖家，您可选择出售您的一个或多个预留实例。您可选择出售清单中的全部或部分实例。此外，您可以列示任何类型的预留实例 - 包括实例类型、平台、区域和可用区的任何配置。

如果您决定取消您的实例出售清单，且实例出售清单的一部分已经售出，则取消不会在已售出的部分生效。仅实例出售清单中未售出的部分在预留实例市场中将不再可用。

给您的预留实例定价

预付费用是您可为正在出售的预留实例指定的唯一费用。预付费用是买方在购买预留实例时支付的一次性费用。您无法指定使用费或周期性费用；买方将支付与最初购买预留时设定的使用费或周期性费用相同的费用。

要注意以下重要限制：

- 您每年可出售的预留实例价值最多为 50000 美元。要出售更多预留实例，请填写[提高 Amazon EC2 预留实例销售限制申请表单](#)。
- 最低价格为 \$0。预留实例市场中允许的最低价格为 \$0.00。

您无法直接修改您的实例出售清单。然而，您可通过先取消它然后再用新参数创建另一个实例出售清单来改变您的实例出售清单。

只要您的实例出售清单处于 `active` 状态，您就可以随时将其取消。您无法取消已经匹配或正在为销售进行处理的实例出售清单。如果您的实例出售清单中的某些实例已匹配且您取消了实例出售清单，则仅剩余的未匹配的实例将从实例出售清单中删除。

设置定价表

由于预留实例的价值随时间的推移而降低，因此，在默认情况下，AWS 可设定要以同样的变化量逐月降低的价格。但是，您可根据预留实例出售的时间设置不同的预付价格。

例如，如果您的预留实例剩余期限为九个月，您可以指定客户如需购买这个剩余九个月的预留实例，您愿意接受的价格。您还可以分别设置剩余期限为五个月、一个月的价格。

使用 AWS CLI 列出您的预留实例

使用 AWS CLI 列出 预留实例市场 中的预留实例

1. 通过调用`aws ec2 describe-reserved-instances`获得您的预留实例的列表。

2. 指定您要列出的预留实例的 ID 并调用 `aws ec2 create-reserved-instances-listing`。您必须指定以下必需参数：

- 预留实例 ID
- 实例计数
- 月份:价格

要查看您的实例出售清单

- 使用 `aws ec2 describe-reserved-instances-listings` 命令获取有关您的实例出售清单的详细信息。

取消并更改您的实例出售清单

- 使用 `aws ec2 cancel-reserved-instances-listings` 命令取消您的实例出售清单。

使用 Amazon EC2 API 列出您的预留实例

使用 Amazon EC2 API 在预留实例市场中列示预留实例

1. 通过调用 `DescribeReservedInstances` 获得您的预留实例的列表。记下您要在预留实例市场中列示的预留实例的 ID。
2. 使用 `CreateReservedInstancesListing` 创建实例出售清单。

要查看您的实例出售清单

1. 调用 `DescribeReservedInstancesListings` 可得到关于您的实例出售清单的详细信息。

要取消您的实例出售清单

1. 运行 `CancelReservedInstancesListing`。
2. 确认已通过调用 `DescribeReservedInstancesListings` 来取消实例出售清单。

使用 AWS 管理控制台列出您的预留实例

若要在预留实例市场中列出预留实例，可使用 AWS 管理控制台

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择要列示的预留实例，然后选择 Sell Reserved Instances。
4. 在 Configure Your Reserved Instance Listing 页面上，在相关列中设置要出售的实例数并为剩余期限设定预付价格。单击 Months Remaining 列旁边的箭头，了解您的预留的价值是如何随着剩余期限的变化而变化的。
5. 如果您是高级用户且想对定价进行自定义，那么您可为后续月输入一个不同的值。要返回默认的线性价格降低，请选择 Reset。
6. 当您完成配置您的实例出售清单后，请选择 Continue。
7. 在 Confirm Your Reserved Instance Listing 页面上确认您的实例出售清单的详细信息并且对此类信息感到满意，请选择 List Reserved Instance。

在控制台中查看您的实例出售清单

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Reserved Instances。
3. 选择您列出的预留实例，然后选择 My Listings。

预留实例出售清单状态

Listing State 显示您的实例出售清单的当前状态：

Listing State 显示的信息与您在预留实例市场中的实例出售清单的状态有关。它与 Reserved Instances 页面中的 State 列显示的状态信息不同。此 State 信息是关于您的预留的。

- active - 实例出售清单可供购买。
- cancelled - 实例出售清单已取消，并且在预留实例市场中不再可供购买。
- closed - 预留实例未列示。预留实例可能因实例出售清单已完成销售而处于 closed 状态。

有关更多信息，请参阅 [预留实例状态 \(p. 172\)](#)。

实例出售清单的生命周期

现在您已创建了实例出售清单，以下是出售时的情形。

当实例出售清单中的所有实例都匹配且售出时，My Listings 选项卡将指示 Total instance count 匹配 Sold 下方列出的计数。此外，实例出售清单中没有 Available 实例，并且其 Status 为 closed。

当您的实例出售清单中只有一部分售出时，AWS 将停用实例出售清单中的预留实例并创建与剩余预留实例数量相等的预留实例。因此，实例出售清单 ID 及其代表的实例出售清单（现在具有较少的待售预留）仍处于激活状态。

以此方式处理此实例出售清单中任何未来预留实例销售。当实例出售清单中的所有预留实例售出后，AWS 会将实例出售清单标记为 closed。

例如，您创建了一个所列数量为 5 的预留实例出售清单 ID 5ec28771-05ff-4b9b-aa31-9e57dexample。

Reserved Instance 控制台页中的 My Listings 选项卡将按以下所示显示实例出售清单：

预留实例出售清单 ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 0
- 可用 = 5
- 状态 = 已激活

我们假设某个买家购买了其中两个预留，这使得三个预留的计数依然可供销售。由于此部分销售，AWS 创建了一个实例计数为 3 的新预留，以表示剩下的三个预留依然可供销售。

这是您的实例出售清单在 My Listings 选项卡中的显示方式：

预留实例出售清单 ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 2
- 可用 = 3
- 状态 = 已激活

如果您决定取消您的实例出售清单，且实例出售清单的一部分已经售出，取消操作不会影响到已售出的部分。仅实例出售清单中未售出的部分在预留实例市场中将不再可用。

在您的预留实例出售后

当您的预留实例售出后，AWS 会向您发送一个电子邮件通知。每天如有任何类型的活动，您会收到一封电子邮件通知，其中包含当天的所有活动。例如，可能您创建或销售了实例出售清单，或 AWS 将资金发送到您的账户。

要在控制台中跟踪预留实例出售清单的状态，请依次选择 Reserved Instance 和 My Listings。My Listings 选项卡包含 Listing State 值，还包含期限信息、标价以及实例出售清单中可用、等待、售出和取消的实例数量明细。您也可以使用 `ec2-describe-reserved-instances-listings` CLI 命令或 `DescribeReservedInstancesListings` API 调用，借助合适的筛选器来获取有关您的实例出售清单的信息。

修改您的标准预留实例

当计算需求改变时，您可以修改标准预留实例并继续利用账单优势。可转换预留实例可以使用交换过程进行调整。有关更多信息，请参阅 [交换可转换预留实例 \(p. 182\)](#)。

以下主题将指导您完成标准预留实例上修改过程：

主题

- [修改的要求 \(p. 178\)](#)
- [修改预留的实例大小 \(p. 179\)](#)
- [提交修改请求 \(p. 180\)](#)

修改不会更改标准预留实例的剩余期限；预留实例的结束日期将保持不变。不会产生任何费用，因此您不会收到任何新账单或发票。修改与购买无关，不会对您使用、购买或销售标准预留实例产生任何影响。您可通过以下一种或多种方式修改您的整个预留或预留的一部分：

- 在相同区域内更改可用区
- 将预留范围从可用区更改到区域 (反之亦然)
- 在 EC2-VPC 和 EC2-Classic 之间切换
- 在同一实例类型内更改实例的大小

所有平台类型 (Linux 和 Windows) 都支持可用区、范围和网络平台修改。仅 Linux 平台类型支持实例类型修改。但是，由于许可不同，您将无法更改 RedHat 或 SUSE Linux 标准预留实例的实例类型或大小。有关 RedHat 和 SUSE 定价的更多信息，请参阅 [Amazon EC2 预留实例定价](#)。

如果更改预留的可用区域，则容量预留和定价优势自动适用于新可用区域中的实例使用。如果修改预留实例的网络平台 (例如，从 EC2-Classic 到 EC2-VPC)，则容量预留自动适用于新网络平台的实例使用。

如果您将预留范围从可用区更改为区域，则您将放弃可用区灵活性和实例大小灵活性的容量预留优势。借助可用区灵活性，区域中任何可用区内对预留实例的使用可享受预留实例折扣。借助实例大小灵活性，对预留实例系列中的实例的使用可享受预留实例折扣，无论实例大小如何。

Note

仅分配给区域的具有默认租期的 Linux/Unix 预留实例支持实例大小灵活性。预留的账单优势适用于该地区的所有适用实例。

修改之后，预留实例的定价权益仅适用于与新参数匹配的实例。除非您的账户有其他适用的预留，否则将按照按需费率收费对不再符合新参数的实例收费。定价优势同时适用于与预留规范相匹配的 EC2-Classic 和 EC2-VPC 实例。

修改的要求

Amazon EC2 处理您的修改请求的前提是，对于您的目标配置 (如果适用)，有足够的容量，同时满足以下条件。

修改后的预留实例必须：

- 活动
- 没有其他等待处理的修改请求
- 预留实例市场中未列示
- 在同一小时（不是分钟或秒）内终止

您的修改请求必须：

- 范围、实例类型、实例大小、产品类别和网络平台属性的独特组合
- 有效预留的实例大小占用空间与目标配置匹配

限制

- 只能修改标准预留实例。

如果预留实例不处于活动状态或无法修改，则 AWS 管理控制台中的 Modify Reserved Instances（修改预留实例）按钮不会启用。如果要修改的一个或多个预留实例是用于不允许修改实例类型的平台，则 Modify Reserved Instances 页面不会显示用于更改任何所选预留实例的实例类型的选项。有关更多信息，请参阅 [修改预留的实例大小 \(p. 179\)](#)。

您可以随时修改您的预留；但是，对于未完成上次修改请求的预留，您不能提交修改请求。在提交修改请求后，您也无法更改或取消等待处理的修改请求。修改成功完成后，您可以提交另一个修改请求，以回滚您所做的任何更改。有关更多信息，请参阅 [确定修改的状态 \(p. 181\)](#)。

要修改预留实例市场中列出的预留实例，请取消列表，请求修改预留实例，然后再次列出这些实例。此外，您无法在购买前或购买时修改产品。有关更多信息，请参阅 [预留实例市场 \(p. 163\)](#)。

修改预留的实例大小

如果有 Amazon Linux 预留的实例类型具有多种大小，您可以调整标准预留实例的实例大小。请记住，仅当其他属性（如区域、使用类型、租期、平台、结束日期和小时）匹配并且容量可用时，才允许修改实例大小。不能修改 Windows 预留实例的实例大小。

Note

实例按照系列（依据存储或 CPU 容量）、类型（为特定的使用案例而设计）和大小分组。例如，`c4` 实例类型属于计算优化型的实例系列，并且有多个大小可用。当 `c3` 实例属于同一系列时，您无法将 `c4` 实例修改进入 `c3` 实例，因为它们的硬件规格不同。有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

有关修改过程和步骤的信息，请参阅 [提交修改请求 \(p. 180\)](#)。

以下实例无法进行修改，因为没有其他大小：

- `t1.micro`
- `cc1.4xlarge`
- `cc2.8xlarge`
- `cg1.8xlarge`
- `cr1.8xlarge`
- `hi1.4xlarge`
- `hs1.8xlarge`
- `g2.2xlarge`

如果容量存在，并且修改未更改预留实例的实例大小占用空间，则您的请求成功。

了解实例大小占用空间

每个预留实例都有实例大小占用空间，占用空间由预留中实例类型的标准化因子和实例数量决定。

标准化因子是基于实例类型中的实例大小确定的（例如，在 m1 实例类型中的 m1.xlarge 实例）。只有在同一实例类型中才有意义。不能从一个实例类型修改为另一个实例类型。在 Amazon EC2 控制台中，这是按单位计量的。下表说明在实例类型中应用的标准化因子。

| 实例大小 | 标准化因子 |
|----------|-------|
| nano | 0.25 |
| 微型 | 0.5 |
| small | 1 |
| medium | 2 |
| large | 4 |
| xlarge | 8 |
| 2xlarge | 16 |
| 4xlarge | 32 |
| 8xlarge | 64 |
| 10xlarge | 80 |
| 16xlarge | 128 |
| 32xlarge | 256 |

如果目标配置的占用空间与原始配置的占用空间不匹配，则不会处理修改请求。

要计算预留实例的实例占用空间大小，请将实例数量乘以标准化因子。例如，m1.medium 的标准化因子为 2，因此四个 m1.medium 实例的预留相当于 8 个单位的占用空间。

只要预留的实例大小占用空间保持不变，您就可以将预留分配给相同实例类型中的不同实例大小。例如，您可以将一个 m1.large (1 x 4) 实例的预留划分为四个 m1.small (4 x 1) 实例，也可以将四个 m1.small 实例的预留合并为一个 m1.large 实例。但是您不能将两个 m1.small (2 x 1) 实例的预留更改为一个 m1.large (1 x 4) 实例。因为当前预留的现有实例大小占用空间小于计划的预留空间。

有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

提交修改请求

AWS 提供多种查看和处理修改请求的方法：您可以使用 AWS 管理控制台直接与 Amazon EC2 API 交互，也可以使用命令行界面。

主题

- [AWS 管理控制台 \(p. 181\)](#)
- [命令行界面 \(p. 181\)](#)
- [Amazon EC2 API \(p. 181\)](#)
- [确定修改的状态 \(p. 181\)](#)

AWS 管理控制台

Modify Reserved Instances 页面上的每个目标配置行均跟踪当前实例类型的实例数量 (Count) , 以及您的预留相对于其实例类型的实例大小占用空间 (Units)。有关更多信息 , 请参阅 [了解实例大小占用空间 \(p. 180\)](#)。

如果您指定的预留实例数量多于或少于可修改的数量 , 则分配的总额显示为红色。在您为可修改的所有预留实例指定更改之后 , 总数变为绿色 , 然后您可以选择 Continue。

修改预留的一部分时 , Amazon EC2 会将您的原始预留实例分为两个或更多的新预留实例。例如 , 如果您在 us-east-1a 中有 10 个实例的预留 , 并决定将其中 5 个实例移动至 us-east-1b , 则修改请求会生成两个新的预留 : 一个用于 us-east-1a (原始可用区) 中的 5 个实例 , 另一个用于 us-east-1b 中的 5 个实例。

使用 AWS 管理控制台修改预留实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Reserved Instances 页面上 , 选择一个或多个要修改的预留实例 , 然后选择 Modify Reserved Instances。

Note

修改表中的第一个条目是原始的未修改预留。要修改所有预留的属性 , 请从菜单中选择新规格。要仅修改或拆分某些预留 , 请为每个更改添加一行。

3. 对于每个附加属性更改选择 Add , 并为 Count 输入要修改的预留的数量。
 - 要更改可用区 , 请在 Availability Zone 列表中选择值。
 - 要更改网络平台 , 请在 Network 列表中选择值。
 - 要更改实例类型 , 请在 Instance Type 列表中选择值。
4. 要删除某个指定的属性 , 请选择相应行的 X。

Note

如果 Modify Reserved Instances 页面仅包含一个属性更改行 , 则不能删除该行。要修改多个预留实例属性 , 请先为新规格添加一行 , 然后删除原始行。

5. 选择 Continue (继续)。
6. 指定好目标配置之后 , 若要确认您的修改选择 , 请选择 Submit Modifications。如果您在任何时候改变了主意 , 请选择 Cancel 退出向导。

命令行界面

您也可以使用 AWS CLI ([modify-reserved-instances](#))、适用于 Windows PowerShell 的 AWS 工具 ([Edit-EC2ReservedInstance](#))、Amazon EC2 API ([ModifyReservedInstances](#)) 以及[适用于 Java 的 AWS 开发工具包](#)以编程方式完成修改任务。

Amazon EC2 API

您可以使用 [ModifyReservedInstances](#) 操作来修改预留实例。有关更多信息 , 请参阅 [Amazon EC2 API 参考](#)。

确定修改的状态

您可以通过查看所修改的预留实例的状态 来确定修改请求的状态。返回的状态将请求显示为 `in-progress`、`fulfilled` 或 `failed`。使用以下资源可获取这些信息 :

- AWS 管理控制台中的 State 字段
- [DescribeReservedInstancesModifications](#) API 操作
- `-describe-reserved -instances-modifications` AWS CLI 命令
- [Get-EC2ReservedInstancesModifications](#) 适用于 Windows PowerShell 的 AWS 工具 命令

下表说明了 AWS 管理控制台中可能的 State 值。

| 状态 | 说明 |
|--------------------------------|--|
| 活动(等待修改) | 原始预留实例的转换状态。 |
| retired (pending modification) | 创建新预留实例时原始预留实例的转换状态。 |
| 停用 | 已成功修改和替换预留实例。 |
| 活动 | 从成功的修改请求创建的新预留实例。 -或者- 修改请求失败后的原始预留实例。 |

Note

如果您使用 [DescribeReservedInstancesModifications](#) API 操作，则修改请求的状态应显示为 processing、fulfilled 或 failed。

如果您的修改请求成功：

- 修改的预留会立即生效，并且定价优惠将于进行修改请求时这一小时的开始应用于新实例。例如，如果您在晚上 9:15 成功修改了预留，则定价优惠将在晚上 9:00 转移到新实例。(您可以使用 [DescribeReservedInstances](#) API 操作或 `describe-reserved-instances` 命令 (AWS CLI) 获取所修改的预留实例的 effective date。)
- 原始预留将停用。其结束日期是新预留的开始日期，而新预留的结束日期与原始预留实例的结束日期相同。如果您修改一个剩余期限为 16 个月的三年期预留，则修改后得到的预留是为期 16 个月的预留，其结束日期与原始预留相同。
- 已修改的预留将列出 0 美元固定价格，而不是原始预留的固定价格。

Note

已修改的预留实例的固定价格不影响您的账户的折扣定价套餐计算，后者基于原始预留的固定价格。

如果您的修改请求失败：

- 您的预留实例将保持原始配置。
- 您的预留实例可立即用于另一个修改请求。

有关无法修改某些预留实例的原因的更多信息，请参阅[修改的要求 \(p. 178\)](#)。

交换可转换预留实例

您可以使用可转换预留实例交换具有不同配置的其他可转换预留实例，包括实例系列。您执行交换的次数没有限制，只要目标可转换预留实例的值高于您正在交换的可转换预留实例。

交换可转换预留实例的要求

如果满足以下条件，Amazon EC2 过程将处理您的交换请求：

可转换预留实例必须：

- 活动

- 没有其他等待处理的交换请求
- 在同一小时 (不是分钟或秒) 内终止

限制：

- 可转换预留实例只能交换当前由AWS提供的其他可转换预留实例。
- 无法修改可转换预留实例。要更改预留的配置，请将其交换为另一个。
- 可转换预留实例只能交换相同或更高付款选项。例如，部分预付可转换预留实例可以交换全部预付可转换预留实例，但不能交换没有预付可转换预留实例。

如果可转换预留实例不处于活动状态或无法交换，则 AWS 管理控制台中的 Exchange Reserved Instances (交换预留实例) 按钮不会启用。

您可以随时交换您的预留；但是，对于未完成上次交换请求的预留，您不能提交交换请求。

计算可转换预留实例交换

交换可转换预留实例是免费的。但是，您可能需要支付调整费用，即您拥有的可转换预留实例与您通过交换收到的可转换预留实例之间差额的比例预付费用。

每个可转换预留实例都具有列表值。该列表值对应于您想要的可转换预留实例的列表值，以确定您可通过交换收到的预留数。

例如：您有 1 个 35 美金列表值的可转换预留实例，您希望交换为列表值为 10 美金的全新实例类型。

\$35 / \$10 = 3.5

您可以使用可转换预留实例交换三个 10 美金的可转换预留实例。无法购买半预留；购买额外的可转换预留实例可涵盖剩余部分：

3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved Instance.

第四个可转换预留实例与其他三个具有相同的结束日期。如果您要交换部分或全部预付可转换预留实例，需要支付第四个预留的调整费用。如果您的可转换预留实例的剩余预付成本为 500 美元，而目标预留通常按比例分摊为 600 美元，则您需要支付 100 美元。

\$600 prorated upfront cost of new reservations - \$500 remaining upfront cost of original reservations = \$100 difference.

提交交换请求

AWS 提供多种查看和处理交换请求的方法：您可以使用 AWS 管理控制台直接与 Amazon EC2 API 交互，也可以使用命令行界面。

主题

- [AWS 管理控制台 \(p. 183\)](#)
- [命令行界面 \(p. 184\)](#)
- [Amazon EC2 API \(p. 184\)](#)

AWS 管理控制台

您可以搜索可转换预留实例产品并从提供的选项中选择新配置。

使用 AWS 管理控制台交换可转换预留实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Reserved Instances，再选择一个或多个要交换的可转换预留实例，然后依次选择 Actions 和 Exchange Reserved Instances。
3. 选择新配置。可使用默认设置 Any，也可以使用下拉菜单指定所需的配置。
4. 选择 Find Offering。
5. 从提供的列表中选择新的可转换预留实例，然后选择 Exchange。

已交换的预留实例将停用，AWS 管理控制台中将显示新的预留实例。此过程可能需要几分钟才能传播。

命令行界面

您可以使用 AWS CLI 先获取有关可转换预留实例的信息 ([get-reserved-instances-exchange-quote](#))，然后执行交换 ([accept-reserved-instances-exchange-quote](#))，来以编程方式交换可转换预留实例。

Amazon EC2 API

您可以使用 [GetReservedInstancesExchangeQuote](#) 操作获取有关可转换预留实例的信息。然后使用 [AcceptReservedInstancesExchangeQuote](#) 操作执行交换。有关更多信息，请参阅 [Amazon EC2 API 参考](#)。

修改请求故障排除

如果您请求的目标配置设置是唯一的，则您会收到正在处理该请求的消息。此时，Amazon EC2 仅确定了修改请求的参数有效。在处理过程中，您的修改请求仍然可能因无可用容量而失败。

在某些情况下，您可能会收到一个指示修改请求未完成或失败的消息而不是确认。使用此类消息中的信息作为重新提交另一个更改请求的起点。

不是所有选择的预留实例都可以进行修改处理

Amazon EC2 会确定并列出无法修改的预留实例。如果收到与此类似的消息，请转到 AWS 管理控制台中的 Reserved Instances 页面，查看有关这些容量预留的详细信息。

处理修改请求时出错

您提交了一个或多个预留实例进行修改，而且不能处理您的处理请求。根据您修改的预留数量，您可以获取不同版本的消息。

Amazon EC2 会显示无法处理请求的原因。举例来说，您可能已经为正在修改的预留实例的一个或更多子集指定了相同的目标配置 – 可用区和平台的组合。尝试重新提交修改请求，但确保预留的实例详细信息是匹配的，并确保修改的所有子集的目标配置是唯一的。

计划的预留实例

利用计划的预留实例（计划实例），您可以以一年为期限购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的容量预留。您应提前预留容量，以确定其在需要时可用。您需要为计划的实例时间付费，即使您未使用它们也是如此。

对于不持续运行，而是按固定的计划运行的工作负载，计划实例是一个很好的选择。例如，您可以为在工作时间运行的应用程序，或为在周末运行的批处理作业使用计划实例。

如果您需要持续的容量预留，预留实例可能符合您的需求并且可以降低成本。有关更多信息，请参阅 [预留实例 \(p. 161\)](#)。如果您的实例运行时间比较灵活，竞价型实例可能符合您的需求并且可以降低成本。有关更多信息，请参阅 [竞价型实例 \(p. 187\)](#)。

内容

- [计划实例如何运行 \(p. 185\)](#)
- [购买计划实例 \(p. 185\)](#)
- [启动计划实例 \(p. 186\)](#)
- [计划实例限制 \(p. 186\)](#)

计划实例如何运行

Amazon EC2 在每个可用区内都留下了一些 EC2 实例池以用作计划实例。每个池都支持实例类型、操作系统和网络 (EC2-Classic 或 EC2-VPC) 的一个特定组合。

首先，您必须搜索可用的计划。您可在多个池或单个池中进行搜索。在找到合适的计划后，您购买该计划。

计划实例只能在计划时间段内启动，且其启动配置必须与所购买的计划的属性 (实例类型、可用区、网络和平台) 保持一致。当您执行此操作时，Amazon EC2 将根据指定的启动说明代表您启动 EC2 实例。Amazon EC2 必须确保 EC2 实例在当前计划时间段结束时终止，以使容量可用于其为之预留的任何其他计划实例。因此，Amazon EC2 在当前计划时间段结束前三分钟终止 EC2 实例。

您无法停止或重启计划实例，但可以根据需要手动终止它们。如果您在计划实例的当前计划时间段结束前将其终止，可以在几分钟后再次启动它。否则，您必须等到下一个计划时间段。

下图说明了计划实例的生命周期。

购买计划实例

要购买计划实例，可使用计划预留实例预留向导。

Warning

购买计划实例后，您无法取消、修改或转售该购买。

购买计划实例使用控制台

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Scheduled Instances。
3. 选择 Purchase Scheduled Instances。
4. 在 Find available schedules 页面中，执行以下操作：
 - a. 在 Create a schedule 下，从 Starting on 中选择启动日期、从 Recurring 中选择计划重复周期 (每日、每周或每月)，并从 for duration 中选择最短持续时间。请注意，控制台可确保您为达到计划实例所需的最低利用率 (每年 1200 个小时) 的最短持续时间指定一个值。
 - b. 在 Instance details 下，从 Platform 中选择操作系统和网络。要缩小结果范围，请从 Instance type 中选择一个或多个实例类型，或从 Availability Zone 中选择一个或多个可用区。
 - c. 选择 Find schedules。
 - d. 在 Available schedules 下，选择一个或多个计划。对于您选择的每个计划，设置实例的数量，然后选择 Add to Cart。
 - e. 您的购物车显示在页面底部。在购物车中添加或删除完计划以后，选择 Review and purchase。
5. 在 Review and purchase 页面上，验证您的选择并根据需要对其进行编辑。完成后，选择 Purchase。

使用 AWS CLI 购买计划实例

使用 [describe-scheduled-instance-availability](#) 命令列出满足您需求的可用计划，然后使用 [purchase-scheduled-instances](#) 命令完成购买。

启动计划实例

在购买计划实例后，可在计划实例的计划时间段内启动该实例。

使用控制台启动计划实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Scheduled Instances。
3. 选择计划实例，然后选择 Launch Scheduled Instances。
4. 在 Configure 页面上，完成您的计划实例的启动说明，然后选择 Review。

Important

启动规范必须与所购买的计划的实例类型、可用区、网络和平台保持一致。

5. 在 Review 页面上，验证启动配置并根据需要修改它。完成后，选择 Launch。

使用 AWS CLI 启动计划实例

使用 [describe-scheduled-instances](#) 命令列出计划实例，然后使用 [run-scheduled-instances](#) 命令在每个计划实例的计划时间段内启动实例。

计划实例限制

计划实例受以下限制的约束：

- 以下是仅有的几个受支持的实例类型：C4、C3、M4 和 R3。
- 所需的期限为 365 天（一年）。
- 所需的最低利用率为每年 1200 个小时。
- 您最多可以提前三个月购买计划实例。

竞价型实例

竞价型实例使您可以对未使用的 EC2 实例出价，这可以大幅降低您的 Amazon EC2 成本。(每个可用区中的每种实例类型的) 竞价型实例的每小时价格由 Amazon EC2 设置，并根据竞价型实例的供求波动。只要您的出价超过当前市场价格，您的竞价型实例就会运行。

如果您能灵活控制应用程序的运行时间并且应用程序可以中断，那么竞价型实例将是您的经济实惠之选。例如，竞价型实例非常适合数据分析、批处理作业、后台处理和可选的任务。有关更多信息，请参阅 [Amazon EC2 竞价型实例](#)。

竞价型实例和按需实例的主要差别在于，竞价型实例可能无法立即启动，竞价型实例每小时价格会根据需求变动，并且 Amazon EC2 可以根据竞价型实例每小时价格或可用情况的变化终止单个竞价型实例。可以采取的一种策略是启动一组核心按需实例，以便为应用程序维护最低级别的保障计算资源，再适机通过竞价型实例来进行补充。

另一项策略是，启动具有要求的时长的竞价型实例(也被称为竞价型限制)，这些实例不会因现货价格更改而中断。有关更多信息，请参阅 [指定竞价型实例的持续时间 \(p. 197\)](#)。

概念

在开始使用竞价型实例之前，您应该熟悉以下概念：

- 竞价型实例池 - 一组未使用的 EC2 实例，具有相同的实例类型、操作系统、可用区和网络平台 (EC2-Classic 或 EC2-VPC)。
- 现货价格 - 竞价型实例当前的每小时市场价格，该价格由 Amazon EC2 根据执行的最后出价设置。您还可以检索现货价格历史记录。
- 竞价型实例请求 (或竞价出价) - 提供您希望为每个竞价型实例每小时支付的最高价(出价)。当您的出价超过现货价格时，Amazon EC2 会满足您的请求。请注意，竞价型实例请求可以是一次性或持久性请求。Amazon EC2 会在与持久性竞价请求关联的竞价型实例终止之后自动重新提交该请求。您的竞价型实例请求可选择性地为竞价型实例指定一个持续时间。
- 竞价型队列 - 一组基于指定条件启动的竞价型实例。竞价型队列会选择满足您的需要的竞价型实例池，并启动竞价型实例以满足队列的目标容量。默认情况下，在队列中的竞价型实例终止之后，系统会启动替代实例以维持竞价型队列的目标容量。它们也可以作为一次性请求来提交，这种请求在实例终止后不会被保留。
- 竞价型实例中断 - 当现货价格超过您的出价时，或者不再有任何未使用的 EC2 实例时，Amazon EC2 将终止您的竞价型实例。Amazon EC2 将竞价型实例标记为终止并提供竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。
- 出价状态 - 提供有关您的竞价出价最新状态的详细信息。

如何开始

您需要做的第一件事是为使用 Amazon EC2 进行设置。在启动竞价型实例之前，若拥有启动按需实例的经验也会有所帮助。

设置和运行

- [Amazon EC2 的设置 \(p. 15\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 20\)](#)

竞价基本知识

- [竞价型实例运行方式 \(p. 189\)](#)
- [竞价型队列的工作方式 \(p. 191\)](#)

使用竞价型实例

- [准备中断 \(p. 224\)](#)
- [创建竞价型实例请求 \(p. 198\)](#)
- [获取出价状态信息 \(p. 222\)](#)

使用竞价型队列

- [竞价型队列先决条件 \(p. 204\)](#)
- [创建竞价型队列请求 \(p. 206\)](#)

相关服务

您可以直接使用 Amazon EC2 预配竞价型实例。您也可以使用 AWS 中的其他服务预置竞价型实例。有关更多信息，请参阅以下文档。

Auto Scaling 和竞价型实例

您可以通过出价创建启动配置，这样 Auto Scaling 可以启动竞价型实例。有关更多信息，请参阅 Auto Scaling 用户指南 中的[在 Auto Scaling 组中启动竞价型实例](#)。

Amazon EMR 和竞价型实例

有时候，在 Amazon EMR 群集中运行竞价型实例会非常有帮助。有关更多信息，请参阅 Amazon EMR 开发人员指南 中的[通过竞价型实例降低成本](#)。

AWS CloudFormation 模板

AWS CloudFormation 使您能够使用 JSON 格式的模板来创建和管理 AWS 资源集合。AWS CloudFormation 模板可以包含现货价格。有关更多信息，请参阅[EC2 竞价型实例更新 - Auto Scaling 和 CloudFormation 集成](#)。

AWS SDK for Java

您可以使用 Java 编程语言来管理竞价型实例。有关更多信息，请参阅[教程：Amazon EC2 竞价型实例](#)和[教程：高级 Amazon EC2 竞价请求管理](#)。

适用于 .NET 的 AWS 开发工具包

您可以使用 .NET 编程环境来管理竞价型实例。有关更多信息，请参阅[教程：Amazon EC2 竞价型实例](#)。

定价

您为竞价型实例支付现货价格，现货价格由 Amazon EC2 设置，并根据竞价型实例的供求周期性波动。如果您的出价超出当前的现货价格，则 Amazon EC2 会满足您的请求，您的竞价型实例将会运行，直到您选择终止它们或现货价格增长到高于您的出价。

在该期间内，每个人支付的现货价格相同，无论他们的出价是否更高。您每小时支付的金额绝不会超过您的出价，并且常常会低于出价。例如，如果您的出价是每小时 0.25 USD，现货价格是每小时 0.20 USD，您只需支付每小时 0.20 USD 即可。如果现货价格下降，您将支付更低的新价格。如果现货价格提高，在现货价格等于或低于您的出价时，您将按照新价格支付。如果现货价格提高并超过您的出价，则会中断您的竞价型实例。

在每个实例小时开始时，将按照现货价格计费。如果由于竞价超过您的出价导致您的竞价型实例在实例小时的中间被中断，则您无需为中断的不足 1 个小时部分付费。不过，如果您在实例小时的中间中断了竞价型实例，则您需要为该小时付费。

请注意，具有预定义的持续时间的竞价型实例使用的小时固定价格在该实例运行时仍有效。

查看价格

要查看各个区域和实例类型的当前 (每 5 分钟更新一次) 最低现货价格，请参阅[竞价型实例定价](#)页面。

要查看过去三个月的现货价格历史记录，请使用 Amazon EC2 控制台或者 `describe-spot-price-history` 命令 (AWS CLI)。有关更多信息，请参阅[竞价型实例定价历史记录 \(p. 195\)](#)。

注意，我们将可用区独立地映射到每个 AWS 账户的代码。因此，不同账户的相同可用区代码 (如 `us-west-2a`) 可能会返回不同的结果。

查看账单

要查看您的账单，请转至[“AWS 账户活动”页面](#)。您的账单中包含了提供您的账单详情的使用情况报告的链接。有关更多信息，请参阅[AWS Account Billing](#)。

如果您有关于 AWS 账单、账户和事件的问题，请[联系 AWS Support](#)。

竞价型实例运行方式

要使用竞价型实例，请创建一个竞价型实例请求或竞价型队列请求。该请求包括您愿意为每个实例每小时支付的最高价 (您的出价) 以及其他约束 (例如，实例类型和可用区)。如果您的出价超过了指定实例当前的现货价格，并且指定的实例可用，将立即满足您的请求。否则，只要现货价格低于您的出价或者指定的实例可用，就会完成您的请求。在您终止竞价型实例或者 Amazon EC2 必须终止竞价型实例 (也称为竞价型实例中断) 之前，竞价型实例将保持运行。

当您使用竞价型实例时，您必须做好应对中断的准备。随着对竞价型实例需求的增长，或者竞价型实例供应的减少，在现货价格上涨超过了您的出价时，Amazon EC2 可以中断您的竞价型实例。当 Amazon EC2 将竞价型实例标记为终止时，它会提供一个竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。请注意，您无法为竞价型实例启用终止保护。有关更多信息，请参阅[竞价型实例中断 \(p. 224\)](#)。

请注意，如果 Amazon EBS 支持的实例是竞价型实例，那么您无法停止和启动该实例，但可以重新启动或终止它。

在操作系统级别关闭竞价型实例会导致竞价型实例被终止。这种情况无法改变。

内容

- [竞价市场上供应和需求 \(p. 189\)](#)
- [在启动组中启动竞价型实例 \(p. 190\)](#)
- [在可用区组中启动竞价型实例 \(p. 191\)](#)
- [在 VPC 中启动竞价型实例 \(p. 191\)](#)

竞价市场上供应和需求

AWS 持续评估每个竞价型实例池中有多少竞价型实例可用，监视已经为每个池出了什么价，然后将可用竞价型实例预置给最高出价者。池的现货价格设置为该池中执行的最低出价。因此，您的出价必须高于现货价格，才会立即执行针对单个竞价型实例的竞价请求。

例如，假设您创建了竞价型实例请求，对应的竞价型实例池只有五个竞价型实例可供销售。您的出价为 0.10 USD，这也是当前现货价格。下表按照降序排名显示了当前出价。将执行出价 1-5。出价 5 (最后执行的出价) 将现货价格设置在 0.10 USD。出价 6 未执行。0.10 USD 这一相同出价的出价 3-5 按随机顺序排列。

| 出价 | 出价 | 当前现货价格 | 备注 |
|----|----------|----------|----|
| 1 | 1.00 USD | 0.10 USD | |
| 2 | 1.00 USD | 0.10 USD | |

| 出价 | 出价 | 当前现货价格 | 备注 |
|-----|----------|----------|--|
| 3 | 0.10 USD | 0.10 USD | |
| 4 | 0.10 USD | 0.10 USD | 您的出价 |
| 5 | 0.10 USD | 0.10 USD | 最后执行的出价 (设置现货价格)。每个人在相应时段内都会支付相同的现货价格。 |
| ——— | ——— | | 竞价容量截止 |
| 6 | \$0.05 | | |

现在，假设此池的大小下降为 3。将执行出价 1-3。出价 3 (最后执行的出价) 将现货价格设置在 0.10 USD。出价 4-5 (也就是 0.10 USD) 未执行。如您所见，尽管现货价格没有变化，但由于竞价供应减少，包括您的出价在内的两个竞价将不再执行。

| 出价 | 出价 | 当前现货价格 | 备注 |
|-----|----------|----------|--|
| 1 | 1.00 USD | 0.10 USD | |
| 2 | 1.00 USD | 0.10 USD | |
| 3 | 0.10 USD | 0.10 USD | 最后执行的出价 (设置现货价格)。每个人在相应时段内都会支付相同的现货价格。 |
| ——— | ——— | | 竞价容量截止 |
| 4 | 0.10 USD | | 您的出价 |
| 5 | 0.10 USD | | |
| 6 | \$0.05 | | |

要执行此池中单个实例的竞价请求，您的出价必须超过当前的现货价格 0.10 USD。如果您出价 0.101 USD，则将执行您的请求，出价 3 的竞价型实例将中断，现货价格成为 0.101 USD。如果您出价 2.00 USD，则出价 3 的竞价型实例将中断，现货价格成为 1.00 USD (出价 2 的价格)。

请记住，不论您出价多高，您获得的竞价型实例数都不会超过竞价型实例池中可用的竞价型实例数。如果池的大小下降为零，则该池中的所有竞价型实例都将中断。

在启动组中启动竞价型实例

在竞价型实例请求中指定启动组，可以通知 Amazon EC2 只有在可以全部启动一组竞价型实例时才启动。此外，如果竞价型服务必须终止启动组中的一个实例 (例如，如果现货价格提高并超过您的出价)，则必须终止该组中的所有实例。不过，如果由您终止启动组中的一个或多个实例，Amazon EC2 不会终止该启动组中的剩余实例。

请注意，虽然此选项非常有用，但添加此约束会减少完成您的竞价型实例请求的几率。这还会增加您的竞价型实例被终止的几率。

如果您创建了另一个成功的竞价型实例请求并指定与之前成功请求相同 (现有) 的启动组，则新实例将添加到该启动组中。以后，在该启动组的一个实例终止时，启动组中的所有实例均会终止，这包括第一次请求和第二次请求启动的实例。

在可用区组中启动竞价型实例

在竞价型实例请求中指定可用区组，可以通知竞价服务在同一可用区中启动一组竞价型实例。请注意，Amazon EC2 不必同时终止某个可用区组中的所有实例。如果 Amazon EC2 必须终止可用区组中的某个实例，剩余的实例仍保持运行。

请注意，虽然此选项非常有用，但添加此约束会减少完成您的竞价型实例请求的几率。

如果您在竞价型实例请求中指定了可用区组，但没有指定可用区，则竞价服务所采取的操作将取决于您指定的是 EC2-Classic 网络、默认 VPC 还是非默认 VPC。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅 [支持的平台 \(p. 435\)](#)。

EC2-Classic

Amazon EC2 查找区域中最低价格的可用区，如果该组的最低出价高于该可用区中当前的现货价格，则在该可用区中启动您的竞价型实例。只要现货价格保持低于该组的最低出价，Amazon EC2 就将等待，直至有足够的容量来同时启动您的竞价型实例。

默认 VPC

Amazon EC2 使用指定子网的可用区，如果您没有指定子网，则竞价服务将选择一个可用区及其默认子网，但这可能不是最低价格的可用区。如果您删除了可用区的默认子网，则必须指定其他子网。

非默认 VPC

Amazon EC2 使用指定子网的可用区。

在 VPC 中启动竞价型实例

如果您想在使用竞价型实例时利用 EC2-VPC 的功能，请在您的竞价请求中将您的竞价型实例指定为在 VPC 中启动。按照您为按需实例指定子网的相同方法，为您的竞价型实例指定子网。

对于在 VPC 中启动竞价型实例的竞价型实例请求，其提交过程与在 EC2-Classic 中启动竞价型实例的竞价型实例请求基本相同，但有以下区别：

- 您应该基于 VPC 中竞价型实例的现货价格历史记录来确定您的出价。
- [默认 VPC] 如果希望在特定的低价格可用区中启动您的竞价型实例，您必须在竞价型实例请求中指定对应的子网。如果您没有指定子网，则 Amazon EC2 将为您选择一个子网，而该子网的可用区中的现货价格不一定是最低的。
- [非默认 VPC] 您必须为您的竞价型实例指定子网。

竞价型队列的工作方式

竞价型队列是竞价型实例的集合或队列。竞价型队列会尝试启动适当数量的竞价型实例，以满足在竞价型队列请求中指定的目标容量要求。如果您的竞价型实例由于现货价格或可用容量的变化而中断，则竞价型队列还会尝试维持其目标容量队列。

竞价型实例池 是一组未使用的 EC2 实例，具有相同的实例类型、操作系统、可用区和网络平台 (EC2-Classic 或 EC2-VPC)。在您发出竞价型队列请求时，您可以指定多个启动说明 (因实例类型、AMI、可用区或子网而异)。竞价型队列会基于竞价型队列请求中包含的启动说明以及竞价型队列请求的配置来选择用于执行请求的竞价型实例池。竞价型实例来自所选池。

内容

- [竞价型队列分配策略 \(p. 192\)](#)
- [现货价格覆盖 \(p. 192\)](#)

- 竞价型队列实例权重 (p. 192)
- 演练：将竞价型队列与实例权重结合使用 (p. 193)

竞价型队列分配策略

竞价型队列的分配策略决定了如何根据启动说明从可能的竞价型实例池执行竞价型队列请求。以下是您在竞价型队列请求中可以指定的分配策略：

`lowestPrice`

竞价型实例来自具有最低价格的池。这是默认策略。

`diversified`

竞价型实例分布在所有池中。

选择分配策略

您可以基于您的使用案例来优化竞价型队列。

如果您的队列较小或只是短时间运行，则您的竞价型实例中断的可能性较低（即使所有实例都在同一个竞价型实例池中）。因此，`lowestPrice` 策略可能会满足您的需求，同时提供最低的成本。

如果您的队列较大或长时间运行，则您可以通过在多个池间分配竞价型实例来提高队列的可用性。例如，如果您的竞价型队列请求指定 10 个池，且目标容量为 100 个实例，则竞价型队列会在每个池中启动 10 个竞价型实例。如果一个池的现货价格上涨到超过您对该池的出价，则只有队列的 10% 受到影响。使用此策略还可降低您的队列对单个池的现货价格随时间上涨的敏感度。

请注意，使用 `diversified` 策略时，竞价型队列不在现货价格高于[按需价格](#)的任何池中启动竞价型实例。

维持目标容量

在竞价型实例由于竞价型实例池的现货价格或可用容量发生变化而终止之后，竞价型队列会启动替换竞价型实例。如果分配策略是 `lowestPrice`，则竞价型队列在当前具有最低现货价格的池中启动替换实例。如果分配策略是 `diversified`，则竞价型队列在其余池间分配替换竞价型实例。

现货价格覆盖

每个竞价型队列请求必须包含一个全局现货价格。默认情况下，竞价型队列使用此价格作为每个启动说明的出价。

您可以选择在一个或多个启动说明中指定现货价格。此出价特定于启动说明。如果启动说明包含特定现货价格，则竞价型队列使用此价格作为该启动说明的出价（覆盖全局现货价格）。请注意，不包含特定现货价格的任何其他启动说明仍使用全局现货价格。

竞价型队列实例权重

当请求竞价型实例队列时，您可以使用实例权重 定义每种实例类型对应用程序性能贡献的容量单位，并相应地为每个竞价型实例池调整出价。

默认情况下，您指定的现货价格表示每实例小时的出价。使用实例权重功能时，您指定的现货价格表示每单位小时的出价。您可以通过将实例类型出价除以它表示的单位数来计算每单位小时出价。竞价型队列通过将目标容量除以实例权重来计算要启动的竞价型实例数。如果结果不是整数，则竞价型队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。请注意，竞价型队列可以选择您在启动说明中指定的任意池，即使所启动实例的容量超过请求的目标容量也是如此。

下表中提供了用于为目标容量是 10 的竞价型队列请求确定每单位出价的计算示例。

| 实例类型 | 实例权重 | 每实例小时现货价格 | 每单位小时现货价格 | 启动的实例数 |
|------------|------|-----------|-----------------------|-------------------------|
| r3.xlarge | 2 | \$0.05 | 0.025 (0.05 除以 2) | 5 (10 除以 2) |
| r3.8xlarge | 8 | 0.10 USD | 0.0125 (0.10 除以 8) | 2 (10 除以 8 , 结果向上舍入) |

按如下所示使用竞价型队列实例权重，在执行时具有每单位最低价格的池中预置所需的目标容量：

1. 采用实例（默认设置）或采用所选单位（如虚拟 CPU、内存、存储或吞吐量）为竞价型队列设置目标容量。
2. 设置每单位出价。
3. 对于每个启动配置，指定权重，这是实例类型向目标容量提供的单位数。

实例权重示例

考虑一个具有以下配置的竞价型队列请求：

- 目标容量为 24
- 一个实例类型为 r3.2xlarge 且权重为 6 的启动说明
- 一个实例类型为 c3.xlarge 且权重为 5 的启动说明

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动说明提供了最低的每单位现货价格（r3.2xlarge 每实例小时现货价格除以 6），则竞价型队列会启动四个这样的实例（24 除以 6）。

如果第二个启动说明提供了最低的每单位现货价格（c3.xlarge 每实例小时现货价格除以 5），则竞价型队列会启动五个这样的实例（24 除以 5，结果向上舍入）。

实例权重和分配策略

考虑一个具有以下配置的竞价型队列请求：

- 目标容量为 30
- 一个实例类型为 c3.2xlarge 且权重为 8 的启动说明
- 一个实例类型为 m3.xlarge 且权重为 8 的启动说明
- 一个实例类型为 r3.xlarge 且权重为 8 的启动说明

竞价型队列会启动四个实例（30 除以 8，结果向上舍入）。使用 lowestPrice 策略时，所有四个实例都来自提供最低每单位现货价格的池。使用 diversified 策略时，竞价型队列会在所有三个池中各启动 1 个实例，并在三个池中提供最低每单位现货价格的那个池中启动第四个实例。

演练：将竞价型队列与实例权重结合使用

此演练使用一个名为 Example Corp 的虚构公司演示使用实例权重为竞价型队列出价的过程。

目标

Example Corp 是一家医药公司，该公司想要利用 Amazon EC2 的计算功能来筛查可能用于对抗癌症的化学成分。

计划

Example Corp 首先查看[竞价最佳实践](#)。然后，Example Corp 确定了他们的竞价型队列的以下要求。

实例类型

Example Corp 有一个计算和内存密集型应用程序，该应用程序在至少 60 GB 内存和八个虚拟 CPU (vCPU) 的情况下性能最佳。他们希望以尽可能低的价格为该应用程序提供尽可能多的这些资源。Example Corp 认定以下任意 EC2 实例类型都能满足其需求：

| 实例类型 | 内存 (GiB) | vCPU |
|------------|----------|------|
| r3.2xlarge | 61 | 8 |
| r3.4xlarge | 122 | 16 |
| r3.8xlarge | 244 | 32 |

以单位数表示的目标容量

采用实例权重，目标容量可以等于几个实例（默认）或一些因素（如内核 (vCPU)、内存 (GiB) 和存储 (GB)）的组合。将其应用程序的基本要求（60 GB RAM 和八个 vCPU）作为 1 个单位，Example Corp 决定 20 倍此数量可满足其需求。因此该公司将其竞价型队列请求的目标容量设置为 20。

实例权重

确定目标容量后，Example Corp 计算了实例权重。为了计算每个实例类型的实例权重，他们按如下所示确定每个实例类型需要多少单位才能达到目标容量：

- r3.2xlarge (61.0 GB, 8 vCPUs) = 1 个 20 单位
- r3.4xlarge (122.0 GB, 16 vCPUs) = 2 个 20 单位
- r3.8xlarge (244.0 GB, 32 vCPUs) = 4 个 20 单位

因此，Example Corp 在其竞价型队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时出价

Example Corp 使用每实例小时[按需定价](#)作为其出价的起点。他们也可以使用最近的现货价格或两者的组合。为了计算每单位小时出价，他们用每实例小时的起始出价除以权重。例如：

| 实例类型 | 按需价格 | 实例权重 | 每单位小时价格 |
|------------|---------|------|---------|
| r3.2xLarge | \$0.7 | 1 | \$0.7 |
| r3.4xLarge | 1.4 USD | 2 | \$0.7 |
| r3.8xLarge | \$2.8 | 4 | \$0.7 |

Example Corp 可以输入一个每单位小时 0.7 USD 的全局出价来对全部三个实例类型竞价。他们还可以输入一个每单位小时 0.7 USD 的全局出价并在 r3.8xlarge 启动说明中输入每单位小时 0.9 USD 的特定出价。根据其竞价型队列的预置策略，Example Corp 可以出较低的价格以便进一步降低成本，也可以出较高的价格以便减少可能的中断。

验证权限

在创建竞价型队列请求之前，Example Corp 验证它是否拥有具备所需权限的 IAM 角色。有关更多信息，请参阅[竞价型队列先决条件 \(p. 204\)](#)。

创建请求

Example Corp 为其竞价型队列请求创建一个具有以下配置的文件 config.json：

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-482e4972",  
            "WeightedCapacity": 1  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.4xlarge",  
            "SubnetId": "subnet-482e4972",  
            "WeightedCapacity": 2  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.8xlarge",  
            "SubnetId": "subnet-482e4972",  
            "SpotPrice": "0.90",  
            "WeightedCapacity": 4  
        }  
    ]  
}
```

Example Corp 使用以下 `request-spot-fleet` 命令创建竞价型队列请求：

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关更多信息，请参阅 [竞价型队列请求 \(p. 203\)](#)。

执行

分配策略确定竞价型实例来自哪个竞价型实例池。

使用 `lowestPrice` 策略（这是默认策略）时，竞价型实例来自在执行时具有最低每单位现货价格的池。为了提供 20 个单位的容量，竞价型队列有三种做法：启动 20 个 `r3.2xlarge` 实例（20 除以 1）、10 个 `r3.4xlarge` 实例（20 除以 2）或 5 个 `r3.8xlarge` 实例（20 除以 4）。

如果 Example Corp 使用 `diversified` 策略，则竞价型实例会来自所有三个池。竞价型队列会启动 6 个 `r3.2xlarge` 实例（提供 6 个单位）、3 个 `r3.4xlarge` 实例（提供 6 个单位）和 2 个 `r3.8xlarge` 实例（提供 8 个单位），总共 20 个单位。

竞价型实例定价历史记录

您的出价需要高于现货价格以确保单个竞价请求能够完成。当您的出价超过现货价格时，Amazon EC2 会启动您的竞价型实例，当现货价格上涨到超出您的出价，Amazon EC2 会终止您的竞价型实例。您可以出价超过当前现货价格，以便快速完成竞价请求。不过，在您为竞价型实例指定出价前，我们建议您查看现货价格历史记录。您可以查看最近 90 天的现货价格历史记录，并按照实例类型、操作系统和可用区筛选。

以现货价格历史记录为指导，您可以选择在之前能够满足您的需求的出价。例如，您可以确定什么出价在您查看的时间范围内提供了 75% 的正常运行时间。但请注意，历史趋势不能确保以后的结果。现货价格因实时供需情况而异，过去产生特定现货价格模式的情况可能在未来不会出现。

使用控制台查看现货价格历史记录

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 如果您是首次接触竞价型实例，则会看到欢迎页面；请选择 Get started，滚动到屏幕底部，然后选择 Cancel。
4. 选择 Pricing History。默认情况下，页面显示过去一天中所有可用区中的 Linux t1.micro 实例的数据图。将鼠标移动到图形上可在图形下方的表中显示特定时间的价格。
5. (可选) 要查看特定可用区的现货价格历史记录，请从列表中选择一个可用区。您还可以选择其他产品、实例类型或日期范围。

使用命令行查看现货价格历史记录

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-spot-price-history](#) (AWS CLI)
- [Get-EC2SpotPriceHistory](#) (适用于 Windows PowerShell 的 AWS 工具)

竞价型实例请求

要使用竞价型实例，您需要创建竞价型实例请求，其中包括实例数量、实例类型、可用区以及您愿意为每小时实例使用时间支付的最高价格 (您的出价)。如果您的出价超过当前现货价格，则 Amazon EC2 将立即执行您的请求。否则，Amazon EC2 将等待直至可以执行您的请求，或者直至您取消请求。

以下演示了竞价请求的运行方式。请注意，为竞价型实例中断采取的操作取决于请求类型 (一次性还是持久性)。如果请求是持久性请求，则在竞价型实例终止之后将重新打开请求。

内容

- [竞价型实例请求状态 \(p. 196\)](#)
- [指定竞价型实例的持续时间 \(p. 197\)](#)
- [指定竞价型实例租赁 \(p. 197\)](#)
- [创建竞价型实例请求 \(p. 198\)](#)
- [查找正在运行的竞价型实例 \(p. 200\)](#)
- [标记竞价型实例请求 \(p. 200\)](#)
- [取消竞价型实例请求 \(p. 201\)](#)
- [竞价请求示例启动说明 \(p. 201\)](#)

竞价型实例请求状态

竞价型实例请求可以处于以下某种状态：

- `open` - 请求正在等待执行。
- `active` - 请求已执行并有关联的竞价型实例。
- `failed` - 请求的一个或多个参数错误。
- `closed` - 竞价型实例被中断或终止。
- `cancelled` - 您取消了请求，或者请求已过期。

以下显示了请求状态之间的转换。请注意，转换取决于请求类型 (一次性还是持久性)。

一次性竞价型实例请求在 Amazon EC2 启动竞价型实例、请求过期前或者您取消请求前保持有效。如果现货价格提高并超过您的出价，您的竞价型实例会终止，竞价型实例请求关闭。

持久性竞价型实例请求在过期或您取消它之前保持有效，即使该请求已完成也如此。例如，如果您在现货价格为 0.25 USD 时为一个实例创建持久性竞价型实例请求，当您的出价超过 0.25 USD 时，Amazon EC2 启动您的竞价型实例。如果现货价格上涨超过了您的出价，您的竞价型实例将终止；不过，竞价型实例请求重新打开，Amazon EC2 将在现货价格低于您的出价时启动新的竞价型实例。

您可以通过出价状态跟踪您的竞价型实例请求状态以及启动的竞价型实例状态。有关更多信息，请参阅 [竞价出价状态 \(p. 220\)](#)。

指定竞价型实例的持续时间

当现货价格发生更改时，Amazon EC2 不会终止带有指定持续时间的竞价型实例（也被称作竞价型限制）。这使得此实例非常适合需在有限时间内完成的任务，如批处理、编码和渲染、建模和分析以及连续集成。

您可将持续时间指定为 1、2、3、4、5 或 6 小时。您支付的价格取决于指定的持续时间。要查看 1 小时持续时间或 6 小时持续时间的当前价格，请参阅 [竞价型实例价格](#)。您可使用这些价格来估计 2、3、4 和 5 小时持续时间的费用。在完成带持续时间的请求时，您的竞价型实例的价格是固定的，而且此价格在实例终止前保持有效。您需要按照此价格为实例运行的每个小时或不足一小时支付费用。请注意，未满 1 小时的实例小时，将按 1 小时计费。

在您的竞价请求中指定持续时间时，每个竞价型实例的持续时间段将在该实例收到其实例 ID 后立即开始。竞价型实例将运行，直到您终止它或其持续时间段结束。在持续时间段结束后，Amazon EC2 将竞价型实例标记为终止并提供一个竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。

使用控制台启动具有指定持续时间的竞价型实例

选择合适的请求类型。有关更多信息，请参阅 [创建竞价型实例请求 \(p. 198\)](#)。

使用 AWS CLI 启动具有指定持续时间的竞价型实例

要为您的竞价型实例指定持续时间，请将 `--block-duration-minutes` 选项与 `request-spot-instances` 命令包含在一起。例如，以下命令可创建一个竞价请求，启动运行时间为两小时的竞价型实例：

```
aws ec2 request-spot-instances --spot-price "0.050" --instance-count 5 --block-duration-minutes 120 --type "one-time" --launch-specification file://specification.json
```

使用 AWS CLI 检索带指定的持续时间的竞价型实例的费用

使用 `describe-spot-instance-requests` 命令可检索带指定持续时间的竞价型实例的固定费用。该信息位于 `actualBlockHourlyPrice` 字段中。

指定竞价型实例租赁

您可以在单租户硬件上运行竞价型实例。专用竞价型实例与属于其他 AWS 账户的实例物理隔离。有关更多信息，请参阅 [专用实例 \(p. 237\)](#) 和 [Amazon EC2 专用实例](#) 产品页面。

要运行专用竞价型实例，请执行以下操作之一：

- 在创建竞价型实例请求时，指定租赁 `dedicated`。有关更多信息，请参阅 [创建竞价型实例请求 \(p. 198\)](#)。
- 请求 VPC 中实例租赁为 `dedicated` 的竞价型实例。有关更多信息，请参阅 [创建有专用实例租期的 VPC \(p. 239\)](#)。请注意，如果在 VPC 中请求实例租赁为 `dedicated`，则无法请求租赁为 `default` 的竞价型实例。

以下实例类型支持专用竞价型实例。

最新一代

- c3.8xlarge
- c4.8xlarge
- d2.8xlarge
- g2.8xlarge
- i2.8xlarge
- m4.10xlarge
- m4.16xlarge
- p2.16xlarge
- r3.8xlarge
- r4.16xlarge
- x1.32xlarge

上一代

- cc2.8xlarge
- cg1.4xlarge
- cr1.8xlarge
- hi1.4xlarge

创建竞价型实例请求

请求竞价型实例的过程与启动按需实例的过程相似。请注意，提交请求之后，您无法更改竞价请求的参数，包括出价。

如果您一次请求了多个竞价型实例，Amazon EC2 将创建单独的竞价型实例请求，这样您可以分别跟踪各个请求的状态。有关跟踪竞价请求的更多信息，请参阅[竞价出价状态 \(p. 220\)](#)。

先决条件

在开始之前，请确定您的出价、需要多少个竞价型实例以及要使用的实例类型。要查看现货价格趋势，请参阅[竞价型实例定价历史记录 \(p. 195\)](#)。

使用控制台创建竞价型实例请求

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 如果您是首次接触竞价型实例，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot Instances。
4. 在 Find instance types 页面中，执行以下操作：
 - a. 对于 Request type，默认值为使用竞价型队列创建的一次性竞价请求。有关更多信息，请参阅[竞价型队列请求 \(p. 203\)](#)。要改为使用竞价型限制，请选择 Reserve for duration。
 - b. 对于 Target capacity，输入要请求的单位数量。您可以选择实例或是对应用程序工作负载十分重要的性能特征（如 vCPU、内存和存储）。
 - c. [竞价型限制] 对于 Reserved duration，请选择完成工作所需的小时数。
 - d. 对于 AMI，选择 AWS 提供的一个基本 Amazon 系统映像 (AMI)，或选择 Use custom AMI 以指定您自己的 AMI。
 - e. 对于 Instance type(s)，请选择 Select。选择具有您所需最低硬件规格的实例类型（虚拟 CPU、内存和存储）。

- f. [竞价型队列] 对于 Allocation strategy , 请选择满足您需求的策略。有关更多信息 , 请参阅 [竞价型队列分配策略 \(p. 192\)](#)。
 - g. 对于 Network , 您的账户可能支持 EC2-Classic 和 EC2-VPC 平台 , 或者仅支持 EC2-VPC 平台。要查明您的账户支持的平台 , 请参阅 [支持的平台 \(p. 435\)](#)。
 - [现有 VPC] 选择 VPC。
 - [新 VPC] 选择 Create new VPC 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。
 - [EC2-Classic] 选择 EC2-Classic。
 - h. (可选) 对于 Availability Zones , 默认由 AWS 为您的竞价型实例选择可用区。如果您想使用特定可用区 , 请执行以下操作 :
 - [EC2-VPC] 选择一个或多个可用区。如果您在一个可用区中有多个子网 , 则请从 Subnet 中选择合适的子网。要添加子网 , 请选择 Create new subnet 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。
 - [EC2-Classic] 选择 Select specific zone/subnet , 然后选择一个或多个可用区。
 - i. [竞价型队列] 对于 Maximum price , 您可以使用自动出价 , 也可以指定一个出价。如果您的出价低于所选实例类型的现货价格 , 则您的竞价型实例不会启动。
 - j. 选择 Next。
5. 在 Configure (配置实例详细信息) 页面中 , 执行以下操作 :
- a. (可选) 如果需要更多存储 , 您可以根据实例类型指定实例存储卷或 EBS 卷。
 - b. (可选) 如果您需要运行专用竞价型实例 , 请为 Tenancy 选择 Dedicated。
 - c. (可选) 如果您需要连接到您的实例 , 请使用 Key pair name 指定您的密钥对。
 - d. (可选) 如果您需要启动带有 IAM 角色的竞价型实例 , 请使用 IAM instance profile 指定角色。
 - e. (可选) 如果您要运行任何启动脚本 , 请使用 User data 指定脚本。
 - f. 对于 Security groups , 选择一个或多个安全组。
 - g. [EC2-VPC] 如果需要连接到 VPC 中您的实例 , 请启用 Auto-assign Public IP。
 - h. 默认情况下 , 请求在被执行或被您取消之前保持有效。要创建仅在特定时段内有效的请求 , 请编辑 Request valid from 和 Request valid to。
 - i. [竞价型队列] 默认情况下 , 我们会在请求过期时终止您的竞价型实例。要维持实例在请求过期之后继续运行 , 请清除 Terminate instances at expiration。
 - j. 选择 Review。
6. 在 Review 页面上 , 确认启动配置。要进行更改 , 请选择 Previous。要下载启动配置的副本以便与 AWS CLI 结合使用 , 请选择 JSON config。如果准备就绪 , 请选择 Launch。
7. 在确认页面上 , 请选择 OK。

[竞价型队列] 请求类型为 fleet。执行请求后 , 系统会添加请求类型 instance , 此时其状态为 active 和 fulfilled。

[竞价型限制] 请求类型为 block , 且初始状态为 open。执行请求后 , 状态为 active 和 fulfilled。

使用 AWS CLI 创建竞价型实例请求

使用以下 [request-spot-instances](#) 命令可创建一次性请求 :

```
aws ec2 request-spot-instances --spot-price "0.05" --instance-count 5 --type "one-time" --launch-specification file://specification.json
```

使用以下 [request-spot-instances](#) 命令可创建持久性请求 :

```
aws ec2 request-spot-instances --spot-price "0.05" --instance-count 5 --type "persistent" --launch-specification file://specification.json
```

例如，启动规范文件，请参阅[竞价请求示例启动说明 \(p. 201\)](#)。

当现货价格低于您的出价时，Amazon EC2 将启动您的竞价型实例。竞价型实例将运行，直到它被中断或您自行将它终止。使用以下 `describe-spot-instance-requests` 命令可监控您的竞价型实例请求：

```
aws ec2 describe-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

查找正在运行的竞价型实例

当现货价格低于您的出价时，Amazon EC2 将启动竞价型实例。竞价型实例将会运行，直到出价不再高于现货价格或您自己终止了它。(如果您的出价与现货价格完全一致，那么根据需求情况，您的竞价型实例有机会保持运行。)

使用控制台查找正在运行的竞价型实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。

您可以看到竞价型实例请求和竞价型队列请求。如果竞价型实例请求已执行，那么 Capacity 就是竞价型实例的 ID。对于竞价型队列，Capacity 表示已执行的请求容量。要查看竞价型队列中的实例的 ID，请选择扩展箭头，或者选择队列，然后选择 Instances 选项卡。

3. 或者，在导航窗格中，选择 Instances。在右上角，选择 Show/Hide 图标，然后选择 Lifecycle。对于每个实例，Lifecycle 为 normal、spot 或 scheduled。

使用 AWS CLI 查找正在运行的竞价型实例

要枚举您的竞价型实例，请结合使用 `describe-spot-instance-requests` 命令和 `--query` 选项，如下所示：

```
aws ec2 describe-spot-instance-requests --query SpotInstanceRequests[*].{ID:InstanceId}
```

下面是示例输出：

```
[  
  {  
    "ID": "i-1234567890abcdef0"  
  },  
  {  
    "ID": "i-0598c7d356eba48d7"  
  }  
]
```

或者，您可结合使用 `describe-instances` 命令和 `--filters` 选项来枚举您的竞价型实例，如下所示：

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

标记竞价型实例请求

要对您的竞价型实例请求进行分类和管理，您使用您选择的元数据为它们做标记。您可以使用标记任何其他 Amazon EC2 资源的同样方法来标记您的竞价型实例请求。有关更多信息，请参阅[标记 Amazon EC2 资源 \(p. 626\)](#)。

您可以在创建请求之后为其分配标签。

您为竞价型实例请求创建的标签只适用于该请求。这些标签不会自动添加到竞价服务为完成请求所启动的竞价型实例中。在竞价型实例启动后，您必须自己将标签添加到竞价型实例。

使用 AWS CLI 向您的竞价型实例请求或竞价型实例添加标签

使用以下 [create-tags](#) 命令标记您的资源：

```
aws ec2 create-tags --resources sir-08b93456 i-1234567890abcdef0 --tags  
Key=purpose,Value=test
```

取消竞价型实例请求

如果您不再需要竞价请求，您可以将其取消。您只能取消处于 `open` 或 `active` 状态的竞价型实例请求。当您的请求未执行，且实例没有启动时，您的竞价请求处于 `open` 状态。当您的请求完成，且竞价型实例已启动时，您的竞价请求处于 `active` 状态。如果您的竞价请求处于 `active` 状态，且关联的竞价型实例正在运行，那么取消此请求不会终止该实例；您必须手动终止正在运行的竞价型实例。

如果竞价请求是持久性竞价请求，则会返回 `open` 状态，这样就可以启动新的竞价型实例。要取消持久性竞价请求并终止其竞价型实例，您必须先取消竞价请求，然后终止竞价型实例。否则，竞价请求可以启动新实例。

使用控制台取消竞价型实例请求

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests，然后选择竞价请求。
3. 选择 Actions，然后选择 Cancel spot request。
4. (可选) 如果您使用完关联的竞价型实例，则可以终止这些实例。在导航窗格中，请选择 Instances 并选择实例，然后依次选择 Actions、Instance State、Terminate。

使用 AWS CLI 取消竞价型实例请求

使用以下 [cancel-spot-instance-requests](#) 命令可取消指定的竞价请求：

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

如果您已完成关联的竞价型实例，则可使用以下 [terminate-instances](#) 命令手动终止这些实例：

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

竞价请求示例启动说明

以下示例显示了可与 [request-spot-instances](#) 命令结合使用来创建竞价型实例请求的启动配置。有关更多信息，请参阅 [创建竞价型实例请求 \(p. 198\)](#)。

1. 启动竞价型实例 (p. 201)
2. 在指定的可用区中启动竞价型实例 (p. 202)
3. 在指定的子网中启动竞价型实例 (p. 202)
4. 启动专用竞价型实例 (p. 203)

示例 1：启动竞价型实例

以下示例不包括可用区或子网。Amazon EC2 为您选择可用区。如果您的账户仅支持 EC2-VPC，则 Amazon EC2 将在所选可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则 Amazon EC2 将在所选可用区的 EC2-Classic 中启动实例。

```
{
```

```
"ImageId": "ami-1a2b3c4d",
"KeyName": "my-key-pair",
"SecurityGroupIds": [ "sg-1a2b3c4d" ],
"InstanceType": "m3.medium",
"IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
}
}
```

请注意，您可按 ID 或名称为 EC2-Classic 指定安全组 (使用 `SecurityGroups` 字段)。您必须按 ID 为 EC2-VPC 指定安全组。

示例 2：在指定的可用区中启动竞价型实例

以下示例包括一个可用区。如果您的账户仅支持 EC2-VPC，则 Amazon EC2 将在指定可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则 Amazon EC2 将在指定可用区的 EC2-Classic 中启动实例。

```
{
    "ImageId": "ami-1a2b3c4d",
    "KeyName": "my-key-pair",
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
    "InstanceType": "m3.medium",
    "Placement": {
        "AvailabilityZone": "us-west-2a"
    },
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

示例 3：在指定的子网中启动竞价型实例

以下示例包括一个子网。Amazon EC2 在指定的子网中启动实例。如果 VPC 是一个非默认 VPC，则默认情况下，该实例不会收到公有 IPv4 地址。

```
{
    "ImageId": "ami-1a2b3c4d",
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
    "InstanceType": "m3.medium",
    "SubnetId": "subnet-1a2b3c4d",
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

要将公有 IPv4 地址分配给非默认 VPC 中的实例，请指定 `AssociatePublicIpAddress` 字段，如以下示例所示。请注意，在指定一个网络接口时，必须使用该网络接口 (而不是使用示例 3 中所示的 `SubnetId` 和 `SecurityGroupIds` 字段) 包含子网 ID 和安全组 ID。

```
{
    "ImageId": "ami-1a2b3c4d",
    "KeyName": "my-key-pair",
    "InstanceType": "m3.medium",
    "NetworkInterfaces": [
        {
            "DeviceIndex": 0,
            "SubnetId": "subnet-1a2b3c4d",
            "Groups": [ "sg-1a2b3c4d" ],
            "AssociatePublicIpAddress": true
        }
    ]
}
```

```
],
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

示例 4：启动专用竞价型实例

以下示例请求租赁为 `dedicated` 的竞价型实例。专用竞价型实例必须在 VPC 中启动。

```
{
    "ImageId": "ami-1a2b3c4d",
    "KeyName": "my-key-pair",
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
    "InstanceType": "c3.8xlarge",
    "SubnetId": "subnet-1a2b3c4d",
    "Placement": {
        "Tenancy": "dedicated"
    }
}
```

竞价型队列请求

要使用竞价型队列，您需要创建一个竞价型队列请求，该请求包括目标容量、实例的一个或多个启动说明以及您的出价。当出价发生更改时，Amazon EC2 将尝试维护您的竞价型队列的目标容量。有关更多信息，请参阅 [竞价型队列的工作方式 \(p. 191\)](#)。

您可以创建竞价型队列，以针对所需容量提交一次性 `request`，或者要求其随着时间的推移 `maintain` 目标容量。两种请求类型都可以使用竞价型队列的分配策略。

当您 `request` 目标容量时，竞价型队列会根据需要出价，但在容量减少时，不会尝试补充竞价型实例。如果容量不可用，竞价型队列不会在其他竞价池中提交出价。

如果您要 `maintain` 目标容量，竞价型队列会根据需要提交出价以满足目标容量，并自动补充任何中断的实例。默认情况下，竞价型队列设置为 `maintain` 请求的目标容量。

提交一次性 `request` 后，其目标容量则无法修改。要更改目标容量，请取消请求并重新提交新请求。

竞价型队列请求在过期或您取消它之前保持有效。取消竞价型队列请求时，您可以指定取消竞价型队列请求是否会终止您竞价型队列中的竞价型实例。

每个启动说明包括 Amazon EC2 启动实例所需的信息 – 例如 AMI、实例类型、子网或可用区、一个或多个安全组。

内容

- [竞价型队列请求状态 \(p. 204\)](#)
- [竞价型队列先决条件 \(p. 204\)](#)
- [竞价型队列和 IAM 用户 \(p. 204\)](#)
- [竞价型队列运行状况检查 \(p. 205\)](#)
- [规划竞价型队列请求 \(p. 205\)](#)
- [创建竞价型队列请求 \(p. 206\)](#)
- [监控您的竞价型队列 \(p. 207\)](#)
- [修改竞价型队列请求 \(p. 208\)](#)
- [取消竞价型队列请求 \(p. 208\)](#)
- [竞价型队列示例配置 \(p. 209\)](#)

竞价型队列请求状态

竞价型队列请求可以处于以下某种状态：

- `submitted` - 正在评估竞价型队列请求，并且 Amazon EC2 正准备启动目标数量的竞价型实例。
- `active` - 已验证竞价型队列，并且 Amazon EC2 正在尝试维持目标数量的正在运行的竞价型实例。请求会保持这一状态，直到其被修改或取消。
- `modifying` - 正在修改竞价型队列请求。请求会保持这一状态，直到修改全部完成或竞价型队列被取消。无法修改一次性 `request`，并且这一状态不适用于此类竞价请求。
- `cancelled_running` - 竞价型队列已取消且不会启动其他竞价型实例，但其现有的竞价型实例将继续运行，直到其被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。
- `cancelled_terminating` - 竞价型队列已取消，且其竞价型实例正在终止。请求会保持此状态，直到所有实例都已终止。
- `cancelled` - 竞价型队列已取消，且没有正在运行的竞价型实例。竞价型队列请求将在其实例终止两天后被删除。

以下显示了请求状态之间的转换。请注意，如果您超出了竞价型队列的限制，则请求会被立即取消。

竞价型队列先决条件

如果您使用 AWS 管理控制台创建竞价型队列，则该队列会创建一个命名为 `aws-ec2-spot-fleet-role` 的角色（该角色会授予竞价型队列代表您出价、启动和终止实例的权限），并在您的竞价型队列请求中指定该队列。如果您使用 AWS CLI 或 API 创建竞价型队列，则可以使用该角色（如果存在）或按以下步骤手动创建您自己的角色。

使用 AmazonEC2SpotFleetRole 策略手动创建 IAM 角色

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在导航窗格中，选择 Roles。
3. 选择 Create New Role。
4. 在 Set Role Name 页面上，请键入角色名称，然后选择 Next Step。
5. 在 Select Role Type 页面上，选择 Amazon EC2 Spot Fleet Role 旁的 Select。
6. 在 Attach Policy 页面上，选择 AmazonEC2SpotFleetRole 策略，然后选择 Next Step。
7. 在 Review 页面上，选择 Create Role。

竞价型队列和 IAM 用户

如果 IAM 用户将创建或管理竞价型队列，请确保授予他们所需的权限，如下所示。

授予 IAM 用户竞价型队列的权限

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在导航窗格中选择 Policies，然后选择 Create Policy。
3. 在 Create Policy 页上，选择 Create Your Own Policy 旁的 Select。
4. 在 Review Policy 页上，输入策略名称并将以下文本复制到 Policy Document 部分。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
    "Effect": "Allow",
    "Action": [
        "ec2:/*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole",
        "iam>ListRoles",
        "iam>ListInstanceProfiles"
    ],
    "Resource": "*"
}
]
```

`ec2:*` 使 IAM 用户能够调用所有 Amazon EC2 API 操作。要将用户限制到特定 API 操作，请改为指定这些操作。

`iam:PassRole` 操作使用户能够在竞价型队列请求中指定竞价型实例角色。`iam>ListRoles` 操作使用户能够枚举现有角色。`iam>ListInstanceProfiles` 操作使用户能够枚举现有实例配置文件。Amazon EC2 控制台使用 `iam>ListRoles` 填充 IAM role 列表，使用 `iam>ListInstanceProfiles` 填充 IAM instance profile 列表。要使用户能够通过控制台来创建角色或实例配置文件，您必须添加以下操作：`iam>CreateRole`、`iam>CreateInstanceProfile` 和 `iam>AddRoleToInstanceProfile`。

5. 选择 Create Policy。
6. 在导航窗格中选择 Users，然后选择将提交竞价型队列请求的用户。
7. 在权限选项卡中，请选择添加权限。
8. 选择直接附加现有策略。选择以上您创建的策略，选择 Next: Review，然后选择添加权限。

竞价型队列运行状况检查

竞价型队列每 2 分钟检查一次队列中竞价型实例的运行状况。实例的运行状况为 `healthy` 或 `unhealthy`。竞价型队列将使用 Amazon EC2 提供的状态检查来确定实例的运行状况。如果在连续三次运行状况检查中，实例状态检查或系统状态检查的状态有任一项为 `impaired`，则该实例的运行状况为 `unhealthy`。否则，运行状况为 `healthy`。有关更多信息，请参阅 [实例的状态检查 \(p. 313\)](#)。

您可以配置竞价型队列以替换运行状况不佳的实例。在启用运行状况检查替换后，实例将在其运行状况报告为 `unhealthy` 后被替换。请注意，在替换运行状况不佳的实例时，竞价型队列的容量可能在几分钟内降至其目标容量以下。

要求

- 仅保持目标容量的竞价型队列（而非一次性竞价型队列）支持运行状况检查替换。
- 您可以将竞价型队列配置为仅在您创建它时替换运行状况不佳的实例。
- IAM 用户仅在其有权调用 `ec2:DescribeInstanceStatus` 操作时才能使用运行状况检查替换。

规划竞价型队列请求

在创建竞价型队列请求前，请查看[竞价最佳实践](#)。使用这些最佳实践规划您的竞价型队列请求，以便以可能的最低价格配置需要的实例类型。还建议执行以下操作：

- 确定您要创建的竞价型队列是针对所需目标容量提交一次性 `request`，还是随着时间推移 `maintain` 目标容量。
- 确定满足您的应用程序要求的实例类型。

- 确定您的竞价型队列请求的目标容量。您可以采用实例或自定义单位设置目标容量。有关更多信息，请参阅 [竞价型队列实例权重 \(p. 192\)](#)。
- 确定每实例小时出价。出价较低能够进一步降低成本，而出价较高则可以降低中断发生的可能性。
- 如果您在使用实例权重，请确定您的每单位现货价格。要计算每单位出价，请将每实例小时出价除以该实例表示的单位数（或权重）。（如果不使用实例权重，则默认的每单位出价是每实例小时出价。）
- 查看用于您的竞价型队列请求的可能选项。关于更多信息，请参阅 AWS Command Line Interface Reference 中的 `request-spot-fleet` 命令。有关其他示例，请参阅 [竞价型队列示例配置 \(p. 209\)](#)。

创建竞价型队列请求

创建竞价型队列请求时，您必须指定有关要启动的竞价型实例的信息（例如实例类型和现货价格）。

使用控制台创建竞价型队列请求

1. 在 <https://console.aws.amazon.com/ec2spot> 处打开竞价控制台。
2. 如果您是首次接触竞价，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot Instances。
3. 在 Find instance types 页面中，执行以下操作：
 - a. 对于 Request type，请选择 Request 或 Request and Maintain。
 - b. 对于 Target capacity，输入要请求的单位数量。您可以选择实例或是对应用程序工作负载十分重要的性能特征（如 vCPU、内存和存储）。
 - c. 对于 AMI，选择由 AWS 提供的基础 Amazon 系统映像（AMI）之一，或者选择 Use custom AMI 以使用来自我们用户社区的 AMI、AWS Marketplace 或您自己的 AMI 之一。
 - d. 对于 Instance type(s)，请选择 Select。选择具有您所需最低硬件规格的实例类型（虚拟 CPU、内存和存储）。
 - e. 对于 Allocation strategy，选择满足您的需求的策略。有关更多信息，请参阅 [竞价型队列分配策略 \(p. 192\)](#)。
 - f. 对于 Network，您的账户可能支持 EC2-Classic 和 EC2-VPC 平台，或者仅支持 EC2-VPC 平台。要查明您的账户支持的平台，请参阅 [支持的平台 \(p. 435\)](#)。
 - [现有 VPC] 选择 VPC。
 - [新 VPC] 选择 Create new VPC 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。
 - [EC2-Classic] 选择 EC2-Classic。
 - g. (可选) 对于 Availability Zones，默认由 AWS 为您的竞价型实例选择可用区。如果您想使用特定可用区，请执行以下操作：
 - [EC2-VPC] 选择一个或多个可用区。如果您在一个可用区中有多个子网，则请从 Subnet 中选择合适的子网。要添加子网，请选择 Create new subnet 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。
 - [EC2-Classic] 选择 Select specific zone/subnet，然后选择一个或多个可用区。
 - h. 对于 Maximum price，您可以使用自动出价，也可以指定一个出价。如果您的出价低于所选实例类型的现货价格，则您的竞价型实例不会启动。
 - i. 选择 Next。
4. 在 Configure (配置实例详细信息) 页面中，执行以下操作：
 - a. (可选) 要替换 Request and Maintain 竞价型队列中运行状况不佳的实例，请选择 Replace unhealthy instances。
 - b. (可选) 如果您要运行任何启动脚本，请使用 User data 指定脚本。
 - c. (可选) 如果您需要连接到您的实例，请使用 Key pair name 指定您的密钥对。
 - d. (可选) 如果您需要启动带有 IAM 角色的竞价型实例，请使用 IAM instance profile 指定角色。
 - e. 对于 Security groups，选择一个或多个安全组。

- f. [EC2-VPC] 如果您需要连接到您在 VPC 中的实例，对于 Auto-assign IPv4 Public IP，请选择 Enable。
 - g. 默认情况下，请求在被执行或被您取消之前保持有效。要创建仅在特定时段内有效的请求，请编辑 Request valid from 和 Request valid to。
 - h. (可选) 默认情况下，我们会在请求过期时终止您的竞价型实例。要维持实例在请求过期之后继续运行，请清除 Terminate instances at expiration。
 - i. 选择 Review。
5. 在 Review 页面上，确认启动配置。要进行更改，请选择 Previous。要下载启动配置的副本以便与 AWS CLI 结合使用，请选择 JSON config。如果准备就绪，请选择 Launch。
 6. 在确认页面上，请选择 OK。请求类型为 fleet。执行请求后，系统会添加请求类型 instance，此时其状态为 active 和 fulfilled。

使用 AWS CLI 创建竞价型队列请求

使用以下 [request-spot-fleet](#) 命令可创建竞价型队列请求：

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关示例配置文件，请参阅[竞价型队列示例配置 \(p. 209\)](#)。

下面是示例输出：

```
{  
    "SpotFleetRequestId": "sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

监控您的竞价型队列

当现货价格低于您的出价时，竞价型队列会启动竞价型实例。竞价型实例将会运行，直到出价不再高于现货价格或您自己终止了它们。

使用控制台监控您的竞价型队列

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的竞价型队列请求。配置详细信息在 Description 选项卡中提供。
4. 要列出竞价型队列的竞价型实例，请选择 Instances 选项卡。
5. 要查看竞价型队列的历史记录，请选择 History 选项卡。

使用 AWS CLI 监控您的竞价型队列

使用以下 [describe-spot-fleet-requests](#) 命令可描述竞价型队列请求：

```
aws ec2 describe-spot-fleet-requests
```

使用以下 [describe-spot-fleet-instances](#) 命令可描述指定竞价型队列的竞价型实例：

```
aws ec2 describe-spot-fleet-instances --spot-fleet-request-id sfr-73fbcd2ce-  
aa30-494c-8788-1cee4EXAMPLE
```

使用以下 [describe-spot-fleet-request-history](#) 命令可描述指定竞价型队列请求的历史记录：

```
aws ec2 describe-spot-fleet-request-history --spot-fleet-request-id sfr-73fdb2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2015-05-18T00:00:00Z
```

修改竞价型队列请求

您可以修改活动的竞价型队列请求以完成以下任务：

- 提升目标容量
- 减少目标容量

Note

无法修改一次性竞价型队列请求。

当您提升目标容量时，竞价型队列会根据其竞价型队列请求的分配策略来启动额外的竞价型实例。如果分配策略是 `lowestPrice`，则竞价型队列从竞价型队列请求中价格最低的竞价型实例池启动实例。如果分配策略是 `diversified`，则竞价型队列在竞价型队列请求中的池间分配实例。

当您减少目标容量时，竞价型队列会取消任何超过新目标容量的开放出价。您可以请求竞价型队列终止竞价型实例，直到队列的大小达到新目标容量。如果分配策略是 `lowestPrice`，则竞价型队列会终止每单位价格最高的实例。如果分配策略是 `diversified`，则竞价型队列会在池间终止实例。或者，您可以请求竞价型队列保持当前的队列大小，而不替换已中断或您手动终止的任何竞价型实例。

请注意，当竞价型队列因目标容量下降而终止某个实例时，该实例将收到一条竞价型实例终止通知。

使用控制台修改竞价型队列请求

- 在 <https://console.aws.amazon.com/ec2spot/home/fleet> 处打开竞价控制台。
- 选择您的竞价型队列请求。
- 选择 Actions，然后选择 Modify target capacity。
- 在 Modify target capacity 中，执行以下操作：
 - 输入新的目标容量。
 - (可选) 如果您要减少目标容量，但是要使队列保持其当前大小，请取消选择 Terminate instances。
 - 选择 Submit。

使用 AWS CLI 修改竞价型队列请求

使用以下 `modify-spot-fleet-request` 命令可更新指定竞价型队列请求的目标容量：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fdb2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 20
```

您可以按如下所示修改前面的命令，以减少指定竞价型队列的目标容量而不因此终止任何竞价型实例：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fdb2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 10 --excess-capacity-termination-policy NoTermination
```

取消竞价型队列请求

在使用完竞价型队列后，可以取消竞价型队列请求。这将取消与竞价型队列关联的所有竞价请求，从而不会为您的竞价型队列启动任何新的竞价型实例。您必须指定竞价型队列是否应终止其竞价型实例。如

果您终止实例，则竞价型队列请求会进入 `cancelled_terminating` 状态。否则，竞价型队列请求会进入 `cancelled_running` 状态，并且实例会继续运行，直到它们中断或您手动终止它们。

使用控制台取消竞价型队列请求

1. 在 <https://console.aws.amazon.com/ec2spot/home/fleet> 处打开竞价控制台。
2. 选择您的竞价型队列请求。
3. 选择 Actions，然后选择 Cancel spot request。
4. 在 Cancel spot request 中，确认是否要取消竞价型队列。要使队列保持其当前大小，请取消选择 Terminate instances。如果准备就绪，请选择 Confirm。

使用 AWS CLI 取消竞价型队列请求

使用以下 `cancel-spot-fleet-requests` 命令可取消指定的竞价型队列请求并终止实例：

```
aws ec2 cancel-spot-fleet-requests --spot-fleet-request-ids sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --terminate-instances
```

下面是示例输出：

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE",  
            "CurrentSpotFleetRequestState": "cancelled_terminating",  
            "PreviousSpotFleetRequestState": "active"  
        }  
    ],  
    "UnsuccessfulFleetRequests": []  
}
```

可以按如下所示修改前面的命令，以取消指定的竞价型队列请求而不终止实例：

```
aws ec2 cancel-spot-fleet-requests --spot-fleet-request-ids sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --no-terminate-instances
```

下面是示例输出：

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE",  
            "CurrentSpotFleetRequestState": "cancelled_running",  
            "PreviousSpotFleetRequestState": "active"  
        }  
    ],  
    "UnsuccessfulFleetRequests": []  
}
```

竞价型队列示例配置

下列示例显示了可与 `request-spot-fleet` 命令结合使用以创建竞价型队列请求的启动配置。有关更多信息，请参阅 [创建竞价型队列请求 \(p. 206\)](#)。

1. 使用区域中价格最低的可用区或子网启动竞价型实例 (p. 210)
2. 使用指定列表中价格最低的可用区或子网启动竞价型实例 (p. 210)

3. 使用指定列表中价格最低的实例类型启动竞价型实例 (p. 211)
4. 覆盖请求的现货价格 (p. 213)
5. 使用多样化分配策略启动竞价型队列 (p. 214)
6. 使用实例权重启动竞价型队列 (p. 215)

示例 1：使用区域中价格最低的可用区或子网启动竞价型实例

以下示例指定一个没有可用区或子网的启动说明。如果您的账户仅支持 EC2-VPC，则竞价型队列会在具有默认子网的价格最低的可用区中启动实例。如果您的账户支持 EC2-Classic，则竞价型队列会在价格最低的可用区的 EC2-Classic 中启动实例。请注意，您支付的价格不会超过为请求指定的现货价格。

```
{  
    "SpotPrice": "0.07",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

示例 2：使用指定列表中价格最低的可用区或子网启动竞价型实例

以下示例指定具有的可用区或子网不同但实例类型和 AMI 相同的两种启动说明。

可用区

如果您的账户仅支持 EC2-VPC，则竞价型队列会在您指定的价格最低的可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则竞价型队列会在您指定的价格最低的可用区中启动实例。

```
{  
    "SpotPrice": "0.07",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "Placement": {  
                "AvailabilityZone": "us-west-2a, us-west-2b"  
            },  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

```
        ]
    }
```

Subnets

您可以指定默认子网或非默认子网，并且非默认子网可来自默认 VPC 或非默认 VPC。竞价服务会在位于价格最低的可用区的子网中启动实例。

请注意，您无法在竞价型队列请求中指定来自相同可用区的不同子网。

```
{
  "SpotPrice": "0.07",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "KeyName": "my-key-pair",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "m3.medium",
      "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
      "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
      }
    }
  ]
}
```

如果在默认 VPC 中启动实例，则实例在默认情况下会收到一个公有 IPv4 地址。如果在非默认 VPC 中启动实例，则实例在默认情况下不会收到一个公有 IPv4 地址。在启动说明中使用网络接口来将一个公有 IPv4 地址分配给在非默认 VPC 中启动的实例。请注意，在指定一个网络接口时，您必须使用该网络接口包含子网 ID 和安全组 ID。

```
...
{
  "ImageId": "ami-1a2b3c4d",
  "KeyName": "my-key-pair",
  "InstanceType": "m3.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d",
      "Groups": [ "sg-1a2b3c4d" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
  }
}
...
```

示例 3：使用指定列表中价格最低的实例类型启动竞价型实例

以下示例指定实例类型不同、但 AMI 和可用区或子网相同的两种启动配置。竞价型队列使用价格最低的指定实例类型启动实例。

可用区域

```
{  
    "SpotPrice": "1.00",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        }  
    ]  
}
```

子网

```
{  
    "SpotPrice": "1.00",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

示例 4. 覆盖请求的现货价格

通过为单个启动说明指定现货价格的功能，您可对出价过程进行更多控制。以下示例使用三个启动说明中的两个启动说明单独使用的现货价格来覆盖请求的现货价格。请注意，请求的现货价格用于未单独指定现货价格的任何启动说明。竞价型队列使用价格最低的实例类型启动实例。

可用区域

```
{  
    "SpotPrice": "1.00",  
    "TargetCapacity": 30,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "SpotPrice": "0.10"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.4xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "SpotPrice": "0.20"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        }  
    ]  
}
```

子网

```
{  
    "SpotPrice": "1.00",  
    "TargetCapacity": 30,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "SpotPrice": "0.10"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.4xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "SpotPrice": "0.20"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

```
}
```

示例 5：使用多样化分配策略启动竞价型队列

以下示例使用 `diversified` 分配策略。启动说明具有不同的实例类型，但具有相同的 AMI 和可用区或子网。竞价型队列在 3 个启动说明间分配 30 个实例，每种类型 10 个实例。有关更多信息，请参阅 [竞价型队列分配策略 \(p. 192\)](#)。

可用区域

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

子网

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

```
    ]  
}
```

示例 6：使用实例权重启动竞价型队列

以下示例使用实例权重，这意味着出价是每单位小时出价而不是每实例小时出价。每个启动配置列出不同的实例类型和不同的权重。竞价型队列选择每单位小时价格最低的实例类型。竞价型队列通过将目标容量除以实例权重来计算要启动的竞价型实例数。如果结果不是整数，则竞价型队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。

如果 `r3.2xlarge` 出价成功，竞价将预置 4 个这类实例。(将 20 除以 6 可得到总共 3.33 个实例，然后向上舍入为 4 个实例。)

如果 `c3.xlarge` 出价成功，竞价将预置 7 个这类实例。(将 20 除以 3 可得到总共 6.66 个实例，然后向上舍入为 7 个实例。)

有关更多信息，请参阅 [竞价型队列实例权重 \(p. 192\)](#)。

可用区域

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "WeightedCapacity": 6  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "WeightedCapacity": 3  
        }  
    ]  
}
```

子网

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "WeightedCapacity": 6  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "WeightedCapacity": 3  
        }  
    ]  
}
```

```
    ]  
}
```

优先级

您也可以使用实例权重为可用区或子网指定优先级。例如，以下启动说明几乎完全相同，只是指定了不同的子网和权重。竞价型队列会查找具有最高 `WeightedCapacity` 值的说明，并尝试在相应子网中价格最低的竞价型实例池中为请求预置资源。(请注意，第二个启动说明不包含权重，因此其默认为 1。)

```
{  
    "SpotPrice": "0.42",  
    "TargetCapacity": 40,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.2xlarge",  
            "SubnetId": "subnet-482e4972",  
            "WeightedCapacity": 2  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.2xlarge",  
            "SubnetId": "subnet-bb3337d"  
        }  
    ]  
}
```

竞价型队列的 CloudWatch 指标

Amazon EC2 提供了可用来监控竞价型队列的 Amazon CloudWatch 指标。

Important

为确保准确性，我们建议您在使用这些指标时启用详细监控。有关更多信息，请参阅 [对您的实例启用或禁用详细监控 \(p. 321\)](#)。

有关 Amazon EC2 提供的 CloudWatch 指标的详细信息，请参阅 [使用 CloudWatch 监控您的实例 \(p. 320\)](#)。

竞价型队列指标

AWS/EC2Spot 命名空间包含以下指标以及针对队列中的竞价型实例的 CloudWatch 指标。有关更多信息，请参阅 [实例指标 \(p. 322\)](#)。

AWS/EC2Spot 命名空间包括以下指标。

| 指标 | 描述 |
|-----------------------------|---|
| AvailableInstancePoolsCount | 竞价型队列请求中指定的竞价型实例池。 单位：计数 |
| BidsSubmittedForCapacity | Amazon EC2 已提交竞价的容量。 单位：计数 |
| EligibleInstancePoolCount | 在 Amazon EC2 可以完成出价的竞价型队列请求中指定的竞价型实例池。在您的出价低于现货价格或者现货价格高于按需实例价格的池中，Amazon EC2 不会完成出价。 |

| 指标 | 描述 |
|------------------------------|--|
| | 单位 : 计数 |
| FulfilledCapacity | Amazon EC2 已执行的容量。 单位 : 计数 |
| MaxPercentCapacityAllocation | 在竞价型队列请求中指定的所有竞价型实例池中的 PercentCapacityAllocation 最大值。 单位 : 百分比 |
| PendingCapacity | TargetCapacity 与 FulfilledCapacity 之间的区别。 单位 : 计数 |
| PercentCapacityAllocation | 针对所指定维度的竞价型实例池分配的容量。要获取所有竞价型实例池中记录的最大值 , 请使用 MaxPercentCapacityAllocation。 单位 : 百分比 |
| TargetCapacity | 竞价型队列请求的目标容量。 单位 : 计数 |
| TerminatingCapacity | 由于竞价型实例中断而正终止使用的容量。 单位 : 计数 |

如果指标的度量单位是 Count , 则最有用的统计信息是 Average。

竞价型队列维度

要筛选竞价型队列的数据 , 可使用以下维度。

| 维度 | 说明 |
|------------------|----------------|
| AvailabilityZone | 按照可用区筛选数据。 |
| FleetRequestId | 按照竞价型队列请求筛选数据。 |
| InstanceType | 按实例类型筛选数据。 |

查看竞价型队列的 CloudWatch 指标

可使用 Amazon CloudWatch 控制台查看竞价型队列的 CloudWatch 指标。这些指标显示为监控图表。如果竞价型队列处于活动状态 , 这些图表会显示数据点。

指标首先按命名空间进行分组 , 然后按各命名空间内的各种维度组合进行分组。例如 , 您可以按竞价型队列请求 ID、实例类型或可用区来查看所有竞价型队列指标或竞价型队列指标组。

查看竞价型队列指标

1. 通过以下网址打开 CloudWatch 控制台 : <https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中 , 在 Metrics 下 , 选择 EC2 Spot 命名空间。
3. (可选) 要按维度筛选指标 , 请选择下列选项之一 :

- Fleet Request Metrics - 按竞价型队列请求分组
 - By Availability Zone - 按竞价型队列请求和可用区分组
 - By Instance Type - 按竞价型队列请求和实例类型分组
 - By Availability Zone/Instance Type - 按竞价型队列请求、可用区和实例类型分组
4. 要查看指标的数据，请选中指标旁边的复选框。

竞价型队列的自动扩展

自动扩展 是根据需求自动增加或减少竞价型队列目标容量的能力。竞价型队列能够根据一个或多个扩展策略，在您选择的范围内启动实例（扩展）或终止实例（缩减）。我们建议您创建两个策略，一种用于扩展，一个用于缩减。

扩展策略 使用 CloudWatch 警报来触发扩展流程。例如，如果您希望在 CPU 利用率达到特定水平时扩展，可以使用 Amazon EC2 提供的 `CPUUtilization` 指标创建警报。

在创建扩展策略时，必须指定以下扩展调整类型之一：

- Add — 按指定的容量单位数量或当前容量的指定百分比来增加队列的目标容量。
- Remove — 按指定的容量单位数量或当前容量的指定百分比来缩减队列的目标容量。
- Set to — 将队列的目标容量设为指定的容量单位数量。

当触发警报时，Auto Scaling 过程使用执行容量和扩展策略计算新的目标容量，然后相应地更新目标容量。例如，假设目标容量和执行容量为 10，扩展策略加 1。当触发警报时，Auto Scaling 过程为 10 增加 1 得到 11，因此竞价型队列启动 1 个实例。

如果使用实例加权，请记住，竞价型队列可以根据需要超出目标容量，并且执行容量可以是浮点数，但目标容量必须是整数，因此竞价型队列向上舍入到下一个整数。在您查看触发警报时扩展策略的结果时，必须考虑这些行为。例如，假设目标容量为 30，执行容量为 30.1，扩展策略减 1。当触发报警时，Auto Scaling 过程将 30.1 减 1 得到 29.1，然后将其向上取整为 30，因此不执行扩展操作。再如，假设您选择的实例权重为 2、4 和 8，目标容量为 10，但没有权重 2 实例可用，因此竞价型队列为执行容量为 12 的实例预配置权重为 4 和 8 的实例。如果扩展策略将目标容量减少 20% 并触发警报，则 Auto Scaling 过程将 12 减 12×0.02 得到 9.6，然后将其向上取整为 10，因此不执行扩展操作。

此外，您还可以为扩展策略配置冷却时间。这是扩展活动完成后上一个与触发相关的扩展活动可能影响将来扩展事件的秒数。对于扩大策略，虽然冷却时间有效，但启动冷却的上一个扩大事件所添加的容量将计算为下一次扩大所需容量的一部分。旨在持续（但不过度）扩大。对于缩小策略，冷却时间用于阻止后续缩小请求，直至到期。旨在谨慎地缩小以保护您的应用程序的可用性。但是，如果在缩小后，另一个警报在冷却时间内触发了扩大策略，Auto Scaling 将立即扩大您的可扩展目标。

请注意，当竞价型队列因目标容量下降而终止某个实例时，该实例将收到一条竞价型实例终止通知。

限制

- 竞价型队列请求必须使用 `maintain` 作为请求类型。一次性请求或竞价型限制不支持自动扩展。

先决条件

- 考虑哪些 CloudWatch 指标对您的应用程序比较重要。您可以根据 AWS 提供的指标或您自己的自定义指标来创建 CloudWatch 警报。
- 如果您打算在扩展策略中使用 AWS 指标，请为其启用 CloudWatch 指标集合（如果提供这些指标的服务默认未启用它的话）。
- 使用 AWS 管理控制台为竞价型队列启用自动扩展功能时，它会创建一个名为 `aws-ec2-spot-fleet-autoscale-role` 的角色来授予 Auto Scaling 权限，以描述策略警报、监控队列的当前容量及修改队列的

容量。如果您使用 AWS CLI 或 API 配置自动扩展功能，则可以使用该角色（如果存在）或按以下步骤手动创建您自己的角色。

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在导航窗格中，选择 Roles。
3. 选择 Create New Role。
4. 在 Set Role Name 页面上，请键入角色名称，然后选择 Next Step。
5. 在 Select Role Type 页面上，选择 Amazon EC2 旁的 Select。
6. 在 Attach Policy 页面上，选择 AmazonEC2SpotFleetAutoscaleRole 策略，然后选择 Next Step。
7. 在 Review 页面上，选择 Create Role。
8. 选择您刚创建的角色。
9. 在 Trust Relationships 选项卡上，选择 Edit Trust Relationship。
10. 将 ec2.amazonaws.com 更改为 application-autoscaling.amazonaws.com，然后选择 Update Trust Policy。

创建 CloudWatch 警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Alarms。
3. 选择 Create Alarm。
4. 为 CloudWatch Metrics by Category 选择一个类别，如 EC2 Spot Metrics 或 Fleet Request Metrics。
5. 选择一个指标，然后选择 Next。
6. 对于 Alarm Threshold，请键入警报的名称和描述，并为警报设置阈值和时间段数量。
7. (可选) 如需接收扩展事件通知，请为 Actions 选择 New list，然后键入您的电子邮件地址。当然，您也可以删除通知，待日后需要时再添加。
8. 选择 Create Alarm。

使用控制台为竞价型队列配置自动扩展功能

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的竞价型队列请求，然后选择 Auto Scaling 选项卡。
4. 如果未配置自动扩展，请选择 Configure。
5. 使用 Scale capacity between 设置队列的最小和最大容量。队列的自动扩展操作不会超出最小或最大容量范围。
6. 最初，Scaling policies 包含名为 ScaleUp 和 ScaleDown 的策略。您可以完善这些策略，或选择 Remove policy 来删除它们。您也可以选择 Add policy 来添加策略。
7. 要定义策略，请执行以下操作：
 - a. 在 Policy name 中键入策略的名称。
 - b. 对于 Policy trigger，可以选择现有的警报，或选择 Create new alarm 来打开 Amazon CloudWatch 控制台并创建警报。
 - c. 对于 Modify capacity，请选择扩展调整类型、数字及单位。
 - d. (可选) 要执行步进扩展，请选择 Define steps。默认情况下，添加策略的下限为负无穷，上限为警报阈值。默认情况下，删除策略的下限为警报阈值，上限为正无穷。要添加其他步骤，请选择 Add step。
 - e. (可选) 要修改冷却时间的默认值，请从 Cooldown period 中选择一个数字。
8. 选择 Save。

使用 AWS CLI 为竞价型队列配置自动扩展功能

1. 使用 [register-scalable-target](#) 命令将竞价型队列请求注册为可扩展目标。
2. 使用 [put-scaling-policy](#) 命令创建扩展策略。
3. 使用 [put-metric-alarm](#) 命令创建触发该扩展策略的警报。

竞价出价状态

为帮助您跟踪竞价型实例请求、计划对竞价型实例的使用，以及有策略地进行出价，Amazon EC2 提供了出价状态。例如，出价状态会帮助您了解竞价请求尚未完成的原因或列出会阻碍竞价请求完成的限制。

在此过程（也称为竞价请求生命周期）中的每一步，都有特定的事件确定连续的请求状态。

内容

- [竞价请求的生命周期 \(p. 220\)](#)
- [获取出价状态信息 \(p. 222\)](#)
- [竞价出价状态代码 \(p. 222\)](#)

竞价请求的生命周期

以下图表显示您的竞价请求在其整个生命周期中从提交到终止所遵循的路径。每个步骤用节点表示，每个节点状态代码描述您的竞价请求和竞价型实例的状态。

待评估

当您提交竞价型实例请求之后，除非一个或多个请求参数无效 (`bad-parameters`)，否则就会进入 `pending-evaluation` 状态。

| 状态代码 | 请求状态 | 实例状态 |
|---------------------------------|---------------------|------|
| <code>pending-evaluation</code> | <code>open</code> | 无 |
| <code>bad-parameters</code> | <code>closed</code> | 无 |

备用

如果一个或多个请求约束有效但目前无法满足，或者如果没有足够的容量，那么请求将进入备用状态，等待满足约束。请求选项影响请求完成的可能性。例如，如果您指定的出价低于当前现货价格，您的请求将保持为备用状态，直至现货价格低于您的出价。如果您指定了可用区组，则该请求将保持为备用状态，直至满足可用区的约束。

| 状态代码 | 请求状态 | 实例状态 |
|---|-------------------|------|
| <code>capacity-not-available</code> | <code>open</code> | 无 |
| <code>capacity-oversubscribed</code> | <code>open</code> | 无 |
| <code>price-too-low</code> | <code>open</code> | 无 |
| <code>not-scheduled-yet</code> | <code>open</code> | 无 |
| <code>launch-group-constraint</code> | <code>open</code> | 无 |
| <code>az-group-constraint</code> | <code>open</code> | 无 |
| <code>placement-group-constraint</code> | <code>open</code> | 无 |

| 状态代码 | 请求状态 | 实例状态 |
|----------------------------|------|------|
| constraint-not-fulfillable | open | 无 |

等待评估/最终执行

您的竞价型实例在以下几种情况下可能进入 `terminal` 状态：您创建的请求仅在特定时段内有效，但该时段在您的请求到达等待执行阶段之前过期；您取消了请求；或者，出现系统错误。

| 状态代码 | 请求状态 | 实例状态 |
|---|------------------------|------|
| <code>schedule-expired</code> | <code>closed</code> | 无 |
| <code>canceled-before-fulfillment*</code> | <code>cancelled</code> | 无 |
| <code>bad-parameters</code> | <code>failed</code> | 无 |
| <code>system-error</code> | <code>closed</code> | 无 |

* 如果您取消请求。

等待履行

当您指定的约束（如果有）得到满足且您的出价等于或高于当前现货价格时，您的竞价请求会进入 `pending-fulfillment` 状态。

此时，Amazon EC2 已经准备好为您预置您请求的实例。如果此进程在此时停止，则可能是因为用户在竞价型实例启动之前取消了请求，或者是因为出现了意外的系统错误。

| 状态代码 | 请求状态 | 实例状态 |
|----------------------------------|-------------------|------|
| <code>pending-fulfillment</code> | <code>open</code> | 无 |

已完成

当您的竞价型实例的所有规格都得到满足时，您的竞价请求将会执行。Amazon EC2 会启动竞价型实例，这可能需要几分钟时间。

| 状态代码 | 请求状态 | 实例状态 |
|------------------------|---------------------|--------------------------------|
| <code>fulfilled</code> | <code>active</code> | <code>pending → running</code> |

执行的最终

只要您的出价等于或高于现货价格，您的实例类型拥有备用竞价容量，且您没有终止您的竞价型实例，实例就会继续运行。如果现货价格或可用容量的变化要求 Amazon EC2 终止您的竞价型实例，竞价请求将转入最终状态。例如，如果您的出价等于现货价格，但是在该价格对竞价型实例的订阅过多，那么状态代码为 `instance-terminated-capacity-oversubscribed`。如果您取消竞价请求或终止竞价型实例，请求也将进入最终状态。

| 状态代码 | 请求状态 | 实例状态 |
|--|------------------------|----------------------|
| <code>request-canceled-and-instance-running</code> | <code>cancelled</code> | <code>running</code> |
| <code>marked-for-termination</code> | <code>closed</code> | <code>running</code> |

| 状态代码 | 请求状态 | 实例状态 |
|---|---------------------------|------------|
| instance-terminated-by-price | closed (一次性) , open (持久性) | terminated |
| instance-terminated-by-user | closed 或者 cancelled * | terminated |
| instance-terminated-no-capacity | closed (一次性) , open (持久性) | terminated |
| instance-terminated-capacity-oversubscribed | closed (一次性) , open (持久性) | terminated |
| instance-terminated-launch-group-constraint | closed (一次性) , open (持久性) | terminated |

* 如果您终止实例但未取消出价，则请求状态为 closed。如果您终止实例并取消出价，则请求状态为 cancelled。请注意，即使您在取消实例请求之前终止了竞价型实例，在 Amazon EC2 检测到您的竞价型实例已终止之前仍可能存在延迟。在这种情况下，请求状态可能是 closed 或 cancelled。

持久性请求：

当您的竞价型实例终止时 (由您或由 Amazon EC2)，如果竞价请求为持久性请求，则该请求返回 pending-evaluation 状态，并且在满足约束时，Amazon EC2 可以启动新的竞价型实例。

获取出价状态信息

您可以使用 AWS 管理控制台或命令行工具获取出价状态信息。

使用控制台获取出价状态信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，请选择 Spot Requests，然后选择竞价请求。
3. 在 Description (描述) 选项卡中检查 Status (状态) 的值。

使用命令行获取出价状态信息

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `describe-spot-instance-requests` (AWS CLI)
- `Get-EC2SpotInstanceRequest` (适用于 Windows PowerShell 的 AWS 工具)

竞价出价状态代码

竞价出价状态信息包括出价状态代码、更新时间和状态消息。同时，它们还帮助您决定竞价请求的处置。

以下为竞价出价状态代码：

`az-group-constraint`

Amazon EC2 无法在同一可用区中启动您请求的所有实例。

`bad-parameters`

您的竞价请求的一个或多个参数无效 (例如，您指定的 AMI 不存在)。出价状态消息指示哪个参数无效。`cancelled-before-fulfillment`

用户在请求执行前取消了竞价请求。

`capacity-not-available`

您请求的实例没有足够的容量可用。

`capacity-oversubscribed`

现货价格等于或高于您出价的竞价请求数量超过了此竞价型实例池的可用容量。

`constraint-not-fulfillable`

由于一个或多个约束无效 (例如，可用区不存在)，竞价请求无法完成。出价状态消息指示哪个约束无效。

`fulfilled`

竞价请求处于 `active` 状态，Amazon EC2 正在启动您的竞价型实例。

`instance-terminated-by-price`

现货价格超过您的出价。如果请求是一个持久性出价，过程会重新启动，因此，您的出价等待评估。

`instance-terminated-by-user` 或者 `spot-instance-terminated-by-user`

您终止了已完成的竞价型实例，因此出价状态会变成 `closed` (持久性出价除外)，实例状态为 `terminated`。

`instance-terminated-capacity-oversubscribed`

因为现货价格等于或高于您的出价的竞价请求数量已超出此竞价型实例池的可用容量，您的实例已被终止。(请注意，现货价格可能未更改。)竞价服务随机选择要终止的实例。

`instance-terminated-launch-group-constraint`

您的启动组中的一个或多个实例已终止，因此不再满足启动组的约束。

`instance-terminated-no-capacity`

此实例不再有足够的竞价容量可用。

`launch-group-constraint`

Amazon EC2 无法同时启动您请求的所有实例。启动组内的所有实例都一起启动和终止。

`limit-exceeded`

超过了 EBS 卷数量或总卷存储的限制。有关这些限制的详细信息以及如何请求提高限制，请参阅 Amazon Web Services 一般参考 中的 [Amazon EBS 限制](#)。

`marked-for-termination`

您的竞价型实例被标记为终止。

`not-scheduled-yet`

您的竞价请求在指定日期之前不会被评估。

`pending-evaluation`

当您提交竞价型实例请求之后，该请求会进入 `pending-evaluation` 状态，同时系统会评估您的请求中的参数。

`pending-fulfillment`

Amazon EC2 尝试预置您的竞价型实例。

`placement-group-constraint`

因为竞价型实例目前不能添加到置放群组中，因此尚无法完成竞价请求。

`price-too-low`

由于出价低于现货价格，尚无法执行出价请求。在这种情况下，没有实例启动且您的出价保持 `open`。

`request-cancelled-and-instance-running`

在竞价型实例仍在运行时，您取消了竞价请求。请求为 `cancelled`，但是，实例保持为 `running`。

schedule-expired

由于没有在指定日期前完成，竞价请求已过期。

system-error

出现意外系统错误。如果这是反复出现的问题，请联系客户支持获得帮助。

竞价型实例中断

对竞价型实例的需求在不同时间可能有显著的差异，竞价型实例的可用性也会因为未使用 EC2 实例的数量而差别巨大。此外，不论您的出价有多高，您的竞价型实例仍有可能会中断。因此，必须确保应用程序针对竞价型实例中断做好准备。我们强烈建议您不要为不能中断的应用程序使用竞价型实例。

下面列出了 Amazon EC2 终止您的竞价型实例的可能原因：

- 价格 – 现货价格高于您的出价。
- 容量 – 如果没有足够的未用 EC2 实例来满足对竞价型实例的需求，Amazon EC2 将从出价最低的实例开始终止竞价型实例。如果多个竞价型实例的出价相同，则随机确定实例的终止顺序。
- 约束 - 如果您的请求包含约束，例如启动组或可用区组，那么，当不再满足约束条件时，这些竞价型实例将成组终止。

准备中断

下面提供了在您使用竞价型实例时可以遵循的最佳实践：

- 选择一个合理的出价。您的出价应该足够高，这样您的请求才有机会完成，但又不能高于您愿意支付的价格。这非常重要，因为在长时间供应不足的情况下，现货价格可能会在这段时间内居高不下，因为此时价格依据的是最高出价。我们强烈建议您的出价高于按需实例的价格。
- 使用包含所需软件配置的 Amazon 系统映像 (AMI)，确保您的实例在请求完成时随时可以启动。您还可以使用用户数据在启动时运行命令。
- 在不会受竞价型实例终止影响的位置例行存储重要数据。例如，您可以使用 Amazon S3、Amazon EBS 或 DynamoDB。
- 将工作拆分为小的任务 (使用网格、Hadoop 或基于队列的架构) 或者使用检查点，以便您经常保存工作。
- 使用竞价型实例终止通知监控您的竞价型实例的状态。
- 测试您的应用程序，确保它很好地处理了意外终止的实例。您可以使用按需实例来运行应用程序，然后自行终止该按需实例，以便确认这一点。

竞价型实例终止通知

防范竞价型实例中断的最佳方法是为应用程序设计容错能力。此外，您还可以利用竞价型实例终止通知，该通知可在 Amazon EC2 必须终止您的竞价型实例时，提前两分钟发出警告。

此警告使用实例元数据中的项目，提供给在您的竞价型实例上运行的应用程序。例如，您可以使用以下查询定期检查实例元数据中的此警告 (建议每 5 秒检查一次)：

```
$ if curl -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo terminated; fi
```

有关检索实例元数据的其他方式的信息，请参阅 [检索实例元数据 \(p. 296\)](#)。

如果 Amazon EC2 将您的竞价型实例标记为终止，将存在 `termination-time` 项目，该项目以 UTC 时间指定实例将收到关闭信号的大致时间。例如：

```
2015-01-05T18:02:00Z
```

如果 Amazon EC2 未准备终止实例，或者，如果您自己终止了竞价型实例，则 `termination-time` 项目或者不存在（这样您会收到 HTTP 404 错误），或者包含并非时间值的值。

请注意，虽然我们会尽力在 Amazon EC2 将您的竞价型实例标记为终止时提供此警告，您的竞价型实例仍可能会在 Amazon EC2 提供此警告之前终止。因此，您必须确保应用程序已经准备好处理意外的竞价型实例中断，即使您在监视竞价型实例终止通知的情况下也应如此。

如果 Amazon EC2 未能终止实例，则竞价出价状态将设置为 `fulfilled`。请注意，`termination-time` 会将实例元数据保持原始大致时间（现已成为过去时间）。

竞价型实例数据源

为了帮助您了解您的竞价型实例费用情况，Amazon EC2 通过提供的数据元说明您的竞价型实例的使用情况和定价。此数据源会发送到您在订阅数据源时指定的 Amazon S3 存储桶。

数据源文件一般一小时到达您的存储桶一次，且每小时使用量一般都包含在单个数据文件中。这些文件在传送到您的存储桶前要进行压缩（gzip）。当文件很大时（例如，当一小时的文件内容在压缩前超过 50 MB 时），Amazon EC2 可以将给定小时的使用情况写入多个文件。

Note

如果在特定小时中没有竞价型实例运行，则您不会收到该小时的数据源文件。

内容

- [数据源文件名和格式 \(p. 225\)](#)
- [Amazon S3 存储桶要求 \(p. 226\)](#)
- [订阅您的竞价型实例数据源 \(p. 226\)](#)
- [删除您的竞价型实例数据源 \(p. 226\)](#)

数据源文件名和格式

竞价型实例数据源的文件名采用以下格式（用 UTC 日期和时间）：

```
bucket-name.s3.amazonaws.com/{optional prefix}/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

例如，如果您的存储桶名称为 `myawsbucket` 并且前缀为 `myprefix`，则您的文件名类似如下：

```
myawsbucket.s3.amazonaws.com/myprefix/111122223333.2014-03-17-20.001.pwBdGTJG.gz
```

竞价型实例数据源文件采用制表符分隔格式。数据文件的每一行都对应一小时实例使用时间，并且包含在下表中列出的字段。

| 字段 | 说明 |
|-------------------------|--|
| <code>Timestamp</code> | 使用时间戳来确定针对此一小时实例使用时间收取的费用。 |
| <code>UsageType</code> | 指示使用类型和被收取费用的实例类型。对于 <code>m1.small</code> 竞价型实例，此字段设置为 <code>SpotUsage</code> 。对于所有其他实例类型，此字段设置为 <code>SpotUsage:{instance-type}</code> 。例如： <code>SpotUsage:c1.medium</code> 。 |
| <code>Operation</code> | 指示被收取费用的产品。对于 Linux 竞价型实例，此字段设置为 <code>RunInstances</code> 。对于 Windows 竞价型实例，此字段设置为 <code>RunInstances:0002</code> 。竞价使用情况按照可用区分组。 |
| <code>InstanceID</code> | 生成此一小时实例使用时间的竞价型实例的 ID。 |
| <code>MyBidID</code> | 生成此一小时实例使用时间的竞价型实例请求的 ID。 |

| 字段 | 说明 |
|-------------|----------------------------|
| MyMaxPrice | 为此竞价型实例请求指定的最高价。 |
| MarketPrice | 在 Timestamp 字段中指定的时刻的现货价格。 |
| Charge | 此一小时实例使用时间的价格。 |
| Version | 此记录的数据源文件名中包含的版本。 |

Amazon S3 存储桶要求

在您订阅数据源时，必须指定 Amazon S3 存储桶来存储数据源文件。在为数据源选择 Amazon S3 存储桶之前，请考虑以下内容：

- 您必须使用美国东部（弗吉尼亚北部）区域（也称为 us-east-1 或美国标准区域）中的存储桶。
- 您必须拥有存储桶的 FULL_CONTROL 权限。

- 如果您是存储桶所有者，根据默认情况，您有此权限。或者，存储桶拥有者必须授予您的 AWS 账户此权限。
- 当您创建您的数据源订阅时，Amazon S3 更新指定存储桶的 ACL，向 AWS 数据源账户提供读取和写入权限。
 - 撤销数据源账户的权限不会禁用该数据源。如果您撤销这些权限但不禁用数据源，我们将在数据源账户下次需要写入存储桶时恢复这些权限。
 - 每一个数据源文件都有其自己的 ACL（不同于存储桶的 ACL）。存储桶拥有者具有数据文件的 FULL_CONTROL 权限。数据源账户具有读取和写入权限。
 - 如果您删除您的数据源订阅，Amazon EC2 不会撤销数据源账户在存储桶或数据文件上的读取和写入权限。您必须自行撤销这些权限。

订阅您的竞价型实例数据源

要订阅您的数据源，请使用以下 [create-spot-datafeed-subscription](#) 命令：

```
$ aws ec2 create-spot-datafeed-subscription --bucket myawsbucket [--prefix myprefix]
```

下面是示例输出：

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "111122223333",  
        "Prefix": "myprefix",  
        "Bucket": "myawsbucket",  
        "State": "Active"  
    }  
}
```

删除您的竞价型实例数据源

要删除数据源，请使用以下 [delete-spot-datafeed-subscription](#) 命令：

```
$ aws ec2 delete-spot-datafeed-subscription
```

竞价型实例限量

竞价型实例请求受以下限制的约束：

限制

- 不支持的实例类型 (p. 227)
- 竞价请求限制 (p. 227)
- 竞价出价限制 (p. 227)
- 竞价型队列限制 (p. 227)
- 不支持的 Amazon EBS 加密 (p. 227)

不支持的实例类型

竞价不支持以下实例类型：

- T2
- HS1

一些竞价型实例类型并非在所有区域均可用。要查看某个区域支持的实例类型，请转至[竞价型实例定价](#)并选择区域。

竞价请求限制

默认情况下，每个区域的账户限制为 20 个竞价型实例。如果您终止了竞价型实例，但没有取消请求，那么您请求的次数会算在此限制内，直到 Amazon EC2 检测到终止情况并关闭您的请求为止。

竞价型实例限制是动态的。如果您的账户是新账户，那么您的限制在开始时可能会低于 20，不过随着时间的推移会逐渐增加。此外，您的账户对特定竞价型实例类型可能存在一些限制。如果您提交竞价型实例请求，并且收到错误 `Max spot instance count exceeded`，您可以转到[AWS 支持中心](#)并提交限额提升申请表。对于 Use Case Description，请指出您需要提升您的竞价型实例请求限制。

竞价出价限制

竞价型实例的出价限制为按需价格的十倍。此限制旨在帮助您控制成本。

竞价型队列限制

通用 Amazon EC2 限制 (例如，竞价出价限制、实例限制和卷限制) 适用于竞价型队列所启动的实例。此外，以下限制将适用：

- 每个区域的活动竞价型队列数：1000
- 每个队列的启动说明数：50
- 启动说明中的用户数据大小：16 KB
- 每个竞价型队列的目标容量：3000
- 跨区域中所有竞价型队列的目标容量：5000
- 竞价型队列请求不能跨区域。
- 竞价型队列请求不能跨同一可用区内的不同子网。

不支持的 Amazon EBS 加密

您可以在竞价型实例的启动说明中指定加密的 EBS 卷，但这些卷未加密。

专用主机

Amazon EC2 专用主机是指 EC2 实例容量完全供您专用的物理服务器。专用主机允许您使用现有的按套接字、按内核或按 VM 软件授权的许可证，包括 Windows Server、Microsoft SQL Server、SUSE、Linux Enterprise Server 等。

内容

- [专用主机与专用实例之间的区别 \(p. 228\)](#)
- [定价和记账 \(p. 228\)](#)
- [专用主机的限制 \(p. 229\)](#)
- [专用主机配置 \(p. 230\)](#)
- [使用专用主机 \(p. 230\)](#)
- [监控专用主机 \(p. 236\)](#)

专用主机与专用实例之间的区别

专用主机和专用实例均可用于在专供您使用的物理服务器上启动 Amazon EC2 实例。

专用实例与专用主机上的实例在性能、安全性或物理特性方面没有区别。但是，专用主机可让您更清楚地了解和更有力地控制在物理服务器上放置实例的方式。

使用专用主机时，您可以使用“主机关联”和“实例自动放置”设置控制实例在主机上的放置。使用专用实例时，您无法控制实例在哪个主机上启动和运行。如果您的组织希望使用 AWS，但现有软件许可证具有硬件合规性要求，则可以了解主机硬件以满足要求。

有关专用主机与专用实例之间的区别的更多信息，请参阅 [Amazon EC2 专用主机](#)。

有关使用专用主机和专用实例的更多信息，请参阅 [修改实例租赁 \(p. 233\)](#)。

定价和记账

按需专用主机

按需计费在您将专用主机分配到您的账户时自动激活。

系统将以按需费率每小时对您计费一次。费率因专用主机支持的实例类型和运行专用主机的区域而异。实例类型大小或在专用主机上运行的实例的数量不会影响该主机的费用。

要终止按需计费，您必须先停止在专用主机上运行的实例，然后将其释放。有关更多信息，请参阅 [管理和释放专用主机 \(p. 234\)](#)。

专用预留主机

对比运行按需专用主机，专用预留主机提供账单折扣。预留提供三种付款选项：

- 无费用预付—无费用预付预留为某个期限内的专用主机使用提供折扣，并且不需要预付款。仅提供一年期限。
- 预付部分费用 - 必须支付一部分预留费用，期限内的剩余时间享受折扣。可以选择一年或三年期限。
- 预付全费 - 提供最低的有效价格。提供一年和三年期限，覆盖整个前期费用，无需额外付费。

您的账户中必须有活动的专用主机才能购买预留。在您的账户中，每个预留包含一个特定的专用主机。预留应用于主机上的实例系列，而不是实例大小。如果您有三个具有不同实例大小的专用主机 (m4.xlarge、m4.medium 和 m4.large)，则您可以将一个 m4 预留与所有这些专用主机关联。预留的实例系列和区域必须与您希望与其关联的专用主机匹配。

Note

预留与专用主机关联后，专用主机将无法释放，直到预留期限结束。

购买专用预留主机

您可以使用控制台或 API 购买专用主机预留。

使用控制台购买专用主机预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Dedicated Hosts 页面上，选择 Dedicated Host Reservations。
3. 选择 Purchase Dedicated Host Reservation。
4. 在 Purchase Dedicated Host Reservation 屏幕上，您可以搜索使用默认设置的产品，也可以为该产品指定配置。
 - Host instance family — 所列选项取决于您账户中未分配预留的专用主机。
 - Availability Zone — 您账户中未分配预留的专用主机的可用区。
 - Payment Option — 产品的付款选项。
 - Term — 预留期限。可以是一年或三年。
5. 选择 Find offering。
6. 选择产品。
7. 选择要与专用主机预留关联的专用主机。
8. 选择 Review。
9. 检查订单，然后选择 Purchase 完成交易。

查看专用主机预留

您可以查看与您的预留关联的专用主机的相关信息，如预留期限、选择的付款选项、预留的开始和结束日期等。

查看专用主机预留的详细信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Dedicated Hosts 页面上，选择 Dedicated Host Reservations。
3. 从所提供的列表中选择预留。
4. 有关预留的信息，请选择 Details。
5. 有关该预留关联的专用主机的信息，请选择 Hosts。

专用主机的限制

在分配专用主机之前，请注意以下限制。

- 由 AWS 提供、或者在 AWS Marketplace 中提供的 RHEL、SUSE Linux 和 Windows AMI 均无法用于专用主机。
- 不支持 Amazon EC2 实例自动恢复
- 可为每个区域的每个实例系列分配最多两个按需专用主机。可以请求提高限制：[请求提高 Amazon EC2 专用主机上的分配限制](#)。
- 在专用主机上运行的实例只能在 VPC 中启动。
- 主机限制独立于实例限制。正在专用主机上运行的实例不会计入您的实例限制。
- 不支持 Auto Scaling 组。
- 不支持 Amazon RDS 实例。
- AWS 免费使用套餐不适用于专用主机。
- 实例放置控制是指管理专用主机中的实例启动。专用主机不支持置放群组。

专用主机配置

专用主机配置为支持单个实例类型和大小容量。您可在专用主机上启动的实例的数量取决于专用主机配置所支持的实例类型。例如，如果您分配了一个 c3.xlarge 专用主机，则您有权在该专用主机上启动多达 8 个 c3.xlarge 实例。要确定您可在特定专用主机上运行的实例类型大小的数量，请参阅 [Amazon EC2 专用主机定价](#)。

使用专用主机

要使用专用主机，首先在您的账户中分配 要使用的主机。然后通过为实例指定一个 host 租赁在主机上启动实例。实例自动放置 设置可让您控制某个实例是否可在特定主机上启动。当某个实例停止并重新启动时，主机关联 设置将确定该实例是在同一主机上还是在另一个主机上重新启动。如果您不再需要某个按需主机，则可以停止在该主机上运行的实例，指示它们在另一个主机上启动，然后释放 该专用主机。

内容

- [自带许可 \(p. 230\)](#)
- [分配专用主机 \(p. 230\)](#)
- [在专用主机上启动实例 \(p. 231\)](#)
- [了解实例放置与主机关联 \(p. 232\)](#)
- [修改实例租赁 \(p. 233\)](#)
- [管理和释放专用主机 \(p. 234\)](#)
- [API 和 CLI 命令概览 \(p. 235\)](#)
- [使用 AWS Config 跟踪配置更改 \(p. 235\)](#)

自带许可

您可以在专用主机上使用您自己的软件许可证。为了将您自己的卷许可的虚拟机镜像引入 Amazon EC2，您需要遵循以下常规步骤。

1. 验证控制您的虚拟机镜像 (AMI) 使用的许可证条款是否允许在虚拟化的云环境中使用虚拟机镜像。有关 Microsoft 许可的更多信息，请参阅 [Amazon Web Services 和 Microsoft 许可](#)。
2. 在确认您的虚拟机镜像可在 Amazon EC2 内使用后，使用由 VM Import/Export 工具实现的 ImportImage API 操作导入您的虚拟机镜像。有关限制的更多信息，请参阅 [VM Import/Export 的先决条件](#)。有关如何使用 ImportImage 导入 VM 的信息，请参阅 [使用 ImportImage 将 VM 导入 Amazon EC2](#)。
3. 如果您需要用于跟踪您的镜像在 AWS 中使用的方式的机制，请在 AWS Config 服务中启用主机记录。您可以使用 AWS Config 来记录专用主机的配置更改并将输出用作许可证报告的数据源。有关更多信息，请参阅 [使用 AWS Config 跟踪配置更改 \(p. 235\)](#)。
4. 在导入虚拟机映像后，您可以在您的账户中在活动专用主机上从此映像启动实例。
5. 在运行这些实例时，根据操作系统，您可能需要针对自己的 KMS 服务器（例如，Windows Server 或 Windows SQL Server）激活这些实例。您无法针对 Amazon Windows KMS 服务器激活已导入的 Windows AMI。

分配专用主机

要开始使用专用主机，则需要将它们分配到您的账户。您可以使用 AWS 管理控制台、直接与 API 进行交互或使用命令行界面来执行这些任务。每次分配专用主机时可遵循这些步骤。

将专用主机分配到您的账户

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在专用主机页面上，选择 分配专用主机。

3. 使用提供的选项配置主机：
 - a. 实例类型 - 可在专用主机使用的实例类型。
 - b. 可用区 - 专用主机的可用区。
 - c. Allow instance auto-placement - 默认设置为 Off。专用主机只接受 host 租赁实例启动 (假设容量可用)。当实例自动设置为 On 时，租赁为 host 并且与专用主机的配置匹配的任何实例都可以启动到该主机。
 - d. Quantity - 使用这些设置分配的主机的数量。
4. 选择 Allocate host。

专用主机容量可立即在您的账户中使用。

如果您启动了带有租赁 host 的实例，但您的账户中没有任何活动的专用主机，您将收到一个错误，并且实例启动失败。

在专用主机上启动实例

在分配一个专用主机后，您可以在该主机上启动实例。带有租赁 host 的实例可在特定专用主机上启动，或者可让 Amazon EC2 为您选择合适的专用主机 (自动放置)。如果您的账户中的活动专用主机没有与要启动的实例的实例类型配置相符的可用容量，则您无法启动带有租赁 host 的实例。

Note

在专用主机上启动的实例只能在 VPC 中启动。有关更多信息，请参阅 [VPC 简介](#)。在启动实例之前，请注意限制。有关更多信息，请参阅 [专用主机的限制 \(p. 229\)](#)。

从“Dedicated Hosts”页面将实例启动到专用主机

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Dedicated Hosts 页面上，选择一个主机，选择 Actions，然后选择 Launch Instance(s) onto Host。
3. 选择要使用的 AMI。如果您导入了自己的 AMI，请选择左侧边栏上的 My AMIs，然后选择相关的 AMI。
4. 为专用主机选择实例类型；这是您可在该主机上启动的唯一实例类型。
5. 在 Configure Instance Details 页面上，系统预先选择了 Tenancy 和 Host 选项。您可以将 Affinity 设置切换到 On 或 Off。
 - On - 如果停止，实例将始终在该特定主机上重新启动。
 - Off - 实例启动到指定的专用主机上，但不保证停止后仍在其上重新启动。
6. 完成剩余步骤并选择 Launch Instances。

实例会自动启动到您指定的专用主机上。要在专用主机上查看实例，请转至 Dedicated Hosts 页面，然后选择您在启动该实例时指定的专用主机。

从“Instances”页面将实例启动到特定专用主机

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Instances 页面上，选择 Launch Instance。
3. 从列表中选择一个 AMI。如果您已导入自己的 AMI，则选择 My AMIs，然后选择导入的镜像。并非所有 AMI 均可用于专用主机。
4. 选择要启动的实例的类型。
5. 在 Configure Instance Details 页面上，专用主机设置为：
 - Tenancy - Dedicated host - 在专用主机上启动此实例。如果无法选择此选项，请检查您是否选择了不兼容的 AMI 或实例类型。

- Host - 选择主机。如果无法选择专用主机，请检查：
 - 所选子网是否与主机在不同可用区中。
 - 所选实例类型是否与专用主机支持的实例类型匹配。如果没有匹配的正在运行的主机，则唯一可用选项是 Use auto-placement，但除非您账户中有可用的匹配专用主机容量，否则实例将失败。
- 关联 - 默认设置是 Off。实例启动到指定的专用主机上，但不保证停止后仍在其上重新启动。

Note

如果您无法看到这些设置，请检查是否在 Network 菜单中选择了一个 VPC。

6. 完成剩余的配置步骤。选择 Review and Launch。
7. 选择 Launch 以启动您的实例。
8. 选择现有密钥对或创建新密钥对。选择 Launch Instances。

从“Instances”页面将实例启动到任意专用主机

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Instances 页面上，选择 Launch Instance。
3. 从列表中选择一个 AMI。如果您已导入自己的 AMI，则选择 My AMIs，然后选择导入的镜像。并非所有 AMI 均可用于专用主机。
4. 选择要启动的实例的类型。
5. 在 Configure Instance Details 页面上，专用主机设置为：
 - Tenancy - Dedicated host - Launch this instance on a Dedicated host 如果无法选择此选项，请检查是否选择了不兼容的 AMI 或实例类型。
 - Host - 对于此类启动，请将设置保留为 Use auto-placement。
 - 关联 - 默认设置是 Off。实例启动到您账户中的任意可用专用主机，但不保证停止后仍在其上重新启动。

如果您无法看到这些设置，请检查是否在 Network 菜单中选择了一个 VPC。

6. 完成剩余的配置步骤。选择 Review and Launch。
7. 选择 Launch 以启动您的实例。
8. 选择现有密钥对或创建新密钥对。选择 Launch Instances。

了解实例放置与主机关联

放置控制发生在实例级别和主机级别。

内容

- [实例自动放置 \(p. 232\)](#)
- [主机关联 \(p. 233\)](#)
- [修改实例自动放置和主机关联 \(p. 233\)](#)
- [修改实例主机关联 \(p. 233\)](#)

实例自动放置

自动放置允许您管理所启动的实例是启动到特定主机还是启动到有匹配配置的任意主机。默认设置为 Off。这意味着您所分配的专用主机只接受指定唯一主机 ID 的 host 租赁实例启动。未指定主机 ID 启动的实例不能启动到实例自动放置设置为 Off 的主机。

主机关联

主机关联在实例和专用主机之间建立启动关系。当关联设置为 `host` 时，启动到特定主机的实例在停止时始终在同一主机上重新启动。这适用于定向启动和非定向启动。

如果将关联设置为 `default`，并且您停止并重新启动了实例，则该实例可在任意可用主机上重新启动，但它将尝试回到其上次运行的专用主机上启动(尽力)。

您可以通过将关联从 `host` 更改为 `default` (或相反) 来修改实例与专用主机之间的关系。有关更多信息，请参阅 [修改实例租赁 \(p. 233\)](#)。

修改实例自动放置和主机关联

您可以使用 Amazon EC2 控制台、API 或 CLI 管理实例放置控制。

要修改您的实例的实例放置设置，请先停止实例，然后编辑实例放置设置。

Note

如果实例停止并重新启动，无法保证它在同一专用主机上重新启动。

编辑实例的放置设置 (任何可用主机)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Instances 页面上，选择要编辑的实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 将实例租赁更改为 Launch this instance on a Dedicated host。
6. 选择 This instance can run on any one of my Hosts。实例会启动到任何启用了自动放置的专用主机上。
7. 选择 Save 以继续。
8. 打开实例的上下文 (右键单击) 菜单，选择 Instance State，然后选择 Start。

编辑实例的放置设置 (特定专用主机)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Instances 页面上，选择要编辑的实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 将实例租赁更改为 Launch this instance on a Dedicated host。
6. 选择 This instance can only run on the selected Host。然后为 Target Host 选择一个值，选择是要将实例放置在任意主机上还是特定主机上。
7. 选择 Save 以继续。
8. 打开实例的上下文 (右键单击) 菜单，选择 Instance State，然后选择 Start。

修改实例主机关联

如果您不再希望实例与主机之间存在关联，您可停止实例，并将其关联更改为 `default`。这会消除实例与主机之间的关联性。但当您重新启动实例时，它可能会回到同一专用主机上启动(具体取决于您的账户中的专用主机可用性，尽力)。但如果实例再次被停止，它将不会在同一主机上重新启动。

修改实例租赁

如果某个专用实例的租赁未使用由 Amazon EC2 提供的 Windows、SUSE 或 RHEL AMI，您可以将该租赁从 `dedicated` 更改为 `host`。要执行此操作，您需要停止您的专用实例。带有 `shared` 租赁的实例无法修改为 `host` 租赁。

将实例租赁从 `dedicated` 更改为 `host`

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Instances，然后选择要修改的专用实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 打开实例的上下文 (右键单击) 菜单，选择 Instance Settings，然后选择 Modify Instance Placement。
5. 在 Modify Instance Placement 页面上，执行以下操作：
 - Tenancy - 选择 Launch this instance on a Dedicated host。
 - Affinity - 选择 This instance can run on any one of my Hosts 或 This instance can only run on the selected Host。

如果选择 This instance can run on any one of my Hosts，实例会启动到您账户中的任意可用兼容专用主机。

如果选择 This instance can only run on the selected Host，请为 Target Host 选择一个值。如果未列出目标主机，则您账户中可能没有可用的兼容专用主机。

6. 选择 Save。
7. 当您重启实例时，Amazon EC2 会将实例放在您账户中的可用专用主机上，如果它支持您所启动的实例类型。

管理和释放专用主机

您可以使用控制台，与 API 直接交互，或使用命令行界面来查看主机上单个实例的详细信息并释放按需专用主机。

查看专用主机上实例的详细信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 Dedicated Hosts 页面上，选择要查看更多详细信息的主机。
3. 选择 Description 选项卡以获取有关该主机的信息。选择 Instances 选项卡以获取有关您的主机上运行的实例的信息。

释放专用主机

需要先停止在专用主机上运行的任何实例，然后才能释放主机。这些实例可以迁移至您账户的其他专用主机，这样您就可以继续使用它们。有关更多信息，请参阅 [修改实例自动放置和主机关联 \(p. 233\)](#)。这些步骤只适用于按需专用主机。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在专用主机页面上，选择要释放的专用主机。
3. 选择 Actions、Release Hosts。
4. 通过选择 Release 确认您的选择。

在释放某个专用主机后，您无法再次重用同一主机或主机 ID。

在释放专用主机后，将不再向您收取它产生的按需费用。专用主机状态将更改为 `released`，您无法在该主机上启动任何实例。

如果您最近释放了专用主机，则它们可能要过一段时间才会停止计入您的限制。在此期间，如果尝试分配新的专用主机，可能会遇到 `LimitExceeded` 错误。如果出现这种情况，请在几分钟后再次尝试分配新的主机。

已停止的实例仍可以使用和列在 Instances 页面上。这些实例将保留其 `host` 租赁设置。

API 和 CLI 命令概览

您可以使用 API 或命令行执行本节中所述的任务。

将专用主机分配到您的账户

- [allocate-hosts](#) (AWS CLI)
- [AllocateHosts](#) (Amazon EC2 查询 API)
- [New-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

描述您的专用主机

- [describe-hosts](#) (AWS CLI)
- [DescribeHosts](#) (Amazon EC2 查询 API)
- [Get-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

修改您的专用主机

- [modify-hosts](#) (AWS CLI)
- [ModifyHosts](#) (Amazon EC2 查询 API)
- [Edit-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

修改实例自动放置

- [modify-instance-placement](#) (AWS CLI)
- [ModifyInstancePlacement](#) (Amazon EC2 查询 API)
- [Edit-EC2InstancePlacement](#) (适用于 Windows PowerShell 的 AWS 工具)

释放您的专用主机

- [release-hosts](#) (AWS CLI)
- [ReleaseHosts](#) (Amazon EC2 查询 API)
- [Remove-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 AWS Config 跟踪配置更改

您可以使用 AWS Config 记录专用主机的配置更改以及在这些主机上启动、停止或终止的实例的配置更改。然后，您可以将由 AWS Config 捕获的信息用作许可证报告的数据源。

AWS Config 分别记录专用主机和实例的配置信息并通过关系将这类信息配对。存在三种报告条件。

- AWS Config 记录状态 - 当其状态为 On 时，AWS Config 将记录一个或多个 AWS 资源类型，其中可包含专用主机和专用实例。要捕获许可证报告所需的信息，请使用以下字段验证是否记录了主机和实例。
- 主机记录状态 - 当其状态为 Enabled 时，将记录专用主机的配置信息。
- 实例记录状态 - 当其状态为 Enabled 时，将记录专用实例的配置信息。

如果禁用了这三个条件中的任一个，则 Edit Config Recording 按钮中的图标为红色。要发挥此工具的所有优点，请确保这三种记录方法都已启用。当这三种方法全部启用时，图标为绿色。要编辑设置，请选择 Edit Config Recording。您将被定向到 AWS Config 控制台中的 Set up AWS Config 页面，在该页面中，您可以设置 AWS Config 并启动对您的主机、实例和其他支持的资源类型的记录。有关更多信息，请参阅 AWS Config 开发人员指南 中的 [使用控制台设置 AWS Config](#)。

Note

AWS Config 将在发现您的资源后记录它们，此过程可能需要几分钟。

在 AWS Config 开始记录对您的主机和实例的配置更改后，您可以获取已分配或已释放的任何主机以及已启动、已停止或已终止的任何实例的配置历史记录。例如，在专用主机的配置历史记录中的任何时间点上，您均可以查看在该主机上启动的实例的数量以及该主机上的套接字和内核的数量。对于任何这些实例，您还可以查看其 Amazon 系统映像 (AMI) 的 ID。您可以使用此信息来报告您拥有的服务器端绑定软件 (按套接字或按内核授予许可) 的许可。

您可以采用以下任一方法查看配置历史记录。

- 通过使用 AWS Config 控制台。对于每个已记录的资源，您可以查看一个时间线页面，该页面提供了配置详细信息的历史记录。要查看此页面，请选择 Dedicated Hosts 页面的 Config Timeline 列中的灰色图标。有关更多信息，请参阅 AWS Config 开发人员指南 中的[在 AWS Config 控制台中查看配置详细信息](#)。
- 通过运行 AWS CLI 命令。首先，您可以使用 `list-discovered-resources` 命令获取一个包含所有主机和实例的列表。然后，您可以使用 `get-resource-config-history` 命令获取特定时间间隔内某个主机或实例的配置详细信息。有关更多信息，请参阅 AWS Config 开发人员指南 中的[使用 CLI 查看配置详细信息](#)。
- 通过在您的应用程序中使用 AWS Config API。首先，您可以使用 `ListDiscoveredResources` 操作获取一个包含所有主机和实例的列表。然后，您可以使用 `GetResourceConfigHistory` 操作获取特定时间间隔内某个主机或实例的配置详细信息。

例如，要从 AWS Config 中获取包含您的所有专用主机的列表，请运行 CLI 命令，例如下面的命令：

```
aws configservice list-discovered-resources --resource-type
    AWS::EC2::Host
```

要从 AWS Config 中获取某个专用主机的配置历史记录，请运行 CLI 命令，例如下面的命令：

```
aws configservice get-resource-config-history --resource-type
    AWS::EC2::Instance --resource-id i-36a47fdf
```

使用 AWS 管理控制台管理 AWS Config 设置

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在 Dedicated Hosts 页面上，选择 Edit Config Recording。
- 在 AWS Config 控制台中，按照提供的步骤来启用记录。有关更多信息，请参阅[使用控制台设置 AWS Config](#)。

有关更多信息，请参阅[在 AWS Config 控制台中查看配置详细信息](#)。

使用命令行或 API 激活 AWS Config

- 要使用 AWS CLI，请参阅 AWS Config 开发人员指南 中的[在 AWS Config 控制台中查看配置详细信息](#)。
- 要使用 Amazon EC2 API，请参阅 [GetResourceConfigHistory](#)。

监控专用主机

Amazon EC2 持续监控您的专用主机的状态；更新内容将在 Amazon EC2 控制台上传送。您还可以使用 API 或 CLI 来获取有关您的专用主机的信息。

下表说明了控制台中可能的 State 值。

| 州 | 说明 |
|----------------------------|---|
| available | AWS 未在专用主机上检测到问题；没有制定维护或修复计划。实例可在此专用主机上启动。 |
| released | 已释放专用主机。主机 ID 不再使用。无法重新使用已释放的主机。 |
| under-assessment | AWS 正在寻找专用主机可能存在的问题。如果需要采取措施，系统将通过 AWS 管理控制台或电子邮件通知您。实例无法在处于此状态的专用主机上启动。 |
| permanent-failure | 检测到了一个不可恢复的故障。您将通过您的实例或通过电子邮件接收到一个移出通知。您的实例可能会继续运行。如果在处于此状态的专用主机上停止或终止所有实例，AWS 将重试该主机。实例无法在处于此状态的专用主机上启动。 |
| released-permanent-failure | AWS 一直释放已发生故障的专用主机并且不再在这些主机上运行实例。专用主机 ID 不再可供使用。 |

专用实例

专用实例是在单一客户专用硬件上的 Virtual Private Cloud (VPC) 中运行的 Amazon EC2 实例。您的专用实例与属于其他 AWS 账户的实例在主机硬件级别是实体隔离的。专用实例可与来自同一 AWS 账户中属于非专用实例的其他实例共享硬件。

Note

专用主机 也是指专供您使用的物理服务器。使用专用主机，您可以查看和控制实例在服务器中的放置。有关更多信息，请参阅 [专用主机 \(p. 227\)](#)。

主题

- [专用实例基本信息 \(p. 237\)](#)
- [使用专用实例 \(p. 238\)](#)
- [API 和命令概览 \(p. 240\)](#)

专用实例基本信息

您在 VPC 内启动的每项实例都有一个租期属性。此属性有以下值。

| 值 | 说明 |
|-----------|------------------------------------|
| default | 您的实例在共享硬件上运行。 |
| dedicated | 您的实例在单租户硬件上运行。 |
| host | 您的实例在专用主机上运行，该主机是一个您可以控制其配置的隔离服务器。 |

对于默认实例，您在启动之后便无法更改其租期。您可以在实例启动后将实例的租期从 `dedicated` 更改为 `host`，也可以反方向更改。有关更多信息，请参阅 [更改实例的租期 \(p. 240\)](#)。

每个 VPC 都有相关的实例租期属性。在您创建 VPC 实例之后，您便无法更改实例的租期。此属性有以下值。

| 值 | 描述 |
|-----------|--|
| default | 默认情况下，在该 VPC 中启动的实例将在共享硬件上运行，除非您在实例启动期间显式指定了不同的租户。 |
| dedicated | 默认情况下，在该 VPC 中启动的实例为专用实例，除非您在实例启动期间显式指定了 host 租户。在实例启动期间，您无法指定 default 租户。 |

要创建专用实例，您可以执行以下操作：

- 创建一个实例租期设置为 `dedicated` 的 VPC (在该 VPC 内启动的所有实例都是专用实例)。
- 创建实例租期设置为 `default` 的 VPC，并在启动任何实例时将其租期指定为 `dedicated`。

专用实例限制

某些 AWS 服务或其功能无法用于实例租期设置为 `dedicated` 的 VPC。请检查服务文档以确认是否存在任何限制。

某些实例类型无法启动至实例租期设置为 `dedicated` 的 VPC 中。有关支持的实例类型的更多信息，请参阅 [Amazon EC2 专用实例](#)。

Amazon EBS 与专用实例

当您启动 Amazon EBS 支持的专用实例时，EBS 卷不会在单一租户硬件中运行。

有专用租期的预留实例

为确保您拥有足够的容量来启动专用实例，您可以购买专用预留实例。有关更多信息，请参阅 [预留实例 \(p. 161\)](#)。

如果您购买专用预留实例，也就意味着您同时购买容量并以较低的使用费在 VPC 内启动专用实例；小时费用的价格折扣仅在您启动具有专用租赁的实例的情况下才能使用。但是，如果您购买具有默认租期值的预留实例，则在启动租期为 `dedicated` 的实例时，将不会获得专用预留实例。

此外，您在购买之后，便无法更改预留实例的租期。

专用实例的 Auto Scaling

有关使用 Auto Scaling 启动专用实例的信息，请参阅 Auto Scaling 用户指南 中的 [Amazon Virtual Private Cloud 中的 Auto Scaling](#)。

专用竞价型实例

在创建竞价实例请求时，您可以通过指定租赁 `dedicated` 来运行专用竞价型实例。有关更多信息，请参阅 [指定竞价型实例租赁 \(p. 197\)](#)。

专用实例定价

专用实例定价不同于按需实例定价。有关更多信息，请参阅 [Amazon EC2 专用实例产品页面](#)。

使用专用实例

您可以创建一个实例租期设置为专用的 VPC，以确保在该 VPC 内启动的所有实例都是专用实例。或者，您可以在启动时指定实例的租期。

主题

- [创建有专用实例租期的 VPC \(p. 239\)](#)

- 在 VPC 内启动专用实例 (p. 239)
- 显示租期信息 (p. 239)
- 更改实例的租期 (p. 240)

创建有专用实例租期的 VPC

当您创建 VPC 时，您可以选择指定它的实例租期。您可以在 Amazon VPC 控制台中使用 VPC 向导或 Your VPCs 页面创建 VPC。

创建指定了专用实例租期的 VPC (VPC 向导)

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 从仪表板上，选择 Start VPC Wizard。
3. 选择 VPC 配置，然后选择 Select。
4. 在向导的下一页，从 Hardware tenancy 列表中选择 Dedicated。
5. 选择 Create VPC。

创建指定了专用实例租期的 VPC (创建 VPC 对话框)

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs，然后选择 Create VPC。
3. 对于 Tenancy，选择 Dedicated。指定 CIDR 块，然后选择 Yes, Create。

如果您在实例租期为 `dedicated` 的 VPC 内启动实例，则您的实例无论租期如何，都会自动成为专用实例。

在 VPC 内启动专用实例

您可以使用 Amazon EC2 启动实例向导来启动专用实例。

在使用默认租期的 VPC 中启动具有专用租期的实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页上，选择某个 AMI，然后选择 Select。
4. 在 Choose an Instance Type 页面上，选择实例类型并选择 Next: Configure Instance Details。

Note

确保您选择支持的实例类型作为专用实例。有关更多信息，请参阅 [Amazon EC2 专用实例](#)。

5. 在 Configure Instance Details (配置实例详细信息) 页上，选择 VPC 和子网。从 Tenancy 列表中选择 Dedicated - Run a dedicated instance，然后选择 Next: Add Storage。
6. 根据向导的提示继续。在 Review Instance Launch 页上核查您的选项后，选择 Launch 以选择密钥对并启动专用实例。

有关启动租期为 `host` 的实例的更多信息，请参阅[在专用主机上启动实例 \(p. 231\)](#)。

显示租期信息

显示 VPC 的租期信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 在 Tenancy (租区) 一栏中查看您的 VPC 实例的租区。

4. 如果 Tenancy 列未显示 , 请选择 Edit Table Columns (齿轮形状的图标)、Show/Hide Columns 对话框中的 Tenancy , 然后选择 Close。

显示实例的租期信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中 , 选择 Instances。
3. 在 Tenancy (租期) 一栏中查看您的实例的租期。
4. 如果 Tenancy (租期) 栏未能显示 , 您可以执行以下操作 :
 - 选择 Edit Table Columns (齿轮形状的图标)、Show/Hide Columns 对话框中的 Tenancy , 然后选择 Close。
 - 选择实例。详细信息页面中的 Description (说明) 选项卡中会显示关于实例的信息 , 包括它的租期。

更改实例的租期

根据您的实例类型和平台 , 您可以在已停止的专用实例启动之后将它的租期更改为 host。下次该实例启动时 , 它将在分配给您的账户的专用主机上启动。有关分配和使用专用主机的更多信息 , 以及可以在专用主机上使用的实例类型 , 请参阅[使用专用主机 \(p. 230\)](#)。同样 , 您也可以在启动一个已停止的专用主机实例后将它的租期更改为 dedicated。下次该实例启动时 , 它将会在我们控制的单租户硬件上启动。

更改实例的租期

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中 , 选择 Instances , 然后选择您的实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 在 Tenancy 列表中 , 选择是在专用硬件上还是在专用主机上运行您的实例。选择 Save。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。

创建 VPC 时设置租期选项

- [create-vpc](#) (AWS CLI)
- [New-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

说明对于在 VPC 中启动的实例支持的租期选项

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

为实例设置租期选项在启动过程中

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

说明实例的租期值

- [describe-instances](#) (AWS CLI)

- [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

说明预留实例的租期值

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (适用于 Windows PowerShell 的 AWS 工具)

说明预留实例产品的租期值

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#) (适用于 Windows PowerShell 的 AWS 工具)

修改实例的租期值

- [modify-instance-placement](#) (AWS CLI)
- [Edit-EC2InstancePlacement](#) (适用于 Windows PowerShell 的 AWS 工具)

实例生命周期

通过使用 Amazon EC2 从启动到终止期间对实例进行管理，可确保您的客户对其上托管的应用程序或站点尽可能获得最佳体验。

下图显示实例状态之间的转换。请注意，您无法停止和启动实例存储支持的实例。有关实例存储支持实例的更多信息，请参阅[根设备存储 \(p. 60\)](#)。

实例启动

当您启动实例时，实例进入 `pending` 状态。启动时指定的实例类型将决定您实例的主机硬件。我们使用您在启动时指定的 Amazon 系统映像 (AMI) 来启动实例。当实例准备就绪后，其进入 `running` 状态。您可以连接到正在运行的实例，然后像使用您面前的计算机一样来使用它。

只要您的实例转换为 `running` 状态，实例保持运行的每个小时或不足一小时都会计费；即使实例处于闲置状态并且您并未连接到该实例。

有关更多信息，请参阅[启动实例 \(p. 243\)](#)和[连接到您的 Linux 实例 \(p. 252\)](#)。

停止和启动实例 (仅限 Amazon EBS 支持的实例)

如果您的实例未能通过状态检查或未按预期运行应用程序，并且实例的根卷为 Amazon EBS 卷，则您可以先停止该实例再启动，以尝试解决该问题。

当您停止实例时，它会进入 `stopping` 状态，然后进入 `stopped` 状态。我们不对已停止的示例收取小时使用费或数据传输费，但会对所有 Amazon EBS 卷的存储收费。当实例处于 `stopped` 状态时，您可以修改实例的某些属性，包括实例类型。

当您启动实例时，它会进入 `pending` 状态，在大多数情况下，我们会将该实例移至新主机。(您的实例可能驻留在同一主机上，前提是此主机正常。)当您停止实例再启动时，将丢失先前主机的实例存储卷上的所有数据。

如果您的实例在 EC2-Classic 中运行，它会收到一个新的私有 IPv4 地址，这意味着与私有 IPv4 地址关联的弹性 IP 地址 (EIP) 不再与您的实例关联。如果您的实例在 EC2-VPC 中运行，它会保留其私有 IPv4 地址，这意味着与该私有 IPv4 地址或网络接口关联的 EIP 仍然与您的实例关联。如果您的实例具有 IPv6 地址，则它将保留其 IPv6 地址。

您每次将实例从 `stopped` 状态转换到 `running` 状态时，我们都按一个完整实例小时收费，即使这些转换在一小时内发生多次也一样。

有关更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

实例重启

您可以使用 Amazon EC2 控制台、命令行工具和 Amazon EC2 API 来重新启动实例。我们建议您使用 Amazon EC2 来重启实例，而非在实例中运行操作系统重启命令。

重启实例等同于重启操作系统；实例位于同一主机上并保留其公有 DNS 名称、私有 IP 地址以及其实例存储卷上的所有数据。完成重启通常需要花费几分钟的时间，该时间具体取决于实例配置。

重启实例不会启动新的实例计费小时。

有关更多信息，请参阅 [重启您的实例 \(p. 265\)](#)。

实例停用

实例计划在 AWS 检测到托管实例的底层硬件发生无法弥补的故障时停用。当实例到达其计划的停用日期时，AWS 会将其停止或终止。如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

有关更多信息，请参阅 [实例停用 \(p. 266\)](#)。

实例终止

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，就不再产生与该实例相关的费用。

请注意，如果您启用终止保护，则无法使用控制台、CLI 或 API 来终止实例。

在您终止实例之后，短时间内仍可在控制台中看见该实例，然后该条目将自动被删除。您还可以使用 CLI 和 API 来描述已终止的实例。资源（例如标签）会逐步与终止的实例取消关联，因此过一小段时间后，它们可能在终止的实例上不再可见。您无法连接至或恢复已终止的实例。

每个由 Amazon EBS 支持的实例都支持 `InstanceInitiatedShutdownBehavior` 属性，该属性决定当从实例内部启动关闭命令时（例如，在 Linux 中使用 `shutdown` 命令）实例是停止还是终止。默认行为是停止实例。您可以在实例运行或停止时修改此属性的设置。

每个 Amazon EBS 卷都支持 `DeleteOnTermination` 属性，该属性控制当您终止卷所连接的实例时是删除还是保留该卷。默认为删除根设备卷并保留所有其他 EBS 卷。

有关更多信息，请参阅 [终止您的实例 \(p. 267\)](#)。

重启、停止与终止之间的区别

下表总结重启、停止与终止实例之间的主要区别。

| 性能 | 重启 | 停止/启动（仅限 Amazon EBS 支持的实例） | 终止 |
|---------------|--------------|---------------------------------|----|
| 主机 | 实例保持在同一主机上运行 | 实例在新主机上运行 | 无 |
| 私有和公有 IPv4 地址 | 这些地址保持不变 | EC2-Classic：实例获得新的私有和公有 IPv4 地址 | 无 |

| 性能 | 重启 | 停止/启动 (仅限 Amazon EBS 支持的实例) | 终止 |
|----------------------|----------------|--|--|
| | | EC2-VPC : 实例保留其私有 IPv4 地址。除非实例具有在停止/启动过程中不会更改的弹性 IP 地址 (EIP) , 否则实例会获得新的公有 IPv4 地址。 | |
| 弹性 IP 地址 (IPv4)。 | 弹性 IP 仍然与实例相关联 | EC2-Classic : 弹性 IP 不再与实例相关联 EC2-VPC : 弹性 IP 仍然与实例相关联 | 弹性 IP 不再与实例相关联 |
| IPv6 地址 (仅限 EC2-VPC) | 地址保持不变 | 实例保留其 IPv6 地址 | 无 |
| 实例存储卷 | 数据保留 | 数据将擦除 | 数据将擦除 |
| 根设备卷 | 卷将保留 | 卷将保留 | 默认情况下将删除卷 |
| 计费 | 实例计费小时不更改。 | 实例的状态一旦变为 <code>stopping</code> , 就不再产生与该实例相关的费用。每次实例从 <code>stopped</code> 转换为 <code>running</code> 时 , 我们都会启动新的实例计费小时。 | 实例的状态一旦变为 <code>shutting-down</code> , 就不再产生与该实例相关的费用。 |

请注意 , 操作系统的 shutdown 命令始终会终止实例存储支持实例。您可以控制操作系统 shutdown 命令是停止还是终止 Amazon EBS 支持的实例。有关更多信息 , 请参阅[更改实例的启动关闭操作 \(p. 269\)](#)。

启动实例

实例是 AWS 云中的虚拟服务器。您可以从 Amazon 系统映像 (AMI) 中启动实例。AMI 为实例提供操作系统、应用程序服务器和应用程序。

注册 AWS 后 , 您可以通过[AWS 免费套餐](#)开始免费使用 Amazon EC2。您可以利用免费套餐来免费启动和使用微型实例 , 免费时间为 12 个月。如果您启动不在免费套餐范围内的实例 , 则需要为该实例支付标准 Amazon EC2 使用费。有关更多信息 , 请参阅[Amazon EC2 定价](#)。

您可以使用以下方法启动实例。

| 方法 | 文档 |
|--|--|
| [Amazon EC2 控制台] 使用所选 AMI | 启动实例 (p. 244) |
| [Amazon EC2 控制台] 使用现有实例作为模板 | 使用现有实例作为模板来启动实例 (p. 248) |
| [Amazon EC2 控制台] 使用您创建的 Amazon EBS 快照 | 从备份启动 Linux 实例 (p. 249) |
| [Amazon EC2 控制台] 使用从 AWS Marketplace 购买的 AMI | 启动 AWS Marketplace 实例 (p. 250) |
| [AWS CLI] 使用所选 AMI | 通过 AWS CLI 使用 Amazon EC2 |

| 方法 | 文档 |
|--|---|
| [适用于 Windows PowerShell 的 AWS 工具] 使用所选 AMI | 适用于 Windows PowerShell 的 AWS 工具 中的 Amazon EC2 |

启动实例之后，您可以连接并使用该实例。开始时，实例的状态为 `pending`。当实例状态为 `running` 时，实例已经开始启动。可能要过一小段时间才能连接到实例。实例会获得一个公有 DNS 名称，可用于从 Internet 与该实例通信。实例还会获得一个私有 DNS 名称，相同 Amazon EC2 网络 (EC2-Classic 或 EC2-VPC) 内的其他实例可以用其与该实例通信。有关连接到实例的更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。

当您完成实例时，请确保终止该实例。有关更多信息，请参阅[终止您的实例 \(p. 267\)](#)。

启动实例

在启动实例之前，请确保您已进行了相应设置。有关更多信息，请参阅[Amazon EC2 的设置 \(p. 15\)](#)。

根据您创建账户的时间以及您使用的区域，您的 AWS 账户可能同时支持 EC2-Classic 和 EC2-VPC 平台。要查明您的账户支持的平台，请参阅[支持的平台 \(p. 435\)](#)。如果您的账户支持 EC2-Classic，则可以在任一平台中启动实例。如果您的账户仅支持 EC2-VPC，则只能在 VPC 中启动实例。

Important

当您启动不在 [AWS 免费套餐](#)范围内的实例时，即使该实例处于闲置状态，您也需为该实例运行的时间付费。

从 AMI 启动实例

启动实例时，您必须选择配置 (称为 Amazon 系统映像 (AMI))。AMI 包含创建新实例所需的信息。例如，AMI 可能包含用作 Web 服务器所需的软件：例如 Linux、Apache 和您的网站。

Tip

为确保更快地启动实例，请将大量请求分成较小的批次。例如，创建五个独立的请求批次，每个批次包含 100 个实例启动请求，而不要创建一个包含 500 个实例的启动请求。

启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在屏幕顶部的导航栏中，会显示当前区域。选择实例的区域。该选择很重要，这是因为有些 Amazon EC2 资源可以在区域间共享，另一些却不能。请选择能满足您的需求的区域。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 从 Amazon EC2 控制台控制面板中，选择 Launch Instance。
4. 在 Choose an Amazon Machine Image (AMI) (选择 Amazon 系统映像 (AMI)) 页上，选择某个 AMI，如下所示：
 - a. 在左侧窗格中选择要使用的 AMI 类型：

快速启动

一组精选的常用 AMI 可帮助您快速开始。要确保选择符合免费套餐条件的 AMI，请在左侧窗格中选择 Free tier only。(请注意，这些 AMI 标记为 Free tier eligible (符合条件的免费套餐)。)

我的 AMI

您拥有的私有 AMI，或与您共享的私有 AMI。

AWS Marketplace

一个在线商店，您可以从中购买在 AWS 上运行的软件（包括 AMI）。有关从 AWS Marketplace 启动实例的更多信息，请参阅[启动 AWS Marketplace 实例 \(p. 250\)](#)。

社区 AMI

AWS 社区成员提供给其他人使用的 AMI。要按操作系统筛选 AMI 列表，请在 Operating system 下选中相应复选框。还可以按架构和根设备类型进行筛选。

- b. 检查对每个 AMI 列出的 Root device type。请注意哪些 AMI 是您需要的类型，即 ebs(由 Amazon EBS 支持) 或 instance-store(实例存储支持)。有关更多信息，请参阅[根设备存储 \(p. 60\)](#)。
 - c. 检查对每个 AMI 列出的 Virtualization type(虚拟化类型)。注意哪些 AMI 类型是您需要的类型，即 hvm 或 paravirtual。例如，一些实例类型需要 HVM。有关详细信息，请参阅[Linux AMI 虚拟化类型 \(p. 62\)](#)。
 - d. 选择满足您的需求的 AMI，然后选择 Select。
5. 在 Choose an Instance Type(选择一个实例类型) 页面上，选择要启动的实例的硬件配置和大小。更大的实例类型拥有更多的 CPU 和内存。有关更多信息，请参阅[实例类型 \(p. 135\)](#)。

要保持符合免费套餐条件，请选择 t2.micro 实例类型。有关更多信息，请参阅[T2 实例 \(p. 139\)](#)。

默认情况下，向导显示当前一代实例类型，并根据您选择的 AMI 选择第一可用实例类型。要查看上一代实例类型，请从筛选列表中选择 All generations。

Note

如果您刚刚接触 AWS 并希望快速设置实例以进行测试，那么目前可以选择 Review and Launch 以接受默认配置设置，然后启动您的实例。否则，若要进一步配置实例，请选择 Next: Configure Instance Details。

6. 在 Configure Instance Details 页面上，根据需要更改以下设置（展开 Advanced Details 查看所有设置），然后选择 Next: Add Storage：
 - Number of instances(实例的数量)：输入要启动的实例的数量。

Note

为帮助确保保持正确数量的实例来处理应用程序，您可选择 Launch into Auto Scaling Group 以创建启动配置和 Auto Scaling 组。Auto Scaling 将根据您的规格来扩展组中的实例数。有关更多信息，请参阅[Auto Scaling 用户指南](#)。

- Purchasing option：选择 Request Spot instances 可启动竞价型实例。有关更多信息，请参阅[竞价型实例 \(p. 187\)](#)。
- 您的账户可能支持 EC2-Classic 和 EC2-VPC 平台，或者仅支持 EC2-VPC。要查明您的账户支持的平台，请参阅[支持的平台 \(p. 435\)](#)。如果您的账户仅支持 EC2-VPC，则可以在默认 VPC 或非默认 VPC 中启动实例。否则，您可以在 EC2-Classic 或非默认 VPC 中启动实例。

Note

某些实例类型必须在 VPC 中启动。如果您没有 VPC，可以让向导为您创建一个。

在 EC2-Classic 中启动：

- Network(网络)：选择 Launch into EC2-Classic(在 EC2-Classic 中启动)。
- Availability Zone(可用区)：选择您想使用的可用区。要使 AWS 为您选择可用区，请选择 No preference(无首选项)。

在 VPC 中启动：

- Network：选择 VPC，若要创建新 VPC，请选择 Create new VPC 转到 Amazon VPC 控制台。完成后，返回到向导并选择 Refresh 按钮，以便将您的 VPC 加载到列表中。
- Subnet(子网)：选择您要将实例启动到其中的子网。如果您的账户仅为 EC2-VPC，请选择 No preference(无首选项) 让 AWS 在任何可用区中选择默认子网。要创建新子网，请选择 Create new

subnet 转到 Amazon VPC 控制台。完成此操作后，返回到向导并选择 Refresh 按钮，以便将您的子网加载到列表中。

- 自动分配公有 IP：指定您的实例是否会收到公有 IPv4 地址。默认情况下，默认子网中的实例会收到公有 IPv4 地址，而非默认子网中的实例不会收到。可以选择 Enable (启用) 或 Disable (禁用) 以覆盖子网的默认设置。有关更多信息，请参阅 [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。
- 自动分配 IPv6 IP：指定您的实例是否会收到处于子网范围内的 IPv6 地址。选择启用或禁用可以覆盖子网的默认设置。该选项仅在您已将 IPv6 CIDR 块与您的 VPC 和子网关联的情况下可用。有关更多信息，请参阅 Amazon VPC 用户指南中的 [Your VPC and Subnets](#)。
- IAM role：选择一个 AWS Identity and Access Management (IAM) 角色来与实例关联。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 422\)](#)。
- Shutdown behavior (关闭行为)：选择关闭时实例应该停止还是终止。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 269\)](#)。
- Enable termination protection (启用终止保护)：选中此复选框可防止意外终止。有关更多信息，请参阅 [为实例启用终止保护 \(p. 268\)](#)。
- 监控：请选中此复选框，以使用 Amazon CloudWatch 来启动对您的实例的详细的监控。将收取额外费用。有关更多信息，请参阅 [使用 CloudWatch 监控您的实例 \(p. 320\)](#)。
- EBS-Optimized instance (EBS 优化实例)：Amazon EBS 优化实例使用优化的配置堆栈，为 Amazon EBS I/O 提供附加专用容量。如果实例类型支持此功能，请选中此复选框将其启用。将收取额外费用。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。
- Tenancy：如果您要将实例启动到 VPC，则可选择在独立的专用硬件 (Dedicated) 或专用主机 (Dedicated host) 上运行实例。可能收取额外费用。有关更多信息，请参阅 [专用实例 \(p. 237\)](#) 和 [专用主机 \(p. 227\)](#)。
- Network interfaces：如果您选择了特定的子网，则可为实例指定最多两个网络接口：
 - 对于 Network Interface，选择 New network interface 可让 AWS 创建新的实例，或选择现有且可用的网络接口。
 - 对于 Primary IP，请输入一个您的子网范围内的私有 IPv4 地址，或保留 Auto-assign，让 AWS 为您选择一个私有 IPv4 地址。
 - 对于 Secondary IP addresses，请选择 Add IP 以将多个私有 IPv4 地址分配给所选网络接口。
 - (仅限 IPv6) 对于 IPv6 IP，请选择 Add IP 并输入一个子网范围内 IPv6 地址，或保留 Auto-assign，让 AWS 为您选择一个。
 - 选择 Add Device 可添加次要网络接口。次要网络接口可以与 VPC 位于不同的子网中，但必须位于您的实例所在的可用区内。
有关更多信息，请参阅[弹性网络接口 \(p. 473\)](#)。如果指定多个网络接口，则您的实例无法收到公有 IPv4 地址。此外，如果您将某个现有的网络接口指定为 eth0 接口，则无法使用自动分配公有 IP 来覆盖子网的公有 IPv4 设置。有关更多信息，请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 458\)](#)。

- Kernel ID：(仅对半虚拟化 (PV) AMI 有效) 除非您想使用某个特定内核，否则选择 Use default。
- RAM disk ID：(仅对半虚拟化 (PV) AMI 有效) 除非您想使用某个特定 RAM 磁盘，否则选择 Use default。如果您选择了一个内核，则您可能需要选择带有可支持该内核的驱动程序的某个特定 RAM 磁盘。
- Placement group (置放群组)：置放群组是对您的群集实例加以组织的逻辑分组。选择现有置放群组或创建新群组。仅当您选择了支持置放群组的实例类型时，此选项才可用。有关更多信息，请参阅 [置放群组 \(p. 487\)](#)。
- User data：您可以指定用户数据在启动时配置实例或运行配置脚本。要附加文件，请选择 As file (以文件形式) 选项并浏览到要附加的文件。

7. 在 Add Storage (添加存储) 页面上，除 AMI 指定的卷之外 (例如根设备卷)，您还可以指定要附加到实例的卷。您可以更改以下选项，然后在完成时选择 Next: Add Tags：

- Type (类型)：选择实例存储或 Amazon EBS 卷以便与实例关联。列表中可用的卷类型取决于您选择的实例类型。有关更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#) 和 [Amazon EBS 卷 \(p. 517\)](#)。
- Device (设备)：从卷的可用设备名称列表中进行选择。

- Snapshot (快照)：输入要从其中还原卷的快照的名称或 ID。您还可以通过在 Snapshot (快照) 字段中键入文本来搜索公有快照。快照描述区分大小写。
- Size (大小)：对于 Amazon EBS 支持的卷，您可以指定存储大小。请注意，即使您选择了有资格享用免费套餐的 AMI 和实例，仍需保持总存储大小低于 30 GiB，以便保持在免费套餐限制之内。

Note

Linux AMI 需要将 GPT 分区表和 GRUB 2 用于 2 TiB (2048 GiB) 或更大的引导卷。现在的许多 Linux AMI 都使用 MBR 分区方案，此方案仅支持最高 2047 GiB 的引导卷。如果您的实例不通过 2 TiB 或更大的引导卷启动，您要使用的 AMI 会限制为 2047 GiB 引导卷大小。非引导卷对 Linux 实例没有这种限制。

Note

如果此时增加根卷（或从快照创建的任何其他卷）的大小，则需要扩展该卷上的文件系统以使用额外空间。有关在实例启动之后扩展文件系统的更多信息，请参阅[在 Linux 上修改 EBS 卷的大小、IOPS 或类型 \(p. 543\)](#)。

- Volume Type (卷类型)：对于 Amazon EBS 卷，请选择 通用型 SSD、预配置 IOPS SSD 或磁介质卷。有关更多信息，请参阅[Amazon EBS 卷类型 \(p. 519\)](#)。

Note

如果选择 磁介质 启动卷，则在您完成向导时，系统会提示您将 通用型 SSD 卷设为此实例和未来的控制台启动的默认启动卷。（此首选项保留在浏览器会话中，不会影响具有 预配置 IOPS SSD 启动卷的 AMI。）我们建议您将 通用型 SSD 卷设为默认卷，因为它们可提供更快的体验，是大多数工作负载的最佳卷类型。有关更多信息，请参阅[Amazon EBS 卷类型 \(p. 519\)](#)。

Note

2012 年以前创建的部分 AWS 账户可能可以访问 us-west-1 或 ap-northeast-1 中不支持 预配置 IOPS SSD (io1) 卷的可用区。如果您无法在其中一个区域中创建 io1 卷（或在其块存储设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

- IOPS：如果选择了预配置 IOPS SSD 卷类型，则可以输入卷支持的每秒 I/O 操作数。
 - Delete on Termination (终止时删除)：对于 Amazon EBS 卷，请选中此复选框以在实例终止时删除卷。有关更多信息，请参阅[在实例终止时保留 Amazon EBS 卷 \(p. 270\)](#)。
 - Encrypted (加密)：选中此复选框可加密新的 Amazon EBS 卷。从加密快照还原的 Amazon EBS 卷会自动加密。加密卷只能连接到[支持的实例类型 \(p. 569\)](#)。
8. 在 Add Tags 页面上，通过提供键和值组合来指定[标签 \(p. 626\)](#)。您可以标记实例、卷或两者。选择 Add another tag 向您的资源添加多个标签。完成时选择 Next: Configure Security Group。
 9. 在 Configure Security Group (配置安全组) 页面上，使用安全组为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。所有其他的流量将被忽略。（有关安全组的更多信息，请参阅[Linux 实例的 Amazon EC2 安全组 \(p. 354\)](#)。）按如下所示选择或创建安全组，然后选择 Review and Launch。

选择现有安全组：

1. 选择 Select an existing security group。会显示您的安全组。（如果您要在 EC2-Classic 中启动，则这些是用于 EC2-Classic 的安全组。如果您要在某个 VPC 中启动，则这些是用于该 VPC 的安全组。）
2. 从列表中选择安全组。
3. （可选）您无法编辑现有安全组的规则，但是可以通过选择 Copy to new 将它们复制到新组。随后您可以按下一过程所述添加规则。

1. 选择 Create a new security group。向导会自动定义 launch-wizard-x 安全组。
2. (可选) 您可以编辑安全组的名称和描述。
3. 向导会自动定义入站规则以允许您通过适用于 Linux 的 SSH (端口 22) 或适用于 Windows 的 RDP (端口 3389) 连接到实例。

Warning

此规则使所有 IP 地址 (0.0.0.0/0) 都可以通过指定端口访问您的实例。您可以在本次简短练习中使用此方法，但是在生产环境中使用时，其安全性有所欠缺。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

4. 您可以根据需要添加规则。例如，如果您的实例是 Web 服务器，则打开端口 80 (HTTP) 和 443 (HTTPS) 以允许 Internet 流量。

要添加规则，请选择 Add Rule，选择用于打开网络流量的协议，然后指定源。从 Source 列表中选择 My IP 可让向导添加您计算机的公有 IP 地址。但是，如果您在没有静态 IP 地址的情况下通过 ISP 或从防火墙后面进行连接，则您需要了解客户端计算机使用的 IP 地址范围。

10. 在 Review Instance Launch 页面上，检查您的实例的详细信息，然后选择相应的 Edit 链接进行任何必要更改。

如果准备就绪，请选择 Launch。

11. 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，您可以选择现有密钥对，也可以创建新的密钥对。例如，选择 Choose an existing key pair，然后选择您在进行设置时创建的密钥对。

要启动您的实例，请选中确认复选框，然后选择 Launch Instances。

Important

如果您选择 Proceed without key pair 选项，则将无法连接到此实例，除非您选择配置为允许用户以其他方式登录的 AMI。

12. (可选) 您可以为实例创建一个状态检查警报 (可能需要额外付费)。(如果您不确定，您可以随时在以后添加。)在确认屏幕上，选择 Create status check alarms 并按照指示操作。有关更多信息，请参阅 [创建和编辑状态检查警报 \(p. 316\)](#)。
13. 如果实例状态立即变为 terminated，而不是 running，您可以获取有关实例无法启动的相关原因的信息。有关更多信息，请参阅 [如果实例立即终止，怎么办？\(p. 642\)](#)。

使用现有实例作为模板来启动实例

Amazon EC2 控制台提供启动更多类似项向导选项，通过该选项可以将当前实例用作启动其他实例的模板。此选项自动使用所选实例中的特定配置详细信息来填充 Amazon EC2 启动向导。

Note

启动更多类似项向导选项不克隆所选实例；仅复制某些配置详细信息。要创建实例的副本，请先从它创建 AMI，然后从 AMI 启动更多实例。

以下配置详细信息会从所选实例复制到启动向导中：

- AMI ID
- 实例类型
- 可用区，或所选实例所在的 VPC 和子网
- 公有 IPv4 地址。如果所选实例当前具有公有 IPv4 地址，则无论所选实例的默认公有 IPv4 地址设置如何，新实例都会收到公有 IPv4 地址。有关公有 IPv4 地址的更多信息，请参阅[公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。
- 置放群组，如果适用

- 与实例关联的 IAM 角色 (如果适用)
- 关闭操作设置 (停止或中止)
- 终止保护设置 (true 或 false)
- CloudWatch 监控 (启用或禁用)
- Amazon EBS 优化的设置 (true 或 false)
- 租期设置 (如果在 VPC (共享或专用) 中启动)
- 内核 ID 和 RAM 磁盘 ID (如果适用)
- 用户数据，如果指定
- 与实例关联的标签 (如果适用)
- 与实例关联的安全组

以下配置详细信息不会从所选实例进行复制；而是由向导应用默认设置或行为：

- (仅限 VPC) 网络接口数量：默认为一个网络接口，即主网络接口 (eth0)。
- Storage (存储)：默认存储配置由 AMI 和实例类型确定。

将当前实例用作模板

1. 在“实例”页面上，选择要使用的实例。
2. 选择 Actions，然后选择 Launch More Like This。
3. 启动向导会在 Review Instance Launch (查看实例启动) 页面上打开。您可以查看实例的详细信息，然后通过单击相应的 Edit (编辑) 链接进行任何所需更改。

准备就绪时，请选择 Launch 以选择密钥对并启动实例。

从备份启动 Linux 实例

对于 Amazon EBS 支持的 Linux 实例，您可以通过创建快照备份实例的根设备卷。如果您有某个实例的根设备卷快照，则您可以终止该实例并在稍后从该快照启动一个新的实例。如果您没有从其中启动实例的原始 AMI，但是需要能够使用同一映像启动实例，这将会很有用。

Important

虽然您可以从快照中创建一个 Windows AMI，但您不能从该 AMI 中成功启动实例。

请注意，某些 Linux 分配 (如 Red Hat Enterprise Linux (RHEL) 和 SUSE Linux Enterprise Server (SLES)) 使用与 AMI 关联的账单产品代码来验证程序包更新的订阅状态。从 EBS 快照创建 AMI 不会保留此账单代码，并且从此类 AMI 启动的后续实例不能连接到程序包更新基础设施。要保留账单产品代码，请从实例而非快照中创建 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 或 [创建由实例存储支持的 Linux AMI \(p. 78\)](#)。

按照以下过程，使用控制台从实例的根卷创建 AMI。如果您愿意，可以改用下列命令之一：[register-image](#) (AWS CLI) 或 [Register-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)。可使用块储存设备映射指定快照。

使用控制台从根卷创建 AMI

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Snapshots。
3. 选择 Create Snapshot。
4. 对于 Volumes，开始键入根卷的名称或 ID，然后从选项列表中选择它。
5. 选择刚才创建的快照，然后依次选择 Actions 和 Create Image。

6. 在 Create Image from EBS Snapshot 对话框中，提供以下信息，然后选择 Create。如果要重新创建父实例，请选择与父实例相同的选项。
 - Architecture：对 32 位选择 i386，对 64 位选择 x86_64。
 - Root device name：输入相应的根卷名称。有关更多信息，请参阅 [Linux 实例上的设备命名 \(p. 608\)](#)。
 - Virtualization type：选择是从此 AMI 使用半虚拟化 (PV) 还是硬件虚拟机 (HVM) 虚拟化启动实例。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。
 - (仅限 PV 虚拟化类型) Kernel ID 和 RAM disk ID：从列表中选择 AKI 和 ARI。如果选择默认 AKI 或不选择 AKI，则每次使用此 AMI 启动实例时系统都会要求您指定 AKI。此外，如果默认 AKI 与实例不兼容，对您的实例进行的运行状况检查可能会失败。
 - (可选) Block Device Mappings：添加卷或扩展 AMI 根卷的默认大小。有关调整实例上的文件系统大小以扩展卷的更多信息，请参阅 [调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。
7. 在导航窗格中，选择 AMIs。
8. 选择您刚刚创建的 AMI，然后选择 Launch。按照向导启动您的实例。有关如何在向导的每个步骤进行配置的更多信息，请参阅 [启动实例 \(p. 244\)](#)。

启动 AWS Marketplace 实例

您可以订阅 AWS Marketplace 产品，可以使用 Amazon EC2 启动向导从产品的 AMI 启动实例。有关付费 AMI 的更多信息，请参阅 [付费 AMI \(p. 72\)](#)。要在启动之后取消订阅，必须先停止从订阅运行的所有实例。有关更多信息，请参阅 [管理 AWS Marketplace 订阅 \(p. 75\)](#)。

使用启动向导从 AWS Marketplace 启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从 Amazon EC2 控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择左侧的 AWS Marketplace 类别。通过浏览类别或使用搜索功能查找合适的 AMI。选择 Select 以选择产品。
4. 对话框中会显示所选产品的概览。您可以查看定价信息，以及供应商提供的任何其他信息。准备就绪后，选择 Continue。

Note

在使用 AMI 启动实例之前，您无需为使用产品付费。记下每种支持的实例类型的定价，向导的下一页会提示您选择实例类型。还可能对产品征收其他税款。

5. 在 Choose an Instance Type (选择一个实例类型) 页面上，选择要启动的实例的硬件配置和大小。完成后，选择 Next: Configure Instance Details。
6. 在向导的后续页面上，可以配置实例、添加存储和添加标签。有关可以配置的不同选项的更多信息，请参阅 [启动实例 \(p. 244\)](#)。选择 Next，直至到达 Configure Security Group 页面。

向导会根据产品的供应商规格来创建新的安全组。安全组中的规则可能允许通过 Linux 上的 SSH (端口 22) 或 Windows 上的 RDP (端口 3389) 进行所有 IPv4 地址 (0.0.0.0/0) 访问。我们建议您调整这些规则，以仅允许特定地址或地址范围通过这些端口访问您的实例。

准备就绪后，选择 Review and Launch。

7. 在 Review Instance Launch (查看实例启动) 页面上，检查要通过其启动实例的 AMI 的详细信息，以及向导中设置的其他配置详细信息。准备就绪后，选择 Launch 以选择或创建密钥对，然后启动实例。
8. 根据订阅的产品，实例可能需要几分钟或更多时间来启动。您需要先订阅产品，然后才可启动实例。如果存在与信用卡详细信息有关的任何问题，会提示您更新账户详细信息。启动确认页面显示时，选择 View Instances 转到“Instances”页面。

Note

只要实例在运行 (即使处于空闲状态)，就会收取订阅费用。如果实例停止，仍会收取存储费。

- 当实例处于正在运行状态时，可以连接到实例。为此，请在列表中选择实例并选择 Connect。按照对话框中的说明执行。有关连接到实例的更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。

Important

仔细查看供应商的使用说明，因为您可能需要使用特定用户名登录实例。有关访问订阅详细信息的更多信息，请参阅[管理 AWS Marketplace 订阅 \(p. 75\)](#)。

使用 API 和 CLI 启动 AWS Marketplace AMI 实例

要使用 API 或命令行工具从 AWS Marketplace 产品启动实例，请首先确保订阅了产品。然后您可使用以下方法通过该产品的 AMI ID 启动一个实例：

| 方法 | 文档 |
|---------------------------------|---|
| AWS CLI | 使用 run-instances 命令或参阅以下主题以了解更多信息： 启动实例 。 |
| 适用于 Windows PowerShell 的 AWS 工具 | 使用 New-EC2Instance 命令，或参阅以下主题了解更多信息： 使用 Windows PowerShell 启动 Amazon EC2 实例 |
| 查询 API | 使用 RunInstances 请求。 |

连接到您的 Linux 实例

了解如何连接到您启动的 Linux 实例，以及如何在您的本地计算机与实例之间传输文件。

如需连接到 Windows 实例，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[连接到您的 Windows 实例](#)。

| 您的计算机 | 主题 |
|---------|--|
| Linux | 使用 SSH 连接到 Linux 实例 (p. 252) |
| Windows | 使用 PuTTY 从 Windows 连接到 Linux 实例 (p. 256) |
| 全部 | 使用 MindTerm 连接到 Linux 实例 (p. 261) |

连接到您的实例后，可以尝试其中一个教程，例如[教程：在 Amazon Linux 上安装 LAMP Web 服务器 \(p. 26\)](#)或[教程：使用 Amazon Linux 托管 WordPress 博客 \(p. 35\)](#)。

使用 SSH 连接到 Linux 实例

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

Note

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查 - 您可以在 Instances (实例) 页上的 Status Checks (状态检查) 列中查看此信息。

以下说明介绍如何使用 SSH 客户端连接到您的实例。如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

先决条件

在连接到 Linux 实例之前，请先完成以下先决条件：

- 安装 SSH 客户端

默认情况下，您的 Linux 计算机最可能包括 SSH 客户端。您可以通过在命令行键入 ssh 来检查 SSH 客户端。如果您的计算机不能识别该命令，OpenSSH 项目提供了整套 SSH 工具免费使用的功能。有关更多信息，请参阅 <http://www.openssh.com>。

- 安装 AWS CLI 工具

(可选) 如果您使用的是来自第三方的公用 AMI，请使用命令行工具验证指纹。有关安装 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南 中的[开始设置](#)。

- 获得实例的 ID

您可以通过使用 Amazon EC2 控制台（位于 Instance ID (实例 ID) 列中）获得您的实例的 ID。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- 获得实例的公有 DNS 名称

您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选中 Public DNS (IPv4) 列；如果此列处于隐藏状态，请选择 Show/Hide 图标并选择 Public DNS (IPv4))。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- (仅限 IPv6) 获得实例的 IPv6 地址

如果您已将 IPv6 地址分配给您的实例，则可选择使用实例的 IPv6 地址而非公共 IPv4 地址或公共 IPv4 DNS 主机名来连接实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。可使用 Amazon

EC2 控制台 (选中 IPv6 IPs 字段) 获取实例的 IPv6 地址。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。有关 IPv6 的更多信息，请参阅[IPv6 地址 \(p. 455\)](#)。

- **查找私有密钥**

您需要使用您在启动实例时指定的密钥对的 .pem 文件的完全限定路径。

- **允许从您的 IP 地址到您的实例的入站 SSH 流量**

确保与您的实例关联的安全组允许来自您的 IP 地址的传入 SSH 流量。有关更多信息，请参阅[授权网络访问您的实例](#)。

Important

默认情况下，您的默认安全组不允许传入 SSH 流量。

连接到 Linux 实例

通过以下过程使用 SSH 客户端连接到您的 Linux 实例。如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

使用 SSH 连接到您的实例

1. (可选) 您可以在本地系统 (而不是实例) 上使用以下命令之一验证正在运行的实例上的 RSA 密钥指纹。如果您从第三方的公用 AMI 启动了实例，则可能需要这样做。找到 `SSH HOST KEY FINGERPRINTS` 部分，记下 RSA 指纹 (例如 `1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f`) 并将它与实例的指纹进行比较。
 - [get-console-output](#) (AWS CLI)

```
aws ec2 get-console-output --instance-id instance_id
```

Note

确保实例处于 `running` 状态，而不是 `pending` 状态。`SSH HOST KEY FINGERPRINTS` 部分仅在实例首次启动之后可用。

2. 在命令行 shell 中，将目录更改为您在启动实例时创建的私有密钥文件的位置。
3. 使用 `chmod` 命令确保您的私有密钥文件不是公开可见的。例如，如果您的私有密钥文件的名称是 `my-key-pair.pem`，请使用以下命令：

```
chmod 400 /path/my-key-pair.pem
```

4. 使用 `ssh` 命令连接到实例。您可以指定私有密钥 (.pem) 文件和 `user_name@public_dns_name`。对于 Amazon Linux，用户名为 `ec2-user`。对于 RHEL，用户名是 `ec2-user` 或 `root`。对于 Ubuntu，用户名是 `ubuntu` 或 `root`。对于 CentOS，用户名是 `centos`。对于 Fedora，用户名是 `ec2-user`。对于 SUSE，用户名是 `ec2-user` 或 `root`。另外，如果 `ec2-user` 和 `root` 无法使用，请与您的 AMI 供应商核实。

```
ssh -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com
```

您会看到如下响应。

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'  
can't be established.  
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
```

Are you sure you want to continue connecting (yes/no)?

5. (仅限 IPv6) 或者，您可以使用 IPv6 地址连接到实例。请在 ssh 命令中指定私有密钥 (.pem) 文件路径的和适当的用户名。对于 Amazon Linux，用户名为 ec2-user。对于 RHEL，用户名是 ec2-user 或 root。对于 Ubuntu，用户名是 ubuntu 或 root。对于 CentOS，用户名是 centos。对于 Fedora，用户名是 ec2-user。对于 SUSE，用户名是 ec2-user 或 root。另外，如果 ec2-user 和 root 无法使用，请与您的 AMI 供应商核实。

```
ssh -i /path/my-key-pair.pem ec2-user@2001:db8:1234:1a00:9691:9503:25ad:1761
```

6. (可选) 验证安全警报中的指纹是否与在步骤 1 中获取的指纹匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。
7. 输入 yes。

您会看到如下响应。

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)  
to the list of known hosts.
```

使用 SCP 将文件从 Linux 传输到 Linux 实例

在您的本地计算机与 Linux 实例之间传输文件的一种方法是使用安全复制 (SCP)。本节介绍了如何使用 SCP 传输文件。这个程序和使用 SSH 连接到实例的程序非常相似。

先决条件

- 安装 SCP 客户端

默认情况下，大多数 Linux、Unix 和 Apple 计算机都包含 SCP 客户端。如果您的计算机不含 SSH 客户端，OpenSSH 项目提供了整套 SSH 工具免费使用的功能，包括 SCP 客户端。更多信息，请参阅 <http://www.openssh.org>。

- 获得实例的 ID

您可以通过使用 Amazon EC2 控制台（位于 Instance ID (实例 ID) 列中）获得您的实例的 ID。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- 获得实例的公有 DNS 名称

您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选中 Public DNS (IPv4) 列；如果此列处于隐藏状态，请选择 Show/Hide 图标并选择 Public DNS (IPv4))。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- (仅限 IPv6) 获得实例的 IPv6 地址

如果您已将 IPv6 地址分配给您的实例，则可选择使用实例的 IPv6 地址而非公共 IPv4 地址或公共 IPv4 DNS 主机名来连接实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。可使用 Amazon EC2 控制台（选中 IPv6 IPs 字段）获取实例的 IPv6 地址。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。有关 IPv6 的更多信息，请参阅[IPv6 地址 \(p. 455\)](#)。

- 查找私有密钥

您需要使用您在启动实例时指定的密钥对的 .pem 文件的完全限定路径。

- 允许从您的 IP 地址到您的实例的入站 SSH 流量

确保与您的实例关联的安全组允许来自您的 IP 地址的传入 SSH 流量。有关更多信息，请参阅[授权网络访问您的实例](#)。

Important

默认情况下，您的默认安全组不允许传入 SSH 流量。

以下步骤将引导您使用 SCP 来传输文件。如果您已经使用 SSH 连接到实例，且已确认实例指纹，您可以从包含 SCP 命令的步骤（步骤 4）开始。

使用 SCP 来传输文件

1. (可选) 您可以在本地系统（而不是实例）上使用以下命令之一验证实例上的 RSA 密钥指纹。如果您从第三方的公用 AMI 启动了实例，则可能需要这样做。找到 `SSH HOST KEY FINGERPRINTS` 部分，记下 RSA 指纹（例如 `1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f`）并将它与实例的指纹进行比较。

- `get-console-output` (AWS CLI)

```
aws ec2 get-console-output --instance-id instance_id
```

Note

`SSH HOST KEY FINGERPRINTS` 部分仅在实例首次启动之后可用。

2. 在命令 shell 中，将目录更改为您启动实例时所指定的私有密钥文件的位置。
3. 使用 `chmod` 命令确保您的私有密钥文件不是公开可见的。例如，如果您的私有密钥文件的名称是 `my-key-pair.pem`，请使用以下命令：

```
chmod 400 /path/my-key-pair.pem
```

4. 使用实例的公有 DNS 名称将文件传输到您的实例。举例来说，如果私有密钥文件的名称是 `my-key-pair`、要传输的文件是 `SampleFile.txt`、实例的公有 DNS 名称是 `ec2-198-51-100-1.compute-1.amazonaws.com`，则可以使用以下命令将文件复制到 `ec2-user` 主目录。

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-
user@ec2-198-51-100-1.compute-1.amazonaws.com:~
```

Tip

对于 Amazon Linux，用户名为 `ec2-user`。对于 RHEL，用户名是 `ec2-user` 或 `root`。对于 Ubuntu，用户名是 `ubuntu` 或 `root`。对于 CentOS，用户名是 `centos`。对于 Fedora，用户名是 `ec2-user`。对于 SUSE，用户名是 `ec2-user` 或 `root`。另外，如果 `ec2-user` 和 `root` 无法使用，请与您的 AMI 供应商核实。

您会看到如下响应。

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

5. (仅限 IPv6) 或者，您可以使用实例的 IPv6 地址传输文件。IPv6 地址必须用方括号 (`[]`) 括起，方括号必须转义 (`\[]`)。

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-user@
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~
```

6. (可选) 验证安全警报中的指纹是否与在步骤 1 中获取的指纹匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。

7. 输入 yes。

您会看到如下响应。

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
Sending file modes: C0644 20 SampleFile.txt
Sink: C0644 20 SampleFile.txt
SampleFile.txt                                         100%    20      0.0KB/s   00:00
```

Note

如果您收到一条“bash: scp: command not found”错误，则必须先在您的 Linux 实例上安装 scp。对于某些操作系统，此命令会位于 `openssh-clients` 程序包中。对于 Amazon Linux 变体（如经 Amazon ECS 优化的 AMI），使用以下命令安装 scp。

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

8. 若要反方向传输文件（从 Amazon EC2 实例中传输到本地计算机），则只需要简单地颠倒主机参数的顺序。例如，要将 `SampleFile.txt` 文件从您的 EC2 实例传回到您的本地计算机上的主目录，并且另存为 `SampleFile2.txt`，则可在您的本地计算机上使用以下命令。

```
scp -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/SampleFile2.txt
```

- 9.（仅限 IPv6）或者，您可以使用实例的 IPv6 地址反方向传输文件。

```
scp -i /path/my-key-pair.pem ec2-user@[2001:db8:1234:1a00:9691:9503:25ad:1761]:~/SampleFile.txt ~/SampleFile2.txt
```

使用 PuTTY 从 Windows 连接到 Linux 实例

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

Note

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查 - 您可以在 Instances (实例) 页上的 Status Checks (状态检查) 列中查看此信息。

以下说明介绍如何使用 PuTTY（适用于 Windows 的免费 SSH 客户端）连接到您的实例。如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

先决条件

使用 PuTTY 连接到您的 Linux 实例之前，请先完成以下先决条件：

- 安装 PuTTY

从 [PuTTY 下载页面](#)下载并安装 PuTTY。如果您安装的是旧版本的 PuTTY，建议您下载最新版本。确保安装整个套件。

- 获得实例的 ID

您可以通过使用 Amazon EC2 控制台（位于 Instance ID (实例 ID) 列中）获得您的实例的 ID。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- 获得实例的公有 DNS 名称

您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选中 Public DNS (IPv4) 列；如果此列处于隐藏状态，请选择 Show/Hide 图标并选择 Public DNS (IPv4))。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- (仅限 IPv6) 获取实例的 IPv6 地址

如果您已将 IPv6 地址分配给您的实例，则可选择使用实例的 IPv6 地址而非公共 IPv4 地址或公共 IPv4 DNS 主机名来连接实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。可使用 Amazon EC2 控制台 (选中 IPv6 IPs 字段) 获取实例的 IPv6 地址。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。有关 IPv6 的更多信息，请参阅[IPv6 地址 \(p. 455\)](#)。

- 查找私有密钥

您需要使用您在启动实例时指定的密钥对的 .pem 文件的完全限定路径。

- 允许从您的 IP 地址到您的实例的入站 SSH 流量

确保与您的实例关联的安全组允许来自您的 IP 地址的传入 SSH 流量。有关更多信息，请参阅[授权网络访问您的实例](#)。

Important

默认情况下，您的默认安全组不允许传入 SSH 流量。

使用 PuTTYgen 转换您的私有密钥

PuTTY 本身不支持 Amazon EC2 生成的私有密钥格式 (.pem)。PuTTY 有一个名为 PuTTYgen 的工具，可将密钥转换成所需的 PuTTY 格式 (.ppk)。您必须将私有密钥转换为此格式 (.ppk)，然后才能尝试使用 PuTTY 连接到您的实例。

转换您的私有密钥

1. 启动 PuTTYgen (例如，在开始菜单中，选择 All Programs > PuTTY > PuTTYgen)。
2. 在 Type of key to generate 下，选择 RSA。

Note

如果您使用的是旧版本的 PuTTYgen，请选择 SSH-2 RSA。

3. 选择 Load。在默认情况下，PuTTYgen 仅显示扩展名为 .ppk 的文件。要找到您的 .pem 文件，请选择显示所有类型的文件的选项。
4. 选择您在启动实例时指定的密钥对的 .pem 文件，然后选择 打开。选择 OK 关闭确认对话框。
5. 选择 Save private key，以 PuTTY 可以使用的格式保存密钥。PuTTYgen 显示一条关于在没有口令的情况下保存密钥的警告。选择是。

Note

私有密钥的口令是一层额外保护，因此，即使您的私有密钥被泄露，在没有口令的情况下，该密钥仍不可用。使用口令的缺点是让自动化变得更难，因为登录到实例或复制文件到实例需要进行人为干预。

6. 为该密钥指定与密钥对相同的名称 (如，my-key-pair)。PuTTY 自动添加 .ppk 文件扩展名。

您的私有密钥格式现在是正确的 PuTTY 使用格式了。您现在可以使用 PuTTY 的 SSH 客户端连接到实例。

启动 PuTTY 会话

通过以下过程使用 PuTTY 连接到您的 Linux 实例。您需要使用为私有密钥创建的 .ppk 文件。如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

启动 PuTTY 会话

1. (可选) 您可以在本地系统 (而不是实例) 上使用以下命令之一验证实例上的 RSA 密钥指纹。如果您从第三方的公用 AMI 启动了实例，则可能需要这样做。找到 SSH HOST KEY FINGERPRINTS 部分，记下 RSA 指纹 (例如 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f) 并将它与实例的指纹进行比较。

- [get-console-output \(AWS CLI\)](#)

```
aws ec2 get-console-output --instance-id instance_id
```

以下代码段提供了您应查找的内容的示例：

```
\r\nec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----\r\nec2: ...  
\r\nec2: 2048 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f  
      root@ip-192-0-2-0 (RSA)  
...  
\r\nec2: -----END SSH HOST KEY FINGERPRINTS-----
```

Note

SSH HOST KEY FINGERPRINTS 部分仅在实例首次启动之后可用。

2. 启动 PuTTY (在开始菜单中，选择 All Programs > PuTTY > PuTTY)。
3. 在“Category (类别)”窗格中，选择 Session (会话) 并填写以下字段：
 - a. 在 Host Name (主机名) 框中，输入 *user_name@public_dns_name*。确保为您的 AMI 指定相应的用户名。例如：
 - 对于 Amazon Linux AMI，用户名为 `ec2-user`。
 - 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
 - 对于 Ubuntu AMI，用户名是 `ubuntu` 或 `root`。
 - 对于 Centos AMI，用户名是 `centos`。
 - 对于 Fedora AMI，用户名是 `ec2-user`。
 - 对于 SUSE，用户名是 `ec2-user` 或 `root`。
 - 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。
 - b. (仅限 IPv6) 要使用实例的 IPv6 地址连接，请输入 *user_name@ipv6_address*。确保为您的 AMI 指定相应的用户名。例如：
 - 对于 Amazon Linux AMI，用户名为 `ec2-user`。
 - 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
 - 对于 Ubuntu AMI，用户名是 `ubuntu` 或 `root`。
 - 对于 Centos AMI，用户名是 `centos`。
 - 对于 Fedora AMI，用户名是 `ec2-user`。
 - 对于 SUSE，用户名是 `ec2-user` 或 `root`。
 - 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。
 - c. 在 Connection type (连接类型) 下，选择 SSH。
 - d. 确保 Port (端口) 为 22。

4. 在 Category (类别) 窗格中，展开 Connection (连接)，再展开 SSH，然后选择 Auth (身份验证)。完成以下操作：
 - a. 选择 Browse。
 - b. 选择您为密钥对生成的 .ppk 文件，然后选择打开。
 - c. (可选) 如果打算稍后重新启动此会话，则可以保存此会话信息以便日后使用。在类别树中选择会话，在 Saved Sessions 中输入会话名称，然后选择保存。
 - d. 选择打开以便开始 PuTTY 会话。
5. 如果这是您第一次连接到此实例，PuTTY 会显示安全警告对话框，询问您是否信任您要连接到的主机。
6. (可选) 验证安全警报对话框中的指纹是否与之前在步骤 1 中获取的指纹匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。
7. 选择是。此时会打开一个窗口并且您连接到了您的实例。

Note

如果您在将私有密钥转换成 PuTTY 格式时指定了口令，当您登录到实例时，您必须提供该口令。

如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

使用 PuTTY 安全复制客户端将文件传输到您的 Linux 实例

PuTTY 安全复制客户端 (PSCP) 是一个命令行工具，您可以用它在 Windows 计算机与 Linux 实例之间传输文件。如果您更喜欢图形用户界面 (GUI)，您可以使用一种叫作“WinSCP”的开源 GUI 工具。有关更多信息，请参阅[使用 WinSCP 将文件传输到您的 Linux 实例 \(p. 259\)](#)。

要使用 PSCP，您需要使用在[使用 PuTTYgen 转换您的私有密钥 \(p. 257\)](#)中生成的私有密钥。您还需要使用 Linux 实例的公有 DNS 地址。

以下示例将文件 Sample_file.txt 从 Windows 计算机上的 C:\ 驱动器传输到 Linux 实例上的 /usr/local 目录：

```
C:\> pscp -i C:\Keys\my-key-pair.ppk C:\Sample_file.txt user_name@public_dns:/usr/local/  
Sample_file.txt
```

(仅限 IPv6) 以下示例使用实例的 IPv6 地址传输文件 Sample_file.txt。IPv6 地址必须以方括号 ([]]) 括起。

```
C:\> pscp -i C:\Keys\my-key-pair.ppk C:\Sample_file.txt user_name@[ipv6-address]:/usr/  
local/Sample_file.txt
```

使用 WinSCP 将文件传输到您的 Linux 实例

WinSCP 是适用于 Windows 的基于 GUI 的文件管理器，您可以通过它来使用 SFTP、SCP、FTP 和 FTPS 协议将文件上传并传输到远程计算机。通过 WinSCP，您可以将 Windows 计算机中的文件拖放到 Linux 实例或同步这两个系统之间的所有目录结构。

要使用 WinSCP，您需要使用在[使用 PuTTYgen 转换您的私有密钥 \(p. 257\)](#)中生成的私有密钥。您还需要使用 Linux 实例的公有 DNS 地址。

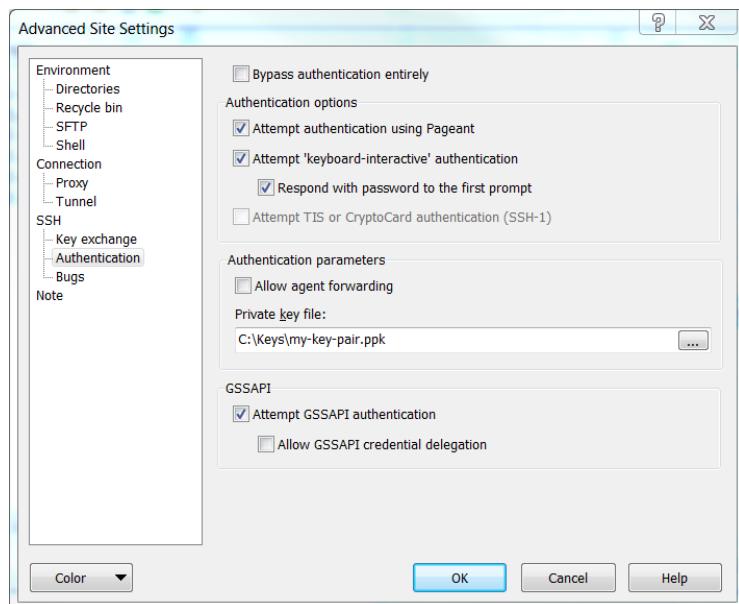
1. 从 <http://winscp.net/eng/download.php> 上下载并安装 WinSCP。对于大多数用户而言，采用默认安装选项就可以了。
2. 启动 WinSCP。
3. 在 WinSCP 登录屏幕中，对于 Host name，请输入实例的公有 DNS 主机名称或公有 IPv4 地址。

Note

(仅限 IPv6) 要使用实例的 IPv6 地址登录，请输入实例的 IPv6 地址。

4. 对于 User name (用户名)，请输入默认的 AMI 用户名。对于 Amazon Linux AMI，用户名是 `ec2-user`。对于 Red Hat AMI，用户名是 `root`，而对于 Ubuntu AMI，用户名则是 `ubuntu`。
5. 为您的实例指定私有密钥。对于 Private key，请输入私有密钥的路径，或选择“...”按钮以浏览文件。对于更新版本的 WinSCP，您需要选择 Advanced 以打开高级站点设置，然后在 SSH 下选择 Authentication 以查找 Private key file 设置。

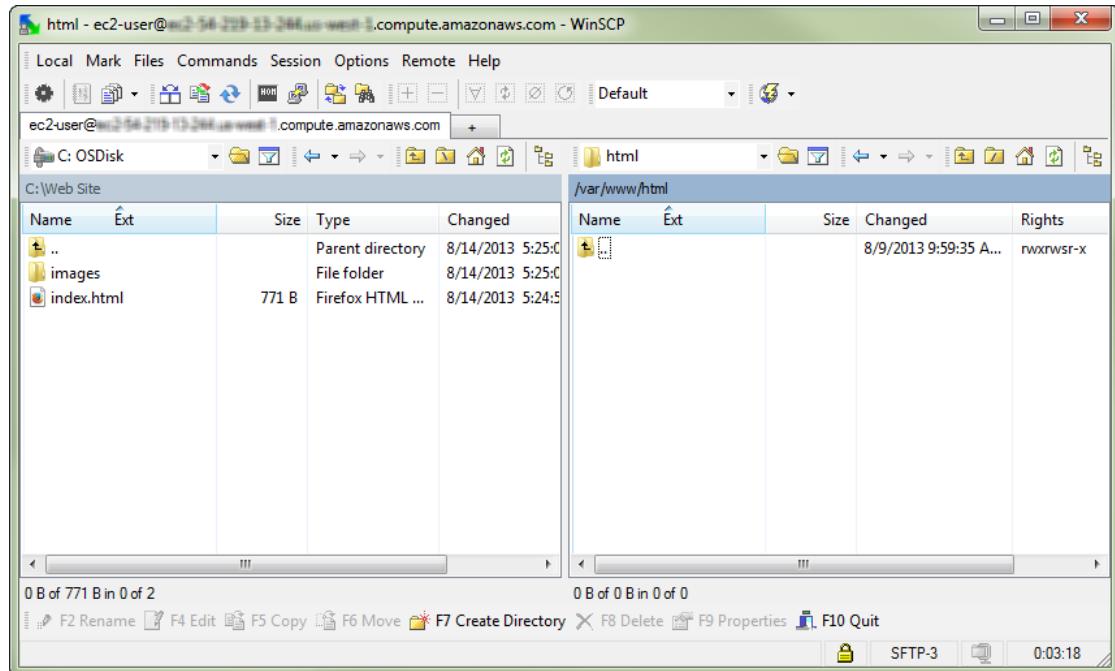
以下是 WinSCP 版本 5.9.4 中的屏幕截图：



Note

WinSCP 需要 PuTTY 私有密钥文件 (.ppk)。您可以使用 PuTTYgen 将 .pem 安全密钥文件转换成 .ppk 格式。有关更多信息，请参阅 [使用 PuTTYgen 转换您的私有密钥 \(p. 257\)](#)。

6. (可选) 在左侧面板中，选择 Directories，然后对于 Remote directory，请输入要将文件添加到其中的目录路径。对于更新版本的 WinSCP，您需要选择 Advanced 以打开高级站点设置，然后在 Environment 下选择 Directories 以查找 Remote directory 设置。
7. 选择 Login 进行连接，然后选择 Yes，将主机指纹添加到主机缓存。



8. 建立连接后，在连接窗口中，您的 Linux 实例显示在右侧，本地计算机显示在左侧。您可以直接将文件从本地计算机拖放到远程文件系统。有关 WinSCP 的更多信息，请参阅 <http://winscp.net/eng/docs/start> 中的项目文档。

Note

如果您收到一条“Cannot execute SCP to start transfer”错误，则必须先在您的 Linux 实例上安装 scp。对于某些操作系统，此命令会位于 `openssh-clients` 程序包中。对于 Amazon Linux 变体 (如经 Amazon ECS 优化的 AMI)，使用以下命令安装 scp。

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

使用 MindTerm 连接到 Linux 实例

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

Note

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查 - 您可以在 Instances (实例) 页上的 Status Checks (状态检查) 列中查看此信息。

以下说明介绍如何使用 MindTerm 通过 Amazon EC2 控制台连接到您的实例。如果您在尝试连接到您的实例时收到错误消息，请参阅[排查实例的连接问题](#)。

Important

Chrome 浏览器不支持 NPAPI 插件，因此无法运行 MindTerm 客户端。有关更多信息，请参阅 [Chromium NPAPI 弃用文章](#)。您可以使用 Firefox、Safari，或者 Internet Explorer 9 或更高版本。

先决条件

- 安装 Java

您的 Linux 计算机很可能已经包含有 Java。如果未包含，请参阅[如何在 Web 浏览器中启用 Java？](#)在 Windows 或 Mac 客户端上，您必须使用管理员证书运行浏览器。对于 Linux 客户端，如果您不是作为 root 用户登录，则可能还需执行其他步骤。

- 在 浏览器中启用 Java

有关说明，请参阅 https://java.com/en/download/help/enable_browser.xml。

- 查找私有密钥

您需要使用您在启动实例时指定的密钥对的 .pem 文件的完全限定路径。

- 允许从您的 IP 地址到您的实例的入站 SSH 流量

确保与您的实例关联的安全组允许来自您的 IP 地址的传入 SSH 流量。有关更多信息，请参阅[授权网络访问您的实例](#)。

Important

默认情况下，您的默认安全组不允许传入 SSH 流量。

启动 MindTerm

使用含有 MindTerm 的 Web 浏览器连接到您的实例

1. 在 Amazon EC2 控制台的导航窗格中，请选择实例。
2. 选择该实例，然后选择 Connect。
3. 选择 A Java SSH client directly from my browser (Java required)。
4. Amazon EC2 会自动检测实例的公有 DNS 名称，并为您填写公有 DNS。它还会检测您在启动实例时指定的密钥对名称。完成以下步骤，然后选择 Launch SSH Client。
 - a. 在 User name (用户名) 中，输入用户名以登录您的实例。

Tip

对于 Amazon Linux，用户名为 ec2-user。对于 RHEL，用户名是 ec2-user 或 root。对于 Ubuntu，用户名是 ubuntu 或 root。对于 Centos，用户名是 centos。对于 Fedora，用户名是 ec2-user。对于 SUSE，用户名是 ec2-user 或 root。另外，如果 ec2-user 和 root 无法使用，请与您的 AMI 供应商核实。

- b. 在 Private key path 中，输入私有密钥 (.pem) 文件的完全限定路径，包括密钥对名称；例如：

C:\KeyPairs\my-key-pair.pem

- c. (可选) 选择 Store in browser cache 以将私有密钥的位置存储在您的浏览器缓存中。这使得 Amazon EC2 可在后续的浏览器会话中检测私有密钥的位置，直到您清除浏览器缓存为止。

5. 如有必要，请选择 Yes 以信任证书，然后选择 Run 以运行 MindTerm 客户端。
6. 如果这是您第一次运行 MindTerm，则会出现一系列对话框，要求您接受许可协议、确认主目录的设置以及确认已知主机目录的设置。确认这些设置。
7. 一个对话框会提示您向已知主机集添加主机。如果您不想在本地计算机上存储主机密钥信息，请选择 No。
8. 此时会打开一个窗口并且您连接到了您的实例。

Note

如果您在上一步中选择了否，则会看到以下消息：

Verification of server key disabled in this session.

停止和启动您的实例

您可以停止和重启将 Amazon EBS 卷作为其根设备的实例。实例会保留其实例 ID，但是可以按照“概述”部分所述的方式进行修改。

当您终止一个实例时，我们会将其关闭。我们不对已停止的示例收取小时使用费或数据传输费，但我们会对所有 Amazon EBS 卷的存储收费。您每次启动一个已停止的实例，我们都计为一个实例小时，即使这些转换在一小时内发生多次也是如此。

当实例停止时，您可以像对待所有其他卷一样修改根卷（例如，修复文件系统问题或更新软件）。您只需从停止的实例断开卷，将其连接到运行中的实例并进行修改，然后将其断开，再次连接到该已停止实例即可。请确保您已使用设备名称被指定为实例块储存设备映射中的根设备对其进行重新连接。

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，我们就会停止收取与该实例相关的费用。有关更多信息，请参阅 [终止您的实例 \(p. 267\)](#)。

内容

- [概述 \(p. 263\)](#)
- [停止和启动您的实例 \(p. 264\)](#)
- [修改已停止的实例 \(p. 265\)](#)
- [故障排除 \(p. 265\)](#)

概述

您只能停止由 Amazon EBS 支持的实例。要验证您的实例的根设备类型，请描述实例并检查其根卷的设备类型是 `ebs`（由 Amazon EBS 支持的实例）还是 `instance store`（由实例存储支持的实例）。有关更多信息，请参阅 [确定 AMI 的根设备类型 \(p. 60\)](#)。

当您停止运行实例时，将出现以下情况：

- 实例正常关闭并停止运行；其状态变为 `stopping`，然后变为 `stopped`。
- 所有 Amazon EBS 卷保持连接至实例，而且其数据将保留下。
- 存储在主机 RAM 或主机实例存储卷中的所有数据都不复存在。
- 大多数情况下，实例会在启动时迁移到新的底层主机。
- EC2-Classic：当您停止实例时，我们会释放该实例的公有和私有 IPv4 地址，并在您重启实例时为其分配新的 IPv4 地址。

EC2-VPC：实例会在停止和重启时保留其私有 IPv4 地址以及任何 IPv6 地址。我们会释放公有 IPv4 地址并在您重启实例时为其分配新的 IPv4 地址。

- EC2-Classic：对于与该实例关联的所有弹性 IP 地址，我们会取消其关联。您需要对未与该实例关联的弹性 IP 地址支付费用。当您重启实例时，必须将弹性 IP 地址与该实例关联；我们不自动执行此操作。

EC2-VPC：实例会保留其关联的弹性 IP 地址。您需要对所有与已停止实例关联的弹性 IP 地址付费。

- 当您停止和启动 Windows 实例时，EC2Config 服务会对该实例执行任务，例如，更改所有附加的 Amazon EBS 卷的驱动器号。有关这些默认值以及如何更改它们的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[使用 EC2Config 服务配置 Windows 实例](#)。
- 如果您在负载均衡器上注册该实例，那么当您停止并重启该实例后，负载均衡器很可能不能向您的实例传输数据流量。停止实例后，您必须从该负载均衡器取消注册，然后在启动后重新注册。有关更多信息，请参阅 传统负载均衡器 指南 中的[在传统负载均衡器中注册或注销 EC2 实例](#)。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。有关更多信息，请参阅 Auto Scaling 用户指南 中的[Auto Scaling 实例的健康检查](#)。
- 当您停止 ClassicLink 实例时，它会从链接的 VPC 取消链接。您必须在重新启动之后将实例再次链接到 VPC。有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 436\)](#)。

有关更多信息，请参阅 [重启、停止与终止之间的区别 \(p. 242\)](#)。

只有在实例停止时，您才能修改以下实例属性：

- 实例类型
- 用户数据
- 内核
- RAM 磁盘

如果您在实例运行时尝试修改这些属性，Amazon EC2 会返回 `IncorrectInstanceState` 错误。

停止和启动您的实例

您可以使用控制台或命令行启动和停止由 Amazon EBS 支持的实例。

在默认情况下，当您通过由 Amazon EBS 支持的实例启动关闭（使用 `shutdown`、`halt` 或 `poweroff` 命令）时，该实例会停止。您可以更改此行为，以便使其终止。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 269\)](#)。

使用控制台停止和启动由 Amazon EBS 支持的实例

1. 在导航窗格中，选择 `Instances`，然后选择实例。
2. [EC2-Classic] 如果实例具有关联的弹性 IP 地址，则写下详细信息窗格中显示的弹性 IP 地址和实例 ID。
3. 依次选择 `Actions`、`Instance State` 和 `Stop`。如果 `Stop`（停止）处于禁用状态，则表示要么实例已停止，要么其根设备是一个实例存储卷。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，选择 `Yes, Stop`。停止实例可能需要几分钟时间。

[EC2-Classic] 当实例状态变为 `stopped` 时，详细信息窗格中的 `Elastic IP`、`Public DNS (IPv4)`、`Private DNS` 和 `Private IPs` 字段为空，表明旧值不再与实例关联。

5. 当实例停止时，您可以修改特定的实例属性。有关更多信息，请参阅 [修改已停止的实例 \(p. 265\)](#)。
6. 要重启已停止的实例，请选择该实例，然后依次选择 `Actions`、`Instance State` 和 `Start`。
7. 在确认对话框中，选择 `Yes, Start`。实例进入 `running` 状态可能需要几分钟时间。

[EC2-Classic] 当实例状态变为 `running` 时，详细信息窗格中的 `Public DNS (IPv4)`、`Private DNS` 和 `Private IPs` 字段包含我们分配给实例的新值。

8. [EC2-Classic] 如果您的实例具有关联的弹性 IP 地址，则您必须按以下方式对其进行重新关联：
 - a. 在导航窗格中，选择 `Elastic IPs`。
 - b. 选择您在停止实例前所记下的弹性 IP 地址。
 - c. 选择 `Actions`，然后选择 `Associate address`。
 - d. 选择您在停止实例前所记下的实例 ID，然后选择 `Associate`。

使用命令行停止和启动由 Amazon EBS 支持的实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `stop-instances` 和 `start-instances` (AWS CLI)
- `Stop-EC2Instance` 和 `Start-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

修改已停止的实例

您可以使用 AWS 管理控制台或命令行界面来更改已停止实例的实例类型、用户数据或 EBS 优化属性。您无法使用 AWS 管理控制台修改 DeleteOnTermination、内核或 RAM 磁盘属性。

修改实例属性

- 要更改实例类型，请参阅[调整您的实例大小 \(p. 156\)](#)。
- 要更改您的实例的用户数据，请参阅[使用用户数据配置实例 \(p. 298\)](#)。
- 要为您的实例启用或禁用 EBS 优化，请参阅[修改 EBS 优化 \(p. 567\)](#)。
- 要更改您的实例的根卷的 DeleteOnTermination 属性，请参阅[更新正在运行的实例的块储存设备映射 \(p. 615\)](#)。

使用命令行修改实例属性

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (适用于 Windows PowerShell 的 AWS 工具)

故障排除

如果停止了 Amazon EBS 支持的实例，该实例“卡在”了 `stopping` 状态，则可以强制停止它。有关更多信息，请参阅[排查实例的停止问题 \(p. 649\)](#)。

重启您的实例

实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。重启实例时，其仍驻留在相同的物理主机上，因此您的实例将保留其公有 DNS 名称 (IPv4)、私有 IPv4 地址、IPv6 地址 (如果适用) 及其实例存储卷上的任何数据。

重启实例不会启动新的实例计费时间，这与停止并重新启动您的实例不同。

为进行必要的维护 (例如，为了应用需要重启的升级)，我们可能会为您的实例预定一次重启。您无需进行任何操作；我们建议您在其预定重启窗口期间等待重启完成。有关更多信息，请参阅[实例的计划事件 \(p. 317\)](#)。

我们建议您使用 Amazon EC2 来重启实例，而非在实例中运行操作系统重启命令。如果您使用 Amazon EC2 重启实例，而实例在 4 分钟内未完全关闭，我们会执行硬重启。如果您使用 AWS CloudTrail，则使用 Amazon EC2 重启实例还会创建一条关于实例重启时间的 API 记录。

使用控制台重启实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances。
3. 选择相应实例，选择 Actions，然后依次选择 Instance State 和 Reboot。
4. 当系统提示您确认时，选择 Yes, Reboot。

使用命令行重启实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `reboot-instances` (AWS CLI)

- [Restart-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

实例停用

实例计划在 AWS 检测到托管实例的底层硬件发生无法弥补的故障时停用。当实例到达其计划的停用日期时，AWS 会将其停止或终止。如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。启动停止的实例会将其迁移到新的硬件。如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

主题

- [确认计划停用的实例 \(p. 266\)](#)
- [使用计划停用的实例 \(p. 266\)](#)

有关实例事件类型的更多信息，请参阅[实例的计划事件 \(p. 317\)](#)。

确认计划停用的实例

如果实例已计划停用，您将在事件发生之前收到包含实例 ID 和停用日期的电子邮件。该电子邮件将发送至与您账户关联的地址，也就是您用于登录 AWS 管理控制台的电子邮件地址。如果您使用的是并不定期检查的电子邮件账户，则可以使用 Amazon EC2 控制台或命令行确定是否有计划停用的实例。要更新您账户的联系人信息，请转到[Account Settings \(账户设置\)](#) 页面。

使用控制台确认计划停用的实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 EC2 Dashboard。在 Scheduled Events (计划的事件) 下方，您可以看到与您的 Amazon EC2 实例和卷相关的事件，这些事件按区域划分。
3. 如果您的某个实例列有计划的事件，请选择区域名称下方的链接，以访问 Events 页面。
4. Events (事件) 页面会列出与事件相关的所有资源。要查看计划停用的实例，请从第一个筛选列表中选择 Instance resources，然后从第二个筛选列表中选择 Instance stop or retirement。
5. 如果筛选结果显示有实例被计划停用，请选择该实例，并注意详细信息窗格中开始时间字段中的日期和时间。这就是您的实例停用的日期。

使用命令行确认计划停用的实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-instance-status \(AWS CLI\)](#)
- [Get-EC2InstanceState \(适用于 Windows PowerShell 的 AWS 工具\)](#)

使用计划停用的实例

当您的实例已计划停用时，有多种可使用的操作。您所采取的操作取决于您的实例根设备是 Amazon EBS 卷还是实例存储卷。如果不知道实例根设备的类型，可使用 Amazon EC2 控制台或命令行进行查看。

确定您的实例根设备的类型

使用控制台确定您的实例根设备的类型

1. 在导航窗格中，选择 Events。按上述[确认计划停用的实例 \(p. 266\)](#)步骤所示，使用筛选列表确认停用实例。
2. 在 Resource Id 列中，选择实例 ID 以前往 Instances 页面。

- 选择实例并找到 Description (描述) 选项卡中的 Root device type 字段。如果值为 ebs，则说明您的实例是由 EBS 提供支持。如果值为 instance-store，则说明您的实例是由实例存储提供支持。

使用命令行确定您的实例根设备的类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-instances \(AWS CLI\)](#)
- [Get-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

管理计划停用的实例

您可以执行下列操作中的一种，以保存将要停用的实例上的数据。务必要在实例停止日期前采取此操作，以防止意外的停机和数据丢失。

Warning

如果超过停用日期，由实例存储支持的实例就会停止，且无法恢复实例或存储在该实例上的任何数据。无论您的实例根设备是哪种类型，存储在实例存储卷上的数据都会在停用实例后丢失，即使它们附加到由 EBS 提供支持的实例也是如此。

| 实例根设备类型 | 操作 |
|---------|--|
| EBS | 等到计划的停用日期 (实例停止的日期)，或在停用日期之前自行停止实例。您可随时重新启动实例。有关停止和启动实例以及停止实例后的预期情况 (例如对与实例关联的公有、私有和弹性 IP 地址的影响) 的更多信息，请参阅 停止和启动您的实例 (p. 263) 。 |
| EBS | 从实例创建由 EBS 提供支持的 AMI，并启动替代实例。有关更多信息，请参阅 创建 Amazon EBS 支持的 Linux AMI (p. 75) 。 |
| 实例存储 | 从使用 AMI 工具的实例创建由实例存储支持的 AMI，并启动替换实例。有关更多信息，请参阅 创建由实例存储支持的 Linux AMI (p. 78) 。 |
| 实例存储 | 将数据传输到 EBS 卷，拍摄卷快照，然后从该快照创建 AMI，从而将您的实例转换为由 EBS 提供支持的实例。您可以从新 AMI 启动替换实例。有关更多信息，请参阅 将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI (p. 113) 。 |

终止您的实例

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，就不再产生与该实例相关的费用。

在您终止之后，您将无法连接至或重新启动实例。但是您可以使用同一 AMI 启动其他实例。如果您宁愿停止并重启您的实例，请参阅 [停止和启动您的实例 \(p. 263\)](#)。有关更多信息，请参阅 [重启、停止与终止之间的区别 \(p. 242\)](#)。

内容

- [实例终止 \(p. 268\)](#)
- [终止实例 \(p. 268\)](#)
- [为实例启用终止保护 \(p. 268\)](#)
- [更改实例的启动关闭操作 \(p. 269\)](#)
- [在实例终止时保留 Amazon EBS 卷 \(p. 270\)](#)
- [故障排除 \(p. 271\)](#)

实例终止

在您终止实例之后，短时间内仍可在控制台中看见该实例，然后该条目将自动被删除。您无法自行删除已经终止的实例条目。在实例终止后，标签和卷等资源会逐步与实例取消关联，因此过一小段时间后，它们可能在终止的实例上不再可见。

当实例终止时，与该实例关联的所有实例存储卷上的数据都会被删除。

默认情况下，当实例终止时，Amazon EBS 根设备卷将自动删除。但是，在默认情况下，即使在实例终止后，您在启动时挂载的所有额外 EBS 卷或您挂载到现有实例的所有 EBS 卷也会保留。这一操作是由卷的 `DeleteOnTermination` 属性控制的，您可以对其进行修改。有关更多信息，请参阅 [在实例终止时保留 Amazon EBS 卷 \(p. 270\)](#)。

您可以使用 AWS 管理控制台、CLI 和 API 防止实例被别人意外终止。此功能对 Amazon EC2 实例存储支持的实例和 Amazon EBS 支持的实例都适用。每个实例的 `DisableApiTermination` 属性默认值均为 `false`（可以通过 Amazon EC2 终止实例）。您可以在实例运行或停止时修改此实例属性（如果是由 Amazon EBS 支持的实例）。有关更多信息，请参阅 [为实例启用终止保护 \(p. 268\)](#)。

当使用操作系统中的系统关闭命令从实例启动关闭时，您可以控制是否应该关闭或终止实例。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 269\)](#)。

如果您在实例终止时运行脚本，您的实例可能会出现异常终止的情况，因为我们无法确保关闭脚本运行。Amazon EC2 会尝试彻底关闭实例，并运行任一系统关闭脚本；但某些事件（如硬件故障）可能会妨碍这些系统关闭脚本的运行。

终止实例

您可以使用 AWS 管理控制台或命令行终止实例。

使用控制台终止实例

1. 在终止实例前，请验证您不会丢失任何数据，方法是确认您的 Amazon EBS 卷不会在终止时被删除，并且您已将所需数据从实例存储卷复制到 Amazon EBS 或 Amazon S3。
2. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
3. 在导航窗格中，选择 Instances。
4. 选择相应实例，选择 Actions，然后依次选择 Instance State 和 Terminate。
5. 当系统提示您确认时，请选择 Yes, Terminate。

使用命令行终止实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `terminate-instances` (AWS CLI)
- `Stop-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

为实例启用终止保护

默认情况下，您可以使用 Amazon EC2 控制台、命令行界面或 API 终止您的实例。如果您希望使用 Amazon EC2 防止实例意外终止，可以启用实例终止保护。`DisableApiTermination` 属性可控制是否可以使用控制台、CLI 或 API 终止实例。在默认情况下，终止保护处于禁用状态。您可以在实例启动、运行或已停止时设置该属性值（针对由 Amazon EBS 支持的实例）。

当设置 `InstanceInitiatedShutdownBehavior` 属性时，`DisableApiTermination` 属性不会阻止您通过从实例启动关闭来终止实例（使用操作系统的系统关闭命令）。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 269\)](#)。

限制

您不能为竞价型实例启用终止保护 – 当现货价格超过您的出价时，竞价型实例将终止。不过，您可以准备应用程序来处理竞价型实例中断。有关更多信息，请参阅 [竞价型实例中断 \(p. 224\)](#)。

`DisableApiTermination` 属性不会阻止 Auto Scaling 终止实例。对于 Auto Scaling 组中的实例，请使用下列 Auto Scaling 功能而非 Amazon EC2 终止保护：

- 要阻止作为 Auto Scaling 组一部分的实例在缩小时终止，请使用实例保护。有关更多信息，请参阅 Auto Scaling 用户指南中的[实例保护](#)。
- 要阻止 Auto Scaling 终止运行状况不佳的实例，请暂停 `ReplaceUnhealthy` 流程。有关更多信息，请参阅 Auto Scaling 用户指南中的[暂停和恢复 Auto Scaling 流程](#)。
- 要指定 Auto Scaling 应先终止的实例，请选择终止策略。有关更多信息，请参阅 Auto Scaling 用户指南中的[自定义终止策略](#)。

要在实例启动时启用终止保护

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板中，选择 Launch Instance 并按照向导中的说明操作。
3. 在 Configure Instance Details (配置实例详细信息) 页面上，选中 Enable termination protection (启用终止保护) 复选框。

启用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Termination Protection。
2. 选择 Yes, Enable。

禁用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Termination Protection。
2. 选择 Yes, Disable。

使用命令行启用或禁用终止保护

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (适用于 Windows PowerShell 的 AWS 工具)

更改实例的启动关闭操作

在默认情况下，当通过由 Amazon EBS 支持实例使用关闭命令启动关闭 (使用 `shutdown`、`halt` 或 `poweroff` 等命令) 时，该实例会停止。您可以使用实例的 `InstanceInitiatedShutdownBehavior` 属性更改此操作，以便终止实例。您可以在实例运行或停止时更新此属性。

注意，实例存储支持的实例可以终止，但无法停止。

您可以使用 Amazon EC2 控制台或命令行更新 `InstanceInitiatedShutdownBehavior` 属性。`InstanceInitiatedShutdownBehavior` 属性只在您从实例自身的操作系统执行关闭操作时适用；在您使用 `StopInstances` API 或 Amazon EC2 控制台停止实例时不适用。

使用控制台更改实例的关闭行为

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Instances。
3. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Shutdown Behavior。已选定当前操作。
4. 要更改该操作，请从 Shutdown behavior 列表中选择一个选项，然后选择 Apply。

使用命令行更改实例的关闭行为

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-instance-attribute \(AWS CLI\)](#)
- [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在实例终止时保留 Amazon EBS 卷

当实例终止时，Amazon EC2 会使用每个挂载的 Amazon EBS 卷的 DeleteOnTermination 属性的值来确定是保留还是删除该卷。

默认情况下，实例的根卷的 DeletionOnTermination 属性将设置为 true。因此，当某个实例终止时，默认为删除该实例的根卷。

默认情况下，当您将 EBS 卷挂载到某个实例时，其 DeleteOnTermination 属性将设置为 false。因此，默认认为保留这些卷。在该实例终止后，您可以为保留的卷拍摄快照，或将其挂载到另一个实例。

要验证使用中的 EBS 卷的 DeleteOnTermination 属性的值，请查看该实例的块储存设备映射。有关更多信息，请参阅 [查看实例块储存设备映射中的 EBS 卷 \(p. 615\)](#)。

在启动该实例或在该实例正在运行时，您可以更改卷的 DeleteOnTermination 属性的值。

示例

- [使用控制台将根卷更改为在启动时持久保留 \(p. 270\)](#)
- [使用命令行将根卷更改为在启动时持久保留 \(p. 271\)](#)
- [使用命令行更改要持久保留正在运行的实例的根卷 \(p. 271\)](#)

使用控制台将根卷更改为在启动时持久保留

当您启动实例时，可以使用控制台更改 DeleteOnTermination 属性。要对正在运行的实例更改此属性，您必须使用命令行。

使用控制台在启动时更改实例要持久保留的根卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从控制台控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择一个 AMI，然后选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面上，取消选中根卷的 Delete On Termination (终止时删除) 复选框。
6. 完成其余向页面上的操作，然后选择 Launch。

您可以通过实例的详细信息窗格查看根设备卷的详细信息以验证设置。在 Block devices (块储存设备) 旁，单击根设备卷的条目。默认情况下，Delete on termination (终止时删除) 为 True。如果您更改默认行为，Delete on termination (终止时删除) 将为 False。

使用命令行将根卷更改为在启动时持久保留

当您启动 EBS 支持的实例时，可以使用下列命令之一将根设备卷更改为持久保留。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

例如，将以下选项添加到 `run-instances` 命令：

```
--block-device-mappings file://mapping.json
```

在 `mapping.json` 中指定以下内容：

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false,  
      "SnapshotId": "snap-1234567890abcdef0",  
      "VolumeType": "gp2"  
    }  
  }  
]
```

使用命令行更改要持久保留正在运行的实例的根卷

您可以使用下列命令之一将正在运行的 EBS 支持实例的根设备卷更改为持久保留。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

例如，使用以下命令：

```
$ aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-  
mappings file://mapping.json
```

在 `mapping.json` 中指定以下内容：

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

故障排除

如果您的实例处于 `shutting-down` 状态的时间超出正常范围，Amazon EC2 服务中的自动进程最终将对其进行清理（终止）。有关更多信息，请参阅 [排查实例的终止（关闭）问题 \(p. 650\)](#)。

恢复您的实例

您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。有关使用 Amazon CloudWatch 警报恢复实例的更多信息，请参阅[创建停止、终止、重启或恢复实例的警报 \(p. 332\)](#)。要对实例恢复故障进行故障排除，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[排除实例恢复故障](#)。

当 `StatusCheckFailed_System` 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您会注意到，实例在已恢复的实例上重启。

导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题影响网络连通状态

当 AWS 因底层硬件降级而安排停止或停用某个实例时，也可能会触发恢复操作。有关计划事件的更多信息，请参阅[实例的计划事件 \(p. 317\)](#)。

只有具有以下特性的实例支持恢复操作：

- 使用 C3、C4、M3、M4、R3、R4、T2 或 X1 实例类型
- 在 VPC 中（非 EC2-Classic 中）运行
- 使用共享租赁（租赁属性设置为 `default`）
- 仅使用 EBS 卷（不配置实例存储卷）。有关更多信息，请参阅[已禁用“恢复此实例”](#)。

如果您的实例具有公有 IPv4 地址，它会在恢复后保留公有 IPv4 地址。

配置您的 Amazon Linux 实例

在成功启动和登录您的 Amazon Linux 实例之后，您可以对其进行修改。可以通过许多不同方式配置实例以满足特定应用程序的需求。下面是一些可帮助您入门的常见任务。

内容

- [常见配置方案 \(p. 273\)](#)
- [在 Linux 实例上管理软件 \(p. 273\)](#)
- [在 Linux 实例上管理用户账户 \(p. 280\)](#)
- [您的 EC2 实例的处理器状态控制 \(p. 282\)](#)
- [为 Linux 实例设置时间 \(p. 286\)](#)
- [更改 Linux 实例的主机名 \(p. 289\)](#)
- [在 Linux 实例上设置动态 DNS \(p. 291\)](#)
- [启动时在 Linux 实例上运行命令 \(p. 292\)](#)
- [实例元数据和用户数据 \(p. 295\)](#)

常见配置方案

Amazon Linux 的基本发布版包含基本服务器操作所需的许多软件包和实用工具。但是，各种软件存储库还提供许多软件包，还有更多软件包可供您从源代码进行构建。有关从这些位置安装和构建软件的更多信息，请参阅[在 Linux 实例上管理软件 \(p. 273\)](#)。

Amazon Linux 实例预配置有 `ec2-user` 账户，但是，您可能需要添加没有超级用户权限的其他用户账户。有关添加和删除用户账户的更多信息，请参阅[在 Linux 实例上管理用户账户 \(p. 280\)](#)。

Amazon Linux 实例的默认时间配置使用网络时间协议在实例上设置系统时间。默认时区为 UTC。有关设置实例的时区或使用自有时间服务器的更多信息，请参阅[为 Linux 实例设置时间 \(p. 286\)](#)。

如果您自己有注册了域名的网络，则可以更改实例的主机名，将它自身标识为该域名的一部分。您还可以在不更改主机名设置的情况下更改系统提示，以显示更有意义的名称。有关更多信息，请参阅[更改 Linux 实例的主机名 \(p. 289\)](#)。您可以将实例配置成使用动态 DNS 服务提供商。有关更多信息，请参阅[在 Linux 实例上设置动态 DNS \(p. 291\)](#)。

当您在 Amazon EC2 中启动实例时，可以选择将用户数据传递到可用于执行常见配置任务甚至在实例启动后运行脚本的实例。您可以将两类用户数据传递到 Amazon EC2，`cloud-init` 指令和 Shell 脚本。有关更多信息，请参阅[启动时在 Linux 实例上运行命令 \(p. 292\)](#)。

在 Linux 实例上管理软件

Amazon Linux 的基本发布版包含基本服务器操作所需的许多软件包和实用工具。但是，各种软件存储库还提供许多软件包，还有更多软件包可供您从源代码进行构建。

内容

- [更新实例软件 \(p. 273\)](#)
- [添加存储库 \(p. 276\)](#)
- [查找软件包 \(p. 278\)](#)
- [安装软件包 \(p. 279\)](#)
- [准备编译软件 \(p. 279\)](#)

使软件保持最新非常重要。Linux 发布版中的许多程序包会经常更新，以修复错误、添加功能，以及防止安全漏洞。有关更多信息，请参阅[更新实例软件 \(p. 273\)](#)。

默认情况下，Amazon Linux 实例启动时启用两个存储库：`amzn-main` 和 `amzn-updates`。尽管在 Amazon Web Services 更新的这些存储库中有许多程序包，但是您需要安装的程序包可能在其他存储库中。有关更多信息，请参阅[添加存储库 \(p. 276\)](#)。有关在启用的存储库中查找程序包的帮助，请参阅[查找软件包 \(p. 278\)](#)。有关在 Amazon Linux 实例上安装软件的信息，请参阅[安装软件包 \(p. 279\)](#)。

并非所有软件均可在存储库中存储的软件包中获得；有些软件必须在实例上从其源代码进行编译。有关更多信息，请参阅[准备编译软件 \(p. 279\)](#)。

Amazon Linux 实例使用 yum 程序包管理器管理其软件。yum 程序包管理器可安装、删除和更新软件，以及管理每个包的所有依赖关系。基于 Debian 的 Linux 分发版本（如 Ubuntu）使用 apt-get 命令和 dpkg 程序包管理器，因此，下面几节中的 yum 示例不适用于这些分发版本。

更新实例软件

使软件保持最新非常重要。Linux 发布版中的许多程序包会经常更新，以修复错误、添加功能，以及防止安全漏洞。当您首次启动并连接到 Amazon Linux 实例时，您可能会看到出于安全目的要求您更新软件包的消息。本节介绍如何更新整个系统或仅更新单个程序包。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

```
 _|_(_/_ / Amazon Linux AMI
  \_\_\_|_
https://aws.amazon.com/amazon-linux-ami/2013.03-release-notes/
There are 12 security update(s) out of 25 total update(s) available
Run "sudo yum update" to apply all updates.
[ec2-user ~]$
```

更新 Amazon Linux 实例上的所有程序包

1. (可选) 启动 Shell 窗口中的 screen 会话。有时您可能会遇到网络中断，这样会断开到实例的 SSH 连接。如果在较长的软件更新期间发生这种情况，实例处于混乱、但可恢复的状态。即使连接中断，通过 screen 会话也可继续运行更新，您稍后可重新连接到此会话，不会有问题。

- a. 执行 screen 命令开始会话。

```
[ec2-user ~]$ screen
```

- b. 如果会话中断，请再次登录实例并列出可用屏幕。

```
[ec2-user ~]$ screen -ls
There is a screen on:
  17793.pts-0.ip-12-34-56-78 (Detached)
  1 Socket in /var/run/screen/S-ec2-user.
```

- c. 使用 screen -r 命令和前一命令的进程 ID 重新连接到 screen。

```
[ec2-user ~]$ screen -r 17793
```

- d. 使用完 screen 后，使用 exit 命令关闭会话。

```
[ec2-user ~]$ exit
[screen is terminating]
```

2. 运行 yum update 命令。您可以选择添加 --security 标记，这样仅应用安全更新。

```
[ec2-user ~]$ sudo yum update
Loaded plugins: priorities, security, update-motd, upgrade-helper
amzn-main                                         | 2.1 kB     00:00
amzn-updates                                      | 2.3 kB     00:00
Setting up Update Process
Resolving Dependencies
--> Running transaction check
--> Package aws-apitools-ec2.noarch 0:1.6.8.1-1.0.amzn1 will be updated
--> Package aws-apitools-ec2.noarch 0:1.6.10.0-1.0.amzn1 will be an update
--> Package gnupg2.x86_64 0:2.0.18-1.16.amzn1 will be updated
--> Package gnupg2.x86_64 0:2.0.19-8.21.amzn1 will be an update
--> Package libgcrypt.i686 0:1.4.5-9.10.amzn1 will be updated
--> Package libgcrypt.x86_64 0:1.4.5-9.10.amzn1 will be updated
--> Package libgcrypt.i686 0:1.4.5-9.12.amzn1 will be an update
--> Package libgcrypt.x86_64 0:1.4.5-9.12.amzn1 will be an update
--> Package openssl.x86_64 1:1.0.0e-4.53.amzn1 will be updated
--> Package openssl.x86_64 1:1.0.0e-4.54.amzn1 will be an update
--> Package python-boto.noarch 0:2.9.9-1.0.amzn1 will be updated
--> Package python-boto.noarch 0:2.13.3-1.0.amzn1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved
```

```

  Package           Arch    Version      Repository      Size
=====
Updating:
aws-apitools-ec2      noarch   1.6.10.0-1.0.amzn1   amzn-updates   14 M
gnupg2                  x86_64   2.0.19-8.21.amzn1   amzn-updates   2.4 M
libgcrypt                i686    1.4.5-9.12.amzn1   amzn-updates   248 k
libgcrypt                x86_64   1.4.5-9.12.amzn1   amzn-updates   262 k
openssl                 x86_64   1:1.0.1e-4.54.amzn1   amzn-updates   1.7 M
python-boto              noarch   2.13.3-1.0.amzn1   amzn-updates   1.6 M

Transaction Summary
=====
Upgrade       6 Package(s)

Total download size: 20 M
Is this ok [y/N]:

```

3. 查看所列的程序包，键入 y 和 Enter 接受更新。更新系统上的所有程序包可能需要几分钟。yum 输出显示更新运行状态。

```

Downloading Packages:
(1/6): aws-apitools-ec2-1.6.10.0-1.0.amzn1.noarch.rpm | 14 MB  00:00
(2/6): gnupg2-2.0.19-8.21.amzn1.x86_64.rpm          | 2.4 MB  00:00
(3/6): libgcrypt-1.4.5-9.12.amzn1.i686.rpm          | 248 kB   00:00
(4/6): libgcrypt-1.4.5-9.12.amzn1.x86_64.rpm          | 262 kB   00:00
(5/6): openssl-1.0.1e-4.54.amzn1.x86_64.rpm          | 1.7 MB   00:00
(6/6): python-boto-2.13.3-1.0.amzn1.noarch.rpm        | 1.6 MB   00:00
-----
Total                                         28 MB/s | 20 MB  00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating : libgcrypt-1.4.5-9.12.amzn1.x86_64          1/12
  Updating : gnupg2-2.0.19-8.21.amzn1.x86_64          2/12
  Updating : aws-apitools-ec2-1.6.10.0-1.0.amzn1.noarch 3/12
  Updating : 1:openssl-1.0.1e-4.54.amzn1.x86_64          4/12
...
Complete!

```

4. (可选) 重启实例以确保您使用的是来自更新的最新程序包和库；重启发生前不会加载内核更新。更新任何 glibc 库后也应进行重启。对于用来控制服务的程序包的更新，重新启动服务便足以使更新生效，但系统重启可确保所有之前的程序包和库更新都是完整的。

更新 Amazon Linux 实例上的单个程序包

使用此过程可更新单个程序包（及其依赖关系），而非整个系统。

1. 使用要更新的程序包的名称运行 yum update 命令。

```

[ec2-user ~]$ sudo yum update openssl
Loaded plugins: priorities, security, update-motd, upgrade-helper
amzn-main                                         | 2.1 kB  00:00
amzn-updates                                      | 2.3 kB  00:00
Setting up Update Process
Resolving Dependencies
--> Running transaction check
--> Package openssl.x86_64 1:1.0.1e-4.53.amzn1 will be updated
--> Package openssl.x86_64 1:1.0.1e-4.54.amzn1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

```

```
=====
 Package      Arch      Version      Repository      Size
 =====
 Updating:
 openssl      x86_64    1:1.0.1e-4.54.amzn1    amzn-updates   1.7 M

 Transaction Summary
 =====
 Upgrade      1 Package(s)

 Total download size: 1.7 M
 Is this ok [y/N]:
```

2. 查看所列的程序包信息，键入 y 和 Enter 接受更新。如果存在必须解析的程序包依赖关系，有时会列出多个数据包。yum 输出显示更新运行状态。

```
Downloading Packages:
openssl-1.0.1e-4.54.amzn1.x86_64.rpm | 1.7 MB 00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating : 1:openssl-1.0.1e-4.54.amzn1.x86_64          1/2
  Cleanup   : 1:openssl-1.0.1e-4.53.amzn1.x86_64          2/2
  Verifying : 1:openssl-1.0.1e-4.54.amzn1.x86_64          1/2
  Verifying : 1:openssl-1.0.1e-4.53.amzn1.x86_64          2/2

Updated:
  openssl.x86_64 1:1.0.1e-4.54.amzn1

Complete!
```

3. (可选) 重启实例以确保您使用的是来自更新的最新程序包和库；重启发生前不会加载内核更新。更新任何 glibc 库后也应进行重启。对于用来控制服务的程序包的更新，重新启动服务便足以使更新生效，但系统重启可确保所有之前的程序包和库更新都是完整的。

添加存储库

默认情况下，Amazon Linux 实例启动时启用两个存储库：amzn-main 和 amzn-updates。尽管在 Amazon Web Services 更新的这些存储库中有许多程序包，但是您需要安装的程序包可能在其他存储库中。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

要使用 yum 从不同存储库安装程序包，您需要将存储库信息添加到 /etc/yum.conf 文件中，或者添加到 /etc/yum.repos.d 目录中它自己的 `repository.repo` 文件中。您可以手动执行该操作，但大多数 yum 存储库在其存储库 URL 提供各自的 `repository.repo` 文件。

确定已安装的 yum 存储库

- 使用以下命令列出已安装的 yum 存储库：

```
[ec2-user ~]$ yum repolist all
```

输出结果会列出已安装的存储库，并报告每个存储库的状态。启用的存储库会显示其中包含的程序包数量。

| repo id | status | repo name |
|---------|--------|-----------|
|---------|--------|-----------|

```
!amzn-main/latest           amzn-main-Base
                           enabled: 5,612
amzn-main-debuginfo/latest amzn-main-debuginfo
                           disabled
amzn-main-source/latest    amzn-main-source
                           disabled
amzn-nosrc/latest          amzn-nosrc-Base
                           disabled
amzn-preview/latest        amzn-preview-Base
                           disabled
amzn-preview-debuginfo/latest amzn-preview-debuginfo
                           disabled
amzn-preview-source/latest amzn-preview-source
                           disabled
!amzn-updates/latest       amzn-updates-Base
                           enabled: 1,152
amzn-updates-debuginfo/latest amzn-updates-debuginfo
                           disabled
amzn-updates-source/latest amzn-updates-source
                           disabled
epel/x86_64                 Extra Packages for Enterprise Linux 6 - x86_64
                           disabled
epel-debuginfo/x86_64        Extra Packages for Enterprise Linux 6 - x86_64 -
                           Debug      disabled
epel-source/x86_64           Extra Packages for Enterprise Linux 6 - x86_64 -
                           Source     disabled
epel-testing/x86_64          Extra Packages for Enterprise Linux 6 - Testing -
                           x86_64     disabled
epel-testing-debuginfo/x86_64 Extra Packages for Enterprise Linux 6 - Testing -
                           x86_64 - Debug  disabled
epel-testing-source/x86_64   Extra Packages for Enterprise Linux 6 - Testing -
                           x86_64 - Source disabled
```

要将 yum 存储库添加到 `/etc/yum.repos.d`

安装存储库后，必须按照以下过程启用存储库。

- 找到 `.repo` 文件的位置。这随要添加的存储库而异。在该示例中，`.repo` 文件位于 `https://www.example.com/repository.repo`。
- 使用 `yum-config-manager` 命令添加存储库。

```
[ec2-user ~]$ sudo yum-config-manager --add-repo https://
www.example.com/repository.repo
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
grabbing file https://www.example.com/repository.repo to /etc/
yum.repos.d/repository.repo
repository.repo                                         | 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

要在 `/etc/yum.repos.d` 中启用 yum 存储库

- 使用 `--enable repository` 标志执行 `yum-config-manager` 命令。以下命令从 Fedora 项目启用 Extra Packages for Enterprise Linux (EPEL) 存储库。在默认情况下，该存储库出现在 Amazon Linux 实例上的 `/etc/yum.repos.d` 中，但未予启用。

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

Note

有关在其他发行版 (如 Red Hat 和 CentOS) 上启用 EPEL 存储库的信息，请参阅 <https://fedoraproject.org/wiki/EPEL> 上的 EPEL 文档。

查找软件包

您可以使用 `yum search` 命令搜索在您配置的存储库中可用的程序包的描述。如果不知道要安装的程序包的确切名称，这尤其有帮助。只需将关键字搜索附加到此命令；对于多字词搜索，请使用引号括起搜索查询。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

引号中的多个字词搜索查询仅返回符合确切查询的结果。如果您没有看到需要的程序包，请将搜索简化为一个关键字，然后扫描结果。您还可以尝试使用关键字同义词来扩大搜索范围。

```
[ec2-user ~]$ sudo yum search "find"
Loaded plugins: priorities, security, update-motd, upgrade-helper
=====
N/S Matched: find
=====
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface
                             : to File::Find
perl-Module-Find.noarch : Find and use installed modules in a (sub)category
libpuzzle.i686 : Library to quickly find visually similar images (gif, png, jpg)
libpuzzle.x86_64 : Library to quickly find visually similar images (gif, png,
                   : jpg)
mlocate.x86_64 : An utility for finding files by name
```

`yum` 程序包管理器还将多个程序包组合到组中，通过一个命令组就可以执行特定任务 (如安装 Web 服务器或构建软件编译工具)。要列出系统上已安装的组和可安装的可用组，请使用 `yum grouplist` 命令。

```
[ec2-user ~]$ sudo yum grouplist
Loaded plugins: priorities, security, update-motd, upgrade-helper
Setting up Group Process
Installed Groups:
  Development Libraries
  Development tools
  Editors
  Legacy UNIX compatibility
  Mail Server
  MySQL Database
  Network Servers
  Networking Tools
  PHP Support
  Perl Support
  System Tools
  Web Server
Available Groups:
  Console internet tools
  DNS Name Server
  FTP Server
  Java Development
  MySQL Database client
  NFS file server
  Performance Tools
  PostgreSQL Database client (version 8)
  PostgreSQL Database server (version 8)
  Scientific support
  TeX support
  Technical Writing
  Web Servlet Engine
```

Done

通过使用 `yum groupinfo "Group Name"` 命令，可以看到组中的不同程序包，将 `Group Name` 替换为组名称可获取相关信息。此命令列出可随组安装的所有必需、默认和可选程序包。

如果在默认 `amzn-main` 和 `amzn-updates` 存储库中找不到所需的软件，您可以添加更多存储库，例如 Extra Packages for Enterprise Linux (EPEL) 存储库。有关更多信息，请参阅 [添加存储库 \(p. 276\)](#)。

安装软件包

`yum` 程序包管理器是出色的安装软件工具，因为它可以搜索您针对不同软件包启用的所有存储库，还可以处理软件安装过程中的任何依赖关系。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

要从存储库安装程序包，请使用 `yum install package` 命令，将 `package` 替换为要安装的软件的名称。举例来说，若要安装 `links` 基于文本的 Web 浏览器，请输入以下命令。

```
[ec2-user ~]$ sudo yum install links
```

要安装程序包组，请使用 `yum groupinstall Group Name` 命令，将 `Group Name` 替换为要安装的组的名称。例如，若要安装“Performance Tools (性能工具)”组，请输入以下命令。

```
[ec2-user@ip-10-161-113-54 ~]$ sudo yum groupinstall "Performance Tools"
```

默认情况下，`yum` 仅安装组列表中的必需和默认程序包。如果还要安装组中的可选程序包，在执行添加可选程序包的命令时，可以在命令中设置 `group_package_types` 配置参数。

```
[ec2-user ~]$ sudo yum --setopt=group_package_types=mandatory,default,optional groupinstall "Performance Tools"
```

您还可使用 `yum install` 安装您已经从 Internet 下载的 RPM 程序包文件。为此，只需将 RPM 文件的路径名称而不是存储库程序包名称附加到安装命令。

```
[ec2-user ~]$ sudo yum install my-package.rpm
```

准备编译软件

Internet 上有大量开源软件，这些软件尚未预编译，可从程序包存储库下载。您可能最终会发现需要您亲自从源代码编译的软件包。要使系统能够编译软件，您需要安装几个开发工具，如 `make`、`gcc` 和 `autoconf`。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

因为软件编译不是每个 Amazon EC2 实例都需要的任务，所以在默认情况下不安装这些工具，不过，称为“开发工具”的程序包组中提供了这些工具，而这个程序包组可通过 `yum groupinstall` 命令方便地添加到实例。

```
[ec2-user ~]$ sudo yum groupinstall "Development Tools"
```

软件源代码包通常以压缩存档文件（称为 `tarball`）的形式提供下载（从 <https://github.com/> 和 <http://sourceforge.net/> 等网站）。这些 `tarball` 的文件扩展名通常为 `.tar.gz`。您可以使用 `tar` 命令来解压缩这些存档。

```
[ec2-user ~]$ tar -xzf software.tar.gz
```

将源代码包解压并解档后，应在源代码目录中查找 README 或 INSTALL 文件，这些文件包含有关编译和安装源代码的进一步说明。

检索 Amazon Linux 程序包的源代码

Amazon Web Services 提供所维护的程序包的源代码。您可以使用 get_reference_source 命令下载已安装的任何程序包的源代码。

- 运行 get_reference_source -p *package* 命令可下载 *package* 的源代码。例如，若要下载 htop 程序包的源代码，请输入以下命令。

```
[ec2-user ~]$ get_reference_source -p htop
Requested package: htop
Found package from local RPM database: htop-1.0.1-2.3.amzn1.x86_64
Corresponding source RPM to found package : htop-1.0.1-2.3.amzn1.src.rpm

Are these parameters correct? Please type 'yes' to continue: yes
Source RPM downloaded to: /usr/src/srpm/debug/htop-1.0.1-2.3.amzn1.src.rpm
```

该命令输出列出源 RPM 的位置，在本示例中，为 /usr/src/srpm/debug/htop-1.0.1-2.3.amzn1.src.rpm。

在 Linux 实例上管理用户账户

每个 Linux 实例类型均使用默认 Linux 系统用户账户启动。对于 Amazon Linux，用户名为 ec2-user。对于 RHEL，用户名是 ec2-user 或 root。对于 Ubuntu，用户名是 ubuntu 或 root。对于 CentOS，用户名是 centos。对于 Fedora，用户名是 ec2-user。对于 SUSE，用户名是 ec2-user 或 root。另外，如果 ec2-user 和 root 无法使用，请与您的 AMI 供应商核实。

Note

Linux 系统用户不应与 AWS Identity and Access Management (IAM) 用户混淆。有关更多信息，请参阅 IAM 用户指南 中的 [IAM 用户和组](#)。

对于许多应用程序来说，使用默认用户账户就足够了，不过您可选择添加用户账户，以便个人有自己的文件和工作区。为新用户创建用户账户比授予多个（可能缺乏经验的）用户对 ec2-user 的访问权限更安全，因为如果使用不当，该账户可能对系统造成严重破坏。

将新用户添加到系统

要有效地将用户添加到 Linux 实例涉及两个基本操作：将用户添加到系统和为该用户提供远程登录的方式。

- 要将新用户添加到系统，请使用 adduser 命令，后跟所有相关选项和要创建的用户的名称。

Important

如果您将一名用户添加到 Ubuntu 系统，应添加 --disabled-password 选项以免向该账户添加密码。

```
[ec2-user ~]$ sudo adduser newuser
```

此命令将 newuser 账户添加到系统（/etc/passwd 文件中会有一个条目），创建 newuser 组，并在 /home/newuser 中为该账户创建主目录。

- 要提供对此账户的远程访问，您必须在 #####.sshnewuser 目录，并在其中创建一个包含公钥的名为“authorized_keys”的文件。

- a. 切换到新账户，以便使新建的文件具有正确的所有权。

```
[ec2-user ~]$ sudo su - newuser  
[newuser ~]$
```

注意，现在提示 newuser，而不是 ec2-user；您已将 Shell 会话切换到新账户。

- b. 为 authorized_keys 文件创建一个 .ssh 目录。

```
[newuser ~]$ mkdir .ssh
```

- c. 将 .ssh 目录的文件权限更改为 700 (这意味着只有文件所有者能够读取、写入或打开此目录)。

Important

这一步非常重要；如果没有这些确切的文件权限，您将无法使用 SSH 登录此账户。

```
[newuser ~]$ chmod 700 .ssh
```

- d. 在 authorized_keys.SSH #####”的文件。

```
[newuser ~]$ touch .ssh/authorized_keys
```

- e. 将 authorized_keys 文件的文件权限更改为 600 (这意味着只有文件所有者能够读取或写入此文件)。

Important

这一步非常重要；如果没有这些确切的文件权限，您将无法使用 SSH 登录此账户。

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

- f. 使用您常用的文本编辑器编辑 authorized_keys 文件，将您的密钥对的公有密钥添加到该文件中，例如：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnBITntckij7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221Cb5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwi3f05p6KLxEXAMPLE
```

Note

有关创建密钥对的更多信息，请参阅[使用 Amazon EC2 创建密钥对 \(p. 347\)](#)。有关从现有密钥对中检索公钥的更多信息，请参阅[在 Linux 上检索密钥对的公有密钥 \(p. 349\)](#)。

您现在应该能够使用与来自 newuser 的公钥相匹配的私钥通过 SSH 登录实例上的 Step 2.f (p. 281) 账户。

从系统中删除用户

如果不再需要某个用户账户，可以将其删除，使它不再可用。

- 要删除用户账户、用户的主目录和用户的邮件后台打印，请执行 userdel -r 命令，后跟要删除的用户名。

```
[ec2-user ~]$ sudo userdel -r olduser
```

Note

要保留用户的主目录和邮件后台打印，请省略 `-r` 选项。

您的 EC2 实例的处理器状态控制

C 状态控制当核心处于空闲状态时可以进入的睡眠级别。C 状态从 C0 (最浅空闲状态，此时核心完全唤醒并在执行指令) 开始编号，一直增进到 C6 (最深空闲状态，此时核心关闭)。P 状态控制核心的所需性能 (以 CPU 频率的形式)。P 状态从 P0 (最高性能设置，此时核心可以使用 Intel 睿频加速技术提高频率) 开始编号，然后从 P1 (请求最大基准频率的 P 状态) 一直增加到 P15 (可能最低的频率)。

以下实例类型为操作系统提供了控制处理器 C 状态和 P 状态的功能：

- `c4.8xlarge`
- `d2.8xlarge`
- `i3.16xlarge`
- `m4.10xlarge`
- `m4.16xlarge`
- `p2.16xlarge`
- `r4.8xlarge`
- `r4.16xlarge`
- `x1.16xlarge`
- `x1.32xlarge`

改变 C 状态或 P 状态设置可以增加处理器性能一致性，减少延迟，还可以针对特定工作负载对实例进行调校。默认 C 状态和 P 状态设置可提供最大性能，是大多数工作负载的最佳选择。但是，如果您的应用程序更适合以牺牲较高的单核或双核频率的方式来降低延迟，或需要在较低频率下保持稳定性 (而不适合使用突发式睿频加速频率)，那么可以考虑运用对这些实例可用的 C 状态或 P 状态设置。

以下部分介绍了不同的处理器状态配置以及如何监控配置效果。这些步骤专为 Amazon Linux 编写并供其使用，但也适用于搭载 Linux 内核版本 3.9 及更高版本的其他 Linux 分发版。有关其他 Linux 分发版和处理器状态控制的更多信息，请参阅您系统的特定文档。

Note

此页面中的示例使用 `turbostat` 实用工具 (默认情况下可在 Amazon Linux 上获得) 来显示处理器频率和 C 状态信息，并使用 `stress` 命令 (可通过运行 `sudo yum install -y stress` 进行安装) 来模拟工作负载。

内容

- [具有最大睿频加速频率的最高性能 \(p. 282\)](#)
- [通过限制深层 C 状态实现高性能和低延迟 \(p. 283\)](#)
- [变化最少的基准性能 \(p. 284\)](#)

具有最大睿频加速频率的最高性能

这是 Amazon Linux AMI 的默认处理器状态控制配置，推荐大多数工作负载使用。此配置可提供最高性能，且变化更少。允许非活动核心进入深层睡眠状态可提供单核或双核进程所需的热空间，以达到最大睿频加速潜能。

以下示例显示了具有两个有效执行工作且达到其最大处理器睿频加速频率的核心的 c4.8xlarge 实例。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30680] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      5.54 3.44 2.90  0  9.18  0.00 85.28  0.00  0.00  0.00  0.00  0.00
94.04 32.70 54.18  0.00
0   0   0   0.12 3.26 2.90  0  3.61  0.00 96.27  0.00  0.00  0.00
48.12 18.88 26.02  0.00
0   0   18  0.12 3.26 2.90  0  3.61
0   1   1   0.12 3.26 2.90  0  4.11  0.00 95.77  0.00
0   1   19  0.13 3.27 2.90  0  4.11
0   2   2   0.13 3.28 2.90  0  4.45  0.00 95.42  0.00
0   2   20  0.11 3.27 2.90  0  4.47
0   3   3   0.05 3.42 2.90  0  99.91  0.00  0.05  0.00
0   3   21  97.84 3.45 2.90  0  2.11
...
1   1   10  0.06 3.33 2.90  0  99.88  0.01  0.06  0.00
1   1   28  97.61 3.44 2.90  0  2.32
...
10.002556 sec
```

在此示例中，vCPU 21 和 vCPU 28 均以其最大睿频加速频率运行，因为其他核心已进入 c6 睡眠状态以节省性能，并为正在工作的核心提供性能和热空间。vCPU 3 和 vCPU 10（分别与 vCPU 21 和 vCPU 28 共享一个处理器）均处于等待指令的 c1 状态。

在以下示例中，所有 18 个核心均在有效执行工作，因此没有达到最大睿频加速频率的空间，但这些核心都在以 3.2 GHz 的“所有核心睿频加速”速度运行。

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      99.27 3.20 2.90  0  0.26  0.00  0.47  0.00  0.00  0.00  0.00  0.00
228.59 31.33 199.26  0.00
0   0   0   99.08 3.20 2.90  0  0.27  0.01  0.64  0.00  0.00  0.00
114.69 18.55 99.32  0.00
0   0   18  98.74 3.20 2.90  0  0.62
0   1   1   99.14 3.20 2.90  0  0.09  0.00  0.76  0.00
0   1   19  98.75 3.20 2.90  0  0.49
0   2   2   99.07 3.20 2.90  0  0.10  0.02  0.81  0.00
0   2   20  98.73 3.20 2.90  0  0.44
0   3   3   99.02 3.20 2.90  0  0.24  0.00  0.74  0.00
0   3   21  99.13 3.20 2.90  0  0.13
0   4   4   99.26 3.20 2.90  0  0.09  0.00  0.65  0.00
0   4   22  98.68 3.20 2.90  0  0.67
0   5   5   99.19 3.20 2.90  0  0.08  0.00  0.73  0.00
0   5   23  98.58 3.20 2.90  0  0.69
0   6   6   99.01 3.20 2.90  0  0.11  0.00  0.89  0.00
0   6   24  98.72 3.20 2.90  0  0.39
...
```

通过限制深层 C 状态实现高性能和低延迟

C 状态控制当核心处于非活动状态时可能进入的睡眠级别。您可能需要控制 C 状态来调校系统的延迟与性能。将核心置于睡眠状态需要时间，尽管睡眠中的核心可为其他核心提供更多空间以加速至更高频率，但该睡眠中的核心也需要时间来重新唤醒并执行工作。例如，如果某个负责处理网络数据包中断的核心处于睡眠状态，那么在处理此类中断时可能会出现延迟。您可以将系统配置为不使用深层 C 状态，这可以降低处理器的反应延迟，但反过来也会减少其他核心达到睿频加速频率可用的空间。

禁用深层睡眠状态的常见情形是 Redis 数据库应用程序，该应用程序将数据库存储在系统内存中，以实现最快的查询响应。

限制 Amazon Linux 上的深层睡眠状态

1. 使用您选择的编辑器打开 /boot/grub/grub.conf 文件。

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. 编辑第一个条目的 kernel 行并添加 intel_idle.max_cstate=1 选项，将 c1 设为空闲核心的最深层 C 状态。

```
# created by imagebuilder
default=0
timeout=1
hiddenmenu

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
intel_idle.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

3. 保存文件并退出您的编辑器。
4. 重启实例以启用新的内核选项。

```
[ec2-user ~]$ sudo reboot
```

以下示例显示的 c4.8xlarge 实例具有两个以“所有核心睿频加速”核心频率有效执行工作的核心。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5322] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5322] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      5.56 3.20 2.90   0 94.44  0.00  0.00  0.00  0.00  0.00  0.00  0.00
131.90 31.11 199.47 0.00
0   0   0   0.03 2.08 2.90   0 99.97  0.00  0.00  0.00  0.00  0.00
67.23 17.11 99.76 0.00
0   0   18   0.01 1.93 2.90   0 99.99
0   1   1    0.02 1.96 2.90   0 99.98  0.00  0.00  0.00
0   1   19   99.70 3.20 2.90   0 0.30
...
1   1   10   0.02 1.97 2.90   0 99.98  0.00  0.00  0.00
1   1   28   99.67 3.20 2.90   0 0.33
1   2   11   0.04 2.63 2.90   0 99.96  0.00  0.00  0.00
1   2   29   0.02 2.11 2.90   0 99.98
```

在此示例中，vCPU 19 和 vCPU 28 的核心均以 3.2 GHz 的频率运行，而其他核心处于等待指令的 c1 C 状态。虽然运行中的核心没有达到其最大睿频加速频率，但非活动核心对新请求的响应速度将比其处于深层 c6 C 状态时快得多。

变化最少的基准性能

您可以通过 P 状态减少处理器频率的变化。P 状态控制核心的所需性能（以 CPU 频率的形式）。大多数工作负载在 P0 状态下性能更好，该状态要求采用睿频加速频率。但是，您可能需要调校系统以获得稳定性能而非突发式性能，而突发式性能可能会在启用睿频加速频率后出现。

Intel 高级矢量扩展 (AVX 或 AVX2) 工作负载能够以较低的频率较好地运行，而 AVX 指令也可以使用更多性能。通过禁用睿频加速来以较低的频率运行处理器，可以降低所使用的性能并保持更稳定的速度。有关优化您的实例配置和 AVX 工作负载的更多信息，请参阅 <http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/performance-xeon-e5-v3-advanced-vector-extensions-paper.pdf>。

此部分介绍了如何限制深层睡眠状态以及禁用睿频加速 (通过请求 P1 P 状态)，从而为这些类型的工作负载提供低延迟和最少的处理器速度变化。

限制 Amazon Linux 上的深层睡眠状态并禁用睿频加速

1. 使用您选择的编辑器打开 /boot/grub/grub.conf 文件。

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. 编辑第一个条目的 kernel 行并添加 intel_idle.max_cstate=1 选项，将 c1 设为空闲核心的最深层 C 状态。

```
# created by imagebuilder
default=0
timeout=1
hiddenmenu

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
intel_idle.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

3. 保存文件并退出您的编辑器。
4. 重启实例以启用新的内核选项。

```
[ec2-user ~]$ sudo reboot
```

5. 如果您需要 P1 P 状态提供的较少的处理器速度变化，请执行以下命令禁用睿频加速。

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

6. 在工作负载完成后，您可以使用以下命令重新启用睿频加速。

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

以下示例显示的 c4.8xlarge 实例具有两个以基准核心频率有效执行工作的 vCPU，这两个 vCPU 均没有启用睿频加速。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5389] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM%
      5.59 2.90 2.90    0 94.41  0.00  0.00  0.00  0.00  0.00  0.00  0.00
128.48 33.54 200.00  0.00
0   0   0   0.04 2.90 2.90    0 99.96  0.00  0.00  0.00  0.00  0.00  0.00
65.33 19.02 100.00  0.00
0   0   18  0.04 2.90 2.90    0 99.96  0.00  0.00  0.00
0   1   1   0.05 2.90 2.90    0 99.95  0.00  0.00  0.00
0   1   19  0.04 2.90 2.90    0 99.96
0   2   2   0.04 2.90 2.90    0 99.96  0.00  0.00  0.00
0   2   20  0.04 2.90 2.90    0 99.96
```

```
0   3   3   0.05 2.90 2.90   0   99.95   0.00   0.00   0.00
0   3   21  99.95 2.90 2.90   0   0.05
...
1   1   28  99.92 2.90 2.90   0   0.08
1   2   11  0.06 2.90 2.90   0   99.94   0.00   0.00   0.00
1   2   29  0.05 2.90 2.90   0   99.95
```

vCPU 21 和 vCPU 28 的核心以 2.9 GHz 的基准处理器速度有效执行工作，而所有非活动核心也在 c1 C 状态下以基准速度运行，准备接受指令。

为 Linux 实例设置时间

对于许多服务器任务和进程来说，准确一致的时间参考是非常重要的。大多数系统日志包含时间戳，您可以用来确定问题发生的时间以及事件发生的顺序。如果您使用 AWS CLI 或 AWS 开发工具包从您的实例发送请求，这些工具会以您的名义签署请求。如果您的实例的日期和时间设置不正确，签名中的日期可能与请求的日期不匹配，进而导致 AWS 拒绝请求。默认情况下，Amazon Linux 实例配置网络时间协议 (NTP)，系统时间与 Internet 上公用服务器的负载均衡池进行同步，设置为 UTC 时区。有关 NTP 的更多信息，请访问 <http://www.ntp.org/>。

任务

- [更改时区 \(p. 286\)](#)
- [配置网络时间协议 \(NTP\) \(p. 287\)](#)

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

更改时区

默认情况下，Amazon Linux 实例设置为 UTC (协调世界时) 时区，但是您可能想将实例上的时间更改为本地时间或网络中的其他时区。

更改实例上的时区

1. 确定将在实例上使用的时区。`/usr/share/zoneinfo` 目录包含时区数据文件的层次结构。浏览该位置的目录结构，查找针对您的时区的文件。

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile     GB          Indian       Mideast    posixrules  US
America    CST6CDT  GB-Eire    Iran         MST        PRC        UTC
Antarctica Cuba      GMT        iso3166.tab MST7MDT   PST8PDT   WET
Arctic      EET       GMT0       Israel      Navajo    right     W-SU
...
```

该位置的部分条目是目录 (如 `America`)，这些目录包含针对特定城市的时区文件。查找要用于实例的城市 (或时区中的一个城市)。在该示例中，您可以使用洛杉矶的时区文件 `/usr/share/zoneinfo/America/Los_Angeles`。

2. 使用新时区更新 `/etc/sysconfig/clock` 文件。
 - a. 使用您常用的文本编辑器 (如 vim 或 nano) 打开 `/etc/sysconfig/clock` 文件。您需要在编辑器命令中使用 sudo，因为 `/etc/sysconfig/clock` 归 root 所有。
 - b. 查找 `ZONE` 条目，将其更改为时区文件 (省略路径的 `/usr/share/zoneinfo` 部分)。例如，若要更改为洛杉矶时区，请将 `ZONE` 条目更改为以下内容。

```
ZONE="America/Los_Angeles"
```

Note

请勿将 `UTC=true` 条目更改为其他值。此条目用于硬件时钟；如果您在实例上设置了其他时区，则无需调整此条目。

- c. 保存文件，退出文本编辑器。
3. 在 `/etc/localtime` 与时区文件之间创建一个符号链接，以便实例在引用本地时间信息时找到此时区文件。

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. 重启系统，以便所有服务和应用程序接受新时区信息。

```
[ec2-user ~]$ sudo reboot
```

配置网络时间协议 (NTP)

默认情况下，Amazon Linux 实例上配置网络时间协议 (NTP)；但是，实例需要访问 Internet 才能使标准 NTP 配置工作。此外，您的实例的安全组规则必须允许端口 123 (NTP) 的出站 UDP 流量，您的网络 ACL 规则必须允许端口 123 的入站和出站 UDP 流量。本部分中的过程介绍如何验证默认 NTP 配置是否正常工作。如果您的实例无法访问 Internet，您需要将 NTP 配置为在您的私有网络中查询其他服务器，以便保持准确时间。

验证 NTP 是否正常运行

1. 使用 `ntpstat` 命令，查看实例上 NTP 服务的状态。

```
[ec2-user ~]$ ntpstat
```

如果输出类似于以下输出，则 NTP 在实例上正常运行。

```
synchronised to NTP server (12.34.56.78) at stratum 3
    time correct to within 399 ms
    polling server every 64 s
```

如果输出状态为“unsynchronised”，请等待一分钟，然后再试。首次同步可能需要一分钟才能完成。

如果输出状态为“Unable to talk to NTP daemon. Is it running?”，您可能需要启动 NTP 服务，使它在启动时自动启动。

2. (可选) 您可以使用 `ntpq -p` 命令查看 NTP 服务器已知的对等方的列表及其状态的摘要。

```
[ec2-user ~]$ ntpq -p
      remote          refid      st t when poll reach   delay    offset  jitter
=====
+lttlemman.deekay  204.9.54.119    2 u    15   128  377    88.649    5.946   6.876
-bittorrent.tomh  91.189.94.4     3 u   133   128  377   182.673    8.001   1.278
*ntp3.junkemailf  216.218.254.202  2 u    68   128  377    29.377    4.726  11.887
+tesla.selinc.co  149.20.64.28    2 u    31   128  377    28.586   -1.215   1.435
```

如果此命令的输出未显示任何活动，请检查您的安全组、网络 ACL 或防火墙是否已阻止对 NTP 端口的访问。

启动和启用 NTP

1. 使用以下命令启动 NTP 服务。

```
[ec2-user ~]$ sudo service ntpd start
Starting ntpd:                                     [ OK ]
```

2. 利用 chkconfig 命令，启用 NTP，以便在系统启动时启动。

```
[ec2-user ~]$ sudo chkconfig ntpd on
```

3. 使用以下命令验证是否启用了 NTP。

```
[ec2-user ~]$ sudo chkconfig --list ntpd
ntpda          0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

在这里，ntpda 在运行级别 2、3、4 和 5 上为启用状态，这是正确的。

更改 NTP 服务器

您可以决定不使用标准 NTP 服务器，或者您可能需要在自己的私有网络中将自己的 NTP 服务器用于无法访问 Internet 的实例。

1. 打开常用文本编辑器（如 vim 或 nano）中的 /etc/ntp.conf 文件。您需要在编辑器命令中使用 sudo，因为 /etc/ntp.conf 由 root 拥有。
2. 查找 server 部分，这里定义了将针对 NTP 配置进行轮询的服务器。

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.amazon.pool.ntp.org iburst
server 1.amazon.pool.ntp.org iburst
server 2.amazon.pool.ntp.org iburst
server 3.amazon.pool.ntp.org iburst
```

Note

n.amazon.pool.ntp.org DNS 记录旨在对来自 AWS NTP 流量进行负载均衡。但是，这些公有 NTP 服务器位于 pool.ntp.org 项目中，不归 AWS 所有和管理。我们不能保证这些服务器位于您的实例附近的地理位置，甚至不能保证它们位于 AWS 网络中。有关更多信息，请参阅 <http://www.pool.ntp.org/en/>。

3. 通过将“#”字符添加到您不需要使用的服务器定义的开头，注释掉这些服务器。

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.amazon.pool.ntp.org iburst
#server 1.amazon.pool.ntp.org iburst
#server 2.amazon.pool.ntp.org iburst
#server 3.amazon.pool.ntp.org iburst
```

4. 为每个要进行时间同步轮询的服务器添加一个条目。您可以对此条目使用 DNS 名称，或者点分四节 IP 地址（如 10.0.0.254）。

```
server my-ntp-server.my-domain.com iburst
```

5. 重新启动 NTP 服务，以接受这些新服务器。

```
[ec2-user ~]$ sudo service ntpd start
```

```
Starting ntpd:
```

```
[ OK ]
```

- 验证新设置是否工作，以及 NTP 是否功能正常。

```
[ec2-user ~]$ ntpstat
synchronised to NTP server (64.246.132.14) at stratum 2
    time correct to within 99 ms
```

更改 Linux 实例的主机名

当您启动实例时，实例会分配到一个主机名，其形式为私有内部 IPv4 地址。典型的 Amazon EC2 私有 DNS 名称如下所示：ip-12-34-56-78.us-west-2.compute.internal，其中包含内部域、服务（在此示例中为 compute）、区域和某种形式的私有 IPv4 地址。当您登录实例时，Shell 提示符处显示此主机名的一部分（例如，ip-12-34-56-78）。每次停止和重新启动 Amazon EC2 实例时（除非您使用的是弹性 IP 地址），公有 IPv4 地址都会改变，而且公有 DNS 名称、系统主机名和 Shell 提示符也会改变。在 EC2-Classic 中启动的实例在停止和重新启动时，也会收到新的私有 IPv4 地址、私有 DNS 主机名和系统主机名；而在 VPC 中启动的实例则不会收到这些内容。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

更改系统主机名

如果为实例的 IP 地址注册了公用 DNS 名称（如 webserver.mydomain.com），则可以设置系统主机名，以便实例将自己标识为该域的一部分。这还会更改 Shell 提示符，以便它显示此名称的第一部分，而不是 AWS 提供的主机名（例如，ip-12-34-56-78）。如果没有注册公用 DNS 名，还是可以更改主机名，但过程略有差异。

将系统主机名更改为公用 DNS 名称

如果已注册了公用 DNS 名称，请执行此过程。

- 在您的实例上，在您常用的文本编辑器中打开 /etc/sysconfig/network 配置文件，更改 HOSTNAME 条目以反映完全限定域名（例如 webserver.mydomain.com）。

```
HOSTNAME=webserver.mydomain.com
```

- 重启实例以接受新主机名。

```
[ec2-user ~]$ sudo reboot
```

或者，您可以使用 Amazon EC2 控制台重启（在 Instances 页面上，依次选择 Actions、Instance State 和 Reboot）。

- 登录实例，验证主机名是否已更新。您的提示应显示新主机名（显示第一个“.”之前的部分）。并且 hostname 命令应显示完全限定域名。

```
[ec2-user@webserver ~]$ hostname
webserver.mydomain.com
```

在无公用 DNS 名称的情况下更改系统主机名

- 在您常用的文本编辑器中打开 /etc/sysconfig/network 配置文件，更改 HOSTNAME 条目以反映所需的系统主机名（例如 webserver）。

```
HOSTNAME=webserver.localdomain
```

- 在您常用的文本编辑器中打开 /etc/hosts 文件，更改以 127.0.0.1 开始的条目，以匹配以下示例，替换为您自己的主机名。

```
127.0.0.1 webserver.localdomain webserver localhost4 localhost4.localdomain4
```

- 重启实例以接受新主机名。

```
[ec2-user ~]$ sudo reboot
```

或者，您可以使用 Amazon EC2 控制台重启（在 Instances 页面上，依次选择 Actions、Instance State 和 Reboot）。

- 登录实例，验证主机名是否已更新。您的提示应显示新主机名（显示第一个“.”之前的部分）。并且 hostname 命令应显示完全限定域名。

```
[ec2-user@webserver ~]$ hostname  
webserver.localdomain
```

在不影响主机名的情况下更改 Shell 提示符

如果不修改实例的主机名，但是希望显示比 AWS 提供的专用名称（例如 webserver）更有用的系统名称（如 ip-12-34-56-78），您可以编辑 Shell 提示符配置文件，以显示系统别名，而不是主机名。

将 Shell 提示符更改为别名

- 在 /etc/profile.d 中创建一个文件，将名为 NICKNAME 的环境变量设置为要在 Shell 提示符中显示的值。例如，若要将系统别名设置为 webserver，请执行以下命令。

```
[ec2-user ~]$ sudo sh -c 'echo "export NICKNAME=webserver" > /etc/profile.d/prompt.sh'
```

- 在您的常用文本编辑器（如 vim 或 nano）中打开 /etc/bashrc 文件。您需要在编辑器命令中使用 sudo，因为 /etc/bashrc 由 root 拥有。
- 编辑文件，将 Shell 提示符变量（\$PS1）更改为显示别名而不是主机名。在 /etc/bashrc 中找到以下设置 Shell 提示符的行（为了上下文需要，下面多显示了几行；查找以 ["\$PS1" 开头的行）：

```
# Turn on checkwinsize  
shopt -s checkwinsize  
[ "$PS1" = "\s-\v\$ " ] && PS1="\u@\h \w\$ "  
# You might want to have e.g. tty in prompt (e.g. more virtual machines)  
# and console windows
```

将该行中的 \h（hostname 的符号）更改为 NICKNAME 变量的值。

```
# Turn on checkwinsize  
shopt -s checkwinsize  
[ "$PS1" = "\s-\v\$ " ] && PS1="\u@$NICKNAME \w\$ "  
# You might want to have e.g. tty in prompt (e.g. more virtual machines)  
# and console windows
```

- （可选）要将 Shell 窗口上的标题设置为新别名，请完成以下步骤。

- a. 创建名为 /etc/sysconfig/bash-prompt-xterm 的文件。

```
[ec2-user ~]$ sudo touch /etc/sysconfig/bash-prompt-xterm
```

- b. 使用以下命令使该文件可执行。

```
[ec2-user ~]$ sudo chmod +x /etc/sysconfig/bash-prompt-xterm
```

- c. 在您常用的文本编辑器 (如 vim 或 nano) 中打开 /etc/sysconfig/bash-prompt-xterm 文件。您需要在编辑器命令中使用 sudo，因为 /etc/sysconfig/bash-prompt-xterm 归 root 所有。
d. 将以下行添加到该文件。

```
echo -ne "\033]0;${USER}@${NICKNAME}: ${PWD/#$HOME/~}\007"
```

5. 注销，再重新登录，以接受新别名值。

更改其他 Linux 分配上的主机名

上述步骤仅适用于 Amazon Linux。有关其他 Linux 分配的更多信息，请参阅其特定文档和下列文章：

- 如何为运行 RHEL 7 或 Centos 7 的私有 Amazon EC2 实例分配静态主机名？
- 如何为运行 SuSe Linux 的私有 Amazon EC2 实例分配静态主机名？
- 如何为运行 Ubuntu Linux 的私有 Amazon EC2 实例分配静态主机名？

在 Linux 实例上设置动态 DNS

当您启动 EC2 实例时，系统会为它分配公有 IP 地址和公有 DNS (域名系统) 名称，可以用来从 Internet 访问它。因为 Amazon Web Services 域中有非常多主机，所以这些公用名称必须足够长才能使每个名称保持唯一。典型的 Amazon EC2 公用 DNS 名称如下所示：ec2-12-34-56-78.us-west-2.compute.amazonaws.com，其中名称由 Amazon Web Services 域、服务 (在此示例中为 compute)、区域和公有 IP 地址的形式组成。

动态 DNS 服务在其区域中提供自定义主机名，这些主机名便于记忆，也与主机的使用案例更为相关；其中一些服务是免费的。您可以对 Amazon EC2 使用动态 DNS 提供商，可以将实例配置为每次实例启动时都更新与公用 DNS 名称关联的 IP 地址。有许多不同的提供商可以选择，本指南不介绍有关如何选择提供商以及如何向它们注册名称的具体详细信息。

Important

这些过程适用于 Amazon Linux。有关其他发布版本的更多信息，请参阅其具体文档。

对 Amazon EC2 使用动态 DNS

1. 向动态 DNS 服务提供商注册并利用其服务注册公用 DNS 名称。这个过程使用来自 [noip.com/free](#) 的免费服务作为示例。
2. 配置动态 DNS 更新客户端。有了动态 DNS 服务提供商并且使用其服务注册了公用 DNS 名称后，将 DNS 名称指向实例的 IP 地址。很多提供商（包括 [noip.com](#)）允许您从您在其网站上的账户页手动执行此操作，不过很多也支持软件更新客户端。如果您在 EC2 实例上有更新客户端运行，则每次 IP 地址更改（如关机和重启后）都会更新动态 DNS 记录。在本例中，将安装 noip2 客户端，该客户端利用 [noip.com](#) 提供的服务。
 - a. 启用 Extra Packages for Enterprise Linux (EPEL) 存储库，以获取对 noip2 客户端的访问权。

Note

默认情况下，Amazon Linux 实例安装有 EPEL 存储库的 GPG 密钥和存储库信息；但是，Red Hat 和 CentOS 实例必须先安装 `epel-release` 软件包，然后您才能启用 EPEL

存储库。有关更多信息以及要下载此软件包的最新版本，请参阅 <https://fedoraproject.org/wiki/EPEL>。

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

- b. 安装 noip 软件包。

```
[ec2-user ~]$ sudo yum install -y noip
```

- c. 创建 noip2 配置文件。在提示时输入登录名和密码信息，并回答后续问题以配置客户端。

```
[ec2-user ~]$ sudo noip2 -C
```

3. 使用 chkconfig 命令启用 noip 服务。

```
[ec2-user ~]$ sudo chkconfig noip on
```

您可以使用 chkconfig --list 命令验证此服务是否已启用。

```
[ec2-user ~]$ chkconfig --list noip
noip           0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

在这里，noip 在运行级别 2、3、4 和 5 为 on (这是正确的)。现在，每次启动时，更新客户端都会启动并更新公用 DNS 记录，以便指向实例的 IP 地址。

4. 启动 noip 服务。

```
[ec2-user ~]$ sudo service noip start
Starting noip2:                                         [    OK    ]
```

该命令启动客户端，读取先前创建的配置文件 (/etc/no-ip2.conf)，并且更新您选择的公用 DNS 名称的 IP 地址。

5. 验证更新客户端是否已为动态 DNS 名称设置了正确的 IP 地址。等待几分钟使 DNS 记录进行更新，然后尝试使用您在此过程中配置的公有 DNS 名称通过 SSH 连接到实例。

启动时在 Linux 实例上运行命令

当您在 Amazon EC2 中启动实例时，您可以选择将用户数据传递到可用于执行常见自动配置任务甚至在实例启动后运行脚本的实例。您可以将两类用户数据传递到 Amazon EC2：Shell 脚本和 cloud-init 指令。您还可以将这些数据以纯文本、文件 (这非常适合通过命令行工具启动实例) 或者 base64 编码文本 (用于 API 调用) 的形式传递到启动向导中。

如果您对更复杂的自动方案感兴趣，可以考虑使用 AWS CloudFormation 和 AWS OpsWorks。有关更多信息，请参阅 [AWS CloudFormation 用户指南](#) 和 [AWS OpsWorks 用户指南](#)。

有关在启动时在 Windows 实例上运行命令的信息，请参阅 Amazon EC2 用户指南 (适用于 Windows 实例) 中的 [执行用户数据](#) 和 [管理 Windows 实例配置](#)。

在以下示例中，[安装 LAMP Web 服务器教程 \(p. 26\)](#) 中的命令转换成了 Shell 脚本和一组 cloud-init 指令，在实例启动时执行。在每个示例中，以下任务都根据用户数据执行：

- 更新发布版软件包。
- 安装必要的 Web 服务器、php 和 mysql 程序包。
- 通过 chkconfig 启动和打开 httpd 服务。
- 添加 www 组，将 ec2-user 添加到该组。

- 为 Web 目录以及其中的文件设置适当的所有权和文件权限。
- 创建简单网页来测试 Web 服务器和 php 引擎。

Note

默认情况下，用户数据和 cloud-init 指令仅在您启动实例时的首次启动循环过程中运行。但是，AWS Marketplace 供应商和第三方 AMI 的所有者可能会提供自己的自定义项来确定脚本运行的方式和时间。

内容

- [先决条件 \(p. 293\)](#)
- [用户数据和 Shell 脚本 \(p. 293\)](#)
- [用户数据和 cloud-init 指令 \(p. 294\)](#)
- [API 和 CLI 概述 \(p. 295\)](#)

先决条件

以下示例假设实例具有可从 Internet 访问的公用 DNS 名称。有关更多信息，请参阅 [步骤 1：启动实例 \(p. 21\)](#)。您还必须将安全组配置为允许 SSH(端口 22)、HTTP(端口 80) 和 HTTPS(端口 443) 连接。有关这些先决条件的更多信息，请参阅 [Amazon EC2 的设置 \(p. 15\)](#)。

此外，这些指令适用于 Amazon Linux，这些命令和指令可能不适用于其他 Linux 发布版。有关其他发布版的更多信息，如它们对 cloud-init 的支持，请参阅其具体文档。

用户数据和 Shell 脚本

如果您熟悉 Shell 脚本编写，要在启动时将指令发送到实例，这是最简单、最完整的方式，cloud-init 输出日志文件 (`/var/log/cloud-init-output.log`) 捕获控制台输出，因此，如果实例出现意外行为，可在启动后方便地调试脚本。

Important

启动实例后，用户数据脚本和 cloud-init 指令仅在首次启动循环过程中运行。

用户数据 Shell 脚本必须以 `#!` 字符以及指向要读取脚本的解释器的路径 (通常为 `/bin/bash`) 开头。有关 Shell 脚本的精彩介绍，请参阅 Linux 文档项目 (tldp.org) 的 [BASH 编程方法](#)。

作为用户数据输入的脚本是作为 `root` 用户加以执行的，因此在脚本中不使用 `sudo` 命令。请注意，您创建的任何文件都将归 `root` 所有；如果您需要非 `root` 用户具有文件访问权，应在脚本中相应地修改权限。此外，这是因为脚本不交互运行，所以无法包含要求用户反馈的命令 (如 `yum update`，无 `-y` 标志)。

在启动时添加这些任务会增加启动实例所需的时间。您应多等待几分钟让这些任务完成，然后测试用户脚本是否已成功完成。

将 Shell 脚本传递到具有用户数据的实例

1. 根据[从 AMI 启动实例 \(p. 244\)](#)的实例启动过程操作，但是，到达[Step 6 \(p. 245\)](#)时，将用户数据脚本文本粘贴到 User data 字段中，然后完成启动过程。对于以下示例，脚本创建并配置我们的 Web 服务器。

```
#!/bin/bash
yum update -y
yum install -y httpd24 php56 mysql55-server php56-mysqlnd
service httpd start
chkconfig httpd on
groupadd www
usermod -a -G www ec2-user
chown -R root:www /var/www
```

```
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} +
find /var/www -type f -exec chmod 0664 {} +
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

2. 让实例有足够的时间启动和执行脚本中的命令，然后查看脚本是否完成了预期的任务。对于我们的示例，在 Web 浏览器中输入脚本创建的 PHP 测试文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该可以看到 PHP 信息页面。

Tip

如果您未能看到 PHP 信息页，请检查所用的安全组是否包含允许 HTTP (端口 80) 通信的规则。
有关将 HTTP 规则添加到您安全组的信息，请参阅 [向安全组添加规则 \(p. 359\)](#)。

3. (可选) 如果脚本没有完成预期执行的任务，或者您要验证脚本是否正确完成，请检查 `/var/log/cloud-init-output.log` 上的 `cloud-init` 输出日志文件，在输出中查找错误消息。

对于其他调试信息，您可以使用以下指令创建包含 `cloud-init` 数据部分的 Mime 分段存档：

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

此指令将您脚本的命令输出发送到 `/var/log/cloud-init-output.log`。有关 `cloud-init` 数据格式以及创建 Mime 分段存档的更多信息，请参阅 [cloud-init 格式](#)。

用户数据和 `cloud-init` 指令

`cloud-init` 程序包配置新 Amazon Linux 实例在启动时的特定方面；最值得注意的是，它为 `ec2-user` 配置 `.ssh/authorized_keys` 文件，以便您使用自己的私钥登录。

可在启动时将 `cloud-init` 用户指令传递给实例，方式与传递脚本相同，只是语法不同。有关 `cloud-init` 的更多信息，请转到 <http://cloudinit.readthedocs.org/en/latest/index.html>。

Important

启动实例后，用户数据脚本和 `cloud-init` 指令仅在首次启动循环过程中运行。

`cloud-init` 的 Amazon Linux 版本并不支持基程序包中可用的所有指令，其中一些指令已重命名（如 `repo_update`，而不是 `apt-upgrade`）。

在启动时添加这些任务会增加启动实例所需的时间。您应多等待几分钟让这些任务完成，然后测试用户数据指令是否已完成。

将 `cloud-init` 指令传递给具有用户数据的实例

1. 根据[从 AMI 启动实例 \(p. 244\)](#)的实例启动过程操作，但是，到达[Step 6 \(p. 245\)](#)时，将 `cloud-init` 指令文本粘贴到 User data 字段中，然后完成启动过程。对于以下示例，这些指令创建并配置 Web 服务器。

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd24
- php56
- mysql55-server
```

```
- php56-mysqlnd

runcmd:
- service httpd start
- chkconfig httpd on
- groupadd www
- [ sh, -c, "usermod -a -G www ec2-user" ]
- [ sh, -c, "chown -R root:www /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, + ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, + ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

- 让实例有足够的时问启动和执行用户数据中的指令，然后查看指令是否完成了预期的任务。对于我们的示例，在 Web 浏览器中输入指令创建的 PHP 测试文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该可以看到 PHP 信息页面。

Tip

如果您未能看到 PHP 信息页，请检查所用的安全组是否包含允许 HTTP (端口 80) 通信的规则。
有关将 HTTP 规则添加到您安全组的信息，请参阅 [向安全组添加规则 \(p. 359\)](#)。

- (可选) 如果指令没有完成预期执行的任务，或者您要验证指令是否正确完成，请检查 `/var/log/cloud-init-output.log` 上的 `cloud-init` 输出日志文件，在输出中查找错误消息。对于其他调试信息，您可以将以下行添加到指令：

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

该指令将 `runcmd` 输出发送到 `/var/log/cloud-init-output.log`。

API 和 CLI 概述

可以在启动过程中使用以下命令之一将用户数据传递给实例。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- AWS CLI：在 `run-instances` 命令中使用 `--user-data` 参数。使用 `file://` 前缀从文件传入用户数据。
- 适用于 Windows PowerShell 的 AWS 工具：在 `New-EC2Instance` 命令中使用 `-UserData` 参数。
- Amazon EC2 查询 API：在 `RunInstances` 命令中使用 `UserData` 参数。

实例元数据和用户数据

实例元数据 是有关您的实例的数据，可以用来配置或管理正在运行的实例。实例元数据可划分成不同类别。有关更多信息，请参阅 [实例元数据类别 \(p. 302\)](#)。

EC2 实例还可包括动态数据，例如启动实例时生成的实例身份文档。有关更多信息，请参阅 [动态数据类别 \(p. 305\)](#)。

您也可以访问在启动您的实例时所提供的用户数据。例如，您可指定参数以便配置实例，也可连接简单的脚本。您也可以使用这些数据来构建更多可通过启动时提供的配置文件来修改的通用 AMI。例如，如果您为各种小型企业运行 Web 服务器，则这些企业都可以使用相同的 AMI，并在启动时从您在用户数据中指定的 Amazon S3 存储桶中检索其各自的内容。要随时添加一个新客户，您只需为该客户创建一个存储桶，将客户的内容添加进去，然后启动您的 AMI 即可。如果您同时启动多个实例，则用户数据可供该预留中的所有实例使用。

Important

虽然您只能从实例自身内部访问实例元数据和用户数据，但数据并未进行加密保护。可访问实例的人员均可查看其元数据。因此，您应当采取适当的预防措施来保护敏感数据（例如永久加密密钥）。不应将敏感数据（例如密码）存储为用户数据。

内容

- [检索实例元数据 \(p. 296\)](#)
- [使用用户数据配置实例 \(p. 298\)](#)
- [检索用户数据 \(p. 299\)](#)
- [检索动态数据 \(p. 299\)](#)
- [示例：AMI 启动索引值 \(p. 300\)](#)
- [实例元数据类别 \(p. 302\)](#)
- [实例标识文档 \(p. 305\)](#)

检索实例元数据

由于您的正在运行的实例存在实例元数据，因此您无需使用 Amazon EC2 控制台或 AWS CLI。这在您编写脚本以实现从实例运行时非常有用。例如，您可从实例元数据访问您的实例的本地 IP 地址来以管理与外部应用程序的连接。

要从运行实例内部查看所有类别的实例元数据，请使用以下 URI：

```
http://169.254.169.254/latest/meta-data/
```

请注意，您无需为用于检索实例元数据和用户数据的 HTTP 请求付费。

您可以使用一种诸如 curl 的工具，或是如果实例支持，则可以使用 GET 命令；例如：

```
$ curl http://169.254.169.254/latest/meta-data/
```

```
$ GET http://169.254.169.254/latest/meta-data/
```

您也可以下载实例元数据查询工具，通过该工具，您无需键入完整的 URI 或目录名称就可以查询实例元数据：

<http://aws.amazon.com/code/1825>

所有实例元数据以文本形式返回（内容类型 text/plain）。对特定元数据资源的请求会返回一个相应的值，如果该资源不可用，则会返回 HTTP 错误代码 404 – Not Found。

对通用元数据资源的请求（以 / 结尾的 URI）会返回一个可用资源列表，如果此类资源不存在，则会返回 HTTP 错误代码 404 – Not Found。列表中的各个项目位于被换行符（ASCII 10）终止的不同的行上。

检索实例元数据的示例

此示例可以获取实例元数据的可用版本。这些版本不一定与 Amazon EC2 API 版本相关联。如果您有依赖于以前版本中所存在的结构和信息的脚本，则您可使用早期版本。

```
$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
```

```
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
latest
```

此示例获得顶级元数据项目。一些项目只可用于 VPC 中的实例。有关这些项目中每一项的更多信息，请参阅[实例元数据类别 \(p. 302\)](#)。

```
$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
instance-action
instance-id
instance-type
kernel-id
local-hostname
local-ipv4
mac
network/
placement/
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

这些示例获得前面示例中的一些元数据项目的值。

```
$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-12345678
```

```
$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-fea54097
```

```
$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

此示例获得可用公共密钥的列表。

```
$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

此示例显示了公用密钥 0 可用的格式。

```
$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

此示例获得公用密钥 0 (以 OpenSSH 密钥格式)。

```
$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAFICCQD6m7oRw0uXOjANBgqhkkiG9w0BAQFADCBiDELMAkGA1UEBhMC
VVVmxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAstC01BTsBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEg5vb25lQGFTYXpbvi5jb20wHcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAstC01BTsBDb25z
b2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFT
YXpbvi5jb20wgZ8wDQYJKoZIhvCNQEQBBQADgY0AMIGJAOGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/Mb0ITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAARHd1QWIMm2nrAgMBAAEwDQYJKoZIhvCNQEQFBQADgYEAtCu4
nUhVvxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5inNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYSS5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQU5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

此示例显示可用于 EC2-Classic 平台中 NAT 实例上特定网络接口 (由 MAC 地址表示) 的信息。

```
$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/
device-number
local-hostname
local-ipv4s
mac
owner-id
public-hostname
public-ipv4s
```

此示例获得启动至 VPC 的实例的子网 ID。

```
$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/
subnet-id
subnet-be9b61d7
```

限制

我们基于每个实例来限制对实例元数据服务的查询，并且，我们对从实例到实例元数据服务的同时连接数进行限制。

如果您在使用实例元数据服务检索 AWS 安全凭证，请避免在每个事务期间查询凭证或从大量线程或进程中并发查询，因为这可能导致限制。相反，我们建议您缓存凭证，直到凭证开始接近其到期时间。

如果您在访问实例元数据服务时受限，请用指数回退策略重试查询。

使用用户数据配置实例

指定用户数据时，请注意以下几点：

- 用户数据会被视为非透明数据；您提供什么数据您就会得到什么数据。由实例对其进行解释。
- 用户数据被限制在 16 KB 以内。这种限制适用于原始形式的数据，而不是 Base64 编码形式的数据。
- 用户数据必须在提交给 API 前先进行 Base64 编码。AWS CLI 和 Amazon EC2 控制台为您执行 base64 编码。在提交给实例之前，数据会被解码。有关 base64 编码的更多信息，请参阅 <http://tools.ietf.org/html/rfc4648>。
- 用户数据仅在启动时执行。如果停止实例，修改用户数据，然后启动实例，则新的用户数据不会自动执行。

在启动实例时指定用户数据

您可在启动实例时指定用户数据。有关更多信息，请参阅 [启动实例 \(p. 244\)](#)、[cloud-init \(p. 125\)](#) 和[启动时在 Linux 实例上运行命令 \(p. 292\)](#)。

为正在运行的实例修改用户数据

您可以修改现有实例的用户数据。如果实例正在运行，必须首先停止实例。在重启您的实例之后，新用户数据在实例上可用。

修改 Amazon EBS 支持的实例的用户数据

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 单击 Actions，选择 Instance State，然后选择 Stop。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，单击 Yes, Stop。停止实例可能需要几分钟时间。
5. 在实例仍处于选中状态的情况下，选择 Actions，选择 Instance Settings，然后选择 View/Change User Data。请注意，如果实例正在运行，您不能更改用户数据，但是可以查看。
6. 在 View/Change User Data 对话框中，更新用户数据，然后选择 Save。

检索用户数据

要检索用户数据，请使用以下 URI：

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

请求用户数据时，所返回的是未经任何更改的原样数据（内容类型 application/octet-stream）。

此处显示的是返回逗号分隔用户数据的示例。

```
$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

此处显示的是返回行分隔的用户数据的示例。

```
$ curl http://169.254.169.254/latest/user-data
[general]
instances: 4

[instance-0]
s3-bucket: <user_name>

[instance-1]
reboot-on-error: yes
```

检索动态数据

要在运行实例内部检索动态数据，请使用以下 URI：

```
http://169.254.169.254/latest/dynamic/
```

此示例介绍如何检索高级实例标识类别：

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/  
pkcs7  
signature  
document
```

有关动态数据的详细信息和如何对其进行检索的示例，请参阅 [实例标识文档 \(p. 305\)](#)。

示例：AMI 启动索引值

本示例演示如何使用用户数据和实例元数据来配置实例。

Alice 想要启动她最喜欢的数据库 AMI 的四个实例，第一个实例用作主实例，其余三个用作副本。当她启动它们时，她想为每个副本添加有关复制策略的用户数据。她知道这些数据将对所有四个实例都可用，因此她所采用的用户数据构建方式必须能够让每个实例识别出哪些部分适用于自己。她可通过 `ami-launch-index` 实例元数据值来实现这一点，该值对每个实例都是唯一的。

以下是 Alice 所构建的用户数据：

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

`replicate-every=1min` 数据定义第一个副本的配置，`replicate-every=5min` 定义第二个副本的配置，以此类推。Alice 决定以 ASCII 字符串形式提供这些数据，用竖线符号 (|) 来分隔每个实例的数据。

Alice 使用 `run-instances` 命令启动四个实例，并指定以下用户数据：

```
aws ec2 run-instances --image-id ami-12345678 --count 4 --instance-type t2.micro --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

实例启动之后，所有实例都有以下用户数据和常用元数据的副本：

- AMI id: ami-12345678
- 预留 ID : r-1234567890abcabc0
- 公用密钥：无
- 安全组名称：默认值
- 实例类型 : t2.micro

然而，每个实例都包含某些特定的元数据。

实例 1

| 元数据 | 值 |
|------------------|--|
| instance-id | i-1234567890abcdef0 |
| ami-launch-index | 0 |
| public-hostname | ec2-203-0-113-25.compute-1.amazonaws.com |
| public-ipv4 | 67.202.51.223 |
| local-hostname | ip-10-251-50-12.ec2.internal |
| local-ipv4 | 10.251.50.35 |

实例 2

| 元数据 | 值 |
|------------------|---|
| instance-id | i-0598c7d356eba48d7 |
| ami-launch-index | 1 |
| public-hostname | ec2-67-202-51-224.compute-1.amazonaws.com |
| public-ipv4 | 67.202.51.224 |
| local-hostname | ip-10-251-50-36.ec2.internal |
| local-ipv4 | 10.251.50.36 |

实例 3

| 元数据 | 值 |
|------------------|---|
| instance-id | i-0ee992212549ce0e7 |
| ami-launch-index | 2 |
| public-hostname | ec2-67-202-51-225.compute-1.amazonaws.com |
| public-ipv4 | 67.202.51.225 |
| local-hostname | ip-10-251-50-37.ec2.internal |
| local-ipv4 | 10.251.50.37 |

实例 4

| 元数据 | 值 |
|------------------|---|
| instance-id | i-1234567890abcdef0 |
| ami-launch-index | 3 |
| public-hostname | ec2-67-202-51-226.compute-1.amazonaws.com |
| public-ipv4 | 67.202.51.226 |
| local-hostname | ip-10-251-50-38.ec2.internal |
| local-ipv4 | 10.251.50.38 |

Alice 可以使用 ami-launch-index 值确定用户数据的哪个部分适用于哪个特定实例。

1. 她连接到其中一个实例并检索该实例的 ami-launch-index，以确保该实例是副本之一：

```
$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

2. 她将 ami-launch-index 另存为变量：

```
$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-launch-index`
```

3. 她将用户数据另存为变量：

```
$ user_data=`curl http://169.254.169.254/latest/user-data/`
```

4. 最后，Alice 使用 cut 命令提取适用于该实例的用户数据部分：

```
$ echo $user_data | cut -d"|" -f"$ami_launch_index"  
replicate-every=5min
```

实例元数据类别

下表列举了实例元数据的类别。

| Data | 说明 | 引入的版本 |
|-------------------------------------|--|------------|
| ami-id | 用于启动实例的 AMI ID。 | 1.0 |
| ami-launch-index | 如果您同时启动了多个实例，此值表示实例启动的顺序。第一个启动的实例的值是 0。 | 1.0 |
| ami-manifest-path | 指向 Amazon S3 中的 AMI 清单文件的路径。如果您使用 Amazon EBS 支持的 AMI 来启动实例，则返回的结果为 unknown。 | 1.0 |
| ancestor-ami-ids | 为创建此 AMI 而重新绑定的任何实例的 AMI ID。仅当 AMI 清单文件包含一个 ancestor-ams 密钥时，此值才存在。 | 2007-10-10 |
| block-device-mapping/ami | 包含根/启动文件系统的虚拟设备。 | 2007-12-15 |
| block-device-mapping/ebs 否 | 与 Amazon EBS 卷相关联的虚拟设备（如果存在）。如果 Amazon EBS 卷在启动时存在或者在上一次启动该实例时存在，那么这些卷仅在元数据中可用。N 表示 Amazon EBS 卷的索引（例如 ebs1 或 ebs2）。 | 2007-12-15 |
| block-device-mapping/ephemeral 否 | 与短暂设备相关联的虚拟设备，如果存在的话。N 表示临时卷的索引。 | 2007-12-15 |
| block-device-mapping/root | 与根设备相关联的虚拟设备或分区，或虚拟设备上的分区（在根（/ 或 C：）文件系统与给定实例相关联的情况下）。 | 2007-12-15 |
| block-device-mapping/swap | 与 swap 相关联的虚拟设备。并不总是存在。 | 2007-12-15 |
| hostname | 实例的私有 IPv4 DNS 主机名。在存在多个网络接口的情况下，其指的是 eth0 设备（设备号为 0 的设备）。 | 1.0 |
| iam/info | 如果存在与实例关联的 IAM 角色，则包含有关实例配置文件上次更新时间的信息（包括实例的 LastUpdated 日期、InstanceProfileArn 和 | 2012-01-12 |

| Data | 说明 | 引入的版本 |
|---|--|----------------|
| | InstanceProfileId)。如果没有，则不显示。 | |
| iam/security-credentials/role-name | 如果存在与实例关联的 IAM 角色，则 <i>role-name</i> 为角色的名称，并且 <i>role-name</i> 包含与角色关联的临时安全凭证 (有关更多信息，请参阅 通过实例元数据检索安全证书 (p. 423))。如果没有，则不显示。 | 2012-01-12 |
| instance-action | 通知实例在准备打包时重新启动。有效值：none shutdown bundle-pending。 | 2008-09-01 |
| instance-id | 此实例的 ID。 | 1.0 |
| instance-type | 实例的类型。有关更多信息，请参阅 实例类型 (p. 135) 。 | 2007-08-29 |
| kernel-id | 此实例启动的内核的 ID，如果适用的话。 | 2008-02-01 |
| local-hostname | 实例的私有 IPv4 DNS 主机名。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。 | 2007-01-19 |
| local-ipv4 | 实例的私有 IPv4 地址。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。 | 1.0 |
| mac | 实例的媒体访问控制 (MAC) 地址。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/device-number | 与该接口相关联的唯一设备号。设备号与设备名称对应；例如，device-number 为 2 对应于 eth2 设备。此类别对应的是 Amazon EC2 API 和 AWS CLI 的 EC2 命令使用的 DeviceIndex 和 device-index 字段。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/ipv4-associations/public-ip | 与每个 public-ip 地址相关联并被分配给该接口的私有 IPv4 地址。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/ipv6s | 与接口相关联的 IPv6 地址。仅对启动至 VPC 的实例返回。 | 2016-06-30 |
| network/interfaces/macs/mac/local-hostname | 实例的本地主机名称。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/local-ipv4s | 与接口相关联的私有 IPv4 地址。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/mac | 该实例的 MAC 地址。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/owner-id | 网络接口拥有者的 ID。在多个接口的环境中，接口可由第三方连接，如 Elastic Load Balancing。接口拥有者需为接口上的流量付费。 | 2011 年 1 月 1 日 |

| Data | 说明 | 引入的版本 |
|---|--|----------------|
| network/interfaces/macs/mac/public-hostname | 接口的公有 DNS (IPv4)。如果实例在 VPC 中，则仅当 enableDnsHostnames 属性设置为 true 时返回此类别。有关更多信息，请参阅 在您的 VPC 中使用 DNS 。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/public-ipv4s | 与接口相关联的弹性 IP 地址。一个实例上可能有多个 IPv4 地址。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/security-groups | 网络接口所属的安全组。仅对启动至 VPC 的实例返回。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/security-group-ids | 网络接口所属的安全组的 ID。仅对启动至 VPC 的实例返回。有关 EC2-VPC 平台中安全组的更多信息，请参阅 您的 VPC 的安全组 。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/subnet-id | 接口所驻留的子网的 ID。仅对启动至 VPC 的实例返回。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/subnet-ipv4-cidr-block | 接口所在子网的 IPv4 CIDR 块。仅对启动至 VPC 的实例返回。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/subnet-ipv6-cidr-blocks | 接口所在子网的 IPv6 CIDR 块。仅对启动至 VPC 的实例返回。 | 2016-06-30 |
| network/interfaces/macs/mac/vpc-id | 接口所驻留的 VPC 的 ID。仅对启动至 VPC 的实例返回。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/vpc-ipv4-cidr-block | 接口所在 VPC 的 IPv4 CIDR 块。仅对启动至 VPC 的实例返回。 | 2011 年 1 月 1 日 |
| network/interfaces/macs/mac/vpc-ipv4-cidr-blocks | 接口所在 VPC 的 IPv4 CIDR 块。仅对启动至 VPC 的实例返回。 | 2016-06-30 |
| network/interfaces/macs/mac/vpc-ipv6-cidr-blocks | 接口所在 VPC 的 IPv6 CIDR 块。仅对启动至 VPC 的实例返回。 | 2016-06-30 |
| placement/availability-zone | 实例启动的可用区域。 | 2008-02-01 |
| product-codes | 与实例相关联的产品代码，如果有的话。 | 2007-03-01 |
| public-hostname | 实例的公有 DNS。如果实例在 VPC 中，则仅当 enableDnsHostnames 属性设置为 true 时返回此类别。有关更多信息，请参阅 在您的 VPC 中使用 DNS 。 | 2007-01-19 |
| public-ipv4 | 公有 IPv4 地址。如果弹性 IP 地址与实例相关联，返回的值是弹性 IP 地址。 | 2007-01-19 |
| public-keys/0/openssh-key | 公用密钥。仅在实例启动时提供了公用密钥的情况下可用。 | 1.0 |
| ramdisk-id | 启动时指定的 RAM 磁盘的 ID，如果适用的话。 | 2007-10-10 |

| Data | 说明 | 引入的版本 |
|------------------------------------|---|------------|
| <code>reservation-id</code> | 预留的 ID。 | 1.0 |
| <code>security-groups</code> | 应用到实例的安全组的名称。 启动之后，您只能更改正在 VPC 中运行的实例的安全组。这些更改将体现在此处和 <code>network/interfaces/macs/<i>mac</i>/security-groups</code> 中。 | 1.0 |
| <code>services/domain</code> | 用于区域的 AWS 资源的域；例如用于 <code>us-east-1</code> 的 <code>amazonaws.com</code> 。 | 2014-02-25 |
| <code>services/partition</code> | 资源所处的分区。对于标准 AWS 区域，分区是 <code>aws</code> 。如果资源位于其他分区，则分区是 <code>aws-<i>partitionname</i></code> 。例如，位于中国（北京）区域的资源的分区为 <code>aws-cn</code> 。 | 2015-10-20 |
| <code>spot/termination-time</code> | 竞价型实例操作系统将收到关闭信号的大致时间 (UTC)。仅当竞价型实例已由 Amazon EC2 标记为终止时，此项目才会出现并包含时间值（例如， <code>2015-01-05T18:02:00Z</code> ）。如果您自己终止了竞价型实例，那么终止时间项目不会设置时间。 | 2014-11-05 |

动态数据类别

下表列举了动态数据的类别。

| Data | 说明 | 引入的版本 |
|--|---|------------|
| <code>fws/instance-monitoring</code> | 显示客户是否在 CloudWatch 中启用了详细的一分钟监控的值。有效值： <code>enabled</code> <code>disabled</code> | 2009-04-04 |
| <code>instance-identity/document</code> | 包含实例属性（如实例 ID、私有 IP 地址等）的 JSON。请参阅 实例标识文档 (p. 305) 。 | 2009-04-04 |
| <code>instance-identity/pkcs7</code> | 用于验证签名的文档的真实性和内容。请参阅 实例标识文档 (p. 305) 。 | 2009-04-04 |
| <code>instance-identity/signature</code> | 可被其他各方用于验证来源和真实性的数据。请参阅 实例标识文档 (p. 305) 。 | 2009-04-04 |

实例标识文档

实例标识文档是描述实例的 JSON 文件。实例标识文档带有一个签名和一个 PKCS7 签名，这些签名可用于验证文档中提供的信息的准确性、来源和真实性。例如，您可能下载了包含付费更新的免费软件。

实例标识文档在实例启动时生成，并通过[实例元数据 \(p. 295\)](#)向实例公开。它会验证实例的属性，如订购的软件、实例大小、实例类型、操作系统和 AMI。

Important

由于实例标识文档和签名的动态性质，我们建议定期检索一次实例标识文档和签名。

获取实例标识文档和签名

若要取回实例身分文件，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/document

{
    "devpayProductCodes" : null,
    "availabilityZone" : "us-east-1d",
    "privateIp" : "10.158.112.84",
    "version" : "2010-08-31",
    "region" : "us-east-1",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t1.micro",
    "accountId" : "123456789012",
    "pendingTime" : "2015-11-19T16:32:11Z",
    "imageId" : "ami-5fb8c835",
    "kernelId" : "aki-919dcraf8",
    "ramdiskId" : null,
    "architecture" : "x86_64"
}
```

若要取回实例身分签名，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/signature

dExamplesjNQhhJan7pORLpLSr7lJEF4V2DhKGlyoYVBouYrY9njjyBCmhEayaGrhtS/AWY+LPx
1VSQURF5n0gwPNcuO6ICT0fNrm5IH7w9ydyaxexamplejJw8XvWPxbuRkcN0TAA1p4RtCAqm4ms
x2oALjWSCBExample=
```

若要取回 PKCS7 签名，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/pkcs7

MIICiITCCAfICCQD6m7oRw0uXojbABgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgnNVBAstC01BTSBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEg5vb25lQGFTYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0Mja0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgnNVBAstC01BTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFT
YXpvbi5jb20wgZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAoGBAMAk0dn+a4GmWIJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSgv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAArHhd1QWIImn2nrAgMBAAEwDQYJKoZIhvCNQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5inMzGxL0Fkb
FFBjvSfpJ1J00zbhNY5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQ05Yaxu2jXnimvw3rrszlaEXAMPLE
```

示例：验证 PKCS7 签名

通过该地区的AWS公有证书对您的实例进行确认，您可以使用PKCS7签名来对它进行验证。

针对所有公共区域的AWS公有证书如下：

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgCqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIExBXYYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
```

```
ODAxMDUxMjU2MTJaMFwxCzAJBrgNVBAYTA1VTMRkwFwYDVQOIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQOHEwdTZWF0dGx1MSAwHgYDVQOKExdBbWF6b24gV2ViIFN1
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMII1BHwKBgQCjkvcS2bb1VQ4yt/5e
ih5O06kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNnmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmBjNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0CaO/buyu1CiYQk40KNHCCHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5h08Wqd+aTeb+k2tn92BBPqeZqpWRa5P/+jrdKml1qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIZiqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6Rok0k9K
-----END CERTIFICATE-----
```

针对AWS GovCloud (US)地区的AWS公有证书如下：

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAQ0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBrgNVBAYTA1VTMRkw
FwYDVQOIExBXYXNoaW5ndG9u1FN0YXR1MRAwDgYDVQOHEwdTZWF0dGx1MSAwHgYD
VQOKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMII1BHwKBgQCjkvcS2bb1VQ4yt/5e
ih5O06kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNnmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmBjNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0CaO/buyu1CiYQk40KNHCCHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5h08Wqd+aTeb+k2tn92BBPqeZqpWRa5P/+jrdKml1qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIZiqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6Rok0k9K
-----END CERTIFICATE-----
```

有关AWS GovCloud (US)的更多信息，请参阅[AWS GovCloud \(US\) User Guide](#)。

对于其他地区，请联系AWS 支持以获取AWS公有证书。

验证 PKCS7 签名

- 在您的Amazon Linux实例上为PKCS7 签名创建一个临时文件：

```
PKCS7=$(mktemp)
```

- 在文档中加入-----BEGIN PKCS7-----标头，然后附加实例元数据的PKCS7 签名内容、新的一行和-----END PKCS7-----页脚。

```
echo "-----BEGIN PKCS7-----" > $PKCS7
```

```
curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> $PKCS7
```

```
echo "" >> $PKCS7
```

```
echo "-----END PKCS7-----" >> $PKCS7
```

- 为实例身份文件创建一份临时文件，并用您的实例的元数据的文件内容对它进行数据输入：

```
DOCUMENT=$(mktemp)
```

```
curl -s http://169.254.169.254/latest/dynamic/instance-identity/document > $DOCUMENT
```

4. 打开文本编辑器并创建名为 AWSpubkey 的文件。将上述 AWS 公有证书的内容复制粘贴到该文件内并保存。
5. 按照以下方法使用 OpenSSL 工具验证签名：

```
openssl smime -verify -in $PKCS7 -inform PEM -content $DOCUMENT -certfile AWSpubkey -  
noverify > /dev/null  
Verification successful
```

识别混合计算环境中的 EC2 实例

如果您在其他云基础设施上运行计算机资源，例如 Azure 或 Google Cloud Platform，或者如果您使用 VMware、Xen 或 KVM 提供的本地虚拟化，您也许可从通过单一方法来确定虚拟机是否为 EC2 实例中获益。本主题介绍了两种标识 EC2 实例的方法，一种方法快速但可能不准确，另一种方法更严谨明确。

检查 Xen 域 UUID

此部分中介绍的方法通过检查 Xen 域 UUID，以最优方式确定 Linux 虚拟机是否为 EC2 实例。此方法可检查 UUID 的起始 octet 中是否存在字符“ec2”或“EC2”。

Note

对于不在 EC2 中的 Xen 实例，包含这些字符的可能性也很小。

您可以使用以下方法来发现 Xen UUID。有关标识 Windows 实例的信息，请参阅http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/identify_ec2_instances.html。

- 在 Linux VM 上，运行以下命令：

```
$ cat /sys/hypervisor/uuid
```

这将返回 UUID：

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

在此示例中，前缀“ec2”指示您查看的可能是 EC2 实例。

- 或者，仅限在 HVM 实例上，桌面管理接口 (DMI) 中包含与系统序列号和系统 UUID (大写) 相同的 UUID：

```
$ sudo dmidecode --string system-serial-number  
ec2e1916-9099-7caf-fd21-01234example  
$ sudo dmidecode --string system-uuid  
EC2E1916-9099-7CAF-FD21-01234EXAMPLE
```

Note

与以前的方法不同，DMI 方法需要超级用户权限。不过，一些旧的 Linux 内核可能会通过 /sys/ 公开 UUID。

检查实例标识文档

对于标识 EC2 实例的明确且以加密方式验证的方法，请查看实例标识文档，包括其签名。这些文档适用于本地、不可路由地址 `http://169.254.169.254/latest/dynamic/instance-identity/` 处的每个 EC2 实例。有关更多信息，请参阅 [实例标识文档](#)。

监控 Amazon EC2

监控是保持 Amazon Elastic Compute Cloud (Amazon EC2) 实例和 AWS 解决方案的可靠性、可用性和性能的重要部分。您的 AWS 解决方案的所有组成部分都应收集监控数据，以便更轻松地调试出现的多点故障。但是，在开始监控 Amazon EC2 前，您应创建包括以下内容的监控计划：

- 您的监控目标是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

在定义监控目标并创建监控计划后，下一步是在您的环境中建立正常 Amazon EC2 性能的基准。您应该在不同时间和不同负载条件下测量 Amazon EC2 的性能。监控 Amazon EC2 时，您应存储所收集的监控数据的历史记录。您可将当前 Amazon EC2 性能与这些历史数据进行比较，这样可帮助您确定性能的正常模式和异常模式，找出解决问题的方法。例如，您可以监控 Amazon EC2 实例的 CPU 利用率、磁盘 I/O 和网络使用率。如果性能低于您所建立的基准，则您可能需要重新配置或优化实例以降低 CPU 使用率、改进磁盘 I/O 或减少网络流量。

要建立基准，您至少应监控以下各项：

| 要监控的项目 | Amazon EC2 指标 | 监控脚本/CloudWatch Logs |
|---------|----------------------------------|--|
| CPU 利用率 | CPU 利用率 (p. 322) | |
| 内存利用率 | | (Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs |
| 已用内存 | | (Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs |

| 要监控的项目 | Amazon EC2 指标 | 监控脚本/CloudWatch Logs |
|---|--------------------------------------|--|
| 可用内存 | | (Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs |
| 网络使用率 | 网络输入 (p. 322) 网络输出 (p. 322) | |
| 磁盘性能 | 磁盘读取操作 (p. 322) 磁盘写入操作 (p. 322) | |
| 磁盘交换分区利用率 (仅限 Linux 实例) 使用的交换空间 (仅限 Linux 实例) | | 为 Amazon EC2 Linux 实例监控内存和磁盘指标 |
| 页面文件利用率 (仅限 Windows 实例) 使用的页面文件 (仅限 Windows 实例) 可用的页面文件 (仅限 Windows 实例) | | 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs |
| 磁盘读取/写入 | 磁盘读取字节数 (p. 322) 磁盘写入字节数 (p. 322) | |
| 磁盘空间利用率 (仅限 Linux 实例) | | 为 Amazon EC2 Linux 实例监控内存和磁盘指标 |
| 使用的磁盘空间 (仅限 Linux 实例) | | 为 Amazon EC2 Linux 实例监控内存和磁盘指标 |
| 可用磁盘空间 (仅限 Linux 实例) | | 为 Amazon EC2 Linux 实例监控内存和磁盘指标 |

自动和手动监控

AWS 为您提供了各种可以用来监控 Amazon EC2 的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。

主题

- [自动监控工具 \(p. 311\)](#)
- [手动监控工具 \(p. 312\)](#)

自动监控工具

您可以使用以下自动化监控工具来查看 Amazon EC2 并在出现错误时向您报告：

- System Status Checks (系统状态检查) - 监控使用您的实例所需的 AWS 系统，以确保这些系统正常工作。这些检查会检测出需要 AWS 参与修复的实例问题。当一个系统状态检查故障时，您可以等待 AWS 修复故障或者您也可以亲自解决该故障（例如，通过停止和重启或终止和替换实例）。导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题影响网络连通状态

有关更多信息，请参阅 [实例的状态检查 \(p. 313\)](#)。

- Instance Status Checks (实例状态检查) - 监控您的各个实例的软件和网络配置。这些检查检测需要您参与修复的问题。一旦发生实例状态检查故障，一般需要您亲自解决这些问题（例如，通过重启实例或者在您的操作系统中进行修改）。可能导致实例状态检查出现故障的问题示例包括：

- 系统状态检查故障
- 网络或启动配置错误
- 内存耗尽
- 文件系统损坏
- 内核不兼容

有关更多信息，请参阅 [实例的状态检查 \(p. 313\)](#)。

- Amazon CloudWatch 警报 - 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。该操作是向 Amazon Simple Notification Service (Amazon SNS) 主题或 Auto Scaling 策略发送通知。警报只会调用操作进行持续的状态变更。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态，必须改变其状态并维持指定的若干个时间段。有关更多信息，请参阅 [使用 CloudWatch 监控您的实例 \(p. 320\)](#)。
- Amazon CloudWatch Events - 自动化您的 AWS 服务并自动响应系统事件。AWS 服务中的事件将近实时传输到 CloudWatch Events，并且您可以指定要在事件匹配您编写的规则时执行的自动化操作。有关更多信息，请参阅 [什么是 Amazon CloudWatch Events ?](#)。
- Amazon CloudWatch Logs – 监控、存储和访问来自 Amazon EC2 实例、AWS CloudTrail 或其他来源的日志文件。有关更多信息，请参阅 [什么是 Amazon CloudWatch Logs ?](#)。
- Amazon EC2 监控脚本 – 可以使用 Perl 脚本在您的实例中监控内存、磁盘和页面/交换文件使用率。有关更多信息，请参阅 [为 Amazon EC2 Linux 实例监控内存和磁盘指标](#)。
- System Center Operations Manager 的 AWS 管理包 - 链接 Amazon EC2 实例与其内部运行的 Microsoft Windows 或 Linux 操作系统。AWS 管理包是 Microsoft System Center Operations Manager 的一种扩展程序。它使用数据中心内的指定计算机（称为观察程序节点）和 Amazon Web Services API 远程发现并收集 AWS 资源的相关信息。有关更多信息，请参阅 [适用于 Microsoft System Center 的 AWS 管理包](#)。

手动监控工具

监控 Amazon EC2 的另一重要部分需要手动监控一些项目，监控脚本、状态检查和 CloudWatch 警报并不考察这些项目的指标。Amazon EC2 和 CloudWatch 控制台控制面板提供您的 Amazon EC2 环境状态的概览视图。

- Amazon EC2 控制面板显示：
 - 按区域显示服务运行状况和计划的事件
 - 实例状态
 - 状态检查
 - 警报状态
- 实例指标详细信息（在导航窗格中，单击 Instances 选择一个实例，然后单击 Monitoring (监控) 选项卡）
- 卷指标详细信息（在导航窗格中，单击 Volumes (卷) 选择一个卷，然后单击 Monitoring (监控) 选项卡）

- Amazon CloudWatch 控制面板显示：

- 当前警报和状态
- 警报和资源的图表
- 服务运行状况

此外，您还可以使用 CloudWatch 执行以下操作：

- 将 Amazon EC2 监控数据绘制成图表以排除问题和发现趋势
- 搜索并浏览您所有的 AWS 资源指标
- 创建和编辑警报以接收有关问题的通知
- 一目了然地查看您的警报和 AWS 资源的概览信息

监控的最佳实践

使用以下监控最佳实践，帮助您执行 Amazon EC2 监控任务。

- 让监控成为优先事务，阻止小问题演变为大问题。
- 创建并实施从 AWS 解决方案各个部分收集监控数据的监控计划，以便更轻松地调试发生的多点故障。您的监控计划至少应该解决以下问题：
 - 您的监控目标是什么？
 - 您将监控哪些资源？
 - 监控这些资源的频率如何？
 - 您将使用哪些监控工具？
 - 谁负责执行监控任务？
 - 出现错误时应通知谁？
- 尽可能自动监控任务。
- 检查 EC2 实例的日志文件。

监控实例状态

您可以通过查看实例的状态检查和计划事件来监控您的实例状态。状态检查反映 Amazon EC2 自动检查的结果信息。这些自动检查会检测出指定的问题是否影响您的实例。该状态检查信息与 Amazon CloudWatch 提供的数据一起为您的每一个实例提供详细的操作可视性。

您也可以查看您的实例中指定的预定事件的状态。事件提供了关于活动日程信息，例如，根据每个事件预定的开始和结束时间，有计划的重启或指令引退您的实例。

内容

- [实例的状态检查 \(p. 313\)](#)
- [实例的计划事件 \(p. 317\)](#)

实例的状态检查

使用实例状态监控，您可以快速确定 Amazon EC2 是否已经检测到可能阻止您的实例运行应用程序的任何问题。Amazon EC2 将对运行的所有 EC2 实例执行自动检查以识别硬件和软件问题。您可以通过查看这些状态检查的结果来识别指定的和可检测的问题。这些数据扩充了 Amazon EC2 已提供的有关每个实例的预期状态（如 pending、running、stopping）的信息以及 Amazon CloudWatch 监控的利用率指标（CPU 利用率、网络流量和磁盘活动）。

状态检查每分钟进行一次并且每次都会返回一个通过或失败状态。如果所有的检查都通过，则实例的整体状态是OK。如果有一个或多个检查故障，则整体状态为受损。状态检查是内置到 Amazon EC2 中的，所以不能禁用或删除。但是，您可以创建或删除基于状态检查结果触发的警报。例如，您可以创建一个警报来提醒您在一个指定实例上的状态检查中返回了故障状态。有关更多信息，请参阅 [创建和编辑状态检查警报 \(p. 316\)](#)。

内容

- [状态检查的类型 \(p. 314\)](#)
- [查看状态检查 \(p. 314\)](#)
- [报告实例状态 \(p. 315\)](#)
- [创建和编辑状态检查警报 \(p. 316\)](#)

状态检查的类型

状态检查可分为两种类型：系统状态检查和实例状态检查。

系统状态检查

监控使用您的实例所需的 AWS 系统，以确保这些系统正常工作。这些检查会检测出需要 AWS 参与修复的实例问题。如果系统状态检查失败，您可以等待 AWS 修复问题，也可自行解决问题（例如，停止并启动实例，或终止并替换实例）。

以下是可能导致系统状态检查失败的问题的示例：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题影响网络连通状态

实例状态检查

监控您的各个实例的软件和网络配置。这些检查检测需要您参与修复的问题。如果实例状态检查失败，一般需要您自行解决问题（例如，重启实例或更改实例配置）。

以下是可能导致实例状态检查失败的问题的示例：

- 系统状态检查故障
- 网络或启动配置不正确
- 内存耗尽
- 文件系统损坏
- 内核不兼容

查看状态检查

Amazon EC2 为您提供了多种查看和使用状态检查的方法。

使用控制台查看状态

您可使用 AWS 管理控制台查看状态检查。

使用控制台查看状态检查

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Instances。
3. 在 Instances 页面上，Status Checks (状态检查) 列中列出每个实例的运行状态。
4. 要查看特定实例的状态，请选择该实例，然后选择 Status Checks 选项卡。
5. 如果您有一个实例出现过状态检查失败的情况，并且该实例无法访问的时间已超 20 分钟，请选择 AWS Support 提交帮助请求。要自行解决系统或实例状态检查失败问题，请参阅 [通过故障状态检查排查实例故障 \(p. 650\)](#)。

使用命令行或 API 查看状态

您可以使用 `describe-instance-status` (AWS CLI) 命令查看正在运行的实例的状态检查。

要查看所有实例的状态，请使用以下命令：

```
aws ec2 describe-instance-status
```

获取实例状态为 `impaired` 的所有实例的状态：

```
aws ec2 describe-instance-status --filters Name=instance-status.status,Values=impaired
```

要获取单一实例的状态，请使用以下命令：

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

或者，使用以下命令：

- `Get-EC2InstanceState` (适用于 Windows PowerShell 的 AWS 工具)
- `DescribeInstanceStatus` (Amazon EC2 查询 API)

如果您的实例发生了状态检查故障，请参阅 [通过故障状态检查排查实例故障 \(p. 650\)](#)。

报告实例状态

如果您的实例出现了问题但其状态并未显示为受损，或者您想要向 AWS 发送有关您遇到的受损实例相关问题的详细信息，可提供反馈。

我们利用报告的反馈来识别影响到多数客户的问题，但不会对单独的账户问题做出回应。提供反馈并不会改变您当前看到的实例状态检查结果。

使用控制台报告状态反馈

使用控制台报告实例状态

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 选择 Status Checks 选项卡，然后选择 Submit feedback。
5. 填写 Report Instance Status 表单，然后选择 Submit。

使用命令行或 API 报告状态反馈

使用以下 `report-instance-status` (AWS CLI) 命令发送有关受损实例状态的反馈：

```
aws ec2 report-instance-status --instances i-1234567890abcdef0 --status impaired --reason-codes code
```

或者，使用以下命令：

- [Send-EC2InstanceState](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ReportInstanceState](#) (Amazon EC2 查询 API)

创建和编辑状态检查警报

您可以创建实例状态和系统状态警报，以在实例的状态检查失败时向您发出通知。

使用控制台创建状态检查警报

您可以为现有实例创建状态检查警报，以监视实例状态或系统状态。您可以将警报配置为，当实例状态检查或系统状态检查失败时，通过电子邮件向您发出通知或停止、终止或恢复实例。

要创建状态检查警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 选择 Status Checks 选项卡，然后选择 Create Status Check Alarm。
5. 选择 Send a notification to。选择一个现有 SNS 主题，或单击 create topic 以创建新的主题。如果要创建新的主题，请在 With these recipients 中，输入您的电子邮件地址以及任何其他收件人的地址，中间用逗号隔开。
6. (可选) 选择 Take the action，然后选择要采取的操作。
7. 在 Whenever 中，选择想要获得通知的状态检查。

Note

如果您在上一步中选择的是 Recover this instance，则请选择 Status Check Failed (System)。

8. 在 For at least 中，设置所需的评估期间数量，然后在 consecutive periods 中，选择评估期间持续时间，此评估期间结束后才会触发警报并发送电子邮件。
9. (可选) 在 Name of alarm 中，将警报的默认名称替换为其他名称。
10. 选择 Create Alarm。

Important

如果您向收件人列表添加了电子邮件地址或创建了新的主题，则 Amazon SNS 将向每个新地址发送一封订阅确认电子邮件。每个收件人必须通过单击该邮件中包含的链接来确认订阅。警报通知仅发送至经过确认的地址。

在您需要更改实例状态警报时，您可以对其进行编辑。

要编辑状态检查警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，选择 Actions，选择 CloudWatch Monitoring，然后选择 Add/Edit Alarms。
4. 在 Alarm Details 对话框中，选择警报的名称。
5. 在 Edit Alarm 对话框中，进行所需更改，然后选择 Save。

使用 AWS CLI 创建状态检查警报

在以下示例中，当实例的实例检查或系统状态检查在至少两个期间连续失败后，警报将向 SNS 主题 `arn:aws:sns:us-west-2:111122223333:my-sns-topic` 发送通知。指标为 `StatusCheckFailed`。

要使用 CLI 创建状态检查警报

1. 选择一个现有 SNS 主题或创建一个新的主题。有关更多信息，请参阅 AWS Command Line Interface 用户指南 中的 [将 Amazon SNS 与 AWS CLI 结合使用](#)。
2. 使用以下 `list-metrics` 命令查看 Amazon EC2 的可用 Amazon CloudWatch 指标：

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. 使用以下 `put-metric-alarm` 命令创建警报：

```
aws cloudwatch put-metric-alarm --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 --metric-name StatusCheckFailed --namespace AWS/EC2 --statistic Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --unit Count --period 300 --evaluation-periods 2 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

注意

- `--period` 是收集 Amazon CloudWatch 指标的时间范围 (秒)。此示例使用 300，这是 60 秒乘以 5 分钟得到的结果。
- `--evaluation-periods` 是必须将指标数值与阈值相比较的连续周期数。此示例使用 2。
- `--alarm-actions` 是要在此警报触发时执行的操作的列表。每个操作都被指定为一个 Amazon 资源名称 (ARN)。此示例将此警报配置为使用 Amazon SNS 发送电子邮件。

实例的计划事件

AWS 可为您的实例计划事件，例如重启、停止/启动或停用。这些事件不会频繁发生。如果您的一个实例将受某计划事件影响，则 AWS 将在该计划事件发生之前向与您的 AWS 账户关联的电子邮件地址发送电子邮件，其中包含有关该事件的详细信息，包括开始和结束日期。根据事件的不同，您也许能够采取操作来控制事件的发生时间。

要更新账户的联系人信息以确保获得有关计划事件的通知，请转至 [Account Settings](#) 页。

内容

- [计划事件的类型 \(p. 317\)](#)
- [查看计划的事件 \(p. 318\)](#)
- [使用计划停止或停用的实例 \(p. 319\)](#)
- [使用计划为重启的实例 \(p. 319\)](#)
- [使用计划为维护的实例 \(p. 320\)](#)

计划事件的类型

Amazon EC2 为您的实例支持下列类型的计划事件：

- **实例停止**：实例将会停止。再次启动实例时，实例会迁移至新主机。仅适用于 Amazon EBS 支持的实例。
- **实例停用**：实例将停止或终止。
- **重启**：实例将重启 (实例重启) 或实例的主计算机将重启 (系统重启)。

- 系统维护：实例可能会因网络维护或电源维护受到暂时的影响。

查看计划的事件

除了通过电子邮件接收计划事件的通知外，您还可查看计划的事件。

使用控制台查看实例的计划事件

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，单击 Events (事件)。将显示与事件关联的所有资源。您可按资源类型或按特定事件类型进行筛选。您可选择资源来查看详细信息。
3. 或者，在导航窗格中，选择 EC2 Dashboard。Scheduled Events 下将显示与事件关联的所有资源。
4. 请注意，还将显示受影响资源的事件。例如，在导航窗格中，选择 Instances，然后选择一个实例。如果所选实例具有关联事件，则关联事件将显示在底部窗格中。

使用命令行或 API 查看实例的计划事件

使用以下 AWS CLI 命令：

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

以下是显示实例停用事件的示例输出：

```
{  
    "InstanceStatuses": [  
        {  
            "InstanceState": {  
                "Status": "ok",  
                "Details": [  
                    {  
                        "Status": "passed",  
                        "Name": "reachability"  
                    }  
                ]  
            },  
            "AvailabilityZone": "us-west-2a",  
            "InstanceId": "i-1234567890abcdef0",  
            "InstanceState": {  
                "Code": 16,  
                "Name": "running"  
            },  
            "SystemStatus": {  
                "Status": "ok",  
                "Details": [  
                    {  
                        "Status": "passed",  
                        "Name": "reachability"  
                    }  
                ]  
            },  
            "Events": [  
                {  
                    "Code": "instance-stop",  
                    "Description": "The instance is running on degraded hardware",  
                    "NotBefore": "2015-05-23T00:00:00.000Z"  
                }  
            ]  
        }  
    ]  
}
```

```
        ]
    }
}
```

或者，使用以下命令：

- [Get-EC2InstanceState](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeInstanceState](#) (Amazon EC2 查询 API)

使用计划停止或停用的实例

当 AWS 检测到您的实例的基础主机存在无法修复的故障时，它将计划实例停止或终止，这取决于实例根设备的类型。如果根设备为 EBS 卷，则将计划实例停止。如果根设备为实例存储卷，则将计划实例终止。有关更多信息，请参阅 [实例停用 \(p. 266\)](#)。

Important

实例停止或终止之后，实例存储卷上存储的所有数据都将丢失。这包括连接到使用 EBS 卷作为根设备的实例的实例存储卷。在实例停止或终止之前，请务必保存实例存储卷中以后还将需要的数据。

Amazon EBS 支持的实例操作

您可等待实例按计划停止。您也可自行停止并启动实例，这会将实例迁移至新的主计算机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

实例存储支持的实例操作

建议您在实例按计划终止之前，从最新的 AMI 启动替代实例并将所有必需数据迁移至替代实例。然后，您可终止原始实例，或等待其按计划终止。

使用计划为重启的实例

当 AWS 需要执行安装更新或维护基础主机等任务时，它可计划实例或实例的基础主机进行重启。无论是否为任何现有实例计划了重启操作，新启动的实例都不需要重启，因为底层主机已应用更新。

您可确定重启事件为实例重启还是系统重启。

使用控制台查看计划重启事件的类型

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Instance resources，然后选择您的实例。
4. 在底部窗格中，找到 Event type。该值为 system-reboot 或 instance-reboot。

使用 AWS CLI 查看计划重启事件的类型

使用以下 `describe-instance-status` 命令：

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

针对实例重启的操作

您可等待实例重启在其计划的维护时段进行。您也可在方便时自行重启实例。有关更多信息，请参阅 [重启您的实例 \(p. 265\)](#)。

重启实例之后，会立即取消针对实例重启的计划事件，并且更新事件的描述。基础主计算机的所有挂起的维护都将完成，并且在您的实例完全启动后，您可再次开始使用您的实例。

针对系统重启的操作

您无法自行重启系统。我们建议您在系统的计划维护时段内等待系统重启。系统重启通常在几分钟内完成，实例将保留其 IP 地址和 DNS 名称，并且本地实例存储卷上的任何数据将保留。在系统重启后，将清除实例的计划事件，并且您可验证实例上的软件是否按预期运行。

或者，如果必须在其他时间维护实例，您可以停止并启动 EBS 支持的实例，这会将它迁移到新主机。但是，本地实例存储卷上的数据将不会保留。对于实例存储支持的实例，您可以从最新的 AMI 启动替代实例。

使用计划为维护的实例

当 AWS 需要维护实例的基础主计算机时，它将计划实例进行维护。维护事件有两种：网络维护和电源维护。

在网络维护期间，计划的实例会在短时间内失去网络连接。在维护完成后，将恢复与实例的正常网络连接。

在电源维护期间，计划的实例将短时间脱机，然后重启。执行重启后，将保留您的所有实例的配置设置。

在实例重启后（这通常需要几分钟），验证您的应用程序是否按预期运行。此时，您的实例应该不再具有与之关联的计划事件，或者计划事件的描述应该以 [Completed] 开头。有时，此实例状态需要 1 个小时才能更新。已完成的维护事件将在 Amazon EC2 控制台面板上显示长达一周时间。

Amazon EBS 支持的实例操作

您可等待维护按计划进行。您也可停止并启动实例，这会将实例迁移至新的主计算机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

实例存储支持的实例操作

您可等待维护按计划进行。或者，如果您想在计划的维护时段保持正常操作，可从最新的 AMI 启动替代实例，并在计划的维护时段之前将所有必需数据迁移至替代实例，然后终止原始实例。

使用 CloudWatch 监控您的实例

您可以使用 Amazon CloudWatch 监控您的实例，此工具可从 Amazon EC2 收集原始数据，并将数据处理为易读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。

默认情况下，Amazon EC2 每隔 5 分钟向 CloudWatch 发送一次指标数据。要每隔 1 分钟向 CloudWatch 发送一次实例的指标数据，可以对实例启用详细监控。有关更多信息，请参阅 [对您的实例启用或禁用详细监控 \(p. 321\)](#)。

Amazon EC2 控制台将根据来自 Amazon CloudWatch 的原始数据显示一系列图表。根据您的需求，您可能更愿意从 Amazon CloudWatch 而非控制台中的图表中获取实例数据。

有关 Amazon CloudWatch 的更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。

内容

- [对您的实例启用或禁用详细监控 \(p. 321\)](#)
- [列出实例的可用 CloudWatch 指标 \(p. 322\)](#)
- [获取指标的实例的指标的统计数据 \(p. 326\)](#)
- [绘制实例的指标图形 \(p. 331\)](#)
- [为实例创建 CloudWatch 警报 \(p. 331\)](#)
- [创建停止、终止、重启或恢复实例的警报 \(p. 332\)](#)

对您的实例启用或禁用详细监控

默认情况下，已对您的实例启用基本监控。您可以选择启用详细监控。当您启用详细监控后，Amazon EC2 控制台将以 1 分钟为间隔显示实例的监控图表。下表描述对实例的基本和详细监控。

| 类型 | 说明 |
|----|--|
| 基本 | 数据在 5 分钟期间内自动可用，无需收费。 |
| 明细 | 额外付费的情况下，每隔 1 分钟提供一次数据。 要获得此级别的数据，您必须为实例专门启用此监视。对于您已启用详细监视的实例，您还可以跨组（相似实例所在组）获得聚合数据。 有关定价的信息，请参阅 Amazon CloudWatch 产品页 。 |

启用详细监控

在实例启动时或在实例运行或停止后，可对实例启用详细监控。

使用控制台对现有实例启用详细监控

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择所需实例，选择 Actions、CloudWatch Monitoring、Enable Detailed Monitoring。
4. 在 Enable Detailed Monitoring 对话框中，选择 Yes, Enable。
5. 选择 Close。

在使用控制台启动实例时启用详细监控

在使用 AWS 管理控制台启动实例时，请在 Configure Instance Details 页面上选中 Monitoring 复选框。

使用 AWS CLI 对现有实例启用详细监控

使用以下 `monitor-instances` 命令对指定实例启用详细监控。

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

在使用 AWS CLI 启动实例时启用详细监控

结合使用 `run-instances` 命令和 `--monitoring` 标志来启用详细监控。

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

禁用详细监控

在实例启动时或在实例运行或停止后，可对实例禁用详细监控。

使用控制台禁用详细监控

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择所需实例，选择 Actions、CloudWatch Monitoring、Disable Detailed Monitoring.

4. 在 Disable Detailed Monitoring 对话框中，选择 Yes, Disable。
5. 选择 Close。

使用 AWS CLI 禁用详细监控

使用以下 [unmonitor-instances](#) 命令对指定实例禁用详细监控。

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

列出实例的可用 CloudWatch 指标

Amazon EC2 将指标发送到 Amazon CloudWatch。可使用 AWS 管理控制台、AWS CLI 或 API 列出 Amazon EC2 发送到 CloudWatch 的指标。默认情况下，每个数据点中包含的是实例 5 分钟前的活动。如果您启用了详细监控，则每个数据点包含 1 分钟前的活动。

有关获取这些指标的统计数据的信息，请参阅 [获取指标的实例的指标的统计数据 \(p. 326\)](#)。

实例指标

| 指标 | 说明 |
|------------------|---|
| CPUCreditUsage | <p>[T2 实例] 实例使用的 CPU 积分数。一个 CPU 积分等于一个 vCPU 按 100% 利用率运行一分钟，或者 vCPU、利用率和时间的等效组合（例如，一个 vCPU 按 50% 利用率运行两分钟，或者两个 vCPU 按 25% 利用率运行两分钟）。</p> <p>CPU 积分指标每 5 分钟仅可用一次。如果您指定一个大于五分钟的时间段，请使用 Sum 统计数据，而非 Average 统计数据。</p> <p>单位：计数</p> |
| CPUCreditBalance | <p>[T2 实例] 可供实例用于突增至超出基础 CPU 使用率的 CPU 积分数量。获得积分后，积分便存储在积分余额中，到期后便会从积分余额中删除。积分在获得后 24 小时到期。</p> <p>CPU 积分指标每 5 分钟仅可用一次。</p> <p>单位：计数</p> |
| CPUUtilization | <p>当前正在实例上使用的已分配 EC2 计算单位的百分率。该指标确认在选定实例上运行一个应用程序需要的处理能力。</p> <p>Note</p> <p>根据实例类型，如果未向实例分配整个处理器核心，则操作系统中的工具显示的百分率可能低于 CloudWatch。</p> <p>单位：百分比</p> |
| DiskReadOps | <p>在指定时间段内从可供实例使用的所有实例存储卷完成的读取操作数。</p> <p>Note</p> <p>要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。</p> <p>单位：计数</p> |

| 指标 | 说明 |
|-------------------|--|
| DiskWriteOps | <p>在指定时间段内向可供实例使用的所有实例存储卷完成的写入操作数。</p> <p>Note</p> <p>要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。</p> <p>单位：计数</p> |
| DiskReadBytes | <p>从可供实例使用的所有实例存储卷读取的字节数。</p> <p>该指标用来确定应用程序从实例的硬盘读取的数据量。它可以用来确定应用程序的速度。</p> <p>单位：字节</p> |
| DiskWriteBytes | <p>向可供实例使用的所有实例存储卷写入的字节数。</p> <p>该指标用来确定应用程序向实例的硬盘写入的数据量。它可以用来确定应用程序的速度。</p> <p>单位：字节</p> |
| NetworkIn | <p>实例在所有网络接口上收到的字节数。该指标确认单个实例上向应用程序传入的网络流量。</p> <p>单位：字节</p> |
| NetworkOut | <p>实例在所有网络接口上发送的字节数。该指标确认单个实例上向应用程序传出的网络流量。</p> <p>单位：字节</p> |
| NetworkPacketsIn | <p>实例在所有网络接口上收到的数据包的数量。此指标依据单个实例上的数据包数量来标识传入流量的量。此指标仅对基本监控可用。</p> <p>单位：计数</p> <p>统计数据：Minimum、Maximum、Average</p> |
| NetworkPacketsOut | <p>实例在所有网络接口上发送的数据包的数量。此指标依据单个实例上的数据包数量标识传出流量的量。此指标仅对基本监控可用。</p> <p>单位：计数</p> <p>统计数据：Minimum、Maximum、Average</p> |
| StatusCheckFailed | <p>报告两种状况检查之一是否失败的 StatusCheckFailed_Instance 和 StatusCheckFailed_System 组合。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p>Note</p> <p>状况检查指标每 1 分钟可用一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p>单位：计数</p> |

| 指标 | 说明 |
|----------------------------|--|
| StatusCheckFailed_Instance | <p>报告实例在上 1 分钟内是否通过了 Amazon EC2 实例状况检查。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p style="margin-left: 20px;">Note</p> <p style="margin-left: 20px;">状况检查指标每 1 分钟可用一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p style="margin-left: 20px;">单位：计数</p> |
| StatusCheckFailed_System | <p>报告实例在上一分钟内是否通过了 EC2 系统状况检查。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p style="margin-left: 20px;">Note</p> <p style="margin-left: 20px;">状况检查指标每 1 分钟提供一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p style="margin-left: 20px;">单位：计数</p> |
| BurstBalance | <p>仅用于 吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷。提供有关突增存储桶中可用的余额。卷处于活动状态时，数据仅报告给 CloudWatch。如果未挂载卷，则不会报告任何数据。</p> <p style="margin-left: 20px;">单位：百分比</p> |

有关为 EBS 卷提供的指标的信息，请参阅 [Amazon EBS 指标 \(p. 534\)](#)。有关为竞价型队列提供的指标的信息，请参阅 [竞价型队列的 CloudWatch 指标 \(p. 216\)](#)。

Amazon EC2 维度

您可以用以下维度来优化针对您的实例返回的指标。

| 维度 | 说明 |
|----------------------|--|
| AutoScalingGroupName | 该维度筛选您为指定容量组中的所有实例请求的数据。如果您使用 Auto Scaling，Auto Scaling 组就是您定义的实例集合。当实例在上述 Auto Scaling 组中时，该维度仅供 Amazon EC2 指标使用。可供启用了详细或基本监控的实例使用。 |
| ImageId | 该维度筛选您为运行此 Amazon EC2 Amazon 系统映像 (AMI) 的所有实例而请求的数据。可供启用了详细监控功能的实例使用。 |
| InstanceId | 该维度筛选您仅为已识别实例请求的数据。这样有助于您精确定位要对其监控数据的确切实例。 |
| InstanceType | 该维度筛选您为以这一指定实例类型运行的所有实例请求的数据。这样有助于您按运行的实例类型给数据分类。例如，您可以比较 m1.small 实例和 m1.large 实例的数据，以确定哪一个对您的应用程序具有更好的商业价值。可供启用了详细监控功能的实例使用。 |

使用控制台列出指标

指标首先按命名空间进行分组，然后按各命名空间内的各种维度组合进行分组。例如，您可以查看由 Amazon EC2 提供的所有指标或按实例 ID、实例类型、映像 (AMI) ID 或 Auto Scaling 组分组的指标。

按类别查看可用指标

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Metrics。
3. 选择 EC2 指标命名空间。
4. 选择指标维度（例如“Per-Instance Metrics”）。
5. 要对指标进行排序，请使用列标题。要为指标绘制图表，请选中该指标旁的复选框。要按资源进行筛选，请选择资源 ID，然后选择 Add to search。要按指标进行筛选，请选择指标名称，然后选择 Add to search。

使用 AWS CLI 列出指标

使用 `list-metrics` 命令列出实例的 CloudWatch 指标。

列出 Amazon EC2 的所有可用指标

以下示例指定 AWS/EC2 命名空间以查看 Amazon EC2 的所有指标。

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

下面是示例输出：

```
{  
  "Metrics": [  
    {  
      "Namespace": "AWS/EC2",  
      "Dimensions": [  
        {  
          "Name": "InstanceId",  
          "Value": "i-1234567890abcdef0"  
        }  
      ],  
      "MetricName": "NetworkOut"  
    },  
    {  
      "Namespace": "AWS/EC2",  
      "Dimensions": [  
        {  
          "Name": "InstanceId",  
          "Value": "i-1234567890abcdef0"  
        }  
      ],  
      "MetricName": "CPUUtilization"  
    },  
    {  
      "Namespace": "AWS/EC2",  
      "Dimensions": [  
        {  
          "Name": "InstanceId",  
          "Value": "i-1234567890abcdef0"  
        }  
      ],  
      "MetricName": "MemoryUtilization"  
    }  
  ]  
}
```

```
        "Value": "i-1234567890abcdef0"
    }
],
"MetricName": "NetworkIn"
},
...
}
```

列出实例的所有可用指标

以下示例指定 AWS/EC2 命名空间和 InstanceId 维度以仅查看指定实例的结果。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
Name=InstanceId,Value=i-1234567890abcdef0
```

列出跨所有实例的指标

以下示例指定 AWS/EC2 命名空间和指标名称以仅查看指定指标的结果。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

获取指标的实例的指标的统计数据

您可以获取有关实例的 CloudWatch 指标的统计信息。

内容

- 统计数据概述 (p. 326)
- 获取指定实例的统计数据 (p. 327)
- 聚合多实例统计数据 (p. 328)
- 通过 Auto Scaling 组聚合统计数据 (p. 329)
- 按 AMI 聚合统计数据 (p. 330)

统计数据概述

统计数据 是指定时间段内的指标数据聚合。CloudWatch 所提供的统计数据基于您的自定义数据提供给 CloudWatch 或者 AWS 中其他服务提供给该产品的指标数据点。聚合通过使用命名空间、指标名称、维度以及数据点度量单位在您指定的时间段内完成。下表介绍了可用的统计信息。

| 统计数据 | 说明 |
|-------------|--|
| Minimum | 指定时间段内的最低观察值。可以使用此值来决定应用程序的活动量是否较低。 |
| Maximum | 指定时间段内的最高观察值。可以使用此值来决定应用程序的活动量是否较高。 |
| Sum | 为匹配指标所提交的所有的值添加在一起。此统计信息的作用是决定指标的总量。 |
| Average | 指定时间段内 Sum / SampleCount 的值。通过将此统计信息与 Minimum 和 Maximum 进行比较，可以决定指标的完整范围以及平均使用率与 Minimum 和 Maximum 的接近程度。这样的比较可以帮助了解何时应该根据需要增加或减少资源。 |
| SampleCount | 数据点计数 (数量) 用于统计信息的计算。 |
| pNN.NN | 指定的百分位数的值。您可以指定任何百分位数，最多使用两位小数 (例如 p95.45)。 |

获取指定 实例的统计数据

以下示例显示了如何使用 AWS 管理控制台 或 AWS CLI 来确定特定 EC2 实例的最大 CPU 利用率。

要求

- 您必须拥有实例的 ID。您可以使用 AWS 管理控制台 或 [describe-instances](#) 命令获取实例 ID。
- 默认情况下，基本监控已启用，但您可以启用详细监控。有关更多信息，请参阅 [对您的实例启用或禁用详细监控 \(p. 321\)](#)。

使用控制台显示特定实例的 CPU 利用率

- 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
- 在导航窗格中，选择 Metrics。
- 选择 EC2 指标命名空间。
- 选择“Per-Instance Metrics”维度。
- 在搜索字段中，键入 **CPUutilization** 并按 Enter。选择特定实例的行，这将显示该实例的 CPUUtilization 指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
- 要更改指标的统计数据或时段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

使用 AWS CLI 获取特定实例的 CPU 利用率

使用以下 [get-metric-statistics](#) 命令获取指定实例的 CPUUtilization 指标 (使用指定时段和时间间隔)：

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2016-10-18T23:18:00 --end-time 2016-10-19T23:18:00
```

下面是示例输出。每个数值代表一个 EC2 实例的最大 CPU 利用率百分比。

```
{
  "Datapoints": [
    {
      "Timestamp": "2016-10-19T00:18:00Z",
      "Maximum": 0.33000000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-19T03:18:00Z",
      "Maximum": 99.670000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-19T07:18:00Z",
      "Maximum": 0.34000000000000002,
      "Unit": "Percent"
    }
  ]
}
```

```
"Timestamp": "2016-10-19T12:18:00Z",
"Maximum": 0.3400000000000002,
"Unit": "Percent"
},
...
],
"Label": "CPUUtilization"
}
```

聚合多实例统计数据

聚合统计信息适用于已经启用详细监控的实例。聚合中不包含使用基本监控的实例。此外，Amazon CloudWatch 不跨各个区域聚合数据。因此指标在各区域间彼此独立。在获取多实例聚合统计数据前，必须启用详细监控（另外收费），以提供以 1 分钟为间隔的数据。

此示例显示了如何使用详细监控来获取 EC2 实例的平均 CPU 利用率。因为未指定任何维度，所以 CloudWatch 会返回 AWS/EC2 命名空间中所有维度的统计数据。

Important

此方法可以在 AWS 命名空间中检索所有维度，但不适用于发布到 Amazon CloudWatch 的自定义命名空间。对于自定义命名空间，必须指定与任意给定数据关联的完整的维度组，以检索包含数据点的统计数据。

显示实例的平均 CPU 利用率

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Metrics。
3. 选择 EC2 命名空间，然后选择 Across All Instances。
4. 选择包含 CPUUtilization 的行，这将显示所有 EC2 实例的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
5. 要更改指标的统计数据或时段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

要获取实例的平均 CPU 利用率，请执行以下步骤：

使用 `get-metric-statistics` 命令（如下所示）获取实例的平均 CPUUtilization 指标。

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization \
--period 3600 --statistics "Average" "SampleCount" \
--start-time 2016-10-11T23:18:00 --end-time 2016-10-12T23:18:00
```

下面是示例输出：

```
{
  "Datapoints": [
    {
      "SampleCount": 238.0,
      "Timestamp": "2016-10-12T07:18:00Z",
      "Average": 0.038235294117647062,
      "Unit": "Percent"
    },
    {
      "SampleCount": 240.0,
      "Timestamp": "2016-10-12T09:18:00Z",
      "Average": 0.038235294117647062,
      "Unit": "Percent"
    }
  ]
}
```

```
        "Average": 0.1667083333333332,
        "Unit": "Percent"
    },
    {
        "SampleCount": 238.0,
        "Timestamp": "2016-10-11T23:18:00Z",
        "Average": 0.041596638655462197,
        "Unit": "Percent"
    },
    ...
],
"Label": "CPUUtilization"
}
```

通过 Auto Scaling 组聚合统计数据

您可以聚合 Auto Scaling 组中 EC2 实例的统计数据。请注意，Amazon CloudWatch 不能跨各个区域聚合数据。指标在各区域间彼此独立。

此示例说明如何检索为一个 Auto Scaling 组写入磁盘的字节总数。总数以 1 分钟为周期 24 小时为间隔针对指定 Auto Scaling 组中的所有 EC2 实例计算得出。

使用控制台显示一个 Auto Scaling 组中的实例的 DiskWriteBytes

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Metrics。
3. 选择 EC2 命名空间，然后选择 By Auto Scaling Group。
4. 选择 DiskWriteBytes 指标和特定 Auto Scaling 组的行，这将显示 Auto Scaling 组中实例的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
5. 要更改指标的统计数据或时段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

使用 AWS CLI 显示一个 Auto Scaling 组中实例的 DiskWriteBytes

使用 `get-metric-statistics` 命令，如下所示。

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes --
period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2016-10-16T23:18:00 --end-time 2016-10-18T23:18:00
```

下面是示例输出：

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2016-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2016-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ]
},
```

```
    "Label": "DiskWriteBytes"
}
```

按 AMI 聚合统计数据

您可以聚合已启用详细监控的实例的统计数据。不包含使用基本监控的实例。请注意，Amazon CloudWatch 不能跨各个区域聚合数据。指标在各区域间彼此独立。

在获取多实例聚合统计数据前，必须启用详细监控（另外收费），以提供以 1 分钟为间隔的数据。有关更多信息，请参阅 [对您的实例启用或禁用详细监控 \(p. 321\)](#)。

此示例显示了如何确定使用特定 Amazon 系统映像 (AMI) 的所有实例的平均 CPU 利用率。平均值以 60 秒为时间间隔 1 天为周期。

使用控制台按 AMI 显示平均 CPU 利用率

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Metrics。
3. 选择 EC2 命名空间，然后选择 By Image (AMI) Id。
4. 选择 CPUUtilization 指标和特定 AMI 的行，这将显示指定 AMI 的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
5. 要更改指标的统计数据或时段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

要获取映像 ID 的平均 CPU 利用率，请执行以下步骤：

使用 `get-metric-statistics` 命令，如下所示。

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-time 2016-10-10T00:00:00 --end-time 2016-10-11T00:00:00
```

下面是示例输出。每个数值代表运行指定 AMI 的 EC2 实例的平均 CPU 利用率百分比。

```
{
  "Datapoints": [
    {
      "Timestamp": "2016-10-10T07:00:00Z",
      "Average": 0.04100000000000009,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-10T14:00:00Z",
      "Average": 0.079579831932773085,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-10T06:00:00Z",
      "Average": 0.03600000000000011,
      "Unit": "Percent"
    },
    ...
  ],
  "Label": "CPUUtilization"
}
```

绘制实例的指标图形

在您启动实例后，可以打开 Amazon EC2 控制台并在 Monitoring 选项卡上查看实例的监视图形。每个图表以一个可用的 Amazon EC2 指标为基础。

可供使用图形如下：

- CPU 平均利用率 (%)
- 平均读磁盘数 (字节)
- 平均写磁盘数 (字节)
- 最大网络输入 (字节)
- 最大网络输出 (字节)
- 读磁盘操作概括 (计数)
- 写磁盘操作概括 (计数)
- 状态概括 (任意)
- 实例状态概括 (计数)
- 系统状态概括 (计数)

有关指标及其向图表提供的数据的更多信息，请参阅 [列出实例的可用 CloudWatch 指标 \(p. 322\)](#)。

使用 CloudWatch 控制台绘制指标图形

您还可以使用 CloudWatch 控制台将 Amazon EC2 和其他 AWS 服务生成的指标数据绘制成图表。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [绘制指标图形](#)。

为实例创建 CloudWatch 警报

您可以创建 CloudWatch 警报来监视您的其中一个实例的 CloudWatch 指标。当指标达到您指定的阈值时，CloudWatch 将自动向您发送通知。您可以使用 Amazon EC2 控制台创建 CloudWatch 警报，或者使用 CloudWatch 控制台提供的更多高级选项。

使用 CloudWatch 控制台创建警报

例如，请参阅 Amazon CloudWatch 用户指南 中的 [创建 Amazon CloudWatch 警报](#)。

使用 Amazon EC2 控制台创建警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 在 Monitoring 选项卡上，选择 Create Alarm。
5. 在 Create Alarm 页面上，执行以下操作：
 - a. 选择 create topic。对于 Send a notification to，键入 SNS 主题的名称。对于 With these recipients，键入一个或多个用于接收通知的电子邮件地址。
 - b. 为策略指定指标和标准。例如，您可以保留 Whenever 的默认设置 (CPU 使用率平均值)。对于 Is，选择 \geq 并键入 80%。对于 For at least，键入 1 个连续的 5 Minutes 时间段。
 - c. 选择 Create Alarm。

创建停止、终止、重启或恢复实例的警报

利用 Amazon CloudWatch 警报操作，您可创建自动停止、终止、重启或恢复实例的警报。当不再需要某个实例运行时，您可使用停止或终止操作来帮助您节省资金。如果发生了系统损害，您可使用重启和恢复操作自动重启这些实例或将它们恢复到新硬件上。

您创建的每个警报操作均使用警报操作 ARN。一组 ARN 更安全，因为它要求您的账户中有 EC2ActionsAccess IAM 角色。利用此 IAM 角色，您可执行停止、终止或重启操作 - 以前如果您使用的是 IAM 角色，则无法执行操作。使用以前的警报操作 ARN 的现有警报不需要此 IAM 角色，但建议您在编辑使用这些 ARN 的现有警报时更改 ARN 并添加此角色。

EC2ActionsAccess 角色使 AWS 能够代表您执行警报操作。当您首次使用 Amazon EC2 或 Amazon CloudWatch 控制台创建警报操作时，AWS 将自动为您创建此角色。

在许多情况下，您可能需要自动终止或停止实例。例如，您可能拥有专用于批工资单处理工作或科学计算任务的实例，这些实例在运行一段时间后就完成了其工作。与其让这些实例空闲（并产生费用），不如将其停止或终止以节省开支。使用停止警报操作和终止警报操作的主要区别是，停止的警报可以在需要时轻松重启，还可以保留相同的实例 ID 和根卷。而终止的实例则无法重新启动。如此就必须启动一个新的实例。

您可以向为 Amazon EC2 每个实例指标设置的任何警报添加停止、终止、重启或恢复操作，这些指标包括 Amazon CloudWatch 提供的基本和详细监控指标（在 AWS/EC2 命名空间中），以及包含 InstanceId 维度的任何自定义指标，只要其值引用有效运行的 Amazon EC2 实例。

控制台支持

可使用 Amazon EC2 控制台或 CloudWatch 控制台创建警报。本文档中的过程使用 Amazon EC2 控制台。有关使用 CloudWatch 控制台的过程，请参阅 Amazon CloudWatch 用户指南 中的 [创建停止、终止、重新启动或恢复实例的警报](#)。

权限

如果您是 AWS Identity and Access Management (IAM) 用户，您必须拥有以下创建或修改警报的权限：

- `ec2:DescribeInstanceStatus` 和 `ec2:DescribeInstances` - 针对有关 Amazon EC2 实例状态指标的所有警报
- `ec2:StopInstances` - 针对包含停止操作的警报
- `ec2:TerminateInstances` - 针对包含终止操作的警报
- `ec2:DescribeInstanceRecoveryAttribute`, 和 `ec2:RecoverInstances` - 针对包含恢复操作的警报

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 IAM 用户指南 中的 [权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

内容

- 向 Amazon CloudWatch 警报添加停止操作 (p. 333)
- 向 Amazon CloudWatch 警报添加终止操作 (p. 333)
- 向 Amazon CloudWatch 警报添加重启操作 (p. 334)
- 向 Amazon CloudWatch 警报添加恢复操作 (p. 335)
- 使用 Amazon CloudWatch 控制台查看已触发的警报和操作的历史记录 (p. 336)
- Amazon CloudWatch 警报操作场景 (p. 336)

向 Amazon CloudWatch 警报添加停止操作

可以创建当达到一定阈值后停止 Amazon EC2 实例的警报。例如，您可能运行了开发或测试实例而偶尔忘记将其关闭。可以创建当平均 CPU 利用率低于 10% 达 24 小时时触发的警报，同时告知其为空闲并不再使用。可以根据需要调整阈值、时长和时间段，还可以添加 Amazon Simple Notification Service (Amazon SNS) 通知，以便您在触发警报后能够收到电子邮件。

可以停止或终止将 Amazon EBS 卷用作根设备的实例，但只能终止将实例存储用作根设备的实例。

使用 Amazon EC2 控制台创建停止空闲实例的警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Alarm Details for 对话框中，选择 Create Alarm。
5. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for 对话框中，针对 Send a notification to 选择一个现有 Amazon SNS 主题，或者选择 Create Topic 创建一个新主题。

要创建新主题，请对 Send a notification to 输入主题的名称，然后对 With these recipients 输入收件人的电子邮件地址（以逗号分隔）。待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可收到该主题的通知。

6. 选择 Take the action，然后选择 Stop this instance 单选按钮。
7. 如果出现提示，请选择 Create IAM role: EC2ActionsAccess 以自动创建 IAM 角色，这样在此警报触发时 AWS 可自动代表您停止实例。
8. 对于 Whenever，选择想要使用的统计信息，然后选择指标。在此示例中，选择 Average (平均) 和 CPU Utilization (CPU 利用率)。
9. 对于 Is，定义指标阈值。在此示例中，键入 10%。
10. 对于 For at least，选择警报的采样周期。在此示例中，键入 24 个连续 1 小时时间段。
11. 要更改警报的名称，可对 Name this alarm 键入新名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。

Note

可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

12. 选择 Create Alarm。

向 Amazon CloudWatch 警报添加终止操作

可以创建当达到一定阈值时自动终止 EC2 实例的警报（只要该实例未启用终止保护）。例如，某个实例已经完成工作，您不再需要此实例而想将其终止。如果可能在之后使用该实例，则应该选择停止而不是终止。有关对实例启用和禁用终止保护的信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[为实例启用终止保护](#)。

使用 Amazon EC2 控制台创建终止空闲实例的警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Alarm Details for 对话框中，选择 Create Alarm。
5. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for 对话框中，针对 Send a notification to 选择一个现有 Amazon SNS 主题，或者选择 Create Topic 创建一个新主题。

要创建新主题，请对 Send a notification to 输入主题的名称，然后对 With these recipients 输入收件人的电子邮件地址（以逗号分隔）。待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可收到该主题的通知。

6. 选择 Take the action，然后选择 Terminate this instance。
7. 如果出现提示，请选择 Create IAM role: EC2ActionsAccess 以自动创建 IAM 角色，这样在此警报触发时 AWS 可自动代表您停止实例。
8. 对于 Whenever，选择统计数据，然后选择指标。在此示例中，选择 Average (平均) 和 CPU Utilization (CPU 利用率)。
9. 对于 Is，定义指标阈值。在此示例中，键入 10%。
10. 对于 For at least，选择警报的采样周期。在此示例中，键入 24 个连续 1 小时时间段。
11. 要更改警报的名称，可对 Name this alarm 键入新名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。

Note

可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

12. 选择 Create Alarm。

向 Amazon CloudWatch 警报添加重启操作

您可创建监控 Amazon EC2 实例并自动重启此实例的 Amazon CloudWatch 警报。在实例运行状况检查失败时，推荐重启警报操作（与恢复警报操作相反，该操作适合系统运行状况检查失败的情况）。实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。重启实例时，其仍驻留在相同的物理主机上，因此您的实例将保留其公有 DNS 名称、私有 IP 地址及其实例存储卷上的任何数据。

重启实例不会启动新的实例计费时间，这与停止并重新启动您的实例不同。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[重启您的实例](#)。

Important

要避免在重启和恢复操作之间发生竞争情况，我们建议您在创建重启 Amazon EC2 实例的警报时将警报阈值设置为 3（表示 1 分钟）。

使用 Amazon EC2 控制台创建重启实例的警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Alarm Details for 对话框中，选择 Create Alarm。
5. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for 对话框中，针对 Send a notification to 选择一个现有 Amazon SNS 主题，或者选择 Create Topic 创建一个新主题。

要创建新主题，请对 Send a notification to 输入主题的名称，然后对 With these recipients 输入收件人的电子邮件地址（以逗号分隔）。待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可收到该主题的通知。

6. 选择 Take the action，然后选择 Reboot this instance。
7. 如果出现提示，请选择 Create IAM role: EC2ActionsAccess 以自动创建 IAM 角色，这样在此警报触发时 AWS 可自动代表您停止实例。
8. 对于 Whenever，选择“Status Check Failed (Instance)”。
9. 对于 For at least，键入 2。
10. 对于 consecutive period(s) of，选择 1 minute。

11. 要更改警报的名称，可对 Name of alarm 键入新名称。
如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。
12. 选择 Create Alarm。

向 Amazon CloudWatch 警报添加恢复操作

您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。

当 StatusCheckFailed_System 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您会注意到，实例在已恢复的实例上重启。

导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题影响网络连通状态

只有具有以下特性的实例支持恢复操作：

- 使用 C3、C4、M3、M4、R3、R4、T2 或 X1 实例类型
- 在 VPC 中（非 EC2-Classic 中）运行
- 使用共享租赁（租赁属性设置为 default）
- 仅使用 EBS 卷（不配置实例存储卷）。有关更多信息，请参阅[已禁用“恢复此实例”](#)。

如果您的实例具有公有 IP 地址，它会在恢复后保留公有 IP 地址。

Important

要避免在重启和恢复操作之间发生竞争情况，我们建议您在创建恢复 Amazon EC2 实例的警报时将警报阈值设置为 2（表示 1 分钟）。

使用 Amazon EC2 控制台创建恢复实例的警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Alarm Details for 对话框中，选择 Create Alarm。
5. 要在触发警报时接收电子邮件，请在 Create Alarm for 对话框中，针对 Send a notification to 选择一个现有 Amazon SNS 主题，或者选择 Create Topic 创建一个新主题。

要创建新主题，请对 Send a notification to 输入主题的名称，然后对 With these recipients 输入收件人的电子邮件地址（以逗号分隔）。待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可收到该主题的电子邮件。

6. 选择 Take the action，然后选择 Recover this instance。
7. 如果出现提示，请选择 Create IAM role: EC2ActionsAccess 以自动创建 IAM 角色，这样在此警报触发时 AWS 可自动代表您停止实例。

8. 对于 Whenever , 选择“Status Check Failed (System)”。
9. 对于 For at least , 键入 2。
10. 对于 consecutive period(s) of , 选择 1 minute。
11. 要更改警报的名称 , 可对 Name of alarm 键入新名称。

如果不输入警报名称 , 则 Amazon CloudWatch 会自动为您创建一个。

12. 选择 Create Alarm。

使用 Amazon CloudWatch 控制台查看已触发的警报和操作的历史记录

您可以在 Amazon CloudWatch 控制台中查看警报和操作历史记录。Amazon CloudWatch 会保留最近两周的警报和操作历史记录。

要查看已触发的警报和操作的历史记录

1. 通过以下网址打开 CloudWatch 控制台 : <https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中 , 选择 Alarms。
3. 选择一个警报。
4. Details 选项卡显示最近的状态转换以及时间和指标值。
5. 选择 History 选项卡可以查看最近的历史记录条目。

Amazon CloudWatch 警报操作场景

可以使用 Amazon EC2 控制台创建当满足一定条件时停止或终止 Amazon EC2 实例的警报操作。在下方的控制台页面屏幕截图中 , 您设置了警报操作 , 我们对设置进行了编号。我们还对后续场景中的设置进行了编号 , 帮助您创建合适的操作。

场景 1 : 停止空闲开发与测试实例

创建当用于软件开发或测试的实例空闲达到至少 1 小时时停止该实例的警报。

| 设置 | 值 |
|----|------------|
| | Stop |
| | 最高 |
| | CPU 利用率 |
| | <= |
| | 10% |
| | 60 minutes |
| | 1 |

场景 2 : 停止空闲实例

创建一个当实例空闲达到 24 小时时停止该实例并发送电子邮件的警报。

| 设置 | 值 |
|----|----------------|
| | Stop and email |
| | 平均值 |
| | CPU 利用率 |
| | <= |
| | 5% |
| | 60 minutes |
| | 24 |

场景 3：出现异常高流量时发送关于 Web 服务器的电子邮件

创建一个当实例的出站网络流量每天超过 10 GB 时发送电子邮件的警报。

| 设置 | 值 |
|----|------------|
| | 电子邮件 |
| | 总计 |
| | NetworkOut |
| | > |
| | 10GB |
| | 1 天 |
| | 1 |

场景 4：出现异常高流量时停止 Web 服务器

创建当出站流量超过每小时 1 GB 时停止实例并发送短消息 (SMS) 的警报。

| 设置 | 值 |
|----|-------------------|
| | Stop and send SMS |
| | 总计 |
| | NetworkOut |
| | > |
| | 1GB |
| | 1 小时 |
| | 1 |

场景 5：停止出现内存泄漏的实例

创建当内存利用率达到或超过 90% 时停止实例的警报，让应用程序日志可以被检索用于故障排除。

Note

MemoryUtilization 指标是一种自定义指标。要使用 MemoryUtilization 指标，您必须为 Linux 实例安装 Perl 脚本。有关更多信息，请参阅[Amazon EC2 Linux 实例监控内存和磁盘指标](#)。

| 设置 | 值 |
|----|-------------------|
| | Stop |
| | 最高 |
| | MemoryUtilization |
| | >= |
| | 90% |
| | 1 minute |
| | 1 |

场景 6：停止受损的实例

创建当实例连续 3 次状态检查 (每隔 5 分钟执行一次) 皆为故障时将其停止的警报。

| 设置 | 值 |
|----|--------------------------|
| | Stop |
| | 平均值 |
| | StatusCheckFailed_System |
| | >= |
| | 1 |
| | 15 分钟 |
| | 1 |

场景 7：当批处理工作完成时终止实例

创建当实例不再发送结果数据时终止运行批工作的实例的警报。

| 设置 | 值 |
|----|--------------|
| | Terminate |
| | 最高 |
| | 网络输出 |
| | <= |
| | 100000 bytes |
| | 5 minutes |
| | 1 |

使用 CloudWatch Events 实现自动化

利用 Amazon CloudWatch Events，您可以自动执行您的 AWS 服务并自动响应系统事件，例如应用程序可用性问题或资源更改。AWS 服务中的事件将实时传输到 CloudWatch Events。您可以编写简单规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。可能的操作包括调用 AWS Lambda 函数、将事件中继到 Amazon Kinesis Streams、激活 AWS Step Functions 状态机以及其他操作。

一些将 CloudWatch Events 与 Amazon EC2 结合使用的示例包括：

- 在新的 Amazon EC2 实例启动时激活 Lambda 函数。
- 在创建或修改 Amazon EBS 卷时通知 Amazon SNS 主题。
- 当另一个 AWS 服务中发生特定事件时，使用 Amazon EC2 Run Command 向一个或多个 Amazon EC2 实例发送命令。

有关更多信息，请参阅 [Amazon CloudWatch Events 用户指南](#)。

为 Amazon EC2 Linux 实例监控内存和磁盘指标

Amazon CloudWatch 监控脚本（用于基于 Amazon Elastic Compute Cloud (Amazon EC2) Linux 的实例）演示如何生成和使用 Amazon CloudWatch 自定义指标。这些示例 Perl 脚本包含一个功能完备的示例，用于报告 Linux 实例的内存、交换文件和磁盘空间利用率指标。可从 AWS 示例代码库下载[用于 Linux 的 Amazon CloudWatch 监控脚本](#)。

Important

这些脚本只是示例。他们依原样提供且不受支持。

在使用这些脚本时，将对自定义指标收取相应的标准 Amazon CloudWatch 使用费。有关更多信息，请参阅 [Amazon CloudWatch 定价页](#)。

内容

- [支持的系统 \(p. 339\)](#)
- [程序包内容 \(p. 340\)](#)
- [先决条件 \(p. 340\)](#)
- [入门 \(p. 341\)](#)
- [mon-put-instance-data.pl \(p. 342\)](#)
- [mon-get-instance-stats.pl \(p. 344\)](#)
- [在控制台中查看自定义指标 \(p. 345\)](#)
- [故障排除 \(p. 345\)](#)

支持的系统

这些监控脚本专门用于运行 Linux 的 Amazon EC2 实例。这些脚本均使用下列 Amazon 系统映像 (AMI) 在实例上进行过测试（包括 32 位和 64 位版本）：

- Amazon Linux 2014.09.2
- Red Hat Enterprise Linux 6.6
- SUSE Linux Enterprise Server 12
- Ubuntu Server 16.04 和 14.04

您可以使用运行 Windows 的 Amazon EC2 实例上的 EC2Config 来监控内存和磁盘指标，方法是将此数据发送给 CloudWatch Logs。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[将性能计数器发送到 CloudWatch 并将日志发送到 CloudWatch 日志](#)。

程序包内容

监控脚本的程序包中包含以下文件：

- CloudWatchClient.pm – 共享 Perl 模块，以简化从其他脚本调用 Amazon CloudWatch 的过程。
- mon-put-instance-data.pl – 收集 Amazon EC2 实例中的系统指标（内存、交换、磁盘空间利用率）并将其发送到 Amazon CloudWatch。
- mon-get-instance-stats.pl – 查询 Amazon CloudWatch 并显示在其上执行此脚本的 EC2 实例的最近利用率统计数据。
- awscreds.template – AWS 凭据的文件模板，储存您的访问密钥 ID 和秘密访问密钥。
- LICENSE.txt – 包含 Apache 2.0 许可证的文本文件。
- NOTICE.txt – 版权声明。

先决条件

对于 Linux 的某些版本，您必须安装附加模块，监控脚本才能正常运行。

Amazon Linux AMI

如果您在运行 Amazon Linux AMI 版本 2014.03 或更高版本，必须安装附加的 Perl 模块。

安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install perl-Switch perl-Datetime perl-Sys-Syslog perl-LWP-Protocol-https
```

Red Hat Enterprise Linux

您必须安装附加 Perl 模块。

在 Red Hat Enterprise Linux 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install perl-Switch perl-Datetime perl-Sys-Syslog perl-LWP-Protocol-https
perl-Digest-SHA -y
sudo yum install zip unzip
```

SUSE Linux Enterprise Server

您必须安装附加 Perl 模块。

在 SUSE 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。

2. 在命令提示符下，按如下方式安装程序包：

```
sudo zypper install perl-Switch perl-DateTime
sudo zypper install -y "perl(LWP::Protocol::https)"
```

Ubuntu Server

您必须通过如下方式配置您的服务器。

在 Ubuntu 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅 [连接到您的 Linux 实例 \(p. 252\)](#)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo apt-get update
sudo apt-get install unzip
sudo apt-get install libwww-perl libdatatime-perl
```

入门

下列步骤介绍如何在 EC2 Linux 实例上下载、解压缩和配置 CloudWatch 监控脚本。

要下载、安装和配置监控脚本

1. 在命令提示符下，移至希望存储监控脚本的文件夹，并运行以下命令下载监控脚本：

```
curl http://aws-cloudwatch.s3.amazonaws.com/downloads/
CloudWatchMonitoringScripts-1.2.1.zip -O
```

2. 运行以下命令安装您下载的监控脚本：

```
unzip CloudWatchMonitoringScripts-1.2.1.zip
rm CloudWatchMonitoringScripts-1.2.1.zip
cd aws-scripts-mon
```

3. 请确保脚本有权限使用以下选项之一执行 CloudWatch 操作：

- 如果您将 AWS Identity and Access Management (IAM) 角色与您的实例相关联，请验证该角色有权执行以下操作：
 - cloudwatch:PutMetricData
 - cloudwatch:GetMetricStatistics
 - cloudwatch>ListMetrics
 - ec2:DescribeTags
- 在证书文件中指定您的 AWS 证书。首先，请将监控脚本中包含的 `awscreds.template` 文件复制到 `awscreds.conf`，如下所示：

```
cp awscreds.template awscreds.conf
```

在这个文件中添加以下内容：

```
AWSAccessKeyId=my-access-key-id
AWSSecretKey=my-secret-access-key
```

有关如何查看您的 AWS 证书的信息，请参阅 Amazon Web Services 一般参考 中的[了解并获取您的安全凭证](#)。

mon-put-instance-data.pl

此脚本会收集当前系统的内存、交换和磁盘空间利用率数据。然后远程调用 Amazon CloudWatch，以自定义指标的形式报告收集到的数据。

选项

| 名称 | 说明 |
|--------------------------|---|
| --mem-util | 以百分比收集和发送 MemoryUtilization 指标。此选项只报告由应用程序和操作系统分配的内存，不包括缓存和缓冲区中的内存。 |
| --mem-used | 收集和发送 MemoryUsed 指标（以兆字节报告）。此选项只报告由应用程序和操作系统分配的内存，不包括缓存和缓冲区中的内存。 |
| --mem-avail | 收集和发送 MemoryAvailable 指标（以兆字节报告）。此选项会报告应用程序和操作系统可以使用的内存。 |
| --swap-util | 收集和发送 SwapUtilization 指标（以百分比报告）。 |
| --swap-used | 收集和发送 SwapUsed 指标（以兆字节报告）。 |
| --disk-path=PATH | <p>选择要报告的磁盘。</p> <p>PATH 可以为需要报告的文件系统指定装入点或装入点上的任何文件。如需选择多个磁盘，请为每个磁盘分别指定 --disk-path=PATH。</p> <p>要为装载于 /home 和 / 的文件系统选择磁盘，请使用下列参数：</p> <p>--disk-path=/ --disk-path=/home</p> |
| --disk-space-util | <p>收集和发送选定磁盘的 DiskSpaceUtilization 指标。指标以百分比报告。</p> <p>请注意，此脚本计算的磁盘使用率指标与 df -k -l 命令计算的值不同。如果您认为 df -k -l 计算的值更有用，则可以在脚本中更改计算结果。</p> |
| --disk-space-used | <p>收集和发送选定磁盘的 DiskSpaceUsed 指标。指标默认以千兆字节报告。</p> <p>受限于 Linux 操作系统中的保留磁盘空间，已用磁盘空间和可用磁盘空间可能无法准确相加得到磁盘空间总量。</p> |
| --disk-space-avail | <p>收集和发送选定磁盘的 DiskSpaceAvailable 指标。指标以千兆字节报告。</p> <p>受限于 Linux 操作系统中的保留磁盘空间，已用磁盘空间和可用磁盘空间可能无法准确相加得到磁盘空间总量。</p> |
| --memory-units=UNITS | 指定报告内存使用率所采用的单位。如果不指定，则内存以兆字节报告。单位可以是以下一种：字节、千字节、兆字节、千兆字节。 |
| --disk-space-units=UNITS | 指定报告磁盘空间使用率所采用的单位。如果不指定，则磁盘空间以千兆字节报告。单位可以是以下一种：字节、千字节、兆字节、千兆字节。 |

| 名称 | 说明 |
|----------------------------|---|
| --aws-credential-file=PATH | 提供包含 AWS 凭据的文件的位置。 此参数不能与 --aws-access-key-id 和 --aws-secret-key 参数一起使用。 |
| --aws-access-key-id=VALUE | 指定用于识别发起人的 AWS 访问密钥 ID。必须与 --aws-secret-key 选项一起使用。请勿将此选项与 --aws-credential-file 参数一起使用。 |
| --aws-secret-key=VALUE | 指定用于签署 CloudWatch 请求的 AWS 秘密访问密钥。必须与 --aws-access-key-id 选项一起使用。请勿将此选项与 --aws-credential-file 参数一起使用。 |
| --aws-iam-role=VALUE | 指定用于提供 AWS 凭据的 IAM 角色。必须提供 =VALUE 值。如果不指定凭据，则会应用与 EC2 实例关联的默认 IAM 角色。只能使用一个 IAM 角色。如果未找到任何 IAM 角色，或者找到多个 IAM 角色，则脚本会返回一条错误信息。 请勿将此选项与 --aws-credential-file、--aws-access-key-id 或 --aws-secret-key 参数一起使用。 |
| --aggregated[=only] | 为实例类型、AMI ID 及区域整体情况添加聚合指标。=only 值为可选，如果指定，则脚本只会报告聚合指标。 |
| --auto-scaling[=only] | 为 Auto Scaling 组添加聚合指标。=only 值为可选，如果指定，则脚本只会报告 Auto Scaling 指标。使用脚本与 IAM 账户或角色关联的 IAM 策略 需要拥有许可方可调用 EC2 操作 DescribeTags 。 |
| --verify | 会对收集指标的脚本执行一次试运行，准备完整 HTTP 请求，但是不会调用 CloudWatch 以报告数据。此选项还会检查是否已提供凭据。在详细模式中运行时，此选项输出的指标会发送到 CloudWatch。 |
| --from-cron | 从 cron 调用脚本时，请使用此选项。使用此选项时，会阻止所有诊断输出，但错误消息会发送到用户账户的本地系统日志。 |
| --verbose | 显示脚本正在处理的内容的详细信息。 |
| --help | 显示使用率信息。 |
| --version | 显示脚本的版本号。 |

示例

以下示例假设您提供了一个 IAM 角色或 `awscreds.conf` 文件。否则，您必须使用 `--aws-access-key-id` 和 `--aws-secret-key` 参数为这些命令提供凭据。

执行简单试运行而不将数据发布到 CloudWatch

```
./mon-put-instance-data.pl --mem-util --verify --verbose
```

收集所有可用内存指标并将其发送到 CloudWatch

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail
```

为报告到 CloudWatch 的指标制定 cron 计划

1. 使用下列命令开始编辑 crontab：

```
crontab -e
```

2. 添加下列命令，每五分钟将内存和磁盘空间利用率报告到 CloudWatch：

```
*/5 * * * * ~/aws-scripts-mon/mon-put-instance-data.pl --mem-util --disk-space-util --disk-path=/ --from-cron
```

如果脚本遇到错误，则会在系统日志中写下错误消息。

收集 Auto Scaling 组的聚合指标并将其发送到 Amazon CloudWatch，但不报告单独的实例指标

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --auto-scaling=only
```

收集实例类型、AMI ID 和区域的聚合指标并将其发送到 Amazon CloudWatch，但不报告单独的实例指标

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --aggregated=only
```

mon-get-instance-stats.pl

此脚本可在使用最近小时数提供的时间间隔内查询 CloudWatch 中有关内存、交换和磁盘空间指标的统计数据。将为对其执行此脚本的 Amazon EC2 实例提供该数据。

选项

| 名称 | 说明 |
|----------------------------|---|
| --recent-hours=N | 指定报告依据的最近小时数，由 N 表示，其中 N 是一个整数。 |
| --aws-credential-file=PATH | 提供包含 AWS 凭据的文件的位置。 |
| --aws-access-key-id=VALUE | 指定用于识别发起人的 AWS 访问密钥 ID。必须与 --aws-secret-key 选项一起使用。请勿将此选项与 --aws-credential-file 选项一起使用。 |
| --aws-secret-key=VALUE | 指定用于签署 CloudWatch 请求的 AWS 秘密访问密钥。必须与 --aws-access-key-id 选项一起使用。请勿将此选项与 --aws-credential-file 选项一起使用。 |
| --aws-iam-role=VALUE | 指定用于提供 AWS 凭据的 IAM 角色。必须提供 =VALUE 值。如果不指定凭据，则会应用与 EC2 实例关联的默认 IAM 角色。只能使用一个 IAM 角色。如果未找到任何 IAM 角色，或者找到多个 IAM 角色，则脚本会返回一条错误信息。 请勿将此选项与 --aws-credential-file、--aws-access-key-id 或 --aws-secret-key 参数一起使用。 |
| --verify | 会对收集指标的脚本执行一次试运行，准备完整 HTTP 请求，但是不会调用 CloudWatch 以报告数据。此选项还会检查是否已提供凭据。在详细模式中运行时，此选项输出的指标会发送到 CloudWatch。 |
| --verbose | 显示脚本正在处理的内容的详细信息。 |

| 名称 | 说明 |
|-----------|-----------|
| --help | 显示使用率信息。 |
| --version | 显示脚本的版本号。 |

示例

要获得最近 12 小时的利用率统计数据，请运行以下命令：

```
./mon-get-instance-stats.pl --recent-hours=12
```

以下为响应示例：

```
Instance metric statistics for the last 12 hours.

CPU Utilization
    Average: 1.06%, Minimum: 0.00%, Maximum: 15.22%

Memory Utilization
    Average: 6.84%, Minimum: 6.82%, Maximum: 6.89%

Swap Utilization
    Average: N/A, Minimum: N/A, Maximum: N/A

Disk Space Utilization on /dev/xvda1 mounted as /
    Average: 9.69%, Minimum: 9.69%, Maximum: 9.69%
```

在控制台中查看自定义指标

在成功运行 `mon-put-instance-data.pl` 脚本后，您可以在 Amazon CloudWatch 控制台中查看自定义指标。

要查看自定义指标

1. 如前所述运行 `mon-put-instance-data.pl`。
2. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
3. 选择 View Metrics。
4. 对于 Viewing，由脚本发布的自定义指标带有前缀 `System/Linux`。

故障排除

`CloudWatchClient.pm` 模块在本地缓存实例元数据。如果您从运行监控脚本的实例中创建 AMI，在缓存 TTL（默认值：6 小时；对于 Auto Scaling 组为 24 小时）内从此 AMI 启动的任何实例都将使用原始实例的实例 ID 发送指标。缓存 TTL 时间段过后，脚本会检索新数据，监控脚本将使用当前实例的实例 ID。要立即更正此问题，请使用以下命令删除缓存数据：

```
rm /var/tmp/aws-mon/instance-id
```

网络与安全性

Amazon EC2 提供以下网络和安全功能。

特色

- [Amazon EC2 密钥对 \(p. 346\)](#)
- [Linux 实例的 Amazon EC2 个安全组 \(p. 354\)](#)
- [控制对 Amazon EC2 资源的访问 \(p. 366\)](#)
- [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 431\)](#)
- [Amazon EC2 实例 IP 寻址 \(p. 453\)](#)
- [弹性 IP 地址 \(p. 467\)](#)
- [弹性网络接口 \(p. 473\)](#)
- [置放群组 \(p. 487\)](#)
- [EC2 实例的网络最大传输单位 \(MTU\) \(p. 489\)](#)
- [Linux 上的增强联网 \(p. 492\)](#)

如果您使用命令行工具或 API 访问 Amazon EC2，则需要访问密钥 ID 和秘密访问密钥。有关更多信息，请参阅[如何获取安全证书？](#)（在 Amazon Web Services 一般参考 中）。

您可以在以下两个平台之一中启动实例：EC2-Classic 或 EC2-VPC。在 EC2-Classic 或默认 VPC 中启动的实例自动分配有一个公有 IP 地址。在非默认 VPC 中启动的实例可在启动时分配有一个公有 IP 地址。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 435\)](#)。

实例可能会因为您不可控的原因失败或终止。如果一个实例失败了，您又启动了一个替代实例，则该替代实例的公有 IP 地址与原有实例不同。但是，如果您的应用程序需要一个静态 IP 地址，您可以使用弹性 IP 地址。

您可以使用安全组来控制您的实例的访问权限。这些安全组类似于一个传入网络防火墙，使您可以指定允许访问您的实例的协议、端口和源 IP 范围。您可以创建多个安全组，并给每个安全组指定不同的规则。然后您可以给每个实例分配一个或多个安全组，我们将按照这些规则确定允许哪些流量可访问实例。您可以配置一个安全组，以便只有特定的 IP 地址或特定的安全组可以访问实例。

Amazon EC2 密钥对

Amazon EC2 使用公有密钥密码术加密和解密登录信息。公有密钥密码术使用公有密钥加密某个数据（如一个密码），然后收件人可以使用私有密钥解密数据。公有和私有密钥被称为密钥对。

要登录您的实例，您必须创建一个密钥对，并在启动实例时指定密钥对的名称，然后使用私有密钥连接实例。Linux 实例没有密码，您可以使用密钥对和 SSH 登录实例。对于 Windows 实例，您可以使用密钥对获得管理员密码，然后使用 RDP 登录实例。

创建密钥对

您可以使用 Amazon EC2 创建密钥对。有关更多信息，请参阅 [使用 Amazon EC2 创建密钥对 \(p. 347\)](#)。

或者，您也可以使用第三方工具，然后将公有密钥导入 Amazon EC2。有关更多信息，请参阅 [将您自己的公有密钥导入 Amazon EC2 \(p. 348\)](#)。

每个密钥对需要一个名称。切记选择一个容易记住的名称。Amazon EC2 会将公有密钥与您指定的密钥名称相关联。

Amazon EC2 只会存储公有密钥，您需要存储私有密钥。拥有您的私有密钥的任何人都可以解密您的登录信息，因此将您的私有密钥保存在一个安全的位置非常重要。

Amazon EC2 使用的密钥是 2048-bit SSH-2 RSA 密钥。对于每个区域，您可以拥有多达 5000 个密钥对。

启动并连接到您的实例

当您启动实例时，您应该指定计划用于连接到该实例的密钥对的名称。如果在启动实例时未指定现有密钥对的名称，您将无法连接到该实例。连接到实例时，您必须指定与启动该实例时指定的密钥对相对应的私有密钥。

Note

Amazon EC2 不保存私有密钥副本；因此，如果您丢失私有密钥，将无法恢复。如果丢失由实例存储支持的实例的私有密钥，您将无法访问该实例；您应该终止该实例并使用新的密钥对启动另一个实例。如果丢失由 EBS 支持的 Linux 实例的私有密钥，您可以重新获取对实例的访问权限。有关更多信息，请参阅 [丢失私有密钥时连接到 Linux 实例 \(p. 351\)](#)。

多个用户的密钥对

如果您有几个需要访问单个实例的用户，则可以向实例添加用户账户。有关更多信息，请参阅 [在 Linux 实例上管理用户账户 \(p. 280\)](#)。您可以为每个用户创建一个密钥对，并将每个密钥对中的公有密钥信息添加到您实例上的每个用户的 .ssh/authorized_keys 文件。然后，您可以将私有密钥文件分配给您的用户。这样一来，您不必将用于根账户的同一个私有密钥文件分配给多个用户。

内容

- [使用 Amazon EC2 创建密钥对 \(p. 347\)](#)
- [将您自己的公有密钥导入 Amazon EC2 \(p. 348\)](#)
- [在 Linux 上检索密钥对的公有密钥 \(p. 349\)](#)
- [在 Windows 上检索密钥对的公有密钥 \(p. 350\)](#)
- [验证您的密钥对指纹 \(p. 350\)](#)
- [删除您的密钥对 \(p. 351\)](#)
- [丢失私有密钥时连接到 Linux 实例 \(p. 351\)](#)

使用 Amazon EC2 创建密钥对

您可以使用 Amazon EC2 控制台或命令行创建密钥对。创建密钥对之后，您可以在启动实例时指定它。您还可以向运行的实例添加密钥对以便使其他用户可以连接到该实例。有关更多信息，请参阅 [在 Linux 实例上管理用户账户 \(p. 280\)](#)。

使用 Amazon EC2 控制台创建密钥对

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。

Tip

导航窗格位于 Amazon EC2 控制台的左侧。如果您看不到窗格，它可能被最小化了；请选择箭头展开该窗格。

3. 选择 Create Key Pair。
4. 在 Create Key Pair 对话框的 Key pair name 字段中输入新密钥对的名称，然后选择 Create。
5. 您的浏览器会自动下载私有密钥文件。基本文件名是您为密钥对指定的名称，文件扩展名为 .pem。将私有密钥文件保存在安全位置。

Important

这是您保存私有密钥文件的唯一机会。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

6. 如果您将在 Mac 或 Linux 计算机上使用 SSH 客户端连接到您的 Linux 实例，请使用以下命令设置您私有密钥文件的权限，以确保只有您可以读取它。

```
$ chmod 400 my-key-pair.pem
```

使用命令行创建密钥对

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-key-pair \(AWS CLI\)](#)
- [New-EC2KeyPair \(适用于 Windows PowerShell 的 AWS 工具\)](#)

将您自己的公有密钥导入 Amazon EC2

如果不使用 Amazon EC2 创建密钥对，您可以使用第三方工具创建一个 RSA 密钥对，然后将公有密钥导入 Amazon EC2。举例来说，您可以使用 ssh-keygen (通过标准 OpenSSH 安装提供的工具) 创建密钥对。或者，您可以使用 Java、Ruby、Python 和许多其他提供标准库的编程语言来创建 RSA 密钥对。

Amazon EC2 接受以下格式：

- OpenSSH 公有密钥格式 (格式为 ~/.ssh/authorized_keys)
- Base64 编码的 DER 格式
- 如在[RFC4716](#)指定的 SSH 公有密钥文件格式

Amazon EC2 不接受 DSA 密钥。请确保您的密钥生成器被设置为创建 RSA 密钥。

支持的长度：1024、2048 和 4096。

要使用第三方工具创建密钥对

1. 使用您选择的第三方工具生成密钥对。
2. 将公有密钥保存至本地文件。例如，~/.ssh/my-key-pair.pub (Linux) 或 C:\keys\my-key-pair.pub (Windows)。此文件的文件扩展名并不重要。
3. 将私有密钥保存到扩展名为 .pem 的不同本地文件中。例如，~/.ssh/my-key-pair.pem (Linux) 或 C:\keys\my-key-pair.pem (Windows)。将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

使用 Amazon EC2 控制台通过以下步骤导入密钥对。

导入公有密钥

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
3. 选择 Import Key Pair。
4. 在 Import Key Pair 对话框中，选择 Browse，然后选择之前保存的公有密钥文件。在 Key pair name 字段中为新的密钥对键入一个名称，然后选择 Import。

使用命令行导入公有密钥

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [import-key-pair \(AWS CLI\)](#)
- [Import-EC2KeyPair \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在成功导入公有密钥文件后，您可以按照以下说明使用 Amazon EC2 控制台验证密钥对是否成功导入。

验证密钥对是否已导入

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中，选择您在其中创建密钥对的区域。
3. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
4. 验证您导入的密钥对是否在密钥对的显示列表中。

使用命令行查看密钥对

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-key-pairs \(AWS CLI\)](#)
- [Get-EC2KeyPair \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在 Linux 上检索密钥对的公有密钥

在 Linux 实例中，公有密钥内容放在 `~/.ssh/authorized_keys` 内的条目中。此操作在启动时完成，使您无需密码即可安全地访问实例。您可以在编辑器中打开此文件，以查看密钥对的公有密钥。以下是名为 `my-key-pair` 的密钥对的示例条目。它包括后跟密钥对名称的公有密钥。例如：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckij7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAHC0+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwi3f05p6KLxEXAMPLE my-key-pair
```

您可以使用 `ssh-keygen` 获取密钥对的公有密钥。在您已将私有密钥下载到的计算机上运行以下命令：

```
$ ssh-keygen -y
```

在提示输入密钥所在的文件时，请指定您的 `.pem` 文件的路径，例如：

```
/path_to_key_pair/my-key-pair.pem
```

该命令将返回公有密钥：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOwbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUzofz221CBt5IMucxxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

如果此命令失败，请运行以下命令以确保更改对您的密钥对文件的权限，以便只有您才能查看该文件：

```
$ chmod 400 my-key-pair.pem
```

您在启动实例时指定的公有密钥也可以通过实例元数据使用。要查看您在启动实例时指定的公有密钥，请从您的实例中使用以下命令：

```
$ GET http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOwbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUzofz221CBt5IMucxxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

有关更多信息，请参阅 [检索实例元数据 \(p. 296\)](#)。

请注意，如果您更改用于连接到实例的密钥对（如本页最后一部分所示），我们将不会更新实例元数据以显示新的公有密钥；您看到的仍是当您启动实例时在实例元数据中为密钥对指定的公有密钥。

在 Windows 上检索密钥对的公有密钥

在 Windows 上，您可以使用 PuTTYgen 获取密钥对的公有密钥。启动 PuTTYgen，单击 Load (加载)，然后选择 .ppk 或 .pem 文件。PuTTYgen 会显示公有密钥。

您在启动实例时指定的公有密钥也可以通过实例元数据使用。要查看您在启动实例时指定的公有密钥，请从您的实例中使用以下命令：

```
$ GET http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOwbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUzofz221CBt5IMucxxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

有关更多信息，请参阅 [检索实例元数据 \(p. 296\)](#)。

验证您的密钥对指纹

在 Amazon EC2 控制台的 Key Pairs (密钥对) 页面上，Fingerprint (指纹) 列显示从您的密钥对生成的指纹。AWS 根据密钥对是由 AWS 还是第三方工具生成以不同方式计算指纹。如果您是使用 AWS 创建的密钥对，则会使用 SHA-1 哈希函数计算指纹。如果您使用第三方工具创建了密钥对并将公有密钥上传到 AWS，或者如果您从一个现有的 AWS 创建的私有密钥生成了一个新的公有密钥并将其上传到 AWS，则会使用 MD5 哈希函数计算指纹。

您可以使用 Key Pairs (密钥对) 页面上显示的指纹验证您本地计算机上的私有密钥是否与 AWS 中存储的公有密钥匹配。

如果您使用 AWS 创建了密钥对，那么您可以使用 OpenSSL 工具从私有密钥文件生成指纹：

```
$ openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt | openssl
sha1 -c
```

如果您使用第三方工具创建了密钥对并将公有密钥上传到 AWS，则可以使用 OpenSSL 工具从您本地计算机上的私有密钥文件生成指纹。

```
$ openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

输出应与控制台中显示的指纹匹配。

删除您的密钥对

当您删除密钥对时，仅删除 Amazon EC2 的公有密钥副本。删除密钥对不影响您计算机上的私有密钥或是已使用该密钥对启动的任何实例上的公有密钥。您不能使用已删除的密钥对启动新实例，不过，只要您仍然有私有密钥 (.pem) 文件，就可以继续连接到使用已删除的密钥对启动的任何实例。

Note

如果您使用的是 Auto Scaling 组（例如，在 Elastic Beanstalk 环境中），请确保您要删除的密钥对未在启动配置中指定。Auto Scaling 检测到运行不正常的实例时会启动替代实例；但是，如果找不到密钥对，实例将启动失败。

您可以使用 Amazon EC2 控制台或命令行删除密钥对。

使用控制台删除密钥对

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
3. 选择密钥对，然后选择 Delete。
4. 系统提示时，请选择 Yes。

使用命令行删除密钥对

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [delete-key-pair \(AWS CLI\)](#)
- [Remove-EC2KeyPair \(适用于 Windows PowerShell 的 AWS 工具\)](#)

Note

如果您从一个实例创建了一个 Linux AMI，然后在不同区域或账户中使用该 AMI 启动一个新实例，则新实例将包含来自原始实例的公有密钥。这允许您使用与原始实例相同的私有密钥连接到新实例。您可以使用任意文本编辑器从 .ssh/authorized_keys 文件中删除此公有密钥的条目，从而从实例中删除此公有密钥。有关管理您的实例用户和使用特定密钥对提供远程访问的更多信息，请参阅 [在 Linux 实例上管理用户账户 \(p. 280\)](#)。

丢失私有密钥时连接到 Linux 实例

如果丢失由 EBS 支持的实例的私有密钥，您可以重新获取对您实例的访问权限。您必须停止实例，断开根卷并将其作为数据卷连接到另一个实例，然后修改 authorized_keys 文件，将卷移回原始实例，并重启实例。有关启动、连接和停止实例的更多信息，请参阅 [实例生命周期 \(p. 241\)](#)。

对于实例存储支持的实例。若要确定实例的根设备类型，请打开 Amazon EC2 控制台，选择 Instances，选择实例，然后在详细信息窗格中检查 Root device type 的值。该值为 ebs 或 instance store。如果根设备是实例存储卷，则必须拥有私有密钥才能连接到实例。

先决条件

使用 Amazon EC2 控制台或第三方工具创建新的密钥对。如果您要将新密钥对的名称设置为与丢失的私有密钥相同的名称，则必须先删除现有密钥对。

使用另一密钥对连接由 EBS 支持的实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中选择 Instances，然后选择要连接到的实例。(我们将此称为原始实例。)
3. 保存您完成此过程将需要的以下信息。
 - 记下原始实例的实例 ID、AMI ID 和可用区。
 - 在根设备字段中，请记下根卷的设备名称(例如 /dev/sda1 或 /dev/xvda)。选择链接并在 EBS ID 字段中输入卷 ID (vol-xxxxxxxxxxxxxxx)。
 - [EC2-Classic] 如果原始实例拥有关联的弹性 IP 地址，请记下详细信息窗格的 Elastic IP 字段中显示的弹性 IP 地址。
4. 依次选择 Actions、Instance State 和 Stop。如果 Stop (停止) 处于禁用状态，则表示要么实例已停止，要么其根设备是一个实例存储卷。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

5. 选择 Launch Instance，然后使用启动向导通过以下选项启动一个临时实例：
 - 在 Choose an AMI (选择一个 AMI) 页面上，选择您启动原始实例时所用的 AMI。如果此 AMI 不可用，您可以创建一个可在已停止的实例中使用的 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)。
 - 在 Choose an Instance Type (选择一个实例类型) 页上，保留向导为您选择的默认实例类型。
 - 在 Configure Instance Details (配置实例详细信息) 页面上，指定与您要连接的实例所在的可用区。如果您在 VPC 中启动实例，请选择此可用区中的一个子网。
 - 在 Add Tags 页面上，向实例添加标签 Name=Temporary 以指示这是一个临时实例。
 - 在 Review 页面上，选择 Launch。创建新的密钥对，将它下载到您计算机中的安全位置，然后选择 Launch Instances。
6. 在导航窗格中，选择 Volumes，并选择原始实例的根设备卷(您已在上一步骤中记下它的卷 ID)。选择 Actions，然后选择 Detach Volume。等待卷的状态变为 available。(您可能需要选择 Refresh 图标。)
7. 如果卷仍保持选中状态，则选择 Actions，然后选择 Attach Volume。选择临时实例的实例 ID，记下在 Device 下指定的设备名称(例如，/dev/sdf)，然后选择 Yes, Attach。

Note

如果已从 AWS Marketplace AMI 启动原始实例，并且卷包含 AWS Marketplace 代码，则必须先停止临时实例，然后才能附加卷。

8. 连接到临时实例。
9. 在临时实例中，安装连接到实例的卷，以访问其文件系统。例如，如果设备名称为 /dev/sdf，请使用以下命令将卷作为 /mnt/tempvol 安装。

Note

您的实例上显示的设备名称可能不同。例如，作为 /dev/sdf 安装的设备可能在实例上显示为 /dev/xvdf。某些版本的 Red Hat (或其变体，如 CentOS) 甚至可能将尾部字母增加 4 个字符，其中 /dev/sdf 成为 /dev/xvdk。

- a. 使用 lsblk 命令确定卷是否已分区。

```
[ec2-user ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda   202:0    0   8G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf   202:80   0 101G  0 disk
##xvdf1 202:81   0 101G  0 part
```

```
xvdfg      202:96    0    30G  0 disk
```

在以上示例中，`/dev/xvda` 和 `/dev/xvdf` 卷已分区，`/dev/xvdfg` 未分区。如果您的卷已分区，则应在后续步骤中安装分区 (`/dev/xvdf1`) 而不是原始设备 (`/dev/xvdf`)。

- b. 创建临时目录以安装卷。

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

- c. 使用之前确定的卷名称或设备名称在临时安装点安装卷 (或分区)。

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

10. 在临时实例上，使用以下命令将已安装卷上的 `authorized_keys` 更新为来自临时实例 `authorized_keys` 的新公有密钥 (可能需要在以下命令中换入不同的用户名，如用于实例的 `ubuntu`)：

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

如果复制成功，则可以转到下一步骤。

(可选) 如果您没有权限编辑 `/mnt/tempvol` 中的文件，则需要使用 `sudo` 更新文件，然后检查文件的权限，以验证您是否能够登录原始实例。请使用以下命令检查文件权限：

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh  
total 4  
-rw----- 1 222 500 398 Sep 13 22:54 authorized_keys
```

在这个输出示例中，`222` 是用户 ID；`500` 是组 ID。接下来，请使用 `sudo` 重新运行失败的复制命令：

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/  
authorized_keys
```

再次运行以下命令以确定权限是否已更改：

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

如果用户 ID 和组 ID 已经更改，请使用以下命令进行恢复：

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

11. 在临时实例中，卸载已连接的卷，以将其重新连接至原始实例。例如，使用以下命令卸载 `/mnt/tempvol` 处的卷：

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

12. 在 Amazon EC2 控制台中，选择您已记下卷 ID 的卷，选择 Actions，然后选择 Detach Volume。等待卷的状态变为 available。(您可能需要选择 Refresh 图标。)

13. 如果卷仍保持选中状态，则选择操作，然后选择 Attach Volume。选择原始实例的实例 ID，将设备名称指定为您之前在附加原始根设备时记录的名称 (`/dev/sda1` 或 `/dev/xvda`)，然后选择 Yes, Attach。

Warning

如果您不指定与原始附加相同的设备名称，则无法启动原始实例。Amazon EC2 要求根设备卷位于 `sda1` 或 `/dev/xvda`。

14. 选择原始实例，选择 Actions，选择 Instance State，然后选择 Start。在实例进入 running 状态后，您可以使用新密钥对的私有密钥文件连接到该实例。

Note

如果您的新密钥对和相应私有密钥文件的名称不同于原始密钥对的名称，请确保在连接到实例时指定新私有密钥文件的名称。

15. [EC2-Classic] 如果原始实例在停止前拥有相关联的弹性 IP 地址，您必须按照以下说明重新将其与该实例关联起来：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择您在此程序开始时记下的弹性 IP 地址。
 - c. 选择 Actions，然后选择 Associate address。
 - d. 选择原始实例的 ID，然后选择 Associate。
16. (可选) 如果您将不再使用临时实例，可以将其终止。选择临时实例，选择 Actions，选择 Instance State，然后选择 Terminate。

Linux 实例的 Amazon EC2 安全组

安全组 起着虚拟防火墙的作用，可控制一个或多个实例的流量。在您启动实例时，将一个或多个安全组与该实例相关联。为每个安全组添加规则，规定流入或流出其关联实例的流量。您可以随时修改安全组的规则；新规则会自动应用于与该安全组相关联的所有实例。在决定是否允许流量到达实例时，我们会评估与实例相关联的所有安全组中的所有规则。

如果需要允许流量进入 Windows 实例，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[适用于 Windows 实例的 Amazon EC2 安全组](#)。

主题

- [EC2-Classic 安全组 \(p. 354\)](#)
- [EC2-VPC 安全组 \(p. 355\)](#)
- [安全组规则 \(p. 355\)](#)
- [默认安全组 \(p. 357\)](#)
- [自定义安全组 \(p. 357\)](#)
- [使用安全组 \(p. 357\)](#)
- [安全组规则引用 \(p. 361\)](#)

如果有安全组不满足的要求，除了使用安全组外，您还可以在任何一个实例上保持自己的防火墙。

在某些区域，您的账户可能支持 EC2-Classic，具体取决于您创建账户的时间。有关更多信息，请参阅[支持的平台 \(p. 435\)](#)。EC2-Classic 的安全组独立于 EC2-VPC 的安全组。

EC2-Classic 安全组

如果要使用 EC2-Classic，则必须使用为 EC2-Classic 专门创建的安全组。当您在 EC2-Classic 中启动实例时，您必须在实例所在的相同区域指定一个安全组。在 EC2-Classic 中启动实例时，您无法指定为 VPC 创建的安全组。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。但是，您可以向安全组添加或从中删除规则，并且这些更改会自动应用于与该安全组相关联的所有实例。

在 EC2-Classic 中，您可以在每个区域为每个账户创建多达 500 个安全组。您可以将一个实例与多达 500 个安全组关联，并且最多可以为一个安全组添加 100 条规则。

EC2-VPC 安全组

如果您正在使用 EC2-VPC，则必须使用专为 VPC 创建的安全组。在 VPC 中启动实例时，您必须为该 VPC 指定一个安全组。在 VPC 中启动实例时，您无法指定为 EC2-Classic 创建的安全组。EC2-VPC 安全组具有 EC2-Classic 安全组不支持的额外功能。有关详细信息，请参阅 Amazon VPC 用户指南中的 [EC2-Classic 和 EC2-VPC 安全组之间的差异](#)。

在 VPC 中启动实例后，您可以更改其安全组。安全组与网络接口关联。更改实例的安全组也会更改与主网络接口 (eth0) 关联的安全组。想要了解更多有关信息，请参阅 Amazon VPC 用户指南中的 [更改实例的安全组主题](#)。您还可以更改与任何其他网络接口关联的安全组。有关更多信息，请参阅 [更改安全组 \(p. 483\)](#)。

EC2-VPC 的安全组有单独的限制。有关更多信息，请参阅 Amazon VPC 用户指南中的 [Amazon VPC 限制](#)。EC2-Classic 安全组不会根据 EC2-VPC 安全组限额来计数。

您可以为 VPC 启用 IPv6。有关更多信息，请参阅 Amazon VPC 用户指南中的 [您的 VPC 中的 IP 地址](#)。您可以将规则添加到 VPC 安全组以启用入站和出站 IPv6 流量。

安全组规则

安全组规则可控制允许到达与安全组相关联的实例的入站流量以及允许离开实例的出站流量。

以下是您的安全组规则的特征：

- 默认情况下，安全组允许所有出站流量。
- 您无法更改 EC2-Classic 安全组的出站规则。
- 安全组规则始终是宽松的；您无法创建拒绝访问的规则。
- 安全组是有状态的 — 如果您从实例发送一个请求，则无论入站安全组规则如何，都将允许该请求的响应流量流入。对于 VPC 安全组，这还意味着，无论出站规则如何，都允许对允许的入站流量的响应流出。有关更多信息，请参阅 [连接跟踪 \(p. 356\)](#)。
- 您可以随时添加和删除规则。您的更改稍后会自动应用于与安全组相关联的实例。

Note

某些规则变更产生的影响可能会取决于跟踪流量的方式。有关更多信息，请参阅 [连接跟踪 \(p. 356\)](#)。

- 当您将多个安全组与一个实例相关联时，将有效汇总每个安全组的规则，以创建一组规则。我们使用这组规则确定是否允许访问。

Note

您可以给一个实例分配多个安全组，因此一个实例可能会应用数百条规则。访问该实例时，这可能会导致问题。因此，我们建议您尽可能使规则简洁。

对于每个规则，您可以指定以下内容：

- 协议：允许的协议。最常见的协议为 6 (TCP) 17 (UDP) 和 1 (ICMP)。
- 端口范围：对于 TCP、UDP 或自定义协议，允许的端口范围。您可以指定单个端口号（例如 22）或端口号范围（例如 7000-8000）。
- ICMP 类型和代码：对于 ICMP，ICMP 类型和代码。
- 源或目标：流量的源（入站规则）或目标（出站规则）。请指定以下选项之一：
 - 一个单独的 IPv4 地址。您必须在 IPv4 地址后使用 /32 前缀，例如，203.0.113.1/32。
 - （仅限 VPC）一个单独的 IPv6 地址。您必须使用 /128 前缀长度；例如，2001:db8:1234:1a00::123/128。
 - 采用 CIDR 块表示法的 IPv4 地址范围，例如，203.0.113.0/24。
 - （仅限 VPC）采用 CIDR 块表示法的 IPv6 地址范围，例如，2001:db8:1234:1a00::/64。

- 其他安全组。这样，与指定安全组关联的实例就可以访问与该安全组关联的实例。这并不会将源安全组的规则添加到该安全组。您可以指定以下安全组之一：
 - 当前安全组。
 - EC2-Classic：同一区域的另一个 EC2-Classic 安全组。
 - EC2-Classic：同一区域中另一个 AWS 账户的安全组 (添加 AWS 账户 ID 作为前缀；例如，`111122223333/sg-edcd9784`)。
 - EC2-VPC：VPC 对等连接中的同一 VPC 或对等 VPC 的其他安全组。

当您指定一个安全组为规则的源或目标时，该规则会影响与安全组相关联的所有实例。允许的传入流量基于与源安全组相关联的实例的私有 IP 地址 (而不是公有 IP 或弹性 IP 地址)。有关 IP 地址的更多信息，请参阅 [Amazon EC2 实例 IP 寻址 \(p. 453\)](#)。如果您的安全组规则引用对等 VPC 中的一个安全组，并且引用的安全组或 VPC 对等连接已删除，则该规则将会标记为过时。有关更多信息，请参阅 Amazon VPC Peering Guide 中的 [使用过时的安全组规则](#)。

如果特定端口有多条规则，我们会使用最宽松的规则。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)，而另一条规则允许所有人访问 TCP 端口 22，那么所有人都可以访问 TCP 端口 22。

连接跟踪

您的安全组使用连接跟踪来跟踪有关进出实例的流量的信息。将基于流量的连接状态应用规则以确定允许还是拒绝流量。这使安全组可以是有状态的 - 无论出站安全组规则如何都允许对入站流量的响应流出实例，反之亦然。例如，如果您从您的家用计算机对实例启动 ICMP ping 命令，并且您的入站安全组规则允许 ICMP 流量，则会跟踪有关连接的信息 (包括端口信息)。来自 ping 命令的实例的响应流量不会作为新请求来跟踪，而是作为已建立的连接来跟踪，并且可以流出实例，即使您的出站安全组规则限制出站 ICMP 流量也是如此。

并非所有通信流都会被跟踪。如果安全组规则允许所有流量的 TCP 或 UDP 流 (`0.0.0.0/0`)，并且另一个方向存在允许所有响应流量的对应规则 (`0.0.0.0/0`)，则不会跟踪该流量。因此，允许响应流量基于允许响应流量的入站或出站规则流动，而不是基于跟踪信息流动。在以下示例中，安全组具有用于 SSH、HTTP 和 ICMP 流量的特定入站规则，并具有一个允许所有出站流量的出站规则。

| 入站规则 | | |
|------|-----------|-----------------------------|
| 协议类型 | 端口号 | 源 IP |
| TCP | 22 (SSH) | <code>203.0.113.1/32</code> |
| TCP | 80 (HTTP) | <code>0.0.0.0/0</code> |
| ICMP | 全部 | <code>0.0.0.0/0</code> |
| 出站规则 | | |
| 协议类型 | 端口号 | 目的地 IP |
| 全部 | 全部 | <code>0.0.0.0/0</code> |

由于限制性入站规则，将跟踪流入和流出实例的 SSH 流量。无论规则如何，始终跟踪 ICMP 流量。由于入站和出站规则都允许所有 HTTP 流量，因此不跟踪流入和流出实例的 HTTP 流量。

跟踪的现有通信流在您删除支持该流的安全组规则后可能不会被中断。相反，在您或其他主机停止该流至少几分钟 (对于已建立的 TCP 连接，最多 5 天) 后，它才会中断。对于 UDP，这可能需要终止对流的远程操作。如果删除或修改了支持该流的规则，则会立即中断未被跟踪的通信流。例如，如果您删除了允许所有入站 SSH 流量流入实例的规则，则与该实例的现有 SSH 连接将会立即中断。

对于除 TCP、UDP 或 ICMP 以外的协议，仅跟踪 IP 地址和协议编号。如果您的实例将流量发送到另一台主机（主机 B），并且在原始请求或响应的 600 秒内，主机 B 在单独的请求中发起到您的实例的同一类型的流量，则无论入站安全组规则如何，您的实例都将接受该请求，因为该流量被视为响应流量。

对于 VPC 安全组，要确保该流量在您删除安全组规则后立即中断，或确保所有入站流量均遵循防火墙规则，您可以使用您子网的网络 ACL — 网络 ACL 是无状态的，因此不会自动允许响应流量。有关更多信息，请参阅 Amazon VPC 用户指南 中的[网络 ACL](#)。

默认安全组

您的 AWS 账户在每个 VPC 和每个区域都自动拥有一个 EC2-Classic 默认安全组。如果您在启动实例时没有指定安全组，实例会自动与默认安全组关联。

默认安全组名称为 `default`，而且拥有一个由 AWS 分配的 ID。以下是每个默认安全组的默认规则：

- 允许来自与默认安全组关联的其他实例的所有入站流量（该安全组在其入站规则中将其自身指定为源安全组）
- 允许从实例流出的所有出站流量。

您可以添加或删除任何默认安全组的入站规则。您可以添加或删除任何 VPC 默认安全组的出站规则。

您无法删除默认安全组。如果您尝试删除 EC2-Classic 默认安全组，会显示以下错误：

错误：Client.InvalidGroup.Reserved: The security group 'default' is reserved。如果您尝试删除 VPC 默认安全组，会显示以下错误：Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user。

自定义安全组

如果您不希望您的实例使用默认安全组，则可创建自己的安全组，并在启动实例时指定它们。您可以创建多个安全组以反映实例扮演的不同角色；例如，Web 服务器或数据库服务器。

创建安全组时，您必须为其提供名称和描述。安全组的名称和描述最多 255 个字符，而且仅限于以下字符：

- EC2-Classic：ASCII 字符
- EC2-VPC：a-z、A-Z、0-9、空格和 `_:-/()#,@[]+=&;!$*`

以下是您创建的安全组的默认规则：

- 不允许入站流量
- 允许所有出站流量

创建安全组后，您可以更改其入站规则，以反映您希望到达关联实例的入站流量的类型。在 EC2-VPC 中，您也可以更改其出站规则。

有关您可以添加到安全组的规则类型的更多信息，请参阅[安全组规则引用 \(p. 361\)](#)。

使用安全组

您可以使用 Amazon EC2 控制台创建、查看、更新和删除安全组及安全组规则。

内容

- [正在创建安全组 \(p. 358\)](#)
- [描述您的安全组 \(p. 358\)](#)
- [向安全组添加规则 \(p. 359\)](#)

- [从安全组中删除规则 \(p. 360\)](#)
- [正在删除安全组 \(p. 360\)](#)
- [API 和命令概览 \(p. 360\)](#)

正在创建安全组

您可以使用 Amazon EC2 控制台创建自定义安全组。对于 EC2-VPC，您必须指定您正在为其创建安全组的 VPC。

创建新安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 为安全组指定名称和描述。
5. (仅限 EC2-Classic) 要创建在 EC2-Classic 中使用的安全组，请选择无 VPC。
- (EC2-VPC) 对于 VPC，请选择一个 VPC ID，以为该 VPC 创建安全组。
6. 您可以开始添加规则，也可以选择 Create 以立即创建安全组 (您可以在以后随时添加规则)。有关添加规则的更多信息，请参阅[向安全组添加规则 \(p. 359\)](#)。

借助 Amazon EC2 控制台，您可以将规则从现有安全组复制到新的安全组。

复制安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择您要复制的安全组，然后依次选择操作、复制到新项目。
4. Create Security Group (创建安全组) 对话框随即打开，其中预填充了现有安全组中的规则。为新的安全组指定名称和说明。在 VPC 列表中，选择 No VPC 以创建 EC2-Classic 的安全组，或选择 VPC ID 以创建该 VPC 的安全组。完成后，选择 Create。

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。在 VPC 中启动实例后，您可以更改其安全组。想要了解更多信息，请参阅 Amazon VPC 用户指南中的[更改实例的安全组](#)主题。

描述您的安全组

描述您的 EC2-Classic 安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 从筛选列表中选择 Network Platforms，然后选择 EC2-Classic。
4. 选择一个安全组。描述选项卡中将显示常规信息。入站选项卡中将显示入站规则。

描述您的 EC2-VPC 安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。

3. 从筛选列表中选择 Network Platforms，然后选择 EC2-VPC。
4. 选择一个安全组。我们将在 Description (描述) 选项卡上显示常规信息，在 Inbound (入站) 选项卡上显示入站规则，并在 Outbound (出站) 选项卡上显示出站规则。

向安全组添加规则

当您向安全组添加规则时，这一新规则会自动应用于与该安全组相关联的任何实例。

有关选择允许特定类型访问的安全组规则的更多信息，请参阅 [安全组规则引用 \(p. 361\)](#)。

向安全组添加规则

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择安全组，然后选择相应安全组。
3. 在 Inbound 选项卡上，选择 Edit。
4. 在对话框中选择添加规则并执行以下操作：
 - 对于类型，请选择相应协议。
 - 如果您选择自定义 TCP 或 UDP 协议，请在端口范围中指定端口范围。
 - 如果您选择自定义 ICMP 协议，请从协议中选择 ICMP 类型名称，并从端口范围中选择代码名称（如果适用）。
 - 对于源，请选择下列选项之一：
 - 自定义：在提供的字段中，您必须用 CIDR 表示法指定一个 IP 地址、CIDR 块或者其他安全组。
 - 任何位置：自动添加 `0.0.0.0/0` IPv4 CIDR 块。使用此选项后，指定类型的所有流量都可达到您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产中，请仅授权特定 IP 地址或地址范围访问您的实例。

Note

如果您的安全组位于已启用 IPv6 的 VPC 中，选择任何位置选项后，系统会创建两个规则，一个用于 IPv4 流量 (`0.0.0.0/0`)，一个用于 IPv6 流量 (`::/0`)。

- 我的 IP：自动添加本地计算机的公有 IPv4 地址。

有关您可以添加的规则类型的更多信息，请参阅 [安全组规则引用 \(p. 361\)](#)。

5. 选择 Save。
6. 对于 VPC 安全组，您还可以指定出站规则。在出站选项卡中，依次选择编辑、添加规则，并执行以下操作：
 - 对于类型，请选择相应协议。
 - 如果您选择自定义 TCP 或 UDP 协议，请在端口范围中指定端口范围。
 - 如果您选择自定义 ICMP 协议，请从协议中选择 ICMP 类型名称，并从端口范围中选择代码名称（如果适用）。
 - 对于目标，请选择下列选项之一：
 - 自定义：在提供的字段中，您必须用 CIDR 表示法指定一个 IP 地址、CIDR 块或者其他安全组。
 - 任何位置：自动添加 `0.0.0.0/0` IPv4 CIDR 块。此选项允许出站流量流向所有 IP 地址。

Note

如果您的安全组位于已启用 IPv6 的 VPC 中，选择任何位置选项后，系统会创建两个规则，一个用于 IPv4 流量 (`0.0.0.0/0`)，一个用于 IPv6 流量 (`::/0`)。

- 我的 IP：自动添加本地计算机的 IP 地址。

7. 选择 Save。

从安全组中删除规则

当您从安全组中删除规则时，此更改会自动应用于与该安全组相关联的任何实例。

要删除安全组规则

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择一个安全组。
4. 在入站选项卡中（用于入站规则）或出站选项卡中（用于出站规则），请选择编辑。选择要删除的每个规则旁边的删除（十字图标）。
5. 选择 Save。

正在删除安全组

您不能删除与实例相关联的安全组。您不能删除默认安全组。您不能删除由同一 VPC 中其他安全组中的规则引用的安全组。如果您的安全组由自己的一个规则引用，则必须先删除该规则，然后才能删除安全组。

删除安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择一个安全组，然后依次选择操作、删除安全组。
4. 选择 Yes, Delete。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

当您使用命令行工具为非默认 VPC 指定安全组时，必须使用安全组 ID（而非安全组名称）来识别安全组。

创建安全组

- [create-security-group \(AWS CLI\)](#)
- [New-EC2SecurityGroup \(适用于 Windows PowerShell 的 AWS 工具\)](#)

向安全组添加一个或多个传入规则

- [authorize-security-group-ingress \(AWS CLI\)](#)
- [Grant-EC2SecurityGroupIngress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

[EC2-VPC] 向安全组添加一个或多个传出规则

- [authorize-security-group-egress \(AWS CLI\)](#)
- [Grant-EC2SecurityGroupEgress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

说明一个或多个安全组

- [describe-security-groups \(AWS CLI\)](#)
- [Get-EC2SecurityGroup \(适用于 Windows PowerShell 的 AWS 工具\)](#)

[EC2-VPC] 修改实例的安全组

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

从安全组中删除一个或多个传入规则

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

[EC2-VPC] 从安全组中删除一个或多个传出规则

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

删除安全组

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

安全组规则引用

您可以创建安全组，并添加可反映与安全组关联的实例角色的规则。例如，配置为 Web 服务器的实例需要允许入站 HTTP 和 HTTPS 访问的安全组规则，而数据库实例需要允许数据库类型访问的规则，例如通过端口 3306 访问 MySQL。

以下是您可以添加到允许特定类型访问的安全组的规则类型示例。

主题

- [Web 服务器 \(p. 361\)](#)
- [数据库服务器 \(p. 362\)](#)
- [来自同一组内的其他实例的访问 \(p. 363\)](#)
- [从本地计算机进行访问 \(p. 363\)](#)
- [路径 MTU 发现 \(p. 364\)](#)
- [对实例执行 ping 操作 \(p. 364\)](#)
- [DNS 服务器 \(p. 364\)](#)
- [Amazon EFS 文件系统 \(p. 365\)](#)
- [Elastic Load Balancing \(p. 365\)](#)

Web 服务器

以下入站规则允许来自任何 IP 地址的 HTTP 和 HTTPS 访问。如果您为 VPC 启用了 IPv6，则可添加规则以控制来自 IPv6 地址的入站 HTTP 和 HTTPS 流量。

| 协议类型 | 协议编号 | Port | 源 IP | 备注 |
|------|------|-----------|-----------|----------------------------|
| TCP | 6 | 80 (HTTP) | 0.0.0.0/0 | 允许来自任何 IPv4 地址的入站 HTTP 访问。 |

| 协议类型 | 协议编号 | Port | 源 IP | 备注 |
|------|------|-------------|-----------|-------------------------------------|
| TCP | 6 | 443 (HTTPS) | 0.0.0.0/0 | 允许来自任何 IPv4 地址的入站 HTTPS 访问 |
| TCP | 6 | 80 (HTTP) | ::/0 | (仅限 VPC) 允许来自任何 IPv6 地址的入站 HTTP 访问 |
| TCP | 6 | 443 (HTTPS) | ::/0 | (仅限 VPC) 允许来自任何 IPv6 地址的入站 HTTPS 访问 |

数据库服务器

以下入站规则是您可以为数据库访问添加的规则示例，具体取决于您在实例运行的数据库类型。有关 Amazon RDS 实例的更多信息，请参阅 [Amazon Relational Database Service 用户指南](#)。

对于源 IP，请指定以下其中一项：

- 您的本地网络中的特定 IP 地址或 IP 地址范围
- 访问数据库的一组实例的安全组 ID

| 协议类型 | 协议编号 | Port | 备注 |
|------|------|---------------------|--|
| TCP | 6 | 1433 (MS SQL) | 访问 Microsoft SQL Server 数据库的默认端口，例如，在 Amazon RDS 实例上 |
| TCP | 6 | 3306 (MySQL/Aurora) | 访问 MySQL 或 Aurora 数据库的默认端口，例如，在 Amazon RDS 实例上 |
| TCP | 6 | 5439 (Redshift) | 访问 Amazon Redshift 群集数据库的默认端口。 |
| TCP | 6 | 5432 (PostgreSQL) | 访问 PostgreSQL 数据库的默认端口，例如，在 Amazon RDS 实例上 |
| TCP | 6 | 1521 (Oracle) | 访问 Oracle 数据库的默认端口，例如，在 Amazon RDS 实例上 |

(仅限 VPC) 您可以选择限制来自数据库服务器的出站流量，例如，如果您希望允许对 Internet 的访问以便进行软件更新，则请限制所有其他类型的流量。您必须先删除允许所有出站流量的默认出站规则。

| 协议类型 | 协议编号 | Port | 目的地 IP | 备注 |
|------|------|-----------|-----------|---------------------------|
| TCP | 6 | 80 (HTTP) | 0.0.0.0/0 | 允许对任何 IPv4 地址进行出站 HTTP 访问 |

| 协议类型 | 协议编号 | Port | 目的地 IP | 备注 |
|------|------|-------------|-----------|---|
| TCP | 6 | 443 (HTTPS) | 0.0.0.0/0 | 允许对任何 IPv4 地址进行出站 HTTPS 访问 |
| TCP | 6 | 80 (HTTP) | ::/0 | (仅限已启用 IPv6 的 VPC) 允许对任何 IPv6 地址进行出站 HTTP 访问 |
| TCP | 6 | 443 (HTTPS) | ::/0 | (仅限已启用 IPv6 的 VPC) 允许对任何 IPv6 地址进行出站 HTTPS 访问 |

来自同一组内的其他实例的访问

要允许与同一安全组关联的实例之间相互通信，您必须明确添加实现此目的的规则。

下表描述了允许关联的实例互相通信的 VPC 安全组的入站规则。该规则允许所有类型的流量。

| 协议类型 | 协议编号 | 端口 | 源 IP |
|----------|----------|----------|--------|
| -1 (All) | -1 (All) | -1 (All) | 安全组 ID |

下表描述了允许关联的实例互相通信的 EC2-Classic 安全组的入站规则。该规则允许所有类型的流量。

| 协议类型 | 协议编号 | 端口 | 源 IP |
|------|------|-----------------|--------|
| ICMP | 1 | -1 (All) | 安全组 ID |
| TCP | 6 | 0 - 65535 (All) | 安全组 ID |
| UDP | 17 | 0 - 65535 (All) | 安全组 ID |

从本地计算机进行访问

要连接到您的实例，您的安全组必须拥有允许 SSH 访问（适用于 Linux 实例）或 RDP 访问（适用于 Windows 实例）的入站规则。

| 协议类型 | 协议编号 | Port | 源 IP |
|------|------|------------|---|
| TCP | 6 | 22 (SSH) | 您的计算机的公有 IPv4 地址或您的本地网络中的 IP 地址范围。如果您为 VPC 启用了 IPv6，并且您的实例有一个 IPv6 地址，则可以输入一个 IPv6 地址或范围。 |
| TCP | 6 | 3389 (RDP) | 您的计算机的公有 IPv4 地址或您的本地网络中的 IP 地址范围。如果您为 VPC 启用了 IPv6，并 |

| 协议类型 | 协议编号 | Port | 源 IP |
|------|------|------|--------------------------------------|
| | | | 且您的实例有一个 IPv6 地址，则可以输入一个 IPv6 地址或范围。 |

路径 MTU 发现

路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机将返回以下 ICMP 消息：

```
Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
```

要确保您的实例可以收到此消息并且数据包不会丢失，您必须将 ICMP 规则添加到您的入站安全组规则。

| 协议类型 | 协议编号 | ICMP 类型 | ICMP 代码 | 源 IP |
|------|------|-----------------------------|---|--------------------|
| ICMP | 1 | 3 (Destination Unreachable) | 4 (Fragmentation Needed and Don't Fragment was Set) | 与您的实例进行通信的主机 IP 地址 |

对实例执行 ping 操作

ping 命令是一种 ICMP 流量。要对实例执行 ping 操作，您必须添加以下入站 ICMP 规则。

| 协议类型 | 协议编号 | ICMP 类型 | ICMP 代码 | 源 IP |
|------|------|----------|---------|-------------------------------------|
| ICMP | 1 | 8 (Echo) | 不适用 | 您的计算机的公有 IPv4 地址或您的本地网络中的 IPv4 地址范围 |

要使用 ping6 命令对您实例的 IPv6 地址执行 ping 操作，您必须添加以下入站 ICMPv6 规则。

| 协议类型 | 协议编号 | ICMP 类型 | ICMP 代码 | 源 IP |
|--------|------|------------|---------|-----------------------------------|
| ICMPv6 | 58 | 128 (Echo) | 0 | 您的计算机的 IPv6 地址或您的本地网络中的 IPv6 地址范围 |

DNS 服务器

如果您已将 EC2 实例设置为 DNS 服务器，则必须确保 TCP 和 UDP 流量可通过端口 53 访问您的 DNS 服务器。

对于源 IP，请指定以下其中一项：

- 网络中的特定 IP 地址或 IP 地址范围
- 您网络中需要访问 DNS 服务器的一组实例的安全组 ID。

| 协议类型 | 协议编号 | Port |
|------|------|------|
| TCP | 6 | 53 |
| UDP | 17 | 53 |

Amazon EFS 文件系统

如果您将 Amazon EFS 文件系统与 Amazon EC2 实例结合使用，与 Amazon EFS 装载目标关联的安全组必须允许使用 NFS 协议传输的流量。

| 协议类型 | 协议编号 | 端口 | 源 IP | 备注 |
|------|------|------------|---------|-------------------------------------|
| TCP | 6 | 2049 (NFS) | 安全组 ID. | 允许从与该安全组关联的资源 (包括挂载目标) 进行入站 NFS 访问。 |

要在 Amazon EC2 实例上装载 Amazon EFS 文件系统，您必须连接到您的实例。因此，与您的实例关联的安全组必须拥有允许来自本地计算机或本地网络的入站 SSH 的规则。

| 协议类型 | 协议编号 | 端口 | 源 IP | 备注 |
|------|------|----------|-------------------------------|------------------------|
| TCP | 6 | 22 (SSH) | 您的本地计算机的 IP 地址范围或网络的 IP 地址范围。 | 允许从您的本地计算机进行入站 SSH 访问。 |

Elastic Load Balancing

如果您正在使用负载均衡器，则与您的负载均衡器关联的安全组必须具有允许与您的实例或目标进行通信的规则。

| 入站 | | | | |
|------|------|---------|--|-----------------------|
| 协议类型 | 协议编号 | 端口 | 源 IP | 备注 |
| TCP | 6 | 侦听器端口 | 对于面向 Internet 的负载均衡器：0.0.0.0/0 (所有 IPv4 地址) 对于内部负载均衡器：VPC 的 IPv4 CIDR 块 | 在负载均衡器侦听器端口上允许入站流量。 |
| 出站 | | | | |
| 协议类型 | 协议编号 | 端口 | 目的地 IP | 备注 |
| TCP | 6 | 实例侦听器端口 | 实例安全组的 ID | 在实例侦听器端口上允许流向实例的出站流量。 |

| | | | | |
|-----|---|----------|-----------|------------------------|
| TCP | 6 | 运行状况检查端口 | 实例安全组的 ID | 在运行状况检查端口上允许流向实例的出站流量。 |
|-----|---|----------|-----------|------------------------|

您的实例的安全组规则必须允许负载均衡器通过侦听器端口和运行状况检查端口与您的实例进行通信。

| 入站 | | | | |
|------|------|----------|--------------|-------------------------|
| 协议类型 | 协议编号 | 端口 | 源 IP | 备注 |
| TCP | 6 | 实例侦听器端口 | 负载均衡器安全组的 ID | 在实例侦听器端口上允许来自负载均衡器的流量。 |
| TCP | 6 | 运行状况检查端口 | 负载均衡器安全组的 ID | 在运行状况检查端口上允许来自负载均衡器的流量。 |

有关更多信息，请参阅 传统负载均衡器 指南 中的 [为 Classic Load Balancer 配置安全组](#) 和 应用程序负载均衡器 指南 中的 [Application Load Balancer 的安全组](#)。

控制对 Amazon EC2 资源的访问

您的安全证书使 AWS 中的服务可以识别您，并授予您对 AWS 资源（例如您的 Amazon EC2 资源）的无限制使用权限。您可以使用 Amazon EC2 和 AWS Identity and Access Management (IAM) 的功能，在不共享您的安全证书情况下允许其他用户、服务和应用程序使用您的 Amazon EC2 资源。您可以使用 IAM 控制其他用户对您 AWS 账户中资源的使用方式，并且您可以使用安全组来控制对您的 Amazon EC2 实例的访问。您可以选择授予 Amazon EC2 资源的完全使用或限制使用权限。

内容

- [网络访问您的实例](#) : (p. 366)
- [Amazon EC2 权限属性](#) (p. 366)
- [IAM 和 Amazon EC2](#) (p. 367)
- [Amazon EC2 的 IAM 策略](#) (p. 368)
- [适用于 Amazon EC2 的 IAM 角色](#) (p. 422)
- [为您的 Linux 实例授权入站流量](#) (p. 429)

网络访问您的实例：

安全组起着防火墙的作用，可用于控制允许达到一个或多个实例的流量。启动实例时，您可以为其分配一个或多个安全组。您需要添加规则至每个控制实例流量的安全组。您可以随时修改安全组的规则；新规则会自动应用于该安全组所分配到的所有实例。

有关更多信息，请参阅 [为您的 Linux 实例授权入站流量](#) (p. 429)。

Amazon EC2 权限属性

您的组织可拥有多个 AWS 账户。Amazon EC2 让您可以指定其他的 AWS 账户，能够使用您的 Amazon 系统映像 (AMI) 和 Amazon EBS 快照。这些权限仅在 AWS 账户级别有效；您不能限制指定 AWS 账户内特定用户的权限。您指定的 AWS 账户中的所有用户均可使用 AMI 或快照。

每个 AMI 都拥有一个 `LaunchPermission` 属性，用于控制可以访问该 AMI 的 AWS 账户。有关更多信息，请参阅 [将 AMI 设为公用 \(p. 66\)](#)。

每个 Amazon EBS 快照都有一个 `createVolumePermission` 属性，用于控制哪些 AWS 账户可以使用该快照。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

IAM 和 Amazon EC2

IAM 允许您执行以下操作：

- 在您的 AWS 账户下创建用户和组
- 为您的 AWS 账户下的每个用户分配唯一的安全证书
- 控制每个用户使用 AWS 资源执行任务的权限
- 允许另一 AWS 账户的用户共享 AWS 资源
- 创建 AWS 账户角色并定义可以担任这些角色的用户或服务
- 借助企业的现有身份验证，授予使用 AWS 资源执行任务的权限

通过将 IAM 与 Amazon EC2 配合使用，您可以控制组织中的用户能否使用特定的 Amazon EC2 API 操作执行任务，以及他们能否使用特定的 AWS 资源。

本主题有助于回答以下问题：

- 如何在 IAM 中创建组和用户？
- 如何创建策略？
- 在 Amazon EC2 中执行任务时我需要哪些 IAM 策略？
- 如何授予在 Amazon EC2 中执行操作的权限？
- 如何授予在 Amazon EC2 中对特定资源执行操作的权限？

创建 IAM 组和用户

创建 IAM 组

1. 在 <https://console.aws.amazon.com/iam/> 处登录 IAM 控制台。
2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
3. 在 Group Name 框中，为您的组输入一个名称，然后选择 Next Step。
4. 在 Attach Policy 页面上，选择 AWS 管理的策略。例如，对于 Amazon EC2，下列 AWS 管理的策略之一可能符合您的需求：
 - PowerUserAccess
 - ReadOnlyAccess
 - AmazonEC2FullAccess
 - AmazonEC2ReadOnlyAccess
5. 选择 Next Step，然后选择 Create Group。

您的新组列在 Group Name (组名) 下方。

创建 IAM 用户，将该用户添加到您的组中，并为该用户创建密码

1. 在导航窗格中，依次选择 Users、Add user。
2. 输入用户名。
3. 为此组用户选择访问权限类型。选中 Programmatic access 和 AWS Management Console access。

4. 对于 Console password type , 选择以下任一项 :
 - 自动生成的密码。每个用户将获得一个随机生成的密码 , 该密码符合当前生效的密码策略 (如果有)。在转到完成页面后 , 您可以查看或下载密码。
 - 自定义密码。向每个用户分配您在框内键入的密码。
5. 选择下一步 : 权限。
6. 在设置权限页面上 , 选择将用户添加到组。选择您之前创建的组。
7. 依次选择 Next: Review、Create user。
8. 要查看用户的访问密钥 (访问密钥 ID 和秘密访问密钥) , 请选择您要查看的每个密码和秘密访问密钥旁边的 Show。要保存访问密钥 , 请选择下载 .csv , 然后将文件保存到安全位置。

Note

完成此步骤之后您将无法检索秘密访问密钥 ; 如果放错了位置 , 则必须创建一个新的。

9. 选择 Close。
10. 为每个用户提供证书 (访问密钥和密码) ; 让他们根据您为 IAM 组指定的权限享受服务。

相关主题

有关 IAM 的更多信息 , 请参阅下文 :

- [Amazon EC2 的 IAM 策略 \(p. 368\)](#)
- [适用于 Amazon EC2 的 IAM 角色 \(p. 422\)](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [IAM 用户指南](#)

Amazon EC2 的 IAM 策略

默认情况下 , IAM 用户没有创建或修改 Amazon EC2 资源或使用 Amazon EC2 API 执行任务的权限。(这意味着他们不能使用 Amazon EC2 控制台或 CLI 执行这些操作。)要允许 IAM 用户创建或修改资源和执行任务 , 您必须创建 IAM 策略以允许 IAM 用户使用他们所需的特定资源和 API 操作 , 然后将这些策略与需要这些权限的 IAM 用户或组关联起来。

当您将策略与一个用户或一组用户关联时 , 它会授权或拒绝用户使用指定资源执行指定任务。有关 IAM 策略的更多一般信息 , 请参阅 IAM 用户指南 中的[权限与策略](#)。有关管理和创建自定义 IAM 策略的更多信息 , 请参阅[管理 IAM 策略](#)。

入门

IAM 策略必须授予或拒绝使用一个或多个 Amazon EC2 操作的权限。它还必须指定可以用于操作的资源 (可以是所有资源 , 在某些情况下可以是特定资源)。策略还可以包含应用于资源的条件。

Amazon EC2 部分支持资源级权限。这意味着对于某些 EC2 API 操作 , 您无法指定允许用户为哪个资源使用该操作 ; 而必须允许用户为所有资源使用该操作。

| 任务 | 主题 |
|------------|---|
| 了解策略的基本结构 | 策略语法 (p. 369) |
| 在策略中定义操作 | Amazon EC2 操作 (p. 370) |
| 在策略中定义特定资源 | 适用于 Amazon EC2 的 Amazon 资源名称 (p. 370) |

| 任务 | 主题 |
|-------------------------|---|
| 将条件应用于资源的使用 | Amazon EC2 的条件密钥 (p. 372) |
| 使用可用于 Amazon EC2 的资源级权限 | Amazon EC2 API 操作支持的资源级权限 (p. 376) |
| 测试策略 | 检查用户是否具有所需权限 (p. 375) |
| 针对 CLI 或软件开发工具包的策略示例 | 适用于 AWS CLI 或 AWS 开发工具包的策略示例 (p. 398) |
| 针对 Amazon EC2 控制台的策略示例 | 用于 Amazon EC2 控制台的策略示例。 (p. 415) |

策略结构

以下主题说明 IAM 策略的结构。

主题

- [策略语法 \(p. 369\)](#)
- [Amazon EC2 操作 \(p. 370\)](#)
- [适用于 Amazon EC2 的Amazon 资源名称 \(p. 370\)](#)
- [Amazon EC2 的条件密钥 \(p. 372\)](#)
- [检查用户是否具有所需权限 \(p. 375\)](#)

策略语法

IAM 策略是包含一个或多个语句的 JSON 文档。每个语句的结构如下：

```
{  
  "Statement": [  
    {  
      "Effect": "effect",  
      "Action": "action",  
      "Resource": "arn",  
      "Condition": {  
        "condition": {  
          "key": "value"  
        }  
      }  
    }  
  ]  
}
```

组成语句的各个元素如下：

- Effect : 此 effect 可以是 Allow 或 Deny。默认情况下 IAM 用户没有使用资源和 API 操作的权限，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- Action : action 是对其授予或拒绝权限的特定 API 操作。要了解有关指定 action 的信息，请参阅 [Amazon EC2 操作 \(p. 370\)](#)。
- Resource : 操作影响的资源。有些 Amazon EC2 API 操作允许您在策略中包括该操作可以创建或修改的特定资源。要在语句中指定资源，您需要使用其 Amazon 资源名称 (ARN)。有关指定 ARN 值的详细信息，请参阅 [适用于 Amazon EC2 的Amazon 资源名称 \(p. 370\)](#)。有关哪些 ARN 支持哪些 API 操作的更多信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。如果 API 操作不支持 ARN，请使用 * 通配符指定操作可以影响所有资源。
- Condition : 条件是可选的。它们可以用于控制策略生效的时间。想要了解更多有关为 Amazon EC2 指定条件的信息，请参阅 [Amazon EC2 的条件密钥 \(p. 372\)](#)。

想要了解更多有关 Amazon EC2 的示例 IAM 策略语句的信息，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 398\)](#)。

Amazon EC2 操作

在 IAM 策略语句中，您可以从支持 IAM 的任何服务中指定任何 API 操作。对于 Amazon EC2，请使用以下前缀为 API 操作命名：`ec2:`。例如：`ec2:RunInstances` 和 `ec2:CreateImage`。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": ["ec2:action1", "ec2:action2"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名称以单词“Describe”开头的所有操作，如下所示：

```
"Action": "ec2:Describe*"
```

要指定所有 Amazon EC2 API 操作，请使用 * 通配符，如下所示：

```
"Action": "ec2:/*"
```

有关 Amazon EC2 操作的列表，请参阅 Amazon EC2 API Reference 中的[操作](#)主题。

适用于 Amazon EC2 的 Amazon 资源名称

每个 IAM 策略语句适用于您使用资源的 ARN 指定的资源。

Important

当前，并不是所有 API 操作都支持各个 ARN；我们以后将为其他 API 操作添加支持以及为其他 Amazon EC2 资源添加 ARN。有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用以及每个 ARN 支持的条件密钥的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。

ARN 的一般语法如下：

```
arn:aws:[service]:[region]:[account]:resourceType/resourcePath
```

service

服务（例如，`ec2`）。

区域

资源所在区域（例如，`us-east-1`）。

账户

AWS 账户 ID，不包含连字符（例如，`123456789012`）。

resourceType

资源类型（例如，`instance`）。

resourcePath

识别资源的路径。您可以在路径中使用 * 通配符。

例如，您可以使用特定实例 (`i-1234567890abcdef0`) 的 ARN 在语句中指定它，如下所示：

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

要指定所有资源，或者如果特定 API 操作不支持 ARN，请在 `Resource` 元素中使用 * 通配符，如下所示：

```
"Resource": "*"
```

下表介绍了 Amazon EC2 API 操作使用的每种类型资源的 ARN。

| 资源类型 | ARN |
|------------------------------|--|
| 所有 Amazon EC2 资源 | <code>arn:aws:ec2:*</code> |
| 指定账户在指定地区拥有的所有 Amazon EC2 资源 | <code>arn:aws:ec2:region:account:*</code> |
| 客户网关 | <code>arn:aws:ec2:region:account:customer-gateway/cgw-id</code> 其中 <code>cgw-id</code> 是 <code>cgw-xxxxxxxx</code> |
| DHCP 选项集 | <code>arn:aws:ec2:region:account:dhcp-options/dhcp-options-id</code> 其中 <code>dhcp-options-id</code> 是 <code>dopt-xxxxxxxx</code> |
| 图片 | <code>arn:aws:ec2:region::image/image-id</code> 其中 <code>image-id</code> 是 AMI、AKI 或 ARI 的 ID，而不使用 account |
| 实例 | <code>arn:aws:ec2:region:account:instance/instance-id</code> 其中， <code>instance-id</code> 是 <code>i-xxxxxxxxxxxxxx</code> 或 <code>i-xxxxxxxxxxxxxxxxxxxx</code> |
| 实例配置文件 | <code>arn:aws:iam::account:instance-profile/instance-profile-name</code> 其中 <code>instance-profile-name</code> 是实例配置文件的名称，而不使用 region |
| Internet 网关 | <code>arn:aws:ec2:region:account:internet-gateway/igw-id</code> 其中 <code>igw-id</code> 是 <code>igw-xxxxxxxx</code> |
| 密钥对 | <code>arn:aws:ec2:region:account:key-pair/key-pair-name</code> 其中 <code>key-pair-name</code> 是密钥对名称（例如， <code>gsg-keypair</code> ） |
| 网络 ACL | <code>arn:aws:ec2:region:account:network-acl/nacl-id</code> 其中 <code>nacl-id</code> 是 <code>acl-xxxxxxxx</code> |
| 网络接口 | <code>arn:aws:ec2:region:account:network-interface/eni-id</code> 其中 <code>eni-id</code> 是 <code>eni-xxxxxxxx</code> |
| 置放群组 | <code>arn:aws:ec2:region:account:placement-group/placement-group-name</code> 其中 <code>placement-group-name</code> 是置放组名称（例如， <code>my-cluster</code> ） |
| Reserved Instance | <code>arn:aws:ec2:region:account:reserved-instance/reservation-id</code> 其中， <code>reservation-id</code> 为 <code>xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx</code> |
| 路由表 | <code>arn:aws:ec2:region:account:route-table/route-table-id</code> |

| 资源类型 | ARN |
|----------|--|
| | 其中 route-table-id 是 rtb-xxxxxxxx |
| 安全组 | arn:aws:ec2:region:account:security-group/security-group-id 其中 security-group-id 是 sg-xxxxxxxx |
| 快照 | arn:aws:ec2:region::snapshot/snapshot-id 其中 snapshot-id 是 snap-xxxxxxxx 或 snap-xxxxxxxxxxxxxxxxx , 而不使用 account |
| 竞价型实例请求 | arn:aws:ec2:region:account:spot-instance-request/spot-instance-request-id 其中 spot-instance-request-id 是 sir-xxxxxxxx |
| 子网 | arn:aws:ec2:region:account:subnet/subnet-id 其中 subnet-id 是 subnet-xxxxxxxx |
| 卷 | arn:aws:ec2:region:account:volume/volume-id 其中 , volume-id 是 vol-xxxxxxxx 或 vol-xxxxxxxxxxxxxxxx |
| VPC | arn:aws:ec2:region:account:vpc/vpc-id 其中 vpc-id 是 vpc-xxxxxxxx |
| VPC 对等连接 | arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id 其中 vpc-peering connection-id 是 pcx-xxxxxxxx |
| VPN 连接 | arn:aws:ec2:region:account:vpn-connection/vpn-connection-id 其中 vpn-connection-id 是 vpn-xxxxxxxx |
| VPN 网关 | arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id 其中 vpn-gateway-id 是 vgw-xxxxxxxx |

许多 Amazon EC2 API 操作涉及多种资源。例如，`AttachVolume` 将一个 Amazon EBS 卷挂载到一个实例，从而使 IAM 用户必须获得相应权限才能使用该卷和该实例。要在单个语句中指定多种资源，请使用逗号将它们隔开，如下所示：

```
"Resource": ["arn1", "arn2"]
```

更多有关 ARN 的一般信息，请参阅 Amazon Web Services 一般参考 中的 [Amazon 资源名称 \(ARN\)](#) 和 [AWS 服务命名空间](#) 主题。有关 Amazon EC2 操作所创建或修改的资源以及可以在 IAM 策略语句中使用的 ARN 的更多信息，请参阅 Amazon EC2 API Reference 中的 [授予 IAM 用户所需的 Amazon EC2 资源使用权限](#) 主题。

Amazon EC2 的条件密钥

在策略语句中，您可以选择性指定控制策略生效时间的条件。每个条件都包含一个或多个密钥值对。条件密钥不区分大小写。我们已经定义了 AWS 范围内的条件密钥以及其他特定于服务的条件密钥。

如果您指定了多个条件或在单一条件下指定了多个密钥，我们将通过逻辑 AND 操作对其进行评估。如果您在单一条件下指定了一个具有多个值的密钥，我们将通过逻辑 OR 操作对其进行评估。必须匹配所有条件才能授予权限。

在指定条件时，您也可使用占位符。例如，您可以授予 IAM 用户通过指定其 IAM 用户名的标签使用资源的权限。有关更多信息，请参阅 IAM 用户指南 中的[策略变量](#)。

Important

许多条件密钥是特定于某个资源的，而某些 API 操作会使用多个资源。如果您使用条件密钥编写策略，请使用语句的 Resource 元素指定要应用该条件密钥的资源。否则，该策略可能会完全阻止用户执行操作，因为针对未应用条件密钥的资源的条件检查失败。如果您不想指定资源，或者如果您已将策略的 Action 元素编写为包含多个 API 操作，则必须使用 ...IfExists 条件类型以确保对不使用条件密钥的资源忽略条件密钥。有关更多信息，请参阅 IAM 用户指南 中的[...IfExists 条件](#)。

Amazon EC2 实施以下特定于服务的条件键。

| 条件键 | 键值对 | 评估类型 |
|----------------------|--|------------|
| ec2:AcceptorVpc | "ec2:AcceptorVpc":"vpc-arn" 其中，vpc-arn 是 VPC 对等连接中接受方 VPC 的 VPC ARN | ARN , Null |
| ec2:AvailabilityZone | "ec2:AvailabilityZone":"az-api-name" 其中 az-api-name 是可用区的名称 (例如，us-west-2a) 要列出您的可用区，请使用 describe-availability-zones | 字符串 , Null |
| ec2>CreateAction | "ec2>CreateAction":"api-name" 其中，api-name 是资源创建操作的名称 (例如，RunInstances) | 字符串 , Null |
| ec2:EbsOptimized | "ec2:EbsOptimized":"optimized-flag" 其中，optimized-flag 是 true false (对于实例) | 布尔值 , Null |
| ec2:Encrypted | "ec2:Encrypted":"encrypted-flag" 其中，encrypted-flag 为 true false (对于 EBS 卷) | 布尔值 , Null |
| ec2:ImageType | "ec2:ImageType":"image-type-api-name" 其中 image-type-api-name 是 ami aki ari | 字符串 , Null |
| ec2:InstanceProfile | "ec2:InstanceProfile":"instance-profile-arn" 其中 instance-profile-arn 是实例配置文件 ARN | ARN , Null |
| ec2:InstanceType | "ec2:InstanceType":"instance-type-api-name" 其中，instance-type-api-name 是实例类型的名称。 | 字符串 , Null |
| ec2:Owner | "ec2:Owner":"account-id" 其中 account-id 是 amazon aws-marketplace aws-account-id | 字符串 , Null |
| ec2:ParentSnapshot | "ec2:ParentSnapshot":"snapshot-arn" 其中 snapshot-arn 是快照 ARN | ARN , Null |

| 条件键 | 键值对 | 评估类型 |
|----------------------------|--|------------|
| ec2:ParentVolume | "ec2:ParentVolume":"volume-arn" 其中 volume-arn 是卷 ARN | ARN , Null |
| ec2:PlacementGroup | "ec2:PlacementGroup":"placement-group-arn" 其中 placement-group-arn 是置放组 ARN | ARN , Null |
| ec2:PlacementGroupStrategy | "ec2:PlacementGroupStrategy":"placement-group-strategy" 其中 placement-group-strategy 为 cluster | 字符串 , Null |
| ec2:ProductCode | "ec2:ProductCode":"product-code" 其中 product-code 是产品代码 | 字符串 , Null |
| ec2:Public | "ec2:Public":"public-flag" 其中 public-flag 是 true false (对于 AMI) | 布尔值 , Null |
| ec2:Region | "ec2:Region":"region-name" 其中 region-name 是区域的名称 (例如, us-west-2)。要列出您的区域, 请使用 describe-regions 。此条件密钥可用于所有 Amazon EC2 操作。 | 字符串 , Null |
| ec2:RequesterVpc | "ec2:RequesterVpc":"vpc-arn" 其中, vpc-arn 是 VPC 对等连接中请求方 VPC 的 VPC ARN | ARN , Null |
| ec2:ResourceTag/tag-key | "ec2:ResourceTag/tag-key":"tag-value" 其中 tag-key 和 tag-value 是标签键对 | 字符串 , Null |
| ec2:RootDeviceType | "ec2:RootDeviceType":"root-device-type-name" 其中 root-device-type-name 是 ebs instance-store | 字符串 , Null |
| ec2:SnapshotTime | "ec2:SnapshotTime":"time" 其中 time 是快照创建时间 (例如, 2013-06-01T00:00:00Z) | 日期 , Null |
| ec2:Subnet | "ec2:Subnet":"subnet-arn" 其中 subnet-arn 是子网 ARN | ARN , Null |
| ec2:Tenancy | "ec2:Tenancy":"tenancy-attribute" 其中 tenancy-attribute 是 default dedicated host | 字符串 , Null |
| ec2:VolumeIops | "ec2:VolumeIops":"volume-iops" 其中 volume-iops 是每秒输入/输出操作 (IOPS); 其范围是从 100 到 20,000 | 数值 , Null |
| ec2:VolumeSize | "ec2:VolumeSize":"volume-size" 其中 volume-size 是卷的大小 (以 GiB 为单位) | 数值 , Null |

| 条件键 | 键值对 | 评估类型 |
|----------------|--|----------|
| ec2:VolumeType | "ec2:VolumeType":"volume-type-name" 其中，volume-type-name 对于通用型 SSD 卷是 <code>gp2</code> ，对于预配置 IOPS SSD 卷是 <code>io1</code> ，对于吞吐优化 HDD 卷是 <code>st1</code> ，对于 Cold HDD 卷是 <code>sc1</code> ，对于磁介质卷是 <code>standard</code> 。 | 字符串，Null |
| ec2:vpc | "ec2:Vpc":"vpc-arn" 其中 vpc-arn 是 VPC ARN | ARN，Null |

Amazon EC2 还实施 AWS 范围内的条件键 (请参阅[可用键](#))。以下 AWS 条件键目前是特定于 Amazon EC2 的。

| 条件键 | 键值对 | 评估类型 |
|------------------------|--|----------|
| aws:RequestTag/tag-key | "aws:Request/tag-key":"tag-value" 其中，tag-key 和 tag-value 是标签键值对 | 字符串，Null |
| aws:TagKeys | "aws:TagKeys":"tag-key" 其中，tag-key 是标签键列表 (例如，["A","B"]) | 字符串，Null |

有关那个条件密钥可以与那些 Amazon EC2 资源一起使用的信息 (根据操作流程)，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。有关适用于 Amazon EC2 的策略语句示例，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 398\)](#)。

检查用户是否具有所需权限

在您创建 IAM 策略后，建议您检查它是否允许用户使用策略生效前所需的特定 API 操作和资源。

首先，创建一个用于测试目的的 IAM 用户，然后将您创建的 IAM 策略与该测试用户关联起来。然后，以测试用户身份提出请求。

如果您测试的 Amazon EC2 操作创建或修改了一种资源，您在提交请求时应该使用 `DryRun` 参数 (或运行带有 `--dry-run` 选项的 AWS CLI 命令)。在这种情况下，调用会完成身份验证检查，但是不会完成该操作。例如，您可以检查用户能否终止特定实例，但不会真的终止它。如果测试用户具有所需的权限，请求会返回 `DryRunOperation`；否则，它会返回 `UnauthorizedOperation`。

如果策略未授予用户您所期望的权限，您可以根据需要调节策略并重新测试，直到您获得预期的结果。

Important

在其生效之前，它需要几分钟时间将策略更改为适合状态。因此，我们建议您在测试策略更新前，等候五分钟的时间。

如果身份验证检查失败，该请求将返回一个带有诊断信息的代码消息。您可以使用 `DecodeAuthorizationMessage` 操作对消息进行解码。有关更多信息，请参阅 AWS Security Token Service API Reference 中的 [DecodeAuthorizationMessage](#)，以及 AWS Command Line Interface Reference 中的 `decode-authorization-message`。

Amazon EC2 API 操作支持的资源级权限

资源级权限 指的是能够指定允许用户对哪些资源执行操作的能力。Amazon EC2 部分支持资源级权限。这意味着对于某些 Amazon EC2 操作，您可以控制何时允许用户执行操作 (基于必须满足的条件) 或是允许用户使用的特定资源。例如，您可以向用户授予启动实例的权限，但是仅限特定类型的实例，并且只能使用特定的 AMI。

下表介绍当前支持资源级权限的 Amazon EC2 API 操作，以及每个操作支持的资源 (及其 ARN) 和条件密钥。指定 ARN 时，您可以在路径中使用 * 通配符；例如，在无法或不希望指定确切资源 ID 的时候可以这样做。有关使用通配符的示例，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 398\)](#)。

Important

如果某一 Amazon EC2 API 操作在此表中没有列出，则它不支持资源级权限。如果 Amazon EC2 API 操作不支持资源级权限，那么，您可以向用户授予使用该操作的权限，但是必须为策略语句的资源元素指定 *。有关示例，请参阅 [1：只读访问 \(p. 398\)](#)。有关当前不支持资源级权限的 Amazon EC2 API 操作列表，请参阅 Amazon EC2 API Reference 中的 [不支持的资源级权限](#)。所有 Amazon EC2 操作都支持 ec2:Region 条件密钥。有关示例，请参阅 [2：限制对特定区域的访问 \(p. 399\)](#)。

| API 操作 | 资源 | 条件密钥 |
|-----------------------------|---|---|
| AcceptVpcPeeringConnection | VPC 对等连接 | ec2:AccepterVpc |
| | arn:aws:ec2:region:account:vpc-peering-connection/* | ec2:Region |
| | arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id | ec2:ResourceTag/tag-key ec2:RequesterVpc |
| | VPC | ec2:ResourceTag/tag-key |
| AssociateIamInstanceProfile | arn:aws:ec2:region:account:vpc/* | ec2:Region |
| | arn:aws:ec2:region:account:vpc/vpc-id | ec2:Tenancy |
| | 其中 vpc-id 是接受人拥有的 VPC | |
| | 实例 | ec2:AvailabilityZone |
| | arn:aws:ec2:region:account:instance/* | ec2:EbsOptimized |
| | arn:aws:ec2:region:account:instance/instance-id | ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | | |
| | | |
| | | |
| AttachClassicLinkVpc | 实例 | ec2:AvailabilityZone |
| | arn:aws:ec2:region:account:instance/* | ec2:EbsOptimized |
| | | ec2:InstanceProfile |

| API 操作 | 资源 | 条件密钥 |
|--------------|--|---|
| | arn:aws:ec2:region:account:instance/ instance-id | ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | 安全组 arn:aws:ec2:region:account:security- group/* arn:aws:ec2:region:account:security- group/security-group-id 其中的安全组是 VPC 的安全组。 | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |
| AttachVolume | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |

| API 操作 | 资源 | 条件密钥 |
|-------------------------------|---|--|
| | Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id | ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType |
| AuthorizeSecurityGroupEgress | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| AuthorizeSecurityGroupIngress | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| CreateTags | DHCP 选项集 arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id | ec2:CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 图片 arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id | ec2:CreateAction ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType aws:RequestTag/tag-key aws:TagKeys |

| API 操作 | 资源 | 条件密钥 |
|--------|--|---|
| | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2>CreateAction ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | | aws:RequestTag/tag-key aws:TagKeys |
| | Internet 网关 arn:aws:ec2:region:account:internet- gateway/* arn:aws:ec2:region:account:internet- gateway/igw-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key |
| | | aws:RequestTag/tag-key aws:TagKeys |
| | 网络 ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network- acl/nacl-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| | | aws:RequestTag/tag-key aws:TagKeys |
| | 网络接口 arn:aws:ec2:region:account:network- interface/* arn:aws:ec2:region:account:network- interface/eni-id | ec2:AvailabilityZone ec2>CreateAction ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc |

| API 操作 | 资源 | 条件密钥 |
|--------|--|---|
| | | aws:RequestTag/tag-key aws:TagKeys |
| | Reserved Instance arn:aws:ec2:region:account:reserved-instance/* arn:aws:ec2:region:account:reserved-instance/reservation-id | ec2:AvailabilityZone ec2>CreateAction ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |
| | | aws:RequestTag/tag-key aws:TagKeys |
| | 路由表 arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys |
| | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys |
| | 快照 arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id | ec2>CreateAction ec2:Owner ec2:ParentVolume ec2:Region ec2:ResourceTag/tag-key ec2:SnapshotTime ec2:VolumeSize |

| API 操作 | 资源 | 条件密钥 |
|--------|--|---|
| | | aws:RequestTag/tag-key aws:TagKeys |
| | 竞价型实例请求 arn:aws:ec2:region:account:spot-instance-request/* arn:aws:ec2:region:account:spot-instance-request/spot-instance-request-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 子网 arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/subnet-id | ec2:AvailabilityZone ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys |
| | Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id | ec2:AvailabilityZone ec2>CreateAction ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:VolumeLops ec2:VolumeSize ec2:VolumeType aws:RequestTag/tag-key aws:TagKeys |
| | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |

| API 操作 | 资源 | 条件密钥 |
|----------------------------|--|--|
| | | aws:RequestTag/tag-key aws:TagKeys |
| | VPN 连接 arn:aws:ec2:region:account:vpn-connection/* arn:aws:ec2:region:account:vpn-connection/vpn-connection-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | VPN 网关 arn:aws:ec2:region:account:vpn-gateway/* arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id | ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| CreateVolume | Volume arn:aws:ec2:region:account:volume/* | ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType aws:RequestTag/tag-key aws:TagKeys |
| CreateVpcPeeringConnection | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id 其中 vpc-id 是请求者的 VPC | ec2:ResourceTag/tag-key ec2:Region ec2:Tenancy |
| | VPC 对等连接 arn:aws:ec2:region:account:vpc-peering-connection/* | ec2:AcceptorVpc ec2:Region ec2:RequesterVpc |

| API 操作 | 资源 | 条件密钥 |
|-----------------------|--|--|
| DeleteCustomerGateway | 客户网关 arn:aws:ec2:region:account:customer-gateway/* arn:aws:ec2:region:account:customer-gateway/cgw-id | ec2:Region ec2:ResourceTag/tag-key |
| DeleteDhcpOptions | DHCP 选项集 arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id | ec2:Region ec2:ResourceTag/tag-key |
| DeleteInternetGateway | Internet 网关 arn:aws:ec2:region:account:internet-gateway/* arn:aws:ec2:region:account:internet-gateway/igw-id | ec2:Region ec2:ResourceTag/tag-key |
| DeleteNetworkAcl | 网络 ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl/nacl-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| DeleteNetworkAclEntry | 网络 ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl/nacl-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| DeleteRoute | 路由表 arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| DeleteRouteTable | 路由表 arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| DeleteSecurityGroup | 安全组 arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |

| API 操作 | 资源 | 条件密钥 |
|------------|--|--|
| DeleteTags | DHCP 选项集 arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 图片 arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | Internet 网关 arn:aws:ec2:region:account:internet-gateway/* arn:aws:ec2:region:account:internet-gateway/igw-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 网络 ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl-nacl-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 网络接口 arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | Reserved Instance arn:aws:ec2:region:account:reserved-instance/* arn:aws:ec2:region:account:reserved-instance/reservation-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |

| API 操作 | 资源 | 条件密钥 |
|--------|--|--|
| | 路由表 arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 快照 arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 竞价型实例请求 arn:aws:ec2:region:account:spot-instance-request/* arn:aws:ec2:region:account:spot-instance-request/spot-instance-request-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | 子网 arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/subnet-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |

| API 操作 | 资源 | 条件密钥 |
|--------|--|---|
| | VPN 连接 arn:aws:ec2:region:account:vpn-connection/* arn:aws:ec2:region:account:vpn-connection/vpn-connection-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | VPN 网关 arn:aws:ec2:region:account:vpn-gateway/* arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id | ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys |
| | Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id | ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:VolumeLops ec2:VolumeSize ec2:VolumeType |
| | VPC 对等连接 arn:aws:ec2:region:account:vpc-peering-connection/* arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id | ec2:AcceptorVpc ec2:Region ec2:ResourceTag/tag-key ec2:RequesterVpc |
| | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | | |

| API 操作 | 资源 | 条件密钥 |
|-----------------------|--|---|
| | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |
| DetachVolume | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id | ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType |
| DisableVpcClassicLink | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |

| API 操作 | 资源 | 条件密钥 |
|--------------------------------|--|---|
| DisassociateIamInstanceProfile | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| EnableVpcClassicLink | VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id | ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy |
| GetConsoleScreenshot | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| RebootInstances | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |

| API 操作 | 资源 | 条件密钥 |
|--------------------------------------|---|---|
| RejectVpcPeeringConnection | /VPC 对等连接 arn:aws:ec2:region:account:vpc-peering-connection/* arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id | ec2:AcceptorVpc ec2:Region ec2:ResourceTag/tag-key ec2:RequesterVpc |
| ReplaceIamInstanceProfileAssociation | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| RevokeSecurityGroupEgress | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| RevokeSecurityGroupIngress | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| RunInstances | 图片 arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id | ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key |

| API 操作 | 资源 | 条件密钥 |
|--------|---|---|
| | 实例 arn:aws:ec2:region:account:instance/* | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| | | aws:RequestTag/tag-key aws:TagKeys |
| | 密钥对 arn:aws:ec2:region:account:key-pair/* arn:aws:ec2:region:account:key-pair/key-pair-name | ec2:Region |
| | 网络接口 arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id | ec2:AvailabilityZone ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc |
| | 置放群组 arn:aws:ec2:region:account:placement-group/* arn:aws:ec2:region:account:placement-group/placement-group-name | ec2:Region ec2:PlacementGroupStrategy |
| | 安全组 arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |

| API 操作 | 资源 | 条件密钥 |
|----------------|--|---|
| | 快照 arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id | ec2:Owner ec2:ParentVolume ec2:Region ec2:SnapshotTime ec2:ResourceTag/tag-key ec2:VolumeSize |
| | 子网 arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/subnet-id | ec2:AvailabilityZone ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| | Volume arn:aws:ec2:region:account:volume/* | ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:VolumeLops ec2:VolumeSize ec2:VolumeType |
| | | aws:RequestTag/tag-key aws:TagKeys |
| StartInstances | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |

| API 操作 | 资源 | 条件密钥 |
|--------------------|--|---|
| StopInstances | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |
| TerminateInstances | 实例 arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy |

RunInstances 的资源级别权限

[RunInstances](#) API 操作可启动一个或多个实例，并创建和使用许多 Amazon EC2 资源。该操作需要一个 AMI 并创建一个实例；该实例必须与安全组关联。启动到 VPC 中需要子网，会创建网络接口。从由 Amazon EBS 支持的 AMI 启动将创建卷。用户必须具有使用这些资源的权限，因此必须在使用 `ec2:RunInstances` 操作的资源级别权限的任何策略的 `Resource` 元素中指定它们。如果您不打算对 `ec2:RunInstances` 操作使用资源级别权限，则可以在您的语句（而不是单个 ARN）的 `Resource` 元素中指定 * 通配符。

如果您使用的是资源级别权限，下表介绍了使用 `ec2:RunInstances` 操作所需的最少资源。

| 启动类型 | 需要的资源 | 条件密钥 |
|---------------------------------|---------------------------------------|---|
| 使用实例存储支持的 AMI 启动到 EC2-Classic 中 | arn:aws:ec2:region:account:instance/* | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup |

| 启动类型 | 需要的资源 | 条件密钥 |
|---|--|--|
| 使用 Amazon EBS 支持的 AMI 启动到 EC2-Classic 中 | | ec2:Region ec2:RootDeviceType ec2:Tenancy |
| | arn:aws:ec2:region::image/* (或特定 AMI ID) | ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key |
| | arn:aws:ec2:region:account:securitygroup/* (或特定安全组 ID) | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| 使用 Amazon EBS 支持的 AMI 启动到 EC2-VPC 中 | arn:aws:ec2:region:account:instance* | ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy |
| | arn:aws:ec2:region::image/* (或特定 AMI ID) | ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key |
| | arn:aws:ec2:region:account:securitygroup/* (或特定安全组 ID) | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |

| 启动类型 | 需要的资源 | 条件密钥 |
|-------------------------|---|---|
| | arn:aws:ec2:region:account:volume/ec2:AvailabilityZone * | ec2:ParentSnapshot ec2:Region ec2:VolumeIops ec2:VolumeSize ec2:VolumeType |
| 使用实例存储支持的 AMI 启动到 VPC 中 | arn:aws:ec2:region:account:instance/ec2:AvailabilityZone * arn:aws:ec2:region::image/* (或特定 AMI ID) | ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key |
| | arn:aws:ec2:region:account:securitygroup/* (或特定安全组 ID) | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| | arn:aws:ec2:region:account:networkinterface/* (或特定网络接口 ID) | ec2:AvailabilityZone ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc |

| 启动类型 | 需要的资源 | 条件密钥 |
|---------------------------------|--|--|
| | arn:aws:ec2:region:account:subnet/ec2:AvailabilityZone * (或特定子网 ID) | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |
| 使用 Amazon EBS 支持的 AMI 启动到 VPC 中 | arn:aws:ec2:region:account:instance/* ec2:AvailabilityZone * | ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy |
| | arn:aws:ec2:region::image/* (或特定 AMI ID) | ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key |
| | arn:aws:ec2:region:account:securitygroup/* (或特定安全组 ID) | ec2:ResourceTag/tag-key ec2:Vpc |
| | arn:aws:ec2:region:account:networkinterface/* (或特定网络接口 ID) | ec2:AvailabilityZone ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc |

| 启动类型 | 需要的资源 | 条件密钥 |
|------|---|---|
| | arn:aws:ec2:region:account:volume/ec2:AvailabilityZone * arn:aws:ec2:region:account:subnet/ec2:AvailabilityZone * (或特定子网 ID) | ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType |
| | | ec2:Region ec2:ResourceTag/tag-key ec2:Vpc |

建议您还在策略中指定密钥对资源 — 即使不需要启动实例，但没有密钥对，您也无法连接到实例。有关对 `ec2:RunInstances` 操作使用资源级别权限的示例，请参阅[5：启动实例 \(RunInstances\) \(p. 403\)](#)。

有关 Amazon EC2 中资源级权限的更多信息，请参阅发布的以下 AWS 安全博客：[揭秘 EC2 资源级权限](#)。

用于标记的资源级权限

某些资源创建 Amazon EC2 API 操作允许您在创建资源时指定标签。有关更多信息，请参阅[标记您的成员资源 \(p. 626\)](#)。

为使用户能够在创建时标记资源，他们必须具有使用创建该资源的操作的权限，如 `ec2:RunInstances` 或 `ec2>CreateVolume`。如果在资源创建操作中指定了标签，则 Amazon 会对 `ec2:CreateTags` 操作执行额外的授权，以验证用户是否具备创建标签的权限。因此，用户还必须具有使用 `ec2:CreateTags` 操作的显式权限。

对于 `ec2:CreateTags` 操作，您可以使用 `ec2:CreateAction` 条件键将标记权限限制为仅限资源创建操作。例如，下面的策略允许用户启动实例并在启动期间向实例和卷应用任何标签。用户无权标记任何现有资源（他们无法直接调用 `ec2:CreateTags` 操作）。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
        "StringEquals": {
          "AWS:RequestType": "Launch"
        }
      }
    }
  ]
}
```

```
        "ec2:CreateAction" : "RunInstances"
    }
}
]
```

同样，下面的策略允许用户创建卷并在创建卷期间向卷应用任何标签。用户无权标记任何现有资源（他们无法直接调用 `ec2:CreateTags` 操作）。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:/*/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction" : "CreateVolume"
        }
      }
    }
  ]
}
```

仅当用户在资源创建操作中应用了标签时，系统才会评估 `ec2:CreateTags` 操作。因此，如果未在此请求中指定任何标签，则拥有创建资源权限（假定没有标记条件）的用户无需具备使用 `ec2:CreateTags` 操作的权限。但是，如果用户不具备使用 `ec2:CreateTags` 操作的权限而又试图创建带标签的资源，则请求将失败。

您可以使用以下条件键来控制应用到资源的标签键和值：

- `aws:RequestTag`：指示请求中必须存在特定的标签键或标签键和值。也可在此请求中指定其他标签。
- 与 `StringEquals` 条件运算符配合使用，以强制实施特定的标签和键组合，如强制实施标签 `cost-center=cc123`：

```
"StringEquals": "aws:RequestTag/cost-center": "cc123"
```

- 与 `StringLike` 条件运算符配合使用，以在请求中强制实施特定的标签键；如强制实施标签键 `purpose`：

```
"StringLike": "aws:RequestTag/purpose": "*"
```

- `aws:TagKeys`：强制实施在请求中使用的标签键。
- 与 `ForAllValues` 修饰符配合使用，以只强制实施请求中提供的特定标签键（如果在请求中指定了标签，则只允许特定的标签键；不允许任何其他标签）。例如，允许标签键 `environment` 或 `cost-center`：

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment", "cost-center"]}
```

- 与 `ForAnyValue` 修饰符配合使用，以强制请求中至少存在一个指定的标签键。例如，强制请求中至少存在标签键 `environment` 或 `webserver` 中的一个：

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment", "webserver"]}
```

上述条件键可应用于支持标记的资源创建操作，以及 ec2:CreateTags 和 ec2:DeleteTags 操作。

为强制用户指定标签，在创建资源时，您必须使用 aws:RequestTag 条件密钥或 ForAnyValue 条件密钥，并在资源创建操作中使用修饰符 aws:TagKeys。如果用户没有为资源创建操作指定标签，则不会对 ec2:CreateTags 操作进行评估。

标签键和值区分大小写。

有关多值条件的更多信息，请参阅 IAM 用户指南 中的 [创建测试多个键值的条件](#)。有关示例 IAM 策略，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 398\)](#)。

适用于 AWS CLI 或 AWS 开发工具包的策略示例

以下示例显示了您可用于控制 IAM 用户 Amazon EC2 权限的策略语句。这些策略设计用于采用 AWS CLI 或 AWS 开发工具包发出的请求。有关用于 Amazon EC2 控制台的策略示例，请参阅 [用于 Amazon EC2 控制台的策略示例 \(p. 415\)](#)。有关特定于 Amazon VPC 的 IAM 策略示例，请参阅 [控制对 Amazon VPC 资源的访问](#)。

内容

- [1：只读访问 \(p. 398\)](#)
- [2：限制对特定区域的访问 \(p. 399\)](#)
- [3：使用实例 \(p. 399\)](#)
- [4：使用卷 \(p. 400\)](#)
- [5：启动实例 \(RunInstances\) \(p. 403\)](#)
- [6. 使用 ClassicLink \(p. 410\)](#)
- [7. 预留实例的使用 \(p. 412\)](#)
- [8. 标记资源 \(p. 412\)](#)
- [9：使用 IAM 角色 \(p. 414\)](#)

1：只读访问

以下策略授权用户使用名称以 `Describe` 开头的所有 Amazon EC2 API 操作。`Resource` 元素使用通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。

用户无权对资源执行任何操作（除非其他语句向用户授予执行此操作的权限），因为在默认情况下会对用户拒绝使用 API 操作的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": "ec2:Describe*",  
        "Resource": "*"  
    }]  
}
```

2：限制对特定区域的访问

以下策略向用户授予仅在欧洲（法兰克福）内使用所有 Amazon EC2 API 操作的权限。用户无法在任何其他区域中查看、创建、修改或删除资源。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "eu-central-1"  
                }  
            }  
        }  
    ]  
}
```

3：使用实例

主题

- [描述、启动、停止和终止所有实例 \(p. 399\)](#)
- [描述所有实例，以及仅停止、启动和终止特定实例 \(p. 399\)](#)

描述、启动、停止和终止所有实例

以下策略授权用户使用 Action 元素中指定的 API 操作。Resource 元素使用 * 通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。

用户无权使用任何其他 API 操作（除非其他语句允许用户执行此操作），因为用户在默认情况下没有使用 API 操作的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances", "ec2:DescribeImages",  
                "ec2:DescribeKeyPairs", "ec2:DescribeSecurityGroups",  
                "ec2:DescribeAvailabilityZones",  
                "ec2:RunInstances", "ec2:TerminateInstances",  
                "ec2:StopInstances", "ec2:StartInstances"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

描述所有实例，以及仅停止、启动和终止特定实例

以下策略允许用户描述所有实例，但只能启动和停止实例 i-1234567890abcdef0 和 i-0598c7d356eba48d7，且只能终止在美国东部（弗吉尼亚北部）地区 (us-east-1) 中具有“purpose=test”资源标签的实例。

第一条语句为 Resource 元素使用 * 通配符，以指示用户可以对操作指定所有资源；在本例中，用户可以列出所有实例。在 API 操作不支持资源级权限的情况下（在此情况下，为 ec2:DescribeInstances），也需要 *

通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。

第二条语句为 `StopInstances` 和 `StartInstances` 操作使用资源级权限。特定实例在 `Resource` 元素中通过其 ARN 进行指示。

第三条语句允许用户终止在美国东部（弗吉尼亚北部）地区 (`us-east-1`) 中、属于指定 AWS 账户并且具有标签 "`purpose=test`" 的所有实例。当策略语句生效时，`Condition` 元素具备资格。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DescribeInstances",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:StartInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0",  
                "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:TerminateInstances",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/purpose": "test"  
                }  
            }  
        }  
    ]  
}
```

4 : 使用卷

主题

- [挂载和分离卷 \(p. 400\)](#)
- [创建卷 \(p. 401\)](#)
- [创建带标签的卷 \(p. 401\)](#)

挂载和分离卷

在 API 操作需要发起人指定多种资源时，您必须创建一个策略语句，允许用户访问所需的所有资源。如果使用 `Condition` 元素时需要其中一种或多种资源，则必须创建多个语句，如本示例所示。

以下策略允许用户将带有 "`volume_user=iam-user-name`" 标签的卷与带有 "`department=dev`" 标签的实例关联起来，以及将这些卷与这些实例取消关联。如果您将此策略添加到 IAM 群组，`aws:username` 策略变量将授权群组中的每位 IAM 用户向具有 `volume_user` 标签（将用户的 IAM 用户名作为值）的实例挂载卷，或从那些实例分离这些卷。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/department": "dev"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/volume_user": "${aws:username}"
            }
        }
    }
]
```

创建卷

以下策略允许用户使用 [CreateVolume API](#) 操作。系统只允许用户创建加密且大小不足 20 GiB 的卷。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2>CreateVolume"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:VolumeSize" : "20"
                },
                "Bool": {
                    "ec2:Encrypted" : "true"
                }
            }
        }
    ]
}
```

创建带标签的卷

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求用户标记其使用标签 `costcenter=115` 和 `stack=prod` 创建的任何卷。`aws:TagKeys` 条件键使用 `ForAllValues` 修饰符指示只允许在请求中使用键 `costcenter` 和 `stack`(不能指定任何其他标签)。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，用户还必须具备使用 `createTags` 操作的权限。第二个语句使用 `ec2:CreateAction` 条件键使用户只能在 `CreateVolume` 上下文中创建标签。用户无法标记现有卷或任何其他资源。有关更多信息，请参阅 [用标记的资源级权限 \(p. 396\)](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowCreateTaggedVolumes",  
            "Effect": "Allow",  
            "Action": "ec2:CreateVolume",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/costcenter": "115",  
                    "aws:RequestTag/stack": "prod"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": ["costcenter", "stack"]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction" : "CreateVolume"  
                }  
            }  
        }  
    ]  
}
```

下面的策略允许用户创建卷而无需指定标签。仅当用户在 `CreateVolume` 请求中指定了标签时，系统才会评估 `CreateTags` 操作。如果用户指定了标签，则标签必须为 `purpose=test`。请求中不允许使用任何其他标签。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateVolume",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:1234567890:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/purpose": "test",  
                    "ec2:CreateAction" : "CreateVolume"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": "purpose"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

5 : 启动实例 (RunInstances)

[RunInstances](#) API 操作启动一个或多个实例。RunInstances 需要一个 AMI 并创建实例；用户可以在请求中指定密钥对和安全组。启动到 EC2-VPC 中需要子网，会创建网络接口。从由 Amazon EBS 支持的 AMI 启动将创建卷。因此，用户必须拥有使用这些 Amazon EC2 资源的权限。发起人还可以使用 RunInstances 的可选参数配置实例，例如实例类型和子网。您可以创建要求用户指定可选参数或限制用户针对某个参数使用特定值的策略语句。本部分的示例展示了许多可能方法中的一部分，您可使用这些方法控制用户能够启动的实例的配置。

请注意，在默认情况下，用户没有描述、启动、停止或终止所生成实例的权限。授予用户管理所生成实例的权限的一种方法是：为每个实例创建一个特定标签，然后创建一个允许用户使用该标签管理实例的语句。有关更多信息，请参阅 [3 : 使用实例 \(p. 399\)](#)。

主题

- [AMI \(p. 403\)](#)
- [实例类型 \(p. 404\)](#)
- [子网 \(p. 405\)](#)
- [EBS 卷 \(p. 406\)](#)
- [正在应用标签 \(p. 407\)](#)

AMI

以下策略仅允许用户使用拥有与之关联的指定标签“`department=dev`”的 AMI 启动实例。用户无法使用其他 AMI 启动实例，因为第一条语句的 Condition 元素要求用户指定带有此标签的 AMI。用户也不能启动到子网中，因为该策略未授予子网和网络接口资源的权限。但是，用户可以启动到 EC2-Classic 中。第二条语句会使用通配符来允许用户创建实例资源，并要求用户指定密钥对 `project_keypair` 和安全组 `sg-1a2b3c4d`。用户仍能够在没有密钥对的情况下启动实例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/project_keypair",
                "arn:aws:ec2:region:account:security-group/sg-1a2b3c4d"
            ]
        }
    ]
}
```

```
}
```

或者，以下策略仅允许用户使用指定的 AMI、`ami-9e1670f7` 和 `ami-45cf5c3c` 启动实例。用户无法使用其他 AMI 启动实例（除非其他语句授予执行此操作的用户权限），并且用户无法将实例启动到子网中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-9e1670f7",
                "arn:aws:ec2:region::image/ami-45cf5c3c",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

另外，以下策略还允许用户从 Amazon 拥有的所有 AMI 启动实例。第一个语句的 `Condition` 元素测试 `ec2:Owner` 是不是 `amazon`。用户无法使用其他 AMI 启动实例（除非其他语句允许用户执行此操作）。用户能够将实例启动到子网中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Owner": "amazon"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:subnet/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

实例类型

以下策略仅允许用户使用 `t2.micro` 或 `t2.small` 实例类型启动实例，您也可以通过此操作控制成本。用户无法启动更大的实例，因为第一条语句的 `Condition` 元素会测试 `ec2:InstanceType` 是否是 `t2.micro` 或 `t2.small`。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:region:account:instance/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:InstanceType": ["t2.micro", "t2.small"]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:region::image/ami-*",
            "arn:aws:ec2:region:account:subnet/*",
            "arn:aws:ec2:region:account:network-interface/*",
            "arn:aws:ec2:region:account:volume/*",
            "arn:aws:ec2:region:account:key-pair/*",
            "arn:aws:ec2:region:account:security-group/*"
        ]
    }
]
}
```

或者，您可以创建一个策略，对用户拒绝启动除 t2.micro 和 t2.small 实例类型之外的任何实例的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:InstanceType": ["t2.micro", "t2.small"]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:subnet/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

子网

以下策略仅允许用户使用指定子网 subnet-12345678 启动实例。组无法将实例启动到任何其他子网中（除非其他语句授予执行此操作的用户权限）。用户仍能够将实例启动到 EC2-Classic 中。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": "ec2:RunInstances",  
         "Resource": [  
             "arn:aws:ec2:region:account:subnet/subnet-12345678",  
             "arn:aws:ec2:region:account:network-interface/*",  
             "arn:aws:ec2:region:account:instance/*",  
             "arn:aws:ec2:region:account:volume/*",  
             "arn:aws:ec2:region:account:image/ami-*",  
             "arn:aws:ec2:region:account:key-pair/*",  
             "arn:aws:ec2:region:account:security-group/*"  
         ]  
     }  
    ]  
}
```

或者，您可以创建一个策略，拒绝用户将实例启动到任何其他子网。该语句通过拒绝创建网络接口的权限来执行此操作，除非指定了子网 subnet-12345678。此拒绝会覆盖创建的任何其他策略以允许将实例启动到其他子网中。用户仍能够将实例启动到 EC2-Classic 中。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Deny",  
         "Action": "ec2:RunInstances",  
         "Resource": [  
             "arn:aws:ec2:region:account:network-interface/*"  
         ],  
         "Condition": {  
             "ArnNotEquals": {  
                 "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678"  
             }  
         }  
     },  
     {  
         "Effect": "Allow",  
         "Action": "ec2:RunInstances",  
         "Resource": [  
             "arn:aws:ec2:region::image/ami-*",  
             "arn:aws:ec2:region:account:network-interface/*",  
             "arn:aws:ec2:region:account:instance/*",  
             "arn:aws:ec2:region:account:subnet/*",  
             "arn:aws:ec2:region:account:volume/*",  
             "arn:aws:ec2:region:account:key-pair/*",  
             "arn:aws:ec2:region:account:security-group/*"  
         ]  
     }  
}
```

EBS 卷

仅当实例的 EBS 卷为加密卷时，下面的策略才允许用户启动实例。用户必须从使用加密快照创建的 AMI 启动实例，以确保根卷是加密的。此外，用户在启动期间挂载到此实例的任何其他卷也必须是加密的。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region:account:instance/*"  
            ]  
        }  
    ]  
}
```

```
"Action": "ec2:RunInstances",
"Resource": [
    "arn:aws:ec2:*::volume/*"
],
"Condition": {
    "Bool": {
        "ec2:Encrypted": "true"
    }
}
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2::image/ami-*",
        "arn:aws:ec2::network-interface/*",
        "arn:aws:ec2::instance/*",
        "arn:aws:ec2::subnet/*",
        "arn:aws:ec2::key-pair/*",
        "arn:aws:ec2::security-group/*"
    ]
}
]
```

正在应用标签

下面的策略允许用户启动实例并在创建期间标记实例。对于应用标签的资源创建操作，用户必须具备使用 `CreateTags` 操作的权限。第二个语句使用 `ec2:CreateAction` 条件键使用户只能在 `RunInstances` 上下文中且只能为实例创建标签。用户无法标记现有资源，并且用户无法使用 `RunInstances` 请求标记卷。

有关更多信息，请参阅 [用于标记的资源级权限 \(p. 396\)](#)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction" : "RunInstances"
                }
            }
        }
    ]
}
```

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求用户标记使用标签 `environment=production` 和 `purpose=webserver` 通过 `RunInstances` 创建的任何卷。`aws:TagKeys` 条件键使用 `ForAllValues` 修饰符指示只允许在请求中使用键 `environment` 和 `purpose` (不能指定任何其他标签)。如果未在请求中指定任何标签，则请求失败。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region::image/*",  
                "arn:aws:ec2:region:account:subnet/*",  
                "arn:aws:ec2:region:account:network-interface/*",  
                "arn:aws:ec2:region:account:security-group/*",  
                "arn:aws:ec2:region:account:key-pair/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region:account:volume/*",  
                "arn:aws:ec2:region:account:instance/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/environment": "production" ,  
                    "aws:RequestTag/purpose": "webserver"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": ["environment","purpose"]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2>CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:region:account:/*/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2>CreateAction" : "RunInstances"  
                }  
            }  
        }  
    ]  
}
```

下面的策略对 aws:TagKeys 条件使用了 ForAnyValue 修饰符，以指示必须在请求中指定至少一个标签，并且其必须包含键 environment 或 webserver。标签必须应用于实例及卷。可以在请求中指定任何标签值。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region::image/*",  
                "arn:aws:ec2:region:account:subnet/*",  
                "arn:aws:ec2:region:account:volume/*",  
                "arn:aws:ec2:region:account:instance/*"  
            ]  
        }  
    ]  
}
```

```
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:security-group/*",
        "arn:aws:ec2:region:account:key-pair/*"
    ],
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": ["environment", "webserver"]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:region:account:*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
```

在下面的策略中，用户不必在请求中指定标签，但如果用户指定标签，则标签必须为 purpose=test。不允许使用任何其他标签。用户可以在 RunInstances 请求中向任何可标记资源应用标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "test",
                    "ec2:CreateAction" : "RunInstances"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "purpose"
                }
            }
        }
    ]
}
```

```
    ]  
}
```

6. 使用 ClassicLink

您可以为 VPC 启用 ClassicLink，然后将 EC2-Classic 实例链接到 VPC。您还可以查看启用了 ClassicLink 的 VPC 和所有链接到 VPC 的 EC2-Classic 实例。可以为 ec2:EnableVpcClassicLink、ec2:DisableVpcClassicLink、ec2:AttachClassicLinkVpc 和 ec2:DetachClassicLinkVpc 操作创建包含资源级权限的策略，以控制用户对这些操作的使用。ec2:Describe* 操作不支持资源级权限。

主题

- [使用 ClassicLink 的完全权限 \(p. 410\)](#)
- [为 VPC 启用和禁用 ClassicLink \(p. 410\)](#)
- [链接实例 \(p. 411\)](#)
- [断开关联实例 \(p. 411\)](#)

使用 ClassicLink 的完全权限

以下策略授予用户以下权限：查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例，为 VPC 启用和禁用 ClassicLink，以及从启用了 ClassicLink 的 VPC 链接实例和取消与实例的链接。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeClassicLinkInstances", "ec2:DescribeVpcClassicLink",  
                "ec2:EnableVpcClassicLink", "ec2:DisableVpcClassicLink",  
                "ec2:AttachClassicLinkVpc", "ec2:DetachClassicLinkVpc"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

为 VPC 启用和禁用 ClassicLink

以下策略允许用户为具有特定标签“purpose=classiclink”的 VPC 启用和禁用 ClassicLink。用户不能为其他任何 VPC 启用或禁用 ClassicLink。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:*VpcClassicLink",  
            "Resource": "arn:aws:ec2:region:account:vpc/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/purpose": "classiclink"  
                }  
            }  
        }  
    ]  
}
```

链接实例

以下策略向用户授予仅将 m3.large 类型的实例链接到 VPC 的权限。第二条语句允许用户使用 VPC 以及将实例链接到 VPC 所需的安全组资源。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:AttachClassicLinkVpc",  
            "Resource": "arn:aws:ec2:region:account:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:InstanceType": "m3.large"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:AttachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:vpc/*",  
                "arn:aws:ec2:region:account:security-group/*"  
            ]  
        }  
    ]  
}
```

以下策略向用户授予权限，以仅允许用户将实例链接到特定 VPC (vpc-1a2b3c4d) 以及仅将 VPC 中的特定安全组与实例 (sg-1122aabb 和 sg-aabb2233) 关联。用户不能将实例链接到任何其他 VPC，因此他们不能在请求中指定任何 VPC 其他安全组与实例关联。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:AttachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",  
                "arn:aws:ec2:region:account:instance/*",  
                "arn:aws:ec2:region:account:security-group/sg-1122aabb",  
                "arn:aws:ec2:region:account:security-group/sg-aabb2233"  
            ]  
        }  
    ]  
}
```

断开关联实例

以下策略授予用户从 VPC 取消与任何链接的 EC2-Classic 实例的链接的权限，但仅当实例具有标签“unlink=true”时才有效。第二条语句向用户授予权限以使用从 VPC 取消链接实例所需的 VPC 资源。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DetachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:instance/*"  
            ]  
        }  
    ]  
}
```

```
"Condition": {
    "StringEquals": {
        "ec2:ResourceTag/unlink": "true"
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:DetachClassicLinkVpc",
    "Resource": [
        "arn:aws:ec2:region:account:vpc/*"
    ]
}
}
```

7. 预留实例的使用

以下策略授予用户在您账户内查看、修改和购买预留实例的许可。

无法为单个预留实例设置资源级别的许可。此策略表示用户可以访问账户中的所有预留实例。

Resource元素使用的 * 通配符可用于指示用户可以通过操作指定所有资源；在此情况下，他们可以列出并修改账户中的所有预留实例。他们也可以使用账户凭证购买预留实例。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
            "ec2:PurchaseReservedInstancesOffering", "ec2:DescribeAvailabilityZones",
            "ec2:DescribeReservedInstancesOfferings"
        ],
        "Resource": "*"
    }]
}
```

允许用户查看和修改您账户中的预留实例，但是不能购买新的预留实例。

```
//{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
            "ec2:DescribeAvailabilityZones"
        ],
        "Resource": "*"
    }]
}
```

8. 标记资源

仅当标签包含键 environment 和值 production 时，下面的策略才允许用户使用 CreateTags 操作向实例应用标签。ForAllValues 修饰符与 aws:TagKeys 条件键配合使用，以指示只允许在请求中使用键 environment (不允许使用任何其他标签)。用户无法标记任何其他资源类型。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:region:account:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:RequestTag/environment": "production"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": [  
                        "environment"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

下面的策略允许用户标记已具有键为 owner、值为 IAM 用户名的标签的任何可标记资源。此外，用户还必须在请求中指定键为 test、值为 environment 或 prod 的标签。用户可以在请求中指定其他的标签。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:region:account:/*/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/environment": ["test", "prod"],  
                    "ec2:ResourceTag/owner": "${aws:username}"  
                }  
            }  
        }  
    ]  
}
```

您可以创建允许用户删除资源的特定标签的 IAM 策略。例如，当在请求中指定的标签键为 environment 或 cost-center 时，下面的策略允许用户删除卷的标签。可以为此标签指定任何值，但标签键必须匹配某个指定键。

Note

如果删除资源，则所有与资源相关的标签都将被删除。用户无需权限即可使用 ec2:DeleteTags 操作删除有标签的资源，只需要执行删除操作的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DeleteTags",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/cost-center": "environment"  
                }  
            }  
        }  
    ]  
}
```

```
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["environment", "cost-center"]
        }
    }
}
]
```

仅当资源已标记键为 `owner`、值为 IAM 用户名的标签时，此策略才允许用户只删除任何资源上的 `environment=prod` 标签。用户无法删除资源的任何其他标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTags"
            ],
            "Resource": "arn:aws:ec2:region:account:/*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "prod",
                    "ec2:ResourceTag/owner": "${aws:username}"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": ["environment"]
                }
            }
        }
    ]
}
```

9：使用 IAM 角色

以下策略允许用户将 IAM 角色连接、替换到具有标签 `department=test` 的实例或与之分离。替换或分离 IAM 角色需要一个关联 ID，因此策略还允许用户使用 `ec2:DescribeIamInstanceProfileAssociations` 操作。

IAM 用户必须具有使用 `iam:PassRole` 操作的授权，才能将角色传递到实例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation",
                "ec2:DisassociateIamInstanceProfile"
            ],
            "Resource": "arn:aws:ec2:region:account:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        }
    ]
}
```

```
{  
    "Effect": "Allow",  
    "Action": "iam:PassRole",  
    "Resource": "*"  
}  
]  
}
```

以下策略允许用户为所有实例连接或替换 IAM 角色。用户仅可以连接或替换名称以 `TestRole-` 开头的 IAM 角色。对于 `iam:PassRole` 操作，请确保您指定的是 IAM 角色的名称而不是实例配置文件的名称（如果名称不同）。有关更多信息，请参阅 [实例配置文件 \(p. 423\)](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DescribeIamInstanceProfileAssociations",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "arn:aws:iam::account:role/TestRole-*"  
        }  
    ]  
}
```

用于 Amazon EC2 控制台的策略示例。

您可以使用 IAM 策略向用户授予在 Amazon EC2 控制台中查看和使用特定资源的权限。您可以使用上一部分中的策略；但是，这些策略设计用于使用 AWS CLI 或 AWS 开发工具包发出的请求。控制台使用其他 API 操作实现其功能，因此这些策略可能不会按预期方式起作用。例如，只拥有 `DescribeVolumes` API 操作使用权限的用户在控制台中查看卷时会遇到错误。此部分演示使用户可以使用控制台的特定部分的策略。

主题

- [1：只读访问 \(p. 416\)](#)
- [2：使用 EC2 启动向导 \(p. 416\)](#)
- [3：使用卷 \(p. 418\)](#)
- [4：使用安全组 \(p. 419\)](#)
- [5：使用弹性 IP 地址 \(p. 421\)](#)
- [6. 预留实例的使用 \(p. 421\)](#)

Note

为帮助您了解在控制台中执行任务所需的相应 API 操作，您可以使用 AWS CloudTrail 等服务。有关更多信息，请参阅 [AWS CloudTrail User Guide](#)。如果您的策略不授予创建或修改特定资源的权限，则控制台显示一个包含诊断信息的编码消息。您可以使用适用于 AWS STS 的 `DecodeAuthorizationMessage` API 操作或 AWS CLI 中的 `decode-authorization-message` 命令对该消息解码。

有关创建 Amazon EC2 控制台的策略的更多信息，请参阅发布的以下 AWS 安全博客：[授予用户在 Amazon EC2 控制台中工作的权限。](#)

1：只读访问

要允许用户在 Amazon EC2 控制台中查看所有资源，您可以使用与以下示例相同的策略：[1：只读访问 \(p. 398\)](#) 用户无法对这些资源执行任何操作或创建新资源（除非其他语句向用户授予执行此操作的权限）。

a. 查看实例、AMI 和快照

或者，您可以提供对资源子集的只读访问权限。为此，请对每个资源将 `ec2:Describe` API 操作中的 * 通配符替换为特定 `ec2:Describe` 操作。以下策略允许用户在 Amazon EC2 控制台中查看所有实例、AMI 和快照。`ec2:DescribeTags` 操作允许用户查看公用 AMI。控制台需要标记信息来显示公用 AMI；但是，您可以删除此操作以允许用户只查看私有 AMI。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances", "ec2:DescribeImages",  
            "ec2:DescribeTags", "ec2:DescribeSnapshots"  
        ],  
        "Resource": "*"  
    }  
}
```

Note

当前，Amazon EC2 `ec2:Describe*` API 操作不支持资源级权限，因此您无法控制用户可以在控制台中查看的单个资源。因此，在以上语句的 `Resource` 元素中需要 * 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#)。

b. 查看实例和 CloudWatch 指标

以下策略允许用户在 Amazon EC2 控制台中查看实例，以及在 Instances 页面的 Monitoring 选项卡中查看 CloudWatch 警报和指标。Amazon EC2 控制台使用 CloudWatch API 显示警报和指标，因此您必须向用户授予对 `cloudwatch:DescribeAlarms` 和 `cloudwatch:GetMetricStatistics` 操作的使用权。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances",  
            "cloudwatch:DescribeAlarms",  
            "cloudwatch:GetMetricStatistics"  
        ],  
        "Resource": "*"  
    }  
}
```

2：使用 EC2 启动向导

Amazon EC2 启动向导是一系列屏幕，其中包含用于配置和启动实例的选项。您的策略必须包含允许用户使用向导选项的 API 操作使用权限。如果您的策略不包含使用这些操作的权限，则向导中的一些项目无法正确加载，用户无法完成启动。

a. 基本启动向导访问

要成功完成启动，必须向用户授予使用 `ec2:RunInstances` API 操作以及至少以下 API 操作的权限：

- `ec2:DescribeImages`：查看并选择 AMI。
- `ec2:DescribeVPCs`：查看可用网络选项，即 EC2-Classic 和 VPC 列表。即使您不在 VPC 中启动也需要此操作。
- `ec2:DescribeSubnets`：如果在 VPC 中启动，请查看所选 VPC 的所有可用子网。
- `ec2:DescribeSecurityGroups`：查看向导中的安全组页面。用户可以选择现有安全组。
- `ec2:DescribeKeyPairs` 或 `ec2>CreateKeyPair`：选择现有密钥对或创建新密钥对。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances", "ec2:DescribeImages",  
            "ec2:DescribeKeyPairs", "ec2:DescribeVPCs", "ec2:DescribeSubnets",  
            "ec2:DescribeSecurityGroups"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": "*"  
    }  
}
```

您可以向策略添加 API 操作以便为用户提供更多选项，例如：

- `ec2:DescribeAvailabilityZones`：如果启动到 EC2-Classic，请查看并选择特定可用区。
- `ec2:DescribeNetworkInterfaces`：如果启动到 VPC，请查看并选择所选子网的现有网络接口。
- `ec2:CreateSecurityGroup` 创建新安全组；如创建向导推荐的 `launch-wizard-x` 安全组。但是，此操作仅单独创建安全组；不添加或修改任何规则。要添加入站规则，必须向用户授予使用 `ec2:AuthorizeSecurityGroupIngress` API 操作的权限。要向 VPC 安全组添加出站规则，必须向用户授予使用 `ec2:AuthorizeSecurityGroupEgress` API 操作的权限。要修改或删除现有规则，必须向用户授予使用相关 `ec2:RevokeSecurityGroup*` API 操作的权限。
- `ec2:CreateTags`：标记通过 `RunInstances` 创建的资源。有关更多信息，请参阅 [用于标记的资源权限 \(p. 396\)](#)。如果用户没有使用此操作的权限而又尝试在启动向导的标记页上应用标签，则启动失败。

Important

向用户授予使用 `ec2:CreateTags` 操作的权限时请小心谨慎。这会限制您使用 `ec2:ResourceTag` 条件密钥限制其他资源的使用的能力；用户可以更改资源的标签以便绕过这些限制。

当前，Amazon EC2 `Describe*` API 操作不支持资源级权限，因此您无法限制用户可以在启动向导中查看的单个资源。但是，您可以对 `ec2:RunInstances` API 操作应用资源级权限，以限制用户可以用于启动实例的资源。如果用户选择未授权他们使用的选项，则启动会失败。

b. 限制对特定实例类型、子网和区域的访问

以下策略允许用户使用 Amazon 拥有的 AMI 启动 `m1.small` 实例，并且仅在特定子网 (`subnet-1a2b3c4d`) 中启动。用户只能在 `sa-east-1` 区域中启动。如果用户在启动向导中选择不同区域或选择不同实例类型、AMI 或子网，则启动会失败。

第一条语句向用户授予查看启动向导中的选项的权限，如上例所示。第二条语句向用户授予将网络接口、卷、密钥对、安全组和子网资源（在 VPC 中启动实例需要这些资源）用于 ec2:RunInstances 操作的权限。有关使用 ec2:RunInstances 操作的更多信息，请参阅 [5：启动实例（RunInstances）\(p. 403\)](#)。第三和第四条语句分别向用户授予使用实例（仅当实例是 m1.small 实例时）和 AMI 资源（仅当 AMI 由 Amazon 所有时）的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances", "ec2:DescribeImages",  
            "ec2:DescribeKeyPairs", "ec2:DescribeVpcs", "ec2:DescribeSubnets",  
            "ec2:DescribeSecurityGroups"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",  
            "arn:aws:ec2:sa-east-1:111122223333:volume/*",  
            "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",  
            "arn:aws:ec2:sa-east-1:111122223333:security-group/*",  
            "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"  
        ]  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1:111122223333:instance/*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:InstanceType": "m1.small"  
            }  
        }  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1::image/ami-*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:Owner": "amazon"  
            }  
        }  
    }  
}
```

3：使用卷

以下策略向用户授予查看和创建卷以及将卷与特定实例连接和断开的权限。

用户可以将任何卷连接到具有标签“purpose=test”的实例，也可以从这些实例断开卷。要使用 Amazon EC2 控制台连接卷，用户有权使用 ec2:DescribeInstances 操作会很有帮助，因为这可以让他们从 Attach Volume（连接卷）对话框的预填充列表中选择实例。但是，这也会允许用户在控制台的 Instances 页面上查看所有实例，因此，您可以省略此操作。

在第一条语句中，需要 ec2:DescribeVolumeStatus 和 ec2:DescribeAvailabilityZones 操作以确保卷在控制台中正确显示。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeVolumes", "ec2:DescribeVolumeStatus",  
                "ec2:DescribeAvailabilityZones", "ec2>CreateVolume",  
                "ec2:DescribeInstances"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AttachVolume",  
                "ec2:DetachVolume"  
            ],  
            "Resource": "arn:aws:ec2:region:111122223333:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/purpose": "test"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AttachVolume",  
                "ec2:DetachVolume"  
            ],  
            "Resource": "arn:aws:ec2:region:111122223333:volume/*"  
        }  
    ]  
}
```

4 : 使用安全组

a. 查看安全组以及添加和删除规则

以下策略为用户授予的权限可在 Amazon EC2 控制台中查看安全组，并为具有标签 Department=Test

Note

的现有安全组添加和删除入站和出站规则。

您无法为 EC2-Classic 安全组修改出站规则。有关安全组的更多信息，请参阅 [Linux 实例的 Amazon EC2 个安全组 \(p. 354\)](#)。

在第一条语句中，ec2:DescribeTags 操作允许用户在控制台中查看标签，这样，用户更易于识别自己可修改的安全组。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeSecurityGroups", "ec2:DescribeTags"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
{  
    "Effect": "Allow",  
    "Action": [  
        "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",  
        "ec2:AuthorizeSecurityGroupEgress", "ec2:RevokeSecurityGroupEgress"  
    ],  
    "Resource": [  
        "arn:aws:ec2:region:111122223333:security-group/*"  
    ],  
    "Condition": {  
        "StringEquals": {  
            "ec2:ResourceTag/Department": "Test"  
        }  
    }  
}
```

b. 使用 Create Security Group 对话框

您可以创建一个策略，以允许用户使用 Amazon EC2 控制台中的 Create Security Group (创建安全组) 对话框。要使用此对话框，必须向用户授予使用至少以下 API 操作的权限：

- `ec2:CreateSecurityGroup`: 创建新安全组。
- `ec2:DescribeVpcs` 查看 VPC 列表中的现有 VPC 列表。在 EC2-Classic 上创建安全组不需要此操作。

借助这些权限，用户可以成功创建新安全组，但是他们不能向其中添加任何规则。要在 Create Security Group (创建安全组) 对话框中使用规则，您可以向策略添加以下 API 操作：

- `ec2:AuthorizeSecurityGroupIngress` : 添加入站规则。
- `ec2:AuthorizeSecurityGroupEgress` : 向 VPC 安全组添加出站规则。
- `ec2:RevokeSecurityGroupIngress` : 修改或删除现有入站规则。如果要允许用户使用控制台中的 Copy to new 功能，这十分有用。此功能会打开 Create Security Group (创建安全组) 对话框，并使用所选安全组的规则进行填充。
- `ec2:RevokeSecurityGroupEgress` : 修改或删除适用于 VPC 安全组的出站规则。若要允许用户修改或删除所有出站流量的默认出站规则，这十分有用。
- `ec2:DeleteSecurityGroup` : 适用于无效规则无法保存的情况。控制台首先创建安全组，然后添加指定的规则。如果规则无效，则操作会失败，而控制台会尝试删除安全组。用户仍会停留在“Create Security Group”对话框中，这样就能更正无效规则和尝试重新创建安全组。此 API 操作不是必需的，但是如果用户在无权使用它的情况下尝试创建具有无效规则的安全组，则会创建不包含任何规则的安全组，用户必须在之后添加规则。

当前，`ec2:CreateSecurityGroup` API 操作不支持资源级权限；但是，您可以向 `ec2:AuthorizeSecurityGroupIngress` 和 `ec2:AuthorizeSecurityGroupEgress` 操作应用资源级权限以控制用户创建规则的方式。

以下策略向用户授予使用 Create Security Group (创建安全组) 对话框，以及为与特定 VPC (`vpc-1a2b3c4d`) 关联的安全组创建入站和出站规则的权限。用户可以为 EC2-Classic 或其他 VPC 创建安全组，但是无法向它们添加任何规则。同样，用户无法向不与 VPC `vpc-1a2b3c4d` 关联的任何现有安全组添加任何规则。还向用户授予了在控制台中查看所有安全组的权限。这样，用户更易于识别自己可添加入站规则的安全组。此策略还向用户授予删除与 VPC `vpc-1a2b3c4d` 关联的安全组的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",  
                "ec2:AuthorizeSecurityGroupEgress", "ec2:RevokeSecurityGroupEgress"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region:111122223333:security-group/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/Department": "Test"  
                }  
            }  
        }  
    ]  
}
```

```
    "ec2:DescribeSecurityGroups", "ec2>CreateSecurityGroup", "ec2:DescribeVpcs"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "ec2>DeleteSecurityGroup", "ec2:AuthorizeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress"
],
"Resource": "arn:aws:ec2:region:111122223333:security-group/*",
"Condition": {
    "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
    }
}
]
}
```

5：使用弹性 IP 地址

为了让用户能够查看 Amazon EC2 控制台中的弹性 IP 地址，您必须授予用户使用 `ec2:DescribeAddresses` 操作的权限。

要允许用户使用弹性 IP 地址，可将以下操作添加到您策略中。

- `ec2:AllocateAddress`：分配可在 VPC 或 EC2-Classic 中使用的地址。
- `ec2:ReleaseAddress`：解除弹性 IP 地址。
- `ec2:AssociateAddress`：将弹性 IP 地址与实例或网络接口关联。
- `ec2:DescribeNetworkInterfaces` 和 `ec2:DescribeInstances`：使用 Associate Address (关联地址) 屏幕。屏幕显示了您可以将弹性 IP 地址关联到的可用实例或网络接口。对于一个 EC2-Classic 实例，用户只需拥有使用 `ec2:DescribeInstances` 的权限。
- `ec2:DisassociateAddress`：取消弹性 IP 地址与实例或网络接口的关联。

以下策略允许用户查看弹性 IP 地址并将其分配给实例和与实例相关联。用户不可以将弹性 IP 地址与网络接口关联、取消弹性 IP 地址的关联或释放弹性 IP 地址。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

6. 预留实例的使用

以下策略可以附加到 IAM 用户。它可让用户查看和修改您账户中的预留实例，同时也能在 AWS 管理控制台内购买新的预留实例。

该策略允许用户查看账户内的所有预留实例和按需实例。无法为单个预留实例设置资源级别的许可。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": [  
             "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",  
             "ec2:PurchaseReservedInstancesOffering", "ec2:DescribeInstances",  
             "ec2:DescribeAvailabilityZones", "ec2:DescribeReservedInstancesOfferings"  
         ],  
         "Resource": "*"  
    ]  
}
```

必须进行 `ec2:DescribeAvailabilityZones` 操作才能确保 Amazon EC2 控制台可以显示有关您能够购买预留实例的可用区的信息。`ec2:DescribeInstances` 操作不是必须的，但是请确保用户可查看账户内的实例并且能够购买预留实例，以匹配正确的规格。

您可以调整 API 操作，以限制用户访问，例如移除 `ec2:DescribeInstances`，而 `ec2:DescribeAvailabilityZones` 表示用户有只读形式的访问权。

适用于 Amazon EC2 的 IAM 角色

应用程序必须通过 AWS 证书签署 API 请求。因此，如果您是应用程序开发人员，您需要一个策略来为 EC2 实例上运行的应用程序管理证书。例如，您可以安全地将您的 AWS 证书分配至实例，从而允许这些实例上运行的应用程序使用您的证书签署请求，并保护您的证书免受其他用户的影响。但是，要将证书安全地分配至每项实例是有难度的，尤其是以您的名义创建的 AWS，例如竞价型实例或 Auto Scaling 组中的实例。当您更换 AWS 证书时，您还必须能够更新每项实例上的证书。

我们设计了 IAM 角色，以便您的应用程序能够安全地从实例发出 API 请求，而无需管理应用程序使用的安全证书。您可以使用 IAM 角色委托授权以发出 API 请求，而不用创建并分配您的 AWS 证书，如下所示：

1. 创建一个 IAM 角色。
2. 定义能够担任此角色的账户或 AWS 服务。
3. 定义担任角色后应用程序可以使用的 API 操作和资源。
4. 在您启动您的实例时指定角色，或者将角色附加到正在运行或已停止的实例。
5. 让应用程序检索一组临时证书并使用它们。

例如，您可以使用 IAM 角色为在实例上运行的应用程序授予使用 Amazon S3 中的存储桶的权限。您可以通过创建 JSON 格式的策略为 IAM 角色指定权限。这些类似于您为 IAM 用户创建的策略。如果您对某个角色进行了更改，系统会将此更改传播到所有实例。

您不可以将多个 IAM 角色附加到一个实例，但是，您可以将一个 IAM 角色附加到多个实例。有关创建和使用 IAM 角色的更多信息，请参阅 IAM 用户指南 中的 [角色](#)。

您可以将资源级权限应用到您的 IAM 策略，以便控制用户为一个实例附加、替换或分离 IAM 角色的能力。有关更多信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#) 以及以下示例：[9：使用 IAM 角色 \(p. 414\)](#)。

主题

- [实例配置文件 \(p. 423\)](#)
- [通过实例元数据检索安全证书 \(p. 423\)](#)
- [允许 IAM 用户将 IAM 角色传递给实例 \(p. 423\)](#)

- 使用 IAM 角色 (p. 424)

实例配置文件

Amazon EC2 使用实例配置文件 作为 IAM 角色的容器。使用 IAM 控制台创建 IAM 角色时，控制台自动创建实例配置文件，按相应的角色为文件命名。如果您使用 Amazon EC2 控制台启动一个带 IAM 角色的实例或将一个 IAM 角色附加到实例，则请根据实例配置文件列表选择实例。

如果您使用 AWS CLI、API 或 AWS 软件开发工具包创建角色，则以单独操作的形式创建角色和实例配置文件，可以为它们提供不同的名称。如果您使用 AWS CLI、API 或 AWS 软件开发工具包启动带有 IAM 角色的实例，或将 IAM 角色附加到实例，则请指定实例配置文件名称。

一个实例配置文件只能包含一个 IAM 角色。不能提高此限制。

有关更多信息，请参阅 IAM 用户指南 中的[实例配置文件](#)。

通过实例元数据检索安全证书

实例上的应用程序通过实例元数据条目 `iam/security-credentials/role-name` 检索角色提供的安全证书。该应用程序具有使用您通过与角色关联的安全证书为其定义的操作和资源的权限。这些安全证书是临时的，我们会自动更换它们。我们会在旧证书过期前至少五分钟提供可用的新证书。

Warning

如果您使用的服务采用了带有 IAM 角色的实例元数据，请确保服务代表您进行 HTTP 调用时不会泄露您的证书。可能泄露您的证书的服务类型包括 HTTP 代理、HTML/CSS 验证程序服务和支持 XML 包含的 XML 处理程序。

以下命令检索名为 `s3access` 的 IAM 角色的安全证书。

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

下面是示例输出。

```
{  
    "Code" : "Success",  
    "LastUpdated" : "2012-04-26T16:39:16Z",  
    "Type" : "AWS-HMAC",  
    "AccessKeyId" : "AKIAIOSFODNN7EXAMPLE",  
    "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",  
    "Token" : "token",  
    "Expiration" : "2012-04-27T22:39:16Z"  
}
```

对于实例上运行的应用程序、AWS CLI 和 Windows PowerShell 工具 命令，您不必显式获取临时安全凭证 - AWS 软件开发工具包、AWS CLI 和 Windows PowerShell 工具 会自动从 EC2 实例元数据服务获取凭证并使用这些凭证。要使用临时安全凭证在实例外部发出调用 (例如，为了测试 IAM 策略)，您必须提供访问密钥、私有密钥和会话令牌。有关更多信息，请参阅 IAM 用户指南 中的[使用临时安全凭证以请求对 AWS 资源的访问权限](#)。

有关实例元数据的更多信息，请参阅[实例元数据和用户数据 \(p. 295\)](#)。

允许 IAM 用户将 IAM 角色传递给实例

若要支持 IAM 用户启动包含 IAM 角色的实例或为现有实例替换 IAM 角色，您必须授予用户将角色传递给实例的权限。

以下 IAM 策略允许用户启动带有 IAM 角色的实例 (ec2:RunInstances) , 或者为现有实例附加或替换 IAM 角色 (ec2:AssociateIamInstanceProfile 和 ec2:ReplaceIamInstanceProfileAssociation)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances",  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "*"  
        }  
    ]  
}
```

通过在策略中指定资源为“*” , 该策略授权 IAM 用户访问所有角色。但是 , 要考虑启动带有您的角色 (现有的或您即将创建的) 的实例的用户是否会被授予不需要或不应该有的权限。

使用 IAM 角色

在启动过程中或启动之后 , 您可以创建一个 IAM 角色并将其附加到实例。您也可以为实例替换或分离 IAM 角色。

内容

- [创建 IAM 角色 \(p. 424\)](#)
- [启动带有 IAM 角色的实例 \(p. 426\)](#)
- [将 IAM 角色连接到实例 \(p. 427\)](#)
- [分离 IAM 角色 \(p. 428\)](#)
- [替换 IAM 角色 \(p. 429\)](#)

创建 IAM 角色

您必须先创建 IAM 角色 , 然后才能启动带有该角色的实例或将其附加到该实例。

使用 IAM 控制台创建 IAM 角色

1. 在 <https://console.aws.amazon.com/iam/> 处登录 IAM 控制台。
2. 在导航窗格中 , 选择 Roles 和 Create New Role。
3. 在 Set Role Name 页面上 , 输入角色的名称 , 然后选择 Next Step。
4. 在 Select Role Type 页面上 , 选择 Amazon EC2 旁的 Select。
5. 在 Attach Policy 页面上 , 选择 AWS 管理的策略。例如 , 对于 Amazon EC2 , 下列 AWS 管理的策略之一可能符合您的需求 :
 - PowerUserAccess
 - ReadOnlyAccess
 - AmazonEC2FullAccess

- AmazonEC2ReadOnlyAccess

6. 检查角色信息，根据需要编辑角色，然后选择 Create Role。

或者，您可以使用 AWS CLI 创建 IAM 角色。

使用 AWS CLI 创建 IAM 角色和实例配置文件

- 使用允许角色使用 Amazon S3 存储桶的策略创建 IAM 角色。

a. 创建以下信任策略并将其保存在名为 ec2-role-trust-policy.json 的文本文件中。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": { "Service": "ec2.amazonaws.com"},  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

b. 创建 s3access 角色并指定您创建的信任策略。

```
aws iam create-role --role-name s3access --assume-role-policy-document file://ec2-  
role-trust-policy.json  
{  
    "Role": {  
        "AssumeRolePolicyDocument": {  
            "Version": "2012-10-17",  
            "Statement": [  
                {  
                    "Action": "sts:AssumeRole",  
                    "Effect": "Allow",  
                    "Principal": {  
                        "Service": "ec2.amazonaws.com"  
                    }  
                }  
            ]  
        },  
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",  
        "CreateDate": "2013-12-12T23:46:37.247Z",  
        "RoleName": "s3access",  
        "Path": "/",  
        "Arn": "arn:aws:iam::123456789012:role/s3access"  
    }  
}
```

c. 创建访问策略并将其保存在名为 ec2-role-access-policy.json 的文本文件中。例如，此策略向在实例上运行的应用程序授予针对 Amazon S3 管理员权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["s3:*"],  
            "Resource": ["*"]  
        }  
    ]  
}
```

- d. 向角色附加访问策略。

```
aws iam put-role-policy --role-name s3access --policy-name S3-Permissions --policy-document file://ec2-role-access-policy.json
```

- e. 创建名为 s3access-profile 的实例配置文件。

```
aws iam create-instance-profile --instance-profile-name s3access-profile
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

- f. 将 s3access 角色添加到 s3access-profile 实例配置文件。

```
aws iam add-role-to-instance-profile --instance-profile-name s3access-profile --role-name s3access
```

想要了解更多有关这些命令的信息，请参阅 AWS Command Line Interface Reference 中的 [create-role](#)、[put-role-policy](#) 和 [create-instance-profile](#)。

或者，您可以使用以下适用于 Windows PowerShell 的 AWS 工具命令：

- [New-IAMRole](#)
- [Register-IAMRolePolicy](#)
- [New-IAMInstanceProfile](#)

启动带有 IAM 角色的实例

创建一个 IAM 角色之后，您可以启动实例，并在启动过程中将该角色与实例关联。

Important

在创建 IAM 角色之后，可能需要让权限传播几秒钟时间。若您第一次尝试启动带角色的实例失败，请等待几秒然后重试。有关更多信息，请参阅 IAM 用户指南中的[使用角色故障排除](#)。

启动带有 IAM 角色的实例使用控制台

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。
4. 在 Configure Instance Details 页面上，为 IAM role 选择您创建的 IAM 角色。

Note

IAM role (IAM 角色) 列表显示您在创建 IAM 角色时创建的实例配置文件的名称。如果您是使用控制台创建的 IAM 角色，则为您创建了实例配置文件，并提供了与角色相同的名称。如果使用 AWS CLI、API 或 AWS 开发工具包创建了 IAM 角色，则可能对实例配置指定了不同名称。

5. 配置其他详细信息，然后按照向导的其余说明操作，或选择 Review and Launch 接受默认设置并直接转到 Review Instance Launch 页面。

6. 检查设置，然后选择 Launch 以选择密钥对并启动实例。
7. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 AWS 安全证书，并使用它们签署请求。请注意，此操作由 AWS 开发工具包为您执行。

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

或者，您可以在启动过程中使用 AWS CLI 将角色关联到实例。您必须在命令中指定实例配置文件。

使用 AWS CLI 启动带有 IAM 角色的实例

1. 使用 [run-instances](#) 命令启动使用实例配置文件的实例。以下示例演示如何使用实例配置启动实例。

```
aws ec2 run-instances --image-id ami-11aa22bb --iam-instance-profile Name="s3access-profile" --key-name my-key-pair --security-groups my-security-group --subnet-id subnet-1a2b3c4d
```

或者，使用 [New-EC2Instance](#) Windows PowerShell 工具 命令。

2. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 AWS 安全证书，并使用它们签署请求。请注意，此操作由 AWS 开发工具包为您执行。

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

将 IAM 角色连接到实例

在您创建了一个 IAM 角色后，可将其附加到正在运行或已停止的实例。

使用控制台将 IAM 角色连接到实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，再依次选择 Actions、Instance Settings 和 Attach/Replace IAM role。
4. 选择要附加到您的实例的 IAM 然后选择 Apply。

使用 AWS CLI 将 IAM 角色附加到实例

1. 如果需要，请描述您的实例以获取要附加角色的实例的 ID。

```
aws ec2 describe-instances
```

2. 使用 [associate-iam-instance-profile](#) 命令，通过指定实例配置文件，将 IAM 角色附加到实例。您可以使用实例配置文件的亚马逊资源名称 (ARN)，或者使用实例的名称。

```
aws ec2 associate-iam-instance-profile --instance-id i-1234567890abcdef0 --iam-instance-profile Name="TestRole-1"  
  
{  
    "IamInstanceProfileAssociation": {  
        "InstanceId": "i-1234567890abcdef0",  
        "State": "associating",  
        "AssociationId": "iip-assoc-0dbd8529a48294120",  
        "IamInstanceProfile": {  
            "Id": "AIPAJLNLDX3AMYZNWYYAY",  
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
```

```
        }
    }
```

或者，使用以下 Windows PowerShell 工具 命令：

- [Get-EC2Instance](#)
- [Register-EC2IamInstanceProfile](#)

分离 IAM 角色

您可以将 IAM 角色从正在运行或已停止的实例上断开。

使用控制台从实例上断开 IAM 角色

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，再依次选择 Actions、Instance Settings 和 Attach/Replace IAM role。
4. 对于 IAM role，请选择 No Role。选择 Apply。
5. 在确认对话框中，选择 Yes, Detach。

使用 AWS CLI 将 IAM 角色从实例中分离

1. 如果需要，使用[describe-iam-instance-profile-associations](#)描述您的 IAM 实例配置文件关联，并获取要分离的 IAM 实例配置文件的关联 ID。

```
aws ec2 describe-iam-instance-profile-associations

{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. 使用 [disassociate-iam-instance-profile](#) 命令分离使用其关联 ID 的 IAM 实例配置文件。

```
aws ec2 disassociate-iam-instance-profile --association-id iip-assoc-0044d817db6c0a4ba

{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

或者，使用以下 Windows PowerShell 工具 命令：

- [Get-EC2IamInstanceProfileAssociation](#)
- [Unregister-EC2IamInstanceProfile](#)

替换 IAM 角色

您可以替换正在运行的实例的 IAM 角色。如果您想要更改实例的 IAM 角色但又不想先分离现有的角色（例如，为了确保在此实例上运行的应用程序执行的 API 操作不会中断），则可以执行此操作。

使用控制台替换实例的 IAM 角色

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，再依次选择 Actions、Instance Settings 和 Attach/Replace IAM role。
4. 选择要附加到您的实例的 IAM，然后选择 Apply。

使用 AWS CLI 替换实例的 IAM 角色

1. 如果需要，请描述您的 IAM 实例配置文件关联情况，以获取要替换的 IAM 实例配置文件的关联 ID。

```
aws ec2 describe-iam-instance-profile-associations
```

2. 使用 [replace-iam-instance-profile-association](#) 命令，通过为现有实例配置文件或 ARN 指定关联 ID 或指定替换实例配置文件的名称，替换 IAM 实例配置文件。

```
aws ec2 replace-iam-instance-profile-association --association-id iip-assoc-0044d817db6c0a4ba --iam-instance-profile Name="TestRole-2"

{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

或者，使用以下 Windows PowerShell 工具 命令：

- [Get-EC2IamInstanceProfileAssociation](#)
- [Set-EC2IamInstanceProfileAssociation](#)

为您的 Linux 实例授权入站流量

您可以采用安全组控制实例的流量，包括可到达您的实例的流量类型。例如，您可以只允许来自您家庭网络的计算机使用 SSH 访问您的实例。如果您的实例为 Web 服务器，那么您可以允许所有 IP 地址通过 HTTP 访问您的实例，以便外部用户能够浏览您的 Web 服务器上的内容。

若要启用对实例的网络访问，您必须允许该实例的入站流量。要为入站流量打开端口，您需要在启动实例时向与实例关联的安全组添加规则。

要连接到您的实例，您必须设置规则以向来自您计算机的公有 IPv4 地址的 SSH 流量授权。若要允许来自其他 IP 地址范围的 SSH 流量，请为需要授权的每个范围另外添加规则。

如果您已启用了支持 IPv6 的 VPC 并使用 IPv6 地址启动您的实例，则可以使用其 IPv6 地址而非公有 IPv4 地址连接到您的实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。

如果您需要启用对 Windows 实例的网络访问，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[为 Windows 实例授权入站流量](#)。

在您开始之前

确定谁需要访问您的实例；例如，您信任的单个主机或特定网络（例如，本地计算机的公有 IPv4 地址）。Amazon EC2 控制台的安全组编辑器可自动为您检测本地计算机的公有 IPv4 地址。此外，您可以在 Internet 浏览器中使用搜索短语“what is my IP address”，或使用以下服务：<http://checkip.amazonaws.com/>。如果您正通过 ISP 或从防火墙后面连接，没有静态 IP 地址，您需要找出客户端计算机使用的 IP 地址范围。

Warning

如果您使用 `0.0.0.0/0`，则所有 IPv4 地址都可以使用 SSH 访问您的实例。如果您使用 `::/0`，则所有 IPv6 地址都可以访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产中，您将仅授权特定 IP 地址或地址范围访问您的实例。

有关安全组的更多信息，请参阅[Linux 实例的 Amazon EC2 安全组 \(p. 354\)](#)。

针对发送到 Linux 实例的入站 SSH 流量添加规则

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须在安全组中添加规则，以便能够使用 SSH 从您的 IP 地址连接到 Linux 实例。

使用控制台在安全组中为通过 IPv4 的入站 SSH 流量添加规则

1. 在 Amazon EC2 控制台的导航窗格中，选择 Instances。选择实例并查看 Description (描述) 选项卡；Security groups (安全组) 列出了与该实例关联的安全组。选择 view rules，以显示对实例生效的规则列表。
2. 在导航窗格中，选择 Security Groups。选择与您的实例相关联的一个安全组。
3. 在详细信息窗格中的 Inbound 选项卡上，选择 Edit。在对话框中，选择 Add Rule，然后从 Type 列表中选择 SSH。
4. 在源字段中，选择 My IP，以使用本地计算机的公有 IPv4 地址自动填充字段。或者，选择自定义并使用 CIDR 表示法指定计算机的公有 IPv4 地址或网络。例如，如果您的 IPv4 地址为 `203.0.113.25`，请指定 `203.0.113.25/32`，以使用 CIDR 表示法列出此单个 IPv4 地址。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 `203.0.113.0/24`。

有关查找 IP 地址的信息，请参阅[在您开始之前 \(p. 430\)](#)。

5. 选择 Save。

(仅限 VPC) 如果您已启动带有 IPv6 地址的实例并希望使用其 IPv6 地址连接到您的实例，则必须添加允许通过 SSH 的入站 IPv6 流量的规则。

使用控制台在安全组中为通过 IPv6 的入站 SSH 流量添加规则

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。为您的实例选择安全组。
3. 依次选择入站、编辑和添加规则。

4. 对于类型，请选择 SSH。
5. 在源字段中，使用 CIDR 表示法为您的计算机指定 IPv6 地址。例如，如果您的 IPv6 地址为 2001:db8:1234:1a00:9691:9503:25ad:1761，请指定 2001:db8:1234:1a00:9691:9503:25ad:1761/128，以使用 CIDR 表示法列出单个 IP 地址。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 2001:db8:1234:1a00::/64。
6. 选择 Save。

使用命令行向安全组添加规则

您可以使用以下任一命令。请确保此命令在您的本地系统中运行，而不是针对实例本身。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [authorize-security-group-ingress \(AWS CLI\)](#)
- [Grant-EC2SecurityGroupIngress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

向实例分配安全组

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。在 VPC 中启动实例后，您可以更改其安全组。想要了解更多有关信息，请参阅 Amazon VPC 用户指南中的[更改实例的安全组](#)主题。

Amazon EC2 和 Amazon Virtual Private Cloud

通过 Amazon Virtual Private Cloud (Amazon VPC)，您可以在 AWS 云内您自己的逻辑隔离区域中定义虚拟网络，我们称之为 Virtual Private Cloud (VPC)。您可将 AWS 资源（如实例）启动到 VPC 中。您的 VPC 与您可能在自己的数据中心运行的传统网络极其相似，但同时可为您提供利用 AWS 的可扩展基础设施的优势。您可以配置您的 VPC；您可以选择它的 IP 地址范围、创建子网并配置路由表、网关和安全设置。现在您可以将您的 VPC 中的实例连接到 Internet。您可以将 VPC 连接到自己的企业数据中心，利用 AWS 云扩展您的数据中心。要保护各个子网中的资源，您可以利用多种安全层，包括安全组和网络访问控制列表。有关更多信息，请参阅 [Amazon VPC 用户指南](#)。

根据各区域的不同条件，您的账户可能同时支持 EC2-VPC 和 EC2-Classic 平台。如果您的账户是在 2013 年 12 月 4 日之后创建的，则它仅支持 EC2-VPC。要查明您的账户支持的平台，请参阅 [支持的平台 \(p. 435\)](#)。如果您的账户仅支持 EC2-VPC，我们会为您创建一个默认 VPC。默认 VPC 是已配置好可供您使用的 VPC。您可以立即在您的默认 VPC 内启动实例。有关更多信息，请参阅 Amazon VPC 用户指南中的[您的默认 VPC 和子网](#)。如果您的账户支持 EC2-Classic 和 EC2-VPC，则可以在任一平台中启动实例。不论您的账户支持哪种平台，您都可以创建自己的非默认 VPC 并根据需要对其进行配置。

内容

- [使用 VPC 的优势 \(p. 432\)](#)
- [EC2-Classic与 EC2-VPC 的区别 \(p. 432\)](#)
- [在 EC2-Classic 与 EC2-VPC 之间共享和访问资源 \(p. 433\)](#)
- [实例类型仅在 VPC 中可用 \(p. 434\)](#)
- [Amazon VPC 文档 \(p. 435\)](#)
- [支持的平台 \(p. 435\)](#)
- [ClassicLink \(p. 436\)](#)
- [从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 \(p. 445\)](#)

使用 VPC 的优势

通过将实例启动到 VPC (而不是 EC2-Classic) , 您能够 :

- 将静态私有 IPv4 地址分配给在启动和停止时保持不变的实例
- 将多个 IPv4 地址分配给您的实例
- 定义网络接口，并将一个或多个网络接口连接到您的实例
- 在实例运行时更改其安全组成员身份
- 控制您的实例的入站流量(入站筛选)和出站流量(出站筛选)
- 以网络访问控制列表(ACL)的方式为您的实例添加额外的访问控制层
- 在单租户硬件上运行您的实例
- 将 IPv6 地址分配给实例

EC2-Classic与 EC2-VPC 的区别

下表总结了在 EC2-Classic、默认 VPC 以及非默认 VPC 这三种平台中启动的实例之间的区别。

| 性能 | EC2-Classic | 默认 VPC | 非默认 VPC |
|--------------------------------------|--|--|--|
| 公有 IPv4 地址 (来自 Amazon 的公有 IP 地址池) | 您的实例会收到一个公有 IPv4 地址。 | 默认情况下，在默认子网中启动的实例会收到公有 IPv4 地址，除非您在启动过程中另行指定，或者您修改子网的公有 IPv4 地址属性。 | 默认情况下，您的实例不会收到公有 IPv4 地址，除非您在启动过程中另行指定，或者您修改子网的公有 IPv4 地址属性。 |
| 私有 IPv4 地址 | 您的实例会在每次启动时收到一个处于 EC2-Classic 范围内的私有 IPv4 地址。 | 您的实例会收到一个处于默认 VPC 地址范围内的静态私有 IPv4 地址。 | 您的实例会收到一个处于 VPC 地址范围内的静态私有 IPv4 地址。 |
| 多个私有 IPv4 地址 | 我们会为您的实例选择一个私有 IP 地址；不支持多个 IP 地址。 | 您可以将多个私有 IPv4 地址分配给您的实例。 | 您可以将多个私有 IPv4 地址分配给您的实例。 |
| 弹性 IP 地址 (IPv4)。 | 当您停止实例时，弹性 IP 会取消与实例的关联。 | 当您停止实例时，弹性 IP 会保持与实例的关联。 | 当您停止实例时，弹性 IP 会保持与实例的关联。 |
| DNS 主机名 | DNS 主机名默认处于启用状态。 | DNS 主机名默认处于启用状态。 | DNS 主机名默认处于禁用状态。 |
| 安全组 | 安全组可以引用属于其他 AWS 账户的安全组。 您最多可以为每个区域创建 500 个安全组。 | 安全组只能引用您的 VPC 的安全组。 您最多可以为每个 VPC 创建 100 个安全组。 | 安全组只能引用您的 VPC 的安全组。 您最多可以为每个 VPC 创建 100 个安全组。 |
| 安全组关联 | 启动实例时，您可以为其分配无限数量的安全组。 您不能更改正在运行的实例的安全组。您可以修改已分配的安全组的规则，或使用新实例予以替换(从该实例中创建 AMI，通过此 AMI 启动带有您所需的安全组的新实例，取消任意弹性 IP 地址与原有实例的关联并将 | 您最多可以为一个实例分配 5 个安全组。 您可以在启动实例时和实例运行过程中为其分配安全组。 | 您最多可以为一个实例分配 5 个安全组。 您可以在启动实例时和实例运行过程中为其分配安全组。 |

| 性能 | EC2-Classic | 默认 VPC | 非默认 VPC |
|---------------|---|--|--|
| | 其与新实例关联起来，然后终止原有实例)。 | | |
| 安全组规则 | 您只能为入站流量添加规则。 您最多可以为一个安全组添加 100 条规则。 | 您可以为入站和出站流量添加规则。 您最多可以为一个安全组添加 50 条规则。 | 您可以为入站和出站流量添加规则。 您最多可以为一个安全组添加 50 条规则。 |
| 租期 | 您的实例在共享硬件上运行。 | 您可以在共享硬件或单租户硬件上运行您的实例。 | 您可以在共享硬件或单租户硬件上运行您的实例。 |
| 正在访问 Internet | 您的实例可以访问 Internet。您的实例会自动接收公有 IP 地址，并且可以直接通过 AWS 网络边界访问 Internet。 | 默认情况下，您的实例可以访问 Internet。您的实例默认会接收一个公有 IP 地址。一个 Internet 网关连接到您的默认 VPC，并且您的默认子网有一个到 Internet 网关的路由。 | 默认情况下，您的实例不能访问 Internet。您的实例默认不会接收公有 IP 地址。您的 VPC 可能有一个 Internet 网关，具体取决于它的创建方式。 |
| IPv6 寻址 | 不支持 IPv6 寻址。您无法将 IPv6 地址分配给您的实例。 | 您可以选择将一个 IPv6 CIDR 块与 VPC 关联，并将 IPv6 地址分配给 VPC 中的实例。 | 您可以选择将一个 IPv6 CIDR 块与 VPC 关联，并将 IPv6 地址分配给 VPC 中的实例。 |

下图展示了每个平台中的实例。请注意以下几点：

- 实例 1、2、3、和 4 在 EC2-Classic 平台中。1 和 2 由一个账户启动，4 和 3 由不同的账户启动。这些实例可相互通信，并且可以直接访问 Internet。
- 实例 5 和 6 在 EC2-VPC 平台同一 VPC 内的不同子网中。它们的启动账户拥有 VPC；其他账户无法在此 VPC 内启动实例。这些实例可相互通信并且可访问 EC2-Classic 中的实例以及通过 Internet 网关访问 Internet。

在 EC2-Classic 与 EC2-VPC 之间共享和访问资源

AWS 账户中的一些资源和功能可以在 EC2-Classic 与 EC2-VPC 平台之间共享或访问（例如，通过 ClassicLink）。有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 436\)](#)。

如果您的账户支持 EC2-Classic，您可能已经设置在 EC2-Classic 中使用的资源。如果您要从 EC2-Classic 迁移到 VPC，则必须在 VPC 中重新创建这些资源。有关从 EC2-Classic 迁移到 VPC 的更多信息，请参阅[从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 \(p. 445\)](#)。

以下资源可在 EC2-Classic 与 VPC 之间共享或访问。

| 资源 | 备注 |
|------------------|--|
| AMI | |
| 捆绑任务 | |
| EBS 卷 | |
| 弹性 IP 地址 (IPv4)。 | 您可将弹性 IP 地址从 EC2-Classic 迁移至 EC2-VPC。您无法将本来分配为在 VPC 中使用的弹性 |

| 资源 | 备注 |
|-------------------|--|
| | IP 地址迁移至 EC2-Classic。有关更多信息，请参阅 将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 469) 。 |
| 实例 | EC2-Classic 实例可以使用公有 IPv4 地址与 VPC 中的实例进行通信，或者您可以使用 ClassicLink 通过私有 IPv4 地址实现通信。 您不能将实例从 EC2-Classic 迁移到 VPC。不过，您可以将应用程序从 EC2-Classic 中的实例迁移到 VPC 中的实例。有关更多信息，请参阅 从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 (p. 445) 。 |
| 密钥对 | |
| 负载均衡器 | 如果您使用了 ClassicLink，则可以将一个链接的 EC2-Classic 实例注册到某个 VPC 中的负载均衡器，前提是该 VPC 具有与实例位于同一可用区的子网。 您不能将负载均衡器从 EC2-Classic 迁移到 VPC。您不能将 VPC 中的实例注册到 EC2-Classic 中的负载均衡器注册。 |
| 置放群组 | |
| Reserved Instance | 可以将预留实例的网络平台从 EC2-Classic 更改为 EC2-VPC。有关详细信息，请参阅 修改您的标准预留实例 (p. 178) 。 |
| 安全组 | 链接的 EC2-Classic 实例可通过 ClassicLink 使用 VPC 安全组以控制进出 VPC 的流量。VPC 实例不能使用 EC2-Classic 安全组。 您不能将安全组从 EC2-Classic 迁移到 VPC。您可以将规则从 EC2-Classic 中的安全组复制到 VPC 中的安全组。有关更多信息，请参阅 正在创建安全组 (p. 358) 。 |
| 快照 | |

以下资源不能在 EC2-Classic 与 VPC 之间共享或移动：

- 竞价型实例

实例类型仅在 VPC 中可用

EC2-Classic 中不支持以下实例类型的实例，它们必须在 VPC 中启动：

- C4
- I3
- M4
- P2

- R4
- T2
- X 1

如果您的账户支持 EC2-Classic，但您尚未创建非默认 VPC，您可以执行以下操作之一来启动仅 VPC 实例：

- 在请求中指定子网 ID 或网络接口 ID，以便创建非默认 VPC 并将您的仅 VPC 实例启动至该 VPC。请注意，如果您没有默认 VPC 并且使用 AWS CLI、Amazon EC2 API 或 AWS 开发工具包来启动仅限 VPC 的实例，则必须创建非默认 VPC。有关更多信息，请参阅 [创建 Virtual Private Cloud \(VPC\) \(p. 18\)](#)。
- 使用 Amazon EC2 控制台启动仅 VPC 实例。Amazon EC2 控制台在您的账户中创建非默认 VPC 并将实例启动至第一个可用区中的子网。控制台将创建具有以下属性的 VPC：
 - 每个可用区中有一个子网，其公有 IPv4 地址属性设置为 `true`，因此实例会收到一个公有 IPv4 地址。有关更多信息，请参阅 [Amazon VPC 用户指南 中的您的 VPC 中的 IP 地址](#)。
 - 一个 Internet 网关，以及一个将 VPC 中的流量路由到该 Internet 网关的主路由表。这使您在 VPC 中启动的实例可以在 Internet 上通信。有关更多信息，请参阅 [Amazon VPC 用户指南 中的 Internet 网关](#)。
 - VPC 的默认安全组和与每个子网关联的默认网络 ACL。有关更多信息，请参阅 [Amazon VPC 用户指南 中的您的 VPC 中的安全性](#)。

如果您在 EC2-Classic 中有其他资源，则可以采取措施将它们迁移到 EC2-VPC。有关更多信息，请参阅 [从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 \(p. 445\)](#)。

Amazon VPC 文档

有关 Amazon VPC 的更多信息，请参阅以下文档。

| 指南 | 说明 |
|------------------------------------|----------------------------|
| Amazon VPC 入门指南 | 提供关于 Amazon VPC 的实践经验介绍。 |
| Amazon VPC 用户指南 | 提供有关如何使用 Amazon VPC 的详细信息。 |
| Amazon VPC 网络管理员指南 | 帮助网络管理员配置您的客户网关。 |

支持的平台

Amazon EC2 支持以下平台。根据各区域的情况，您的 AWS 账户可以在两个平台或只能在 EC2-VPC 中启动。

| 平台 | 引入版本 | 说明 |
|-------------|------------------|---|
| EC2-Classic | Amazon EC2 的初始版本 | 您的实例会在一个可与其他客户共享的扁平化网络中运行。 |
| EC2-VPC | Amazon VPC 的初始版本 | 您的实例会在一个“逻辑上”与 AWS 账户分离的 Virtual Private Cloud (VPC) 中运行。 |

有关您的账户中任何一个平台的可用性的详细信息，请参阅 [Amazon VPC 用户指南 中的 可用性](#)。有关 EC2-Classic 和 EC2-VPC 之间区别的更多信息，请参阅 [EC2-Classic 与 EC2-VPC 的区别 \(p. 432\)](#)。

在 Amazon EC2 控制台中的所支持的平台

Amazon EC2 控制台会显示在所选区域中您可以启动实例的平台，以及在该区域您是否拥有默认 VPC。

检查您要使用的区域已在导航栏中选定。在 Amazon EC2 控制台控制面板上，从 Account Attributes (账户属性) 下找到 Supported Platforms (支持的平台)。如果有两个值 EC2 和 VPC，您可以将实例启动到两个中的任何一个平台中。如果有一个值 VPC，您只能将实例启动到 EC2-VPC 中。

如果您只能将实例启动为 EC2-VPC，我们会为您创建一个默认 VPC。之后，当您启动实例时，我们会将其启动为默认 VPC，除非您创建了非默认 VPC 并在启动实例时对其进行指定。

EC2-VPC

控制面板在 Account Attributes (账户属性) 下方显示以下内容，表示该账户仅支持 EC2-VPC 平台，且具有一个标识符为 `vpc-1a2b3c4d` 的默认 VPC。

如果您的账户仅支持 EC2-VPC，则可以在使用启动向导启动实例时，从 Network (网络) 列表中选择 VPC，从 Subnet (子网) 列表中选择子网。

EC2-Classic、EC2-VPC

控制面板在 Account Attributes (账户属性) 下显示以下内容，表示该账户同时支持 EC2-Classic 和 EC2-VPC 平台。

如果您的账户支持 EC2-Classic 和 EC2-VPC，通过从 Network (网络) 列表中选择 Launch into EC2-Classic (在 EC2-Classic 中启动)，可以使用启动向导在 EC2-Classic 中启动。要启动到 VPC，您可以选择从 Network (网络) 列表中选择 VPC，并从 Subnet (子网) 列表中选择子网。

相关主题

有关如何区分您可以将实例启动到哪个平台的更多信息，请参阅 Amazon VPC 用户指南中[检测支持的平台](#)。

ClassicLink

ClassicLink 允许将您的 EC2-Classic 实例链接到您账户中位于同一区域内的 VPC。这样，您可以将 VPC 安全组与 EC2-Classic 实例关联，以便允许 EC2-Classic 实例与 VPC 中的实例使用私有 IPv4 地址进行通信。通过 ClassicLink，无需使用公有 IPv4 地址或弹性 IP 地址即可在这些平台中的实例之间进行通信。有关私有和公有 IPv4 地址的更多信息，请参阅[您的 VPC 中的 IP 地址](#)。

ClassicLink 可用于账户支持 EC2-Classic 平台的所有用户，并且可以与任何 EC2-Classic 实例一起使用。要查明您的账户支持的平台，请参阅[支持的平台 \(p. 435\)](#)。有关使用 VPC 的好处的更多信息，请参阅[Amazon EC2 和 Amazon Virtual Private Cloud \(p. 431\)](#)。有关将资源迁移到 VPC 的更多信息，请参阅[从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 \(p. 445\)](#)。

使用 ClassicLink 不收取任何额外费用。采用标准的数据传输和实例使用小时数计费方式。

Note

无法为 IPv6 通信启用 EC2-Classic 实例。您可以将 IPv6 CIDR 块与 VPC 关联，然后将 IPv6 地址分配给 VPC 中的资源，但是，VPC 中的 ClassicLinked 实例和资源之间仅通过 IPv4 进行通信。

主题

- [ClassicLink 基本知识 \(p. 437\)](#)
- [ClassicLink 限制 \(p. 439\)](#)
- [使用 ClassicLink \(p. 439\)](#)
- [API 和 CLI 概述 \(p. 442\)](#)

- [示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 \(p. 444\)](#)

ClassicLink 基本知识

使用 ClassicLink 将 EC2-Classic 实例链接到 VPC 分两步进行。首先，您必须为 VPC 启用 ClassicLink。默认情况下，您账户中的所有 VPC 都未启用 ClassicLink，目的是保持其隔离状态。为 VPC 启用 ClassicLink 之后，您可以将账户中位于同一区域的任何运行的 EC2-Classic 实例链接到该 VPC。链接实例的过程中，要从将与您的 EC2-Classic 实例关联的 VPC 中选择安全组。在您链接实例之后，只要 VPC 安全组允许，实例可以使用其私有 IP 地址与您的 VPC 中的实例通信。EC2-Classic 实例在链接到 VPC 时不会丢失其私有 IP 地址。

Note

将实例链接到 VPC 有时称为连接 实例。

链接的 EC2-Classic 实例可以与 VPC 中的实例通信，但它并不构成 VPC 的一部分。如果您列出自己的实例并按 VPC 筛选，例如，通过 `DescribeInstances` API 请求或使用 Amazon EC2 控制台中的 Instances 屏幕执行此操作，则结果不会返回任何链接到 VPC 的 EC2-Classic 实例。有关如何查看链接的 EC2-Classic 实例的更多信息，请参阅 [查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例 \(p. 441\)](#)。

默认情况下，如果您使用公有 DNS 主机名从链接的 EC2-Classic 实例对 VPC 中的实例进行定位，则该主机名会解析为该实例的公有 IP 地址。如果使用公有 DNS 主机名从 VPC 中的实例对一个链接的 EC2-Classic 实例进行定位，也是同样的情况。如果您希望公有 DNS 主机名解析为私有 IP 地址，可以对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅 [启用 ClassicLink DNS 支持 \(p. 441\)](#)。

如果您不再需要实例与 VPC 之间的 ClassicLink 连接，可以从 VPC 取消与 EC2-Classic 实例的链接。这将断开 VPC 安全组与 EC2-Classic 实例的连接。链接的 EC2-Classic 实例一旦停止，会自动取消与 VPC 的链接。从 VPC 取消链接的所有 EC2-Classic 实例的链接后，您可以为 VPC 禁用 ClassicLink。

使用启用 ClassicLink 的 VPC 中的其他 AWS 服务

链接的 EC2-Classic 实例可以访问 VPC 中的以下 AWS 服务：Amazon Redshift、Amazon ElastiCache、Elastic Load Balancing 和 Amazon RDS。但是，VPC 中的实例无法通过 ClassicLink 访问 EC2-Classic 平台预配置的 AWS 服务。

如果您在 VPC 中使用 Elastic Load Balancing，那么只要实例位于您的 VPC 具有子网的可用区内，便可以向负载均衡器注册您的链接的 EC2-Classic 实例。当您终止链接的 EC2-Classic 实例时，负载均衡器会取消注册该实例。有关在 VPC 中使用负载均衡器的更多信息，请参阅 Elastic Load Balancing 用户指南中的 [Amazon VPC 中的 Elastic Load Balancing](#)。

如果您使用 Auto Scaling，则可以创建一个 Auto Scaling 组，其中包含在启动时自动链接到启用了 ClassicLink 的指定 VPC 的实例。有关更多信息，请参阅 Auto Scaling 用户指南中的 [将 EC2-Classic 实例链接到 VPC](#)。

如果您在 VPC 中使用 Amazon RDS 实例或 Amazon Redshift 群集，并且它们可以公开访问（可通过 Internet 访问），则您用于从链接的 EC2-Classic 实例定位这些资源的终端节点会默认解析为公有 IP 地址。如果这些资源不可公开访问，则终端节点会解析为私有 IP 地址。要使用 ClassicLink 通过私有 IP 定位可公共访问的 RDS 实例或 Redshift 群集，您必须使用其私有 IP 地址或私有 DNS 主机名，或者必须对 VPC 启用 ClassicLink DNS 支持。

如果使用私有 DNS 主机名或私有 IP 地址对 RDS 实例寻址，则链接的 EC2-Classic 实例将无法使用多可用区部署可用的故障转移支持。

您可以使用 Amazon EC2 控制台查找 Amazon Redshift、Amazon ElastiCache 或 Amazon RDS 资源的私有 IP 地址。

查找您的 VPC 中的 AWS 资源的私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Network Interfaces。
3. 在 Description (描述) 列中查看网络接口的描述。Amazon Redshift、Amazon ElastiCache 或 Amazon RDS 所使用网络接口的描述中将包含服务名称。例如，连接到 Amazon RDS 实例的网络接口的描述如下：RDSNetworkInterface。
4. 选择所需的网络接口。
5. 在详细信息窗格中，从 Primary private IPv4 IP 字段中获取私有 IP 地址。

控制 ClassicLink 的使用

默认情况下，IAM 用户无权使用 ClassicLink。您可以创建 IAM 策略，授予用户以下权限：为 VPC 启用或禁用 ClassicLink，将实例链接到启用了 ClassicLink 的 VPC 或取消此链接，查看启用了 ClassicLink 的 VPC 和 EC2-Classic 实例。有关用于 Amazon EC2 的 IAM 策略的更多信息，请参阅 [Amazon EC2 的 IAM 策略 \(p. 368\)](#)。

有关使用 ClassicLink 的策略的更多信息，请参阅以下示例：[6. 使用 ClassicLink \(p. 410\)](#)。

ClassicLink 中的安全组

将 EC2-Classic 实例链接到 VPC 不会对您的 EC2-Classic 安全组造成影响。它们会继续控制实例的所有传入和传出流量。这不包括 VPC 中传入和传出实例的流量，这些流量由与 EC2-Classic 实例关联的 VPC 安全组控制。链接到同一 VPC 的 EC2-Classic 实例无论是否与同一 VPC 安全组关联，都不能通过该 VPC 相互通信。EC2-Classic 实例之间的通信由与这些实例关联的 EC2-Classic 安全组控制。有关安全组配置的示例，请参阅 [示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 \(p. 444\)](#)。

在您将实例链接到 VPC 之后，不可再更改与该实例关联的 VPC 安全组。要将不同安全组与您的实例关联，必须先取消实例链接，然后再将其链接到 VPC 并选择所需的安全组。

ClassicLink 路由

在您为 VPC 启用 ClassicLink 时，会向所有 VPC 路由表添加一个静态路由，其目的地为 10.0.0.0/8，目标为 local。这允许 VPC 中的实例与后来链接到该 VPC 的任意 EC2-Classic 实例之间进行通信。如果您向启用了 ClassicLink 的 VPC 添加自定义路由表，则会自动添加一个静态路由，其目的地为 10.0.0.0/8，目标为 local。在您为 VPC 禁用 ClassicLink 时，会从所有 VPC 路由表中自动删除此路由。

可以为处于 10.0.0.0/16 和 10.1.0.0/16 IP 地址范围内的 VPC 启用 ClassicLink，但仅当这些 VPC 的路由表中没有任何 10.0.0.0/8 IP 地址范围内的现有静态路由时才能如此，并且在创建 VPC 时自动添加的本地路由除外。同样，如果您已经为 VPC 启用了 ClassicLink，那么您不能在路由表中再添加 10.0.0.0/8 IP 地址范围内的任何其他特定路由。

Important

如果您的 VPC CIDR 块为公共可路由 IP 地址范围，则在您将 EC2-Classic 实例链接到 VPC 之前，应考虑安全方面的问题。例如，如果链接的 EC2-Classic 实例从处于 VPC IP 地址范围内的源 IP 地址收到传入的拒绝服务 (DoS) 请求洪流攻击，则响应流量将发送到您的 VPC。我们强烈建议您使用私有 IP 地址范围创建 VPC，具体说明见 [RFC 1918](#)。

有关 VPC 中的路由表和路由的更多信息，请参阅 Amazon VPC 用户指南 中的 [路由表](#)。

为 ClassicLink 启用 VPC 对等连接

如果您在两个 VPC 之间有 VPC 对等连接，而且存在一个或多个 EC2-Classic 实例（这些实例通过 ClassicLink 链接到这两个 VPC 中的一个或两个），则可以扩展 VPC 对等连接以启用 EC2-Classic 实例与 VPC 对等连接另一端的 VPC 中的实例之间的通信。这将使 EC2-Classic 实例和 VPC 中的实例能够使用私有 IP 地址进行通信。为此，您可允许本地 VPC 与对等 VPC 中链接的 EC2-Classic 实例通信，也可允许本地链接的 EC2-Classic 实例与对等 VPC 中的实例通信。

如果您允许本地 VPC 与对等 VPC 中的链接 EC2-Classic 实例通信，则将自动向您的路由表添加一个静态路由（目的地为 10.0.0.0/8，目标为 local）。

有关更多信息和示例，请参阅 Amazon VPC Peering Guide 中的使用 ClassicLink 进行配置。

ClassicLink 限制

要使用 ClassicLink 功能，您需要了解以下限制：

- EC2-Classic 实例一次只能链接到一个 VPC。
- 如果您停止链接的 EC2-Classic 实例，它会自动取消与 VPC 的链接，并且 VPC 安全组不再与实例关联。您可以在重新启动之后，再次将实例链接到 VPC。
- 不能将 EC2-Classic 实例链接到不同区域或不同 AWS 账户中的 VPC。
- 对于配置用于专用租赁的 VPC，无法启用 ClassicLink。您可以联系 AWS Support，申请允许为您的专用租期 VPC 启用 ClassicLink。

Important

EC2-Classic 实例运行在共享硬件上。如果您因法规或安全要求已将 VPC 租赁设置为 dedicated，那么将 EC2-Classic 实例链接到 VPC 可能并不符合这些要求，因为您可以利用共享的租赁资源，使用私有 IP 地址直接对隔离的资源进行寻址。如果您希望为专用 VPC 启用 ClassicLink，请在 AWS Support 请求中提供这么做的详细原因。

- 路由与 EC2-Classic 私有 IP 地址范围 10/8 冲突的 VPC 不能启用 ClassicLink。这不包括在路由表中已有本地路由的 10.0.0.0/16 和 10.1.0.0/16 IP 地址范围的 VPC。有关更多信息，请参阅 [ClassicLink 路由 \(p. 438\)](#)。
- 您不能将 VPC 弹性 IP 地址与链接的 EC2-Classic 实例关联。
- 您可以将运行的竞价型实例链接到 VPC。要在竞价型实例请求中指定实例应当在请求执行时链接到 VPC，您必须使用 Amazon EC2 控制台中的启动向导。
- ClassicLink 不支持 VPC 外的传递关系。链接的 EC2-Classic 实例不能访问与 VPC 关联的任何 VPN 连接、VPC 端点或 Internet 网关。同样，VPN 连接或 Internet 网关另一端的资源也不能访问链接的 EC2-Classic 实例。
- 您不能使用 ClassicLink 将一个 VPC 实例链接到另一个 VPC 或 EC2-Classic 资源。要在 VPC 之间建立私有连接，可以使用 VPC 对等连接。有关更多信息，请参阅 [Amazon VPC Peering Guide](#)。
- 如果您将 EC2-Classic 实例链接到 172.16.0.0/16 范围中的某个 VPC，并在该 VPC 中的 172.16.0.23/32 IP 地址上运行了一个 DNS 服务器，那么您所链接的 EC2-Classic 实例将无法访问 VPC DNS 服务器。要解决此问题，请在该 VPC 中的其他 IP 地址上运行您的 DNS 服务器。

使用 ClassicLink

您可以通过 Amazon EC2 和 Amazon VPC 控制台使用 ClassicLink 功能。您可以为 VPC 启用或禁用 ClassicLink，也可以将 EC2-Classic 实例链接到 VPC 或取消其链接。

Note

ClassicLink 功能仅显示在支持 EC2-Classic 的账户和区域的控制台中。

主题

- [为 VPC 启用 ClassicLink \(p. 440\)](#)
- [将实例链接到 VPC \(p. 440\)](#)
- [创建启用了 ClassicLink 的 VPC \(p. 440\)](#)
- [在启动时将 EC2-Classic 实例链接到 VPC \(p. 440\)](#)
- [查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例 \(p. 441\)](#)

- 启用 ClassicLink DNS 支持 (p. 441)
- 禁用 ClassicLink DNS 支持 (p. 442)
- 从 VPC 取消与 EC2-Classic 实例的链接 (p. 442)
- 对 VPC 禁用 ClassicLink (p. 442)

为 VPC 启用 ClassicLink

要将 EC2-Classic 实例链接到某个 VPC，您必须先为该 VPC 启用 ClassicLink。如果 VPC 的路由与 EC2-Classic 私有 IP 地址范围冲突，则不能为该 VPC 启用 ClassicLink。有关更多信息，请参阅 [ClassicLink 路由 \(p. 438\)](#)。

为 VPC 启用 ClassicLink

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择一个 VPC，然后选择 Actions、Enable ClassicLink。
4. 在确认对话框中，选择 Yes, Enable。

将实例链接到 VPC

为 ClassicLink 启用 VPC 后，您可以将 EC2-Classic 实例与其链接。

Note

您只能将正在运行的 EC2-Classic 实例链接到 VPC。您无法链接处于 stopped 状态的实例。

将实例链接到 VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择正在运行的 EC2-Classic 实例，然后选择 Actions、ClassicLink、Link to VPC。您可以选择多个实例，将其链接到同一 VPC。
4. 在显示的对话框中，从列表中选择一个 VPC。此处仅显示已启用 ClassicLink 的 VPC。
5. 选择要与您的实例关联的一个或多个 VPC 安全组。完成操作后，选择 Link to VPC。

创建启用了 ClassicLink 的 VPC

您可以使用 Amazon VPC 控制台中的 VPC 向导创建新 VPC 并立即为其启用 ClassicLink。

创建启用了 ClassicLink 的 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 从 Amazon VPC 控制面板上，选择 Start VPC Wizard。
3. 选择一个 VPC 配置选项并选择 Select。
4. 在向导的下一页上，对 Enable ClassicLink 选择 Yes。完成向导中的剩余步骤创建您的 VPC。有关使用 VPC 向导的更多信息，请参阅 Amazon VPC 用户指南 中的 [Amazon VPC 情景](#)。

在启动时将 EC2-Classic 实例链接到 VPC

您可以在 Amazon EC2 控制台中使用启动向导启动 EC2-Classic 实例，然后立即将其链接到启用了 ClassicLink 的 VPC。

在启动时将实例链接到 VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从 Amazon EC2 控制面板中，选择 Launch Instance。
3. 选择 AMI，然后选择实例类型。在 Configure Instance Details (配置实例详细信息) 页面上，确保从 Network (网络) 列表中选择 Launch into EC2-Classic (在 EC2-Classic 中启动)。

Note

某些实例类型 (如 T2 实例类型) 只能在 VPC 中启动。请确保您选择的实例类型可以在 EC2-Classic 中启动。

4. 在 Link to VPC (ClassicLink) 部分，从 Link to VPC 中选择一个 VPC。将只显示启用了 ClassicLink 的 VPC。从 VPC 中选择要与实例关联的安全组。完成页面上的其他配置选项，然后完成向导中的剩余步骤启动您的实例。有关如何使用启动向导的更多信息，请参阅[从 AMI 启动实例 \(p. 244\)](#)。

查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例

您可以在 Amazon VPC 控制台中查看启用了 ClassicLink 的所有 VPC，在 Amazon EC2 控制台中查看链接的 EC2-Classic 实例。

查看启用了 ClassicLink 的 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择一个 VPC，然后在 Summary (摘要) 选项卡中找到 ClassicLink 字段。值 Enabled (已启用) 表示已为 VPC 启用了 ClassicLink。
4. 或者，也可以找到 ClassicLink 列，查看为每个 VPC 显示的值 (Enabled (已启用) 或 Disabled (已禁用))。如果看不到此列，请选择 Edit Table Columns (齿轮状图标)，选择 ClassicLink 属性，然后选择 Close。

查看您链接的 EC2-Classic 实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择一个 EC2-Classic 实例，然后在 Description (描述) 选项卡中找到 ClassicLink 字段。如果实例链接到某个 VPC，该字段会显示实例所链接到的 VPC 的 ID。如果实例未链接到任何 VPC，该字段会显示 Unlinked (未链接)。
4. 或者，您可以筛选实例，以便只显示特定 VPC 或安全组的链接的 EC2-Classic 实例。在搜索栏中，开始键入 ClassicLink，选择相关的 ClassicLink 资源属性，然后选择安全组 ID 或 VPC ID。

启用 ClassicLink DNS 支持

您可以对您的 VPC 启用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例和 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。要使此功能起作用，必须对您的 VPC 启用 DNS 主机名和 DNS 解析。

Note

如果您对 VPC 启用 ClassicLink DNS 支持，您关联的 EC2 经典版实例可以访问与 VPC 相关的所有私有托管区域。有关更多信息，请参阅Amazon Route 53 开发人员指南中的[私有托管区域的使用](#)。

启用 ClassicLink DNS 支持

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions、Edit ClassicLink DNS Support。
4. 选择 Yes 启用 ClassicLink DNS 支持，然后选择 Save。

禁用 ClassicLink DNS 支持

您可以对您的 VPC 禁用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例和 VPC 中的实例之间的 DNS 主机名解析为公有 IP 地址而不是私有 IP 地址。

禁用 ClassicLink DNS 支持

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions、Edit ClassicLink DNS Support。
4. 选择 No 禁用 ClassicLink DNS 支持，然后选择 Save。

从 VPC 取消与 EC2-Classic 实例的链接

如果您不再需要 EC2-Classic 实例与 VPC 之间的 ClassicLink 连接，可以从 VPC 取消与该实例的链接。取消实例链接会从实例解除与 VPC 安全组的关联。

Note

停止的实例会从 VPC 自动取消链接。

从 VPC 取消链接一个实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 在 Actions 列表中，选择 ClassicLink，然后选择 Unlink Instance。您可以选择多个实例，将其从同一 VPC 取消链接。
4. 在确认对话框中选择 Yes。

对 VPC 禁用 ClassicLink

如果您不再需要 EC2-Classic 实例与 VPC 之间的连接，可以禁用 VPC 的 ClassicLink。您必须先取消链接到 VPC 的所有链接的 EC2-Classic 实例的链接。

为 VPC 禁用 ClassicLink

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions、Disable ClassicLink。
4. 在确认对话框中，选择 Yes, Disable。

API 和 CLI 概述

您可以使用命令行或查询 API 执行此页面上所述的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

为 VPC 启用 ClassicLink

- [enable-vpc-classic-link](#) (AWS CLI)
- [Enable-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [EnableVpcClassicLink](#) (Amazon EC2 查询 API)

将 EC2-Classic 实例链接 (连接) 到 VPC

- [attach-classic-link-vpc](#) (AWS CLI)
- [Add-EC2ClassicLinkVpc](#) (适用于 Windows PowerShell 的 AWS 工具)
- [AttachClassicLinkVpc](#) (Amazon EC2 查询 API)

从 VPC 取消链接 (断开) EC2-Classic 实例

- [detach-classic-link-vpc](#) (AWS CLI)
- [Dismount-EC2ClassicLinkVpc](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DetachClassicLinkVpc](#) (Amazon EC2 查询 API)

为 VPC 禁用 ClassicLink

- [disable-vpc-classic-link](#) (AWS CLI)
- [Disable-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DisableVpcClassicLink](#) (Amazon EC2 查询 API)

描述 VPC 的 ClassicLink 状态

- [describe-vpc-classic-link](#) (AWS CLI)
- [Get-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcClassicLink](#) (Amazon EC2 查询 API)

阐述链接的 EC2-Classic 实例

- [describe-classic-link-instances](#) (AWS CLI)
- [Get-EC2ClassicLinkInstance](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeClassicLinkInstances](#) (Amazon EC2 查询 API)

为 ClassicLink 启用 VPC 对等连接

- [modify-vpc-peering-connection-options](#) (AWS CLI)
- [Edit-EC2VpcPeeringConnectionOption](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ModifyVpcPeeringConnectionOptions](#) (Amazon EC2 查询 API)

对 VPC 启用 ClassicLink DNS 支持

- [enable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Enable-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [EnableVpcClassicLinkDnsSupport](#) (Amazon EC2 查询 API)

对 VPC 禁用 ClassicLink DNS 支持

- [disable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Disable-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DisableVpcClassicLinkDnsSupport](#) (Amazon EC2 查询 API)

VPC 的 ClassicLink DNS 支持说明

- [describe-vpc-classic-link-dns-support](#) (AWS CLI)
- [Get-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcClassicLinkDnsSupport](#) (Amazon EC2 查询 API)

示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置

在此示例中，您有具有以下三个实例的应用程序：面向公众的 Web 服务器、应用程序服务器和数据库服务器。您的 Web 服务器接收来自 Internet 的 HTTPS 流量，然后通过 TCP 端口 6001 与应用程序服务器通信。然后，您的应用程序服务器通过 TCP 端口 6004 与数据库服务器通信。您正在进行将整个应用程序迁移到账户中的 VPC 的过程。已将您的应用程序服务器和数据库服务器迁移到 VPC。您的 Web 服务器仍在 EC2-Classic 中而且已通过 ClassicLink 链接到 VPC。

您需要一个安全组配置，该配置仅允许流量在这些实例间流动。您具有 4 个安全组：其中两个安全组用于 Web 服务器 (`sg-1a1a1a1a` 和 `sg-2b2b2b2b`)、一个安全组用于应用程序服务器 (`sg-3c3c3c3c`)，一个安全组用于数据库服务器 (`sg-4d4d4d4d`)。

下图显示了实例的架构及其安全组配置。

适用于 Web 服务器的安全组 (`sg-1a1a1a1a` 和 `sg-2b2b2b2b`)

您的一个安全组位于 EC2-Classic 中，另一个安全组位于 VPC 中。当通过 ClassicLink 将您的 Web 服务器实例链接到 VPC 时，是将 VPC 安全组与该实例关联。VPC 安全组使您能够控制从 Web 服务器到应用程序服务器的出站流量。

以下是适用于 EC2-Classic 安全组的安全组规则 (`sg-1a1a1a1a`)。

| 入站 | | | |
|-----------|-------|------|-----------------------------|
| 源 | Type | 端口范围 | 注释 |
| 0.0.0.0/0 | HTTPS | 443 | 允许 Internet 流量到达您的 Web 服务器。 |

以下是适用于 VPC 安全组的安全组规则 (`sg-2b2b2b2b`)。

| 出站 | | | |
|--------------------------|------|------|--|
| 目的地 | Type | 端口范围 | 注释 |
| <code>sg-3c3c3c3c</code> | TCP | 6001 | 在您的 VPC 中允许从 Web 服务器到应用程序服务器（或到与 <code>sg-3c3c3c3c</code> 关联的任何其他实例）的出站流量。 |

适用于您的应用程序服务器的安全组 (`sg-3c3c3c3c`)

以下是适用于与您的应用程序服务器关联的 VPC 安全组的安全组规则。

| 入站 | | | |
|-------------|------|------|--|
| 源 | Type | 端口范围 | 注释 |
| sg-2b2b2b2b | TCP | 6001 | 允许来自 Web 服务器 (或与 sg-2b2b2b2b 关联的任何其他实例) 的指定类型的流量到达应用程序服务器。 |
| 出站 | | | |
| 目的地 | Type | 端口范围 | 注释 |
| sg-4d4d4d4d | TCP | 6004 | 允许从应用程序服务器到数据库服务器 (或到与 sg-4d4d4d4d 关联的任何其他实例) 的出站流量。 |

适用于数据库服务器的安全组 (sg-4d4d4d4d)

以下是适用于与您的数据库服务器关联的 VPC 安全组的安全组规则。

| 入站 | | | |
|-------------|------|------|--|
| 源 | Type | 端口范围 | 注释 |
| sg-3c3c3c3c | TCP | 6004 | 允许来自应用程序服务器 (或与 sg-3c3c3c3c 关联的任何其他实例) 的指定类型的流量到达数据库服务器。 |

从 EC2-Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例

根据您创建账户的时间以及您使用的区域，您的 AWS 账户可能同时支持 EC2-Classic 和 EC2-VPC。有关更多信息以及要查明您账户支持的平台，请参阅 [支持的平台 \(p. 435\)](#)。有关使用 VPC 的好处以及 EC2-Classic 与 EC2-VPC 之间的差异的更多信息，请参阅 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 431\)](#)。

您在 AWS 账户中创建和使用资源。一些资源和功能 (如增强联网和特定实例类型) 只能在 VPC 中使用。一些资源可在 EC2-Classic 和 VPC 之间共享，另一些则不能。有关更多信息，请参阅 [在 EC2-Classic 与 EC2-VPC 之间共享和访问资源 \(p. 433\)](#)。

如果您的账户支持 EC2-Classic，您可能已经设置在 EC2-Classic 中使用的资源。如果您要从 EC2-Classic 迁移到 VPC，则必须在 VPC 中重新创建这些资源。

有两种方式可迁移到 VPC。您可以执行完整迁移，也可以随时间推移执行增量迁移。您选择的方法取决于 EC2-Classic 中的应用程序的大小和复杂性。例如，如果您的应用程序仅由一两个运行静态网站的实例构成，并且您可以承受短时间的停机，那么您可以一次完成迁移。如果您的应用程序是包含不可中断进程的多层应用程序，则可以使用 ClassicLink 执行增量迁移。通过这种方式，您可以按每次一个组件的方式转移功能，直到应用程序完全在 VPC 中运行。

如果需要迁移 Windows 实例，请参阅 Amazon EC2 用户指南 (适用于 Windows 实例) 中的[将 Windows 实例从 EC2-Classic 迁移至 VPC](#)。

内容

- [完整迁移到 VPC \(p. 446\)](#)
- [使用 ClassicLink 增量迁移到 VPC \(p. 450\)](#)

完整迁移到 VPC

完成以下任务可将应用程序从 EC2-Classic 完整迁移到 VPC。

任务

- [步骤 1：创建 VPC \(p. 446\)](#)
- [步骤 2：配置安全组 \(p. 446\)](#)
- [步骤 3：从您的 EC2-Classic 实例创建 AMI \(p. 447\)](#)
- [步骤 4：在 VPC 中启动实例 \(p. 448\)](#)
- [示例：迁移简单的 Web 应用程序 \(p. 449\)](#)

步骤 1：创建 VPC

要开始使用 VPC，请确保您在账户中有 VPC。可以使用下列方法之一创建一个 VPC：

- 使用新的仅限 EC2-VPC 的 AWS 账户。仅限 EC2-VPC 的账户在每个区域中有一个默认 VPC，可供您使用。默认情况下，您启动的实例会在此 VPC 中启动，除非您另行指定。有关默认 VPC 的更多信息，请参阅[您的默认 VPC 和子网](#)。如果您不想自己设置 VPC，或是如果您的 VPC 配置无需特定要求，请使用此选项。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并使用 VPC 向导创建新 VPC。有关更多信息，请参阅[Amazon VPC 情景](#)。如果您要使用向导中的可用配置集之一在现有 EC2-Classic 账户中快速设置 VPC，请使用此选项。您将在每次启动实例时指定此 VPC。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并根据您的要求设置 VPC 的组件。有关更多信息，请参阅[您的 VPC 和子网](#)。如果您对 VPC 有特定要求（如特定数量的子网），请使用此选项。您将在每次启动实例时指定此 VPC。

步骤 2：配置安全组

您不能在 EC2-Classic 与 VPC 之间使用相同的安全组。但是，如果您希望 VPC 中的实例具有与 EC2-Classic 实例相同的安全组规则，则可以使用 Amazon EC2 控制台将现有 EC2-Classic 安全组规则复制到新的 VPC 安全组。

Important

您只能将安全组规则复制到相同区域内相同 AWS 账户中的新安全组。如果您创建了新 AWS 账户，则无法使用此方法将现有安全组规则复制到新账户。您必须创建新安全组，然后自己添加规则。有关创建新安全组的更多信息，请参阅[Linux 实例的 Amazon EC2 个安全组 \(p. 354\)](#)。

将您的安全组规则复制到新安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择与您的 EC2-Classic 实例关联的安全组，再选择 Actions，然后选择 Copy to new。
4. 在 Create Security Group (创建安全组) 对话框中，为您的新安全组指定名称和说明。从 VPC 列表中选择您的 VPC。
5. Inbound (入站) 选项卡会使用您 EC2-Classic 安全组中的规则进行填充。您可以根据需要修改这些规则。在 Outbound (出站) 选项卡中，已自动为您创建允许所有出站流量的规则。有关修改安全组规则的更多信息，请参阅[Linux 实例的 Amazon EC2 个安全组 \(p. 354\)](#)。

Note

如果您在 EC2-Classic 安全组中定义了引用其他安全组的规则，则您将无法在 VPC 安全组中使用相同规则。请将该规则修改为引用同一 VPC 中的安全组。

6. 选择 Create。

步骤 3：从您的 EC2-Classic 实例创建 AMI

AMI 是用于启动实例的模板。您可以基于现有 EC2-Classic 实例创建自己的 AMI，然后使用该 AMI 在 VPC 中启动实例。

用于创建 AMI 的方法取决于您的实例的根设备类型，以及实例运行时所在的操作系统平台。要查明您实例的根设备类型，请转到 Instances 页面，选择您的实例，然后在 Description (说明) 选项卡上的 Root device type 字段中查看信息。如果值为 ebs，则说明您的实例是由 EBS 提供支持。如果值为 instance-store，则说明您的实例是由实例存储提供支持。您还可以使用 [describe-instances](#) AWS CLI 命令查明根设备类型。

下表为您提供用于基于实例的根设备类型和软件平台创建 AMI 的选项。

Important

一些实例类型同时支持半虚拟化 (PV) 和硬件虚拟机 (HVM) 虚拟化，而其他实例类型只支持其中之一。如果您计划使用 AMI 启动与当前实例类型不同的实例类型，请检查该实例类型是否支持 AMI 提供的虚拟化类型。如果 AMI 支持半虚拟化，而您要使用支持硬件虚拟机虚拟化的实例类型，则您可能必须在基础硬件虚拟机 AMI 上重新安装软件。有关半虚拟化和硬件虚拟机虚拟化的更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。

| 实例根设备类型 | 操作 |
|---------|---|
| EBS | 从实例创建由 EBS 支持的 AMI。有关更多信息，请参阅 创建 Amazon EBS 支持的 Linux AMI (p. 75) 。 |
| 实例存储 | 使用 AMI 工具从实例创建由实例存储支持的 AMI。有关更多信息，请参阅 创建由实例存储支持的 Linux AMI (p. 78) 。 |
| 实例存储 | 将您的实例数据传输到 EBS 卷，然后拍摄该卷的快照并从该快照创建 AMI。有关更多信息，请参阅 将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI (p. 113) 。 Note 此方法将由实例存储支持的实例转换为由 EBS 支持的实例。 |

(可选) 在 Amazon EBS 卷上存储您的数据

您可以创建 Amazon EBS 卷并使用它备份和存储实例中的数据（如同使用物理硬盘驱动器一样）。Amazon EBS 卷可以与同一可用区中的任何实例连接和断开。您可以断开卷与 EC2-Classic 中实例的连接，并将它连接到在同一可用区内的 VPC 中启动的新实例。

有关 Amazon EBS 卷的更多信息，请参阅以下主题：

- [Amazon EBS 卷 \(p. 517\)](#)
- [创建 Amazon EBS 卷 \(p. 527\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)

要备份 Amazon EBS 卷上的数据，可以拍摄卷的定期快照。如果您需要，可以从快照还原 Amazon EBS 卷。有关 Amazon EBS 快照的更多信息，请参阅以下主题：

- [Amazon EBS 快照 \(p. 559\)](#)
- [创建 Amazon EBS 快照 \(p. 559\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 529\)](#)

步骤 4：在 VPC 中启动实例

创建了 AMI 之后，您可以在 VPC 中启动实例。实例将具有与现有 EC2-Classic 实例相同的数据和配置。

您可以在已在现有账户中创建的 VPC 中，或是仅限 VPC 的新 AWS 账户中启动实例。

使用现有 EC2-Classic 账户

您可以使用 Amazon EC2 启动向导在 VPC 中启动实例。

在 VPC 中启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (选择一个Amazon 系统映像) 页面上，选择 My AMIs (我的 AMI) 类别，然后选择您创建的 AMI。
4. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择您的 VPC。从 Subnet (子网) 列表中选择所需子网。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
6. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。
7. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 244\)](#)。

使用仅限 VPC 的新账户

要在新 AWS 账户中启动实例，您必须先将创建的 AMI 与新账户共享。随后您可以使用 Amazon EC2 启动向导在默认 VPC 中启动实例。

将 AMI 与新 AWS 账户共享

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 切换到用于创建 AMI 的账户。
3. 在导航窗格中，选择 AMIs。
4. 在 Filter (筛选条件) 列表中，请确保选择了 Owned by me (我拥有的)，然后选择您的 AMI。
5. 在 Permissions 选项卡中，选择 Edit。输入您的新 AWS 账户的账号，选择 Add Permission，然后选择 Save。

在您的默认 VPC 内启动 实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 切换到您的新 AWS 账户。
3. 在导航窗格中，选择 AMIs。
4. 在 Filter (筛选条件) 列表中，选择 Private images (私有映像)。选择您从 EC2-Classic 账户共享的 AMI，然后选择 Launch。
5. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
6. 在 Configure Instance Details (配置实例详细信息) 页面上，应在 Network (网络) 中选择默认 VPC。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
7. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。

8. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 244\)](#)。

示例：迁移简单的 Web 应用程序

在此示例中，您使用 AWS 托管您的园艺网站。为了管理您的网站，您在 EC2-Classic 中有三个正在运行的实例。实例 A 和 B 托管面向公众的 Web 应用程序，您使用 Elastic Load Balancer 对这些实例之间的流量进行负载均衡。您向实例 A 和 B 分配了弹性 IP 地址，从而可将静态 IP 地址用于这些实例上的配置和管理任务。实例 C 存储您网站的 MySQL 数据库。您注册了域名 `www.garden.example.com`，并且使用 Amazon Route 53 创建了一个托管区域，该区域具有与负载均衡器的 DNS 名称关联的别名记录集。

第一部分往 VPC 的迁移决定了适合您需要的 VPC 架构类型。在此情况中，您做出了以下决定：将一个公有子网用于您的 Web 服务器，而将一个私有子网用于您的数据库服务器。随着您网站的发展，您可以向子网添加更多 Web 服务器和数据库服务器。默认情况下，私有子网中的实例无法访问 Internet；但是，您可以通过公有子网中的网络地址转换 (NAT) 设备启用 Internet 访问。您可能需要设置 NAT 设备，以通过 Internet 为数据库服务器提供定期更新和补丁。您将您的弹性 IP 地址迁移到 EC2-VPC，并在公有子网中创建 Elastic Load Balancer 来对 Web 服务器之间的流量进行负载均衡。

要将您的 Web 应用程序迁移到 VPC，您可以执行以下步骤：

- **创建 VPC**：在本例中，您可以使用 Amazon VPC 控制台中的 VPC 向导创建您的 VPC 和子网。第二个向导配置创建具有一个私有子网和一个公有子网的 VPC，并在公有子网中为您启动和配置一个 NAT 设备。有关更多信息，请参阅 Amazon VPC 用户指南 中的[场景 2：带有公有子网和私有子网的 VPC](#)。
- **从您的实例创建 AMI**：从您的一个 Web 服务器创建一个 AMI，并从数据库服务器创建第二个 AMI。有关更多信息，请参阅[步骤 3：从您的 EC2-Classic 实例创建 AMI \(p. 447\)](#)。
- **配置您的安全组**：在 EC2-Classic 环境中，您将一个安全组用于 Web 服务器，并将另一个安全组用于数据库服务器。您可以使用 Amazon EC2 控制台将规则从每个安全组复制到用于您 VPC 的新安全组中。有关更多信息，请参阅[步骤 2：配置安全组 \(p. 446\)](#)。

Tip

首先创建由其他安全组引用的安全组。

- **在新 VPC 中启动实例**：在公有子网中启动替换 Web 服务器，并在私有子网中启动替换数据库服务器。有关更多信息，请参阅[步骤 4：在 VPC 中启动实例 \(p. 448\)](#)。
- **配置您的 NAT 设备**：如果您使用的是 NAT 实例，则必须为其创建安全组，以便允许来自您的私有子网的 HTTP 和 HTTPS 流量。有关更多信息，请参阅[NAT 实例](#)。如果您使用的是 NAT 网关，则会自动允许来自您的私有子网的流量。
- **配置您的数据库**：在 EC2-Classic 中从数据库服务器创建 AMI 时，该实例中存储的所有配置信息都已复制到 AMI。您可能必须连接到新数据库服务器并更新配置详细信息；例如，如果您将数据库配置为向 EC2-Classic 中的 Web 服务器授予完全读取、写入和修改权限，则您必须更新配置文件以改为向新 VPC Web 服务器授予相同权限。
- **配置您的 Web 服务器**：您的 Web 服务器将具有与 EC2-Classic 中的实例相同的配置设置。例如，如果您将 Web 服务器配置为使用 EC2-Classic 中的数据库，请将您 Web 服务器的配置设置更新为指向您的新数据库实例。

Note

默认情况下，不会向在非默认子网中启动的实例分配公有 IP 地址，除非您在启动时另行指定。您的新数据库服务器可能没有公有 IP 地址。在这种情况下，您可以更新您 Web 服务器的配置文件以使用新数据库服务器的私有 DNS 名称。同一 VPC 中的实例通过私有 IP 地址互相通信。

- **迁移您的弹性 IP 地址**：在 EC2-Classic 中从您的 Web 服务器取消与弹性 IP 地址的关联，然后将这些地址迁移到 EC2-VPC。迁移这些地址后，您可在 VPC 中将其与您的新 Web 服务器关联。有关更多信息，请参阅[将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC \(p. 469\)](#)。

- **创建新负载均衡器**：要继续使用 Elastic Load Balancing 对发送到实例的流量进行负载均衡，请确保您了解 VPC 中负载均衡器的各种配置。有关更多信息，请参阅 [Amazon VPC 中的 Elastic Load Balancing](#)。
- **更新您的 DNS 记录**：在公有子网中设置了负载均衡器之后，请确保 www.garden.example.com 域指向您的新负载均衡器。为此，您需要更新您的 DNS 记录并更新 Amazon Route 53 中的别名记录集。有关使用 Amazon Route 53 的更多信息，请参阅 [Amazon Route 53 入门](#)。
- **关闭您的 EC2-Classic 资源**：验证了您的 Web 应用程序是否正在 VPC 架构内运行之后，可以关闭 EC2-Classic 资源以使它们停止产生费用。终止 EC2-Classic 实例，并释放 EC2-Classic 弹性 IP 地址。

使用 ClassicLink 增量迁移到 VPC

通过 ClassicLink 功能可以更容易地管理到 VPC 的增量迁移。借助 ClassicLink，您能够将 EC2-Classic 实例链接到您账户中同一区域的 VPC，以便您的新 VPC 资源可使用私有 IPv4 地址与 EC2-Classic 实例进行通信。您随后可以一步一步地将功能迁移到 VPC。本主题提供用于管理从 EC2-Classic 到 VPC 的增量迁移的一些基本步骤。

有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 436\)](#)。

主题

- [步骤 1：准备迁移序列 \(p. 450\)](#)
- [步骤 2：创建 VPC \(p. 450\)](#)
- [步骤 3：为 VPC 启用 ClassicLink \(p. 450\)](#)
- [步骤 4：从您的 EC2-Classic 实例创建 AMI \(p. 451\)](#)
- [步骤 5：在 VPC 中启动实例 \(p. 452\)](#)
- [步骤 6：将 EC2-Classic 实例链接到 VPC \(p. 452\)](#)
- [步骤 7：完成 VPC 迁移 \(p. 452\)](#)

步骤 1：准备迁移序列

要有效地使用 ClassicLink，您必须先确定必须迁移到 VPC 的应用程序组件，然后确认迁移功能的顺序。

例如，您的一个应用程序依赖于演示 Web 服务器、后端数据库服务器以及用于交易的身份验证逻辑。您可以决定从身份验证逻辑开始迁移过程，然后是数据库服务器，最后是 Web 服务器。

步骤 2：创建 VPC

要开始使用 VPC，请确保您在账户中有 VPC。可以使用下列方法之一创建一个 VPC：

- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并使用 VPC 向导创建新 VPC。有关更多信息，请参阅 [Amazon VPC 情景](#)。如果您要使用向导中的可用配置集之一在现有 EC2-Classic 账户中快速设置 VPC，请使用此选项。您将在每次启动实例时指定此 VPC。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并根据您的要求设置 VPC 的组件。有关更多信息，请参阅 [您的 VPC 和子网](#)。如果您对 VPC 有特定要求（如特定数量的子网），请使用此选项。您将在每次启动实例时指定此 VPC。

步骤 3：为 VPC 启用 ClassicLink

创建 VPC 之后，您可以为它启用 ClassicLink。有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 436\)](#)。

为 VPC 启用 ClassicLink

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后从 Actions 列表中选择 Enable ClassicLink。
4. 在确认对话框中，选择 Yes, Enable。

步骤 4：从您的 EC2-Classic 实例创建 AMI

AMI 是用于启动实例的模板。您可以基于现有 EC2-Classic 实例创建自己的 AMI，然后使用该 AMI 在 VPC 中启动实例。

用于创建 AMI 的方法取决于您的实例的根设备类型，以及实例运行时所在的操作系统平台。要查明您实例的根设备类型，请转到 Instances 页面，选择您的实例，然后在 Description (说明) 选项卡上的 Root device type 字段中查看信息。如果值为 ebs，则说明您的实例是由 EBS 提供支持。如果值为 instance-store，则说明您的实例是由实例存储提供支持。您还可以使用 `describe-instances` AWS CLI 命令查明根设备类型。

下表为您提供用于基于实例的根设备类型和软件平台创建 AMI 的选项。

Important

一些实例类型同时支持半虚拟化 (PV) 和硬件虚拟机 (HVM) 虚拟化，而其他实例类型只支持其中之一。如果您计划使用 AMI 启动与当前实例类型不同的实例类型，请检查该实例类型是否支持 AMI 提供的虚拟化类型。如果 AMI 支持半虚拟化，而您要使用支持硬件虚拟机虚拟化的实例类型，则您可能必须在基础硬件虚拟机 AMI 上重新安装软件。有关半虚拟化和硬件虚拟机虚拟化的更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。

| 实例根设备类型 | 操作 |
|---------|---|
| EBS | 从实例创建由 EBS 支持的 AMI。有关更多信息，请参阅 创建 Amazon EBS 支持的 Linux AMI (p. 75) 。 |
| 实例存储 | 使用 AMI 工具从实例创建由实例存储支持的 AMI。有关更多信息，请参阅 创建由实例存储支持的 Linux AMI (p. 78) 。 |
| 实例存储 | 将您的实例数据传输到 EBS 卷，然后拍摄该卷的快照并从该快照创建 AMI。有关更多信息，请参阅 将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI (p. 113) 。 Note 此方法将由实例存储支持的实例转换为由 EBS 支持的实例。 |

(可选) 在 Amazon EBS 卷上存储您的数据

您可以创建 Amazon EBS 卷并使用它备份和存储实例中的数据（如同使用物理硬盘驱动器一样）。Amazon EBS 卷可以与同一可用区中的任何实例连接和断开。您可以断开卷与 EC2-Classic 中实例的连接，并将它连接到在同一可用区内的 VPC 中启动的新实例。

有关 Amazon EBS 卷的更多信息，请参阅以下主题：

- [Amazon EBS 卷 \(p. 517\)](#)
- [创建 Amazon EBS 卷 \(p. 527\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)

要备份 Amazon EBS 卷上的数据，可以拍摄卷的定期快照。如果您需要，可以从快照还原 Amazon EBS 卷。有关 Amazon EBS 快照的更多信息，请参阅以下主题：

- [Amazon EBS 快照 \(p. 559\)](#)

- [创建 Amazon EBS 快照 \(p. 559\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 529\)](#)

步骤 5：在 VPC 中启动实例

迁移过程的下一步是在 VPC 中启动实例，以便开始向实例转移功能。您可以使用在前面步骤中创建的 AMI 在 VPC 中启动实例。这些实例将具有与现有 EC2-Classic 实例相同的数据和配置。

使用自定义 AMI 在 VPC 中启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (选择一个Amazon 系统映像) 页面上，选择 My AMIs (我的 AMI) 类别，然后选择您创建的 AMI。
4. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择您的 VPC。从 Subnet (子网) 列表中选择所需子网。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
6. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。
7. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 244\)](#)。

实例启动并进入 running 状态之后，可以连接并根据需要配置该实例。

步骤 6：将 EC2-Classic 实例链接到 VPC

配置实例并在 VPC 中提供您的应用程序的功能之后，可以使用 ClassicLink 在新 VPC 实例与您的 EC2-Classic 实例之间启用私有 IP 通信。

将实例链接到 VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您的 EC2-Classic 实例，然后依次选择 Actions、ClassicLink 和 Link to VPC。

Note

验证实例是否处于 running 状态。

4. 在对话框中，选择启用了 ClassicLink 的 VPC (仅显示启用了 ClassicLink 的 VPC)。
5. 选择要与您的实例关联的一个或多个 VPC 安全组。完成操作后，选择 Link to VPC。

步骤 7：完成 VPC 迁移

根据应用程序的大小和必须迁移的功能，重复步骤 4 到 6，直到将应用程序的所有组件都从 EC2-Classic 迁移到 VPC 中。

在 EC2-Classic 与 VPC 实例之间启用内部通信之后，您必须将应用程序更新为指向 VPC 中迁移的服务，而不是 EC2-Classic 平台中的服务。此操作的确切步骤取决于应用程序的设计。通常，这包括更新目标 IP 地址以指向 VPC 实例 (而不是 EC2-Classic 实例) 的 IP 地址。您可将您当前在 EC2-Classic 平台中使用的弹性 IP 地址迁移到 EC2-VPC 平台。有关更多信息，请参阅[将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC \(p. 469\)](#)。

完成此步骤并测试应用程序是否从 VPC 正常工作之后，您可以终止 EC2-Classic 实例并为 VPC 禁用 ClassicLink。您还可以清理所有可能不再需要的 EC2-Classic 资源以免它们产生费用。例如，您可以释放弹性 IP 地址，并删除之前与 EC2-Classic 实例关联的卷。

Amazon EC2 实例 IP 寻址

我们将为您的实例提供 IP 地址和 IPv4 DNS 主机名。这些会因实例的启动位置 (EC2-Classic 平台或 Virtual Private Cloud (VPC) 中) 而异。有关 EC2-Classic 和 EC2-VPC 平台的信息，请参阅[支持的平台 \(p. 435\)](#)。

Amazon EC2 和 Amazon VPC 支持 IPv4 和 IPv6 寻址协议。默认情况下，Amazon EC2 和 Amazon VPC 使用 IPv4 寻址协议；您无法禁用此行为。创建 VPC 时，您必须指定 IPv4 CIDR 块（一系列私有 IPv4 地址）。您可以选择将 IPv6 CIDR 块分配给您的 VPC 和子网，并将来自该块的 IPv6 地址分配给您子网中的实例。IPv6 地址可通过 Internet 访问。有关 IPv6 的更多信息，请参阅 Amazon VPC 用户指南中的[您的 VPC 中的 IP 地址](#)。

EC2-Classic 平台不支持 IPv6。

内容

- [私有 IPv4 地址和内部 DNS 主机名 \(p. 453\)](#)
- [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)
- [弹性 IP 地址 \(IPv4\) \(p. 455\)](#)
- [Amazon DNS 服务器 \(p. 455\)](#)
- [IPv6 地址 \(p. 455\)](#)
- [EC2-Classic 和 EC2-VPC 之间的 IP 地址区别 \(p. 455\)](#)
- [使用实例的 IP 地址 \(p. 456\)](#)
- [多个 IP 地址 \(p. 460\)](#)

私有 IPv4 地址和内部 DNS 主机名

私有 IPv4 地址是指无法通过 Internet 访问的 IP 地址。您可以使用私有 IPv4 地址在同一网络 (EC2-Classic 或 VPC) 中实现实例之间的通信。有关私有 IPv4 地址标准和规范的更多信息，请参阅[RFC 1918](#)。

Note

您可以创建一个具有公共可路由的 CIDR 块（不在 RFC 1918 中指定的私有 IPv4 地址范围内）的 VPC。但是，出于本文档的写作目的，我们的私有 IPv4 地址（或“私有 IP 地址”）指的是位于 VPC 的 IPv4 CIDR 范围内的 IP 地址。

当您启动实例时，我们会使用 DHCP 为实例分配私有 IPv4 地址。另外，还为每个实例指定了一个可解析为实例的私有 IPv4 地址的内部 DNS 主机名，例如，`ip-10-251-50-12.ec2.internal`。您可以使用内部 DNS 主机名在同一网络中实现实例之间的通信，但我们无法解析实例所在网络之外的 DNS 主机名。

在 VPC 中启动的实例将获得一个主要私有 IP 地址（在子网的 IPv4 地址范围内）。有关更多信息，请参阅 Amazon VPC 用户指南 中的[子网大小调整](#)。如果您在启动实例时未指定主要私有 IP 地址，我们会在子网的 IPv4 范围内为您选择一个可用的 IP 地址。VPC 中的每个实例都具有分配了主要私有 IPv4 地址的默认网络接口（`eth0`）。您还可以指定其他私有 IPv4 地址，即辅助私有 IPv4 地址。与主要私有 IP 地址不同的是，辅助私有 IP 地址可以从一个实例重新分配到另一个实例。有关更多信息，请参阅[多个 IP 地址 \(p. 460\)](#)。

对于在 EC2-Classic 中启动的实例，我们在实例停止或终止时释放私有 IPv4 地址。如果您重新启动已停止的实例，该实例会收到新的私有 IPv4 地址。

对于在 VPC 中启动的实例，私有 IPv4 地址会在实例停止并重新启动时保持与网络接口的关联，并在实例终止时释放。

如果您在 EC2-Classic 中创建自定义防火墙配置，那么必须在您的防火墙中创建规则，以允许来自 Amazon DNS 服务器地址的端口 53 (DNS) (目标端口在临时范围内) 的入站流量，否则，实例的内部 DNS 解析会失败。如果您的防火墙无法自动允许 DNS 查询响应，那么您就需要允许来自 Amazon DNS 服务器的 IP 地址的流量。要获取 Amazon DNS 服务器的 IP 地址，请在您的实例中使用以下命令：

- Linux

```
grep nameserver /etc/resolv.conf
```

公有 IPv4 地址和外部 DNS 主机名

公有 IP 地址是指可通过 Internet 访问的 IPv4 地址。您可以使用公用地址在您的实例和 Internet 之间进行通信。

同样，将为接收公有 IP 地址的每个实例指定一个外部 DNS 主机名，例如，`ec2-203-0-113-25.compute-1.amazonaws.com`。我们会将外部 DNS 主机名解析为实例所在网络外的实例的公有 IP 地址，以及实例所在网络内的实例的私有 IPv4 地址。公有 IP 地址通过网络地址转换 (NAT) 映射到主要私有 IP 地址。有关 NAT 的更多信息，请参阅 [RFC 1631: The IP Network Address Translator \(NAT\)](#) 部分。

当您在 EC2-Classic 中启动实例时，我们会自动从 EC2-Classic 公有 IPv4 地址池中为该实例分配一个公有 IP 地址。您不能修改此行为。当您在某个 VPC 中启动实例时，您子网的一个属性会确定在该子网中启动的实例是否从 EC2-VPC 公有 IPv4 地址池接收公有 IP 地址。默认情况下，我们会为在默认 VPC 中启动的实例分配公有 IP 地址，而不会为在非默认子网中启动的实例分配公有 IP 地址。

您可以通过执行以下操作，控制 VPC 中的实例是否接收公有 IP 地址：

- 修改子网的公有 IP 寻址属性。有关更多信息，请参阅 Amazon VPC 用户指南中的[修改子网的公有 IPv4 寻址属性](#)。
- 在启动过程中启用或禁用公有 IP 寻址功能，以覆盖子网的公有 IP 寻址属性。有关更多信息，请参阅[在实例启动期间分配公有 IPv4 地址 \(p. 458\)](#)。

公有 IP 地址将从 Amazon 的公有 IPv4 地址池分配给实例，不与您的 AWS 账户关联。在取消公有 IP 地址与实例的关联后，该地址即会释放回公有 IPv4 地址池中，并且您无法重新使用该地址。

您不能从实例手动关联或取消关联公有 IP 地址。在某些情况下，我们会从您的实例释放公有 IP 地址，或为其分配新的地址：

- 当您的实例已停止或终止后，我们释放它的公有 IP 地址。已停止的实例在重新启动时会接收新的公有 IP 地址。
- 如果您将弹性 IP 地址与实例相关联，或在 VPC 中将弹性 IP 地址与实例的主要网络接口 (`eth0`) 相关联，我们会释放实例的公有 IP 地址。当您从实例取消与弹性 IP 地址的关联时，实例会收到新的公有 IP 地址。
- 如果 VPC 中的实例的公有 IP 地址已释放，则在多个网络接口与实例相连的情况下，该实例不会接收新地址。

如果您需要可根据需要关联到实例并从实例进行关联的永久公有 IP 地址，可改为使用弹性 IP 地址。例如，如果您使用动态 DNS 来将现有 DNS 名称映射到新实例的公有 IP 地址，则可能需要 24 小时，以便 IP 地址通过 Internet 进行传播。其结果是，新的实例可能无法接收流量，而已终止实例继续接收请求。要解决此问题，请使用弹性 IP 地址。您可以分配自己的弹性 IP 地址，并将其与您的实例相关联。有关更多信息，请参阅[弹性 IP 地址 \(p. 467\)](#)。

如果您的实例在 VPC 中且分配有弹性 IP 地址，则在启用 DNS 主机名后，实例会收到一个 IPv4 DNS 主机名。有关更多信息，请参阅 Amazon VPC 用户指南中的[在您的 VPC 中使用 DNS](#)。

Note

通过公有 NAT IP 地址访问其他实例的实例需要支付区域或 Internet 数据传输费用，具体取决于这些实例是否处于同一区域。

弹性 IP 地址 (IPv4)

弹性 IP 地址是指可分配给您的账户的公有 IPv4 地址。您可以根据需要将其关联到实例并从实例进行关联，它分配给您的账户，直到您选择释放。有关弹性 IP 地址及其使用方法的更多信息，请参阅[弹性 IP 地址 \(p. 467\)](#)。

我们不支持对 IPv6 使用弹性 IP 地址。

Amazon DNS 服务器

Amazon 提供了 DNS 服务器，可将 Amazon 提供的 IPv4 DNS 主机名解析为 IPv4 地址。在 EC2-Classic 中，此 Amazon DNS 服务器位于 172.16.0.23。在 EC2-VPC 中，Amazon DNS 服务器位于 VPC 网络范围起始地址 + 2 的位置。有关更多信息，请参阅 Amazon VPC 用户指南中的[Amazon DNS 服务器](#)。

IPv6 地址

您可以选择将 IPv6 CIDR 块与 VPC 关联，并将 IPv6 CIDR 块与子网关联。我们将自动从 Amazon 的 IPv6 地址池中为您的 VPC 分配 IPv6 CIDR 块，因此您无法自行选择范围。有关更多信息，请参阅 Amazon VPC 用户指南中的以下主题：

- 针对 IPv6 的 VPC 和子网大小调整
- 将 IPv6 CIDR 块与 VPC 关联
- 将 IPv6 CIDR 块与子网关联

IPv6 地址具有全局唯一性，因此可通过 Internet 访问。如果您的 VPC 和子网关联了 IPv6 CIDR 块，并且满足以下条件之一，则 VPC 中的实例会收到 IPv6 地址：

- 您的子网配置为在启动期间向实例自动分配 IPv6 地址。有关更多信息，请参阅[修改子网的 IPv6 寻址属性](#)。
- 您在启动期间为实例分配了 IPv6 地址。
- 您在启动后为实例的主网络接口分配了 IPv6 地址。
- 您在启动后为同一子网中的某个网络接口分配了 IPv6 地址，并将此网络接口附加到您的实例。

当实例在启动期间收到 IPv6 地址时，此地址将与实例的主网络接口 (eth0) 关联。您可以取消 IPv6 地址与该网络接口的关联。我们不支持为您的实例使用 IPv6 DNS 主机名。

IPv6 地址会在您停止和启动实例时保留下来，并在您终止实例时释放出来。您无法重新分配已分配给某个网络接口的 IPv6 地址；您必须先取消分配此 IPv6 地址。

通过将 IPv6 地址分配给附加到实例的网络接口，您可以为实例分配更多的 IPv6 地址。可以分配给网络接口的 IPv6 地址数量以及可以附加到实例的网络接口数量因实例类型而异。有关更多信息，请参阅[每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。

EC2-Classic 和 EC2-VPC 之间的 IP 地址区别

下表总结了在 EC2-Classic、默认子网和非默认子网中启动的实例 IP 地址之间的区别。

| 性能 | EC2-Classic | 默认子网 | 非默认子网 |
|-----------------------------------|--|---|---|
| 公有 IP 地址 (来自 Amazon 的公有 IPv4 地址池) | 您的实例会收到一个公有 IP 地址。 | 默认情况下，您的实例不会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。 | 默认情况下，您的实例不会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。 |
| 私有 IPv4 地址 | 您的实例会在每次启动时收到一个来自 EC2-Classic 范围的私有 IP 地址。 | 您的实例会收到一个在您的默认子网 IPv4 地址范围的静态私有 IP 地址。 | 您的实例会收到一个来自您的子网 IPv4 地址范围的静态私有 IP 地址。 |
| 多个 IPv4 地址 | 我们会为您的实例选择一个私有 IP 地址；不支持多个 IP 地址。 | 您可以为实例分配多个私有 IP 地址。 | 您可以为实例分配多个私有 IP 地址。 |
| 网络接口 | IP 地址与实例相关联；不支持网络接口。 | IP 地址与网络接口相关联。每个实例都有一个或多个网络接口。 | IP 地址与网络接口相关联。每个实例都有一个或多个网络接口。 |
| 弹性 IP 地址 (IPv4) | 当您停止实例时，弹性 IP 地址会取消与实例的关联。 | 当您停止实例时，弹性 IP 地址会保持与实例的关联。 | 当您停止实例时，弹性 IP 地址会保持与实例的关联。 |
| DNS 主机名 (IPv4) | DNS 主机名默认处于启用状态。 | DNS 主机名默认处于启用状态。 | 默认情况下 DNS 主机名为禁用状态，但有一种情况除外，即当您在 Amazon VPC 控制台中使用 VPC 向导创建 VPC 时。 |
| IPv6 地址 | 不支持。您的实例无法接收 IPv6 地址。 | 默认情况下，您的实例无法接收 IPv6 地址，除非您已将某个 IPv6 CIDR 块与您的 VPC 和子网关联，并在启动期间指定了一个 IPv6 地址或修改了子网的 IPv6 寻址属性。 | 默认情况下，您的实例无法接收 IPv6 地址，除非您已将某个 IPv6 CIDR 块与您的 VPC 和子网关联，并在启动期间指定了一个 IPv6 地址或修改了子网的 IPv6 寻址属性。 |

使用实例的 IP 地址

您可以查看分配给实例的 IP 地址，在启动期间将公有 IPv4 地址分配给实例，或在启动期间将 IPv6 地址分配给实例。

内容

- [确定您的公有、私有和弹性 IP 地址 \(p. 456\)](#)
- [确定 IPv6 地址 \(p. 458\)](#)
- [在实例启动期间分配公有 IPv4 地址 \(p. 458\)](#)
- [向实例分配 IPv6 地址 \(p. 459\)](#)
- [取消分配给实例的 IPv6 地址 \(p. 460\)](#)

确定您的公有、私有和弹性 IP 地址

您可以使用 Amazon EC2 控制台来确定实例的私有 IPv4 地址、公有 IPv4 地址和弹性 IP 地址。您还可以通过使用实例元数据，从实例内确定实例的公有 IPv4 地址和私有 IPv4 地址。有关更多信息，请参阅 [实例元数据和用户数据 \(p. 295\)](#)。

使用控制台确定实例的私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。在详细信息窗格中，从 Private IPs 字段中获取私有 IPv4 地址，并从 Private DNS 字段中获取内部 DNS 主机名。
4. (仅限 VPC) 如果您为附加到实例的网络接口分配了一个或多个辅助私有 IPv4 地址，则可从 Secondary private IPs 字段中获取这些 IP 地址。
5. (仅限 VPC) 或者，在导航窗格中，选择 Network Interfaces，然后选择与您的实例关联的网络接口。
6. 从 Primary private IPv4 IP 字段中获取主要私有 IP 地址，从 Private DNS (IPv4) 字段中获取内部 DNS 主机名。
7. 如果您为网络接口分配了辅助私有 IP 地址，则可从 Secondary private IPv4 IPs 字段中获取这些 IP 地址。

使用控制台确定实例的公有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。在详细信息窗格中，从 IPv4 Public IP 字段中获取公有 IP 地址，从 Public DNS (IPv4) 字段中获取外部 DNS 主机名。
4. 如果弹性 IP 地址已与实例关联，则可从 Elastic IPs 字段中获取弹性 IP 地址。

Note

如果您已将弹性 IP 地址与实例关联，则 IPv4 Public IP 字段也将显示弹性 IP 地址。

5. (仅限 VPC) 或者，在导航窗格中，选择 Network Interfaces，然后选择与您的实例关联的网络接口。
6. 从 IPv4 Public IP 字段获取公有 IP 地址。星号 (*) 表示映射到主要私有 IPv4 地址的公有 IPv4 地址或弹性 IP 地址。

Note

公有 IPv4 地址在控制台中显示为网络接口的属性，但它通过 NAT 映射到主要私有 IPv4 地址。因此，如果您检查实例网络接口的属性（例如，通过 ifconfig [Linux] 或 ipconfig [Windows]），则不会显示公有 IP 地址。要从实例内确定实例的公有 IPv4 地址，您可以使用实例元数据。

使用实例元数据确定实例的 IPv4 地址

1. 连接到您的实例。
2. 使用以下命令访问私有 IP 地址：
 - Linux

```
$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

- Windows

```
$ wget http://169.254.169.254/latest/meta-data/local-ipv4
```

3. 使用以下命令访问公有 IP 地址：
 - Linux

```
$ curl http://169.254.169.254/latest/meta-data/public-ipv4
```

- Windows

```
$ wget http://169.254.169.254/latest/meta-data/public-ipv4
```

请注意，如果弹性 IP 地址与实例相关联，则返回的值是弹性 IP 地址。

确定 IPv6 地址

(仅限 VPC) 您可以使用 Amazon EC2 控制台确定实例的 IPv6 地址。

使用控制台确定实例的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。在详细信息窗格中，从 IPv6 IPs 字段获取 IPv6 地址。

使用实例元数据确定实例的 IPv6 地址

1. 连接到您的实例。
2. 使用以下命令查看 IPv6 地址 (您可以从 `http://169.254.169.254/latest/meta-data/network/interfaces/macs/` 中获取 MAC 地址)：
 - Linux

```
$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

- Windows

```
$ wget http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

在实例启动期间分配公有 IPv4 地址

如果在 EC2-Classic 中启动实例，则默认情况下，系统会为实例分配公有 IPv4 地址。您不能修改此操作。

在 VPC 中，所有子网都有一个属性可指定是否为子网中启动的实例分配公有 IP 地址。默认情况下，非默认子网的此属性设置为 false，默认子网的此属性设置为 true。启动实例时，您也可以通过公有 IPv4 寻址功能来控制是否为实例分配公有 IPv4 地址；您可以覆盖子网 IP 寻址属性的默认行为。公有 IPv4 地址从 Amazon 的公有 IPv4 地址池进行分配，并分配给设备索引为 eth0 的网络接口。此功能取决于启动实例时的特定条件。

Important

启动后，即无法手动将该公有 IP 地址与您的实例取消关联。在某些情况下，它会自动释放，之后无法重新使用。有关更多信息，请参阅 [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。如果需要可以随意关联或取消关联的永久公有 IP 地址，请在启动后向实例分配弹性 IP 地址。有关更多信息，请参阅 [弹性 IP 地址 \(p. 467\)](#)。

在启动实例时访问公有 IP 地址分配功能

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。

3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。
4. 在配置实例详细信息页面中，为网络选择一个 VPC。这将显示 Auto-assign Public IP 列表。选择 Enable 或 Disable 可覆盖子网的默认设置。

Important

如果您指定多个网络接口，则不能自动分配公有 IP 地址。此外，如果您将某个现有的网络接口指定为 eth0，则无法使用自动分配公有 IP 功能覆盖子网设置。

5. 按照向导中后续页面中的步骤完成实例的设置。有关向导配置选项的更多信息，请参阅[启动实例 \(p. 244\)](#)。在最后的 Review Instance Launch 页面上，检查您的设置，然后选择 Launch 以选择一个密钥对并启动您的实例。
6. 在实例页面中，选择您的新实例，并在详细信息窗格的 IPv4 Public IP 字段中查看其公有 IP 地址。

公有 IP 地址分配功能只在启动时可用。然而，无论您是否在启动时为实例分配公有 IP 地址，您都可以在启动后将弹性 IP 地址与实例相关联。有关更多信息，请参阅[弹性 IP 地址 \(p. 467\)](#)。您还可以修改子网的公有 IPv4 寻址行为。有关更多信息，请参阅[修改子网的公有 IPv4 寻址属性](#)。

使用命令行启用或禁用公有 IP 寻址功能

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。
 - 将 `--associate-public-ip-address` 或 `--no-associate-public-ip-address` 选项与 `run-instances` 命令 (AWS CLI) 结合使用
 - 将 `-AssociatePublicIp` 参数与 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用

向实例分配 IPv6 地址

如果您的 VPC 和子网有与之关联的 IPv6 CIDR 块，则您可以在启动期间或之后向实例分配 IPv6 地址。IPv6 地址从子网的 IPv6 地址范围进行分配，并分配给设备索引为 eth0 的网络接口。

在启动期间向实例分配 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择一个 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

请确保您选择的实例类型支持 IPv6 地址。有关更多信息，请参阅[实例类型 \(p. 135\)](#)。

3. 在配置实例详细信息页面中，为网络选择一个 VPC，为子网选择一个子网。对于自动分配 IPv6 IP，请选择启用。
4. 遵循向导中的剩余步骤来启动您的实例。

或者，您可以在启动后向实例分配 IPv6 地址。

在启动后向实例分配 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择 Save。

Note

如果您使用 Amazon Linux 2016.09.0 或更高版本、或 Windows Server 2008 R2 或更高版本启动实例，则系统已经为 IPv6 配置实例，并且您无需执行其他步骤即可确保实例可以识别 IPv6 地址。如果从旧版 AMI 中启动实例，则可能需要手动配置实例。有关更多信息，请参阅 Amazon VPC 用户指南中的[在实例中配置 IPv6](#)。

使用命令行分配 IPv6 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- 将`--ipv6-addresses`选项与 `run-instances` 命令 (AWS CLI) 结合使用
- 将 `Ipv6Addresses` 属性用于 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 中的 `-NetworkInterface`
- `assign-ipv6-addresses` (AWS CLI)
- `Register-EC2Ipv6AddressList` (适用于 Windows PowerShell 的 AWS 工具)

取消分配给实例的 IPv6 地址

您可以使用 Amazon EC2 控制台取消分配给实例的 IPv6 地址。

取消分配给实例的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择要取消分配的 IPv6 地址对应的 Unassign。
5. 选择是，请更新。

使用命令行取消分配 IPv6 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `unassign-ipv6-addresses` (AWS CLI)
- `Unregister-EC2Ipv6AddressList` (适用于 Windows PowerShell 的 AWS 工具)。

多个 IP 地址

在 EC2-VPC 中，您可以为实例指定多个私有 IPv4 和 IPv6 地址。您可为实例指定的网络接口和私有 IPv4 和 IPv6 地址的数量取决于该实例的类型。有关更多信息，请参阅[每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。

在执行以下操作时，为 VPC 中的实例分配多个 IP 地址会非常有用：

- 在单个服务器上使用多个 SSL 证书，并为每个证书关联一个指定的 IP 地址，以在单个服务器上托管多个网站。
- 操作每个网络接口有多个 IP 地址的网络应用，如防火墙或负载均衡器。
- 当实例发生故障时，可将内部流量重定向到备用实例，方法是为备用实例重新分配辅助 IP 地址。

内容

- [多个 IP 地址如何工作 \(p. 461\)](#)
- [使用多个 IPv4 地址 \(p. 461\)](#)

- [使用多个 IPv6 地址 \(p. 464\)](#)

多个 IP 地址如何工作

下表说明了多个 IP 地址如何与网络接口配合工作：

- 您可以为任何网络接口分配辅助私有 IPv4 地址。网络接口可与实例连接或断开。
- 您可以将多个 IPv6 地址分配给拥有关联 IPv6 CIDR 块的子网中的网络接口。
- 您必须从子网的 IPv4 CIDR 块范围内为网络接口选择辅助 IPv4。
- 您必须从子网的 IPv6 CIDR 块范围内为网络接口选择辅助 IPv6。
- 安全组适用于网络接口，而不适用于 IP 地址。因此，IP 地址受在其中指定 IP 地址的网络接口的安全约束。
- 可将多个 IP 地址分配给附加到正在运行或已停止实例的网络接口，也可以取消分配操作。
- 如果您明确允许，已分配给某个网络接口的辅助私有 IPv4 地址可重新分配给其他网络接口。
- 无法将 IPv6 地址重新分配给其他网络接口；您必须先取消分配给现有网络接口的 IPv6 地址。
- 当使用命令行工具或 API 将多个 IP 地址分配给某个网络接口时，如果其中有一个 IP 地址无法分配，整个操作都会失败。
- 当网络接口与实例断开或附加到其他实例时，主要私有 IPv4 地址、辅助私有 IPv4 地址、弹性 IP 地址以及 IPv6 地址将仍然属于此网络接口。
- 尽管您无法从实例移去主要网络接口，但是您可以将主要网络接口的辅助私有 IPv4 地址重新分配给另一个网络接口。
- 您可以将任何其他网络接口从一个实例移动到另一个。

下表说明了如何将多个 IP 地址与弹性 IP 地址配合使用 (仅限 IPv4)：

- 每个私有 IPv4 地址只能与一个弹性 IP 地址关联，反之亦然。
- 当辅助私有 IPv4 地址重新分配给其他接口时，该辅助私有 IPv4 地址会保留与弹性 IP 地址的相关性。
- 当您取消分配给接口的辅助私有 IPv4 地址时，相关的弹性 IP 地址会自动取消与该辅助私有 IPv4 地址的关联。

使用多个 IPv4 地址

您可以将一个辅助私有 IPv4 地址分配给实例，将弹性 IPv4 地址与辅助私有 IPv4 地址关联，并且取消分配辅助私有 IPv4 地址。

内容

- [分配辅助私有 IPv4 地址 \(p. 461\)](#)
- [在您的实例上配置操作系统以识别辅助私有 IPv4 地址 \(p. 463\)](#)
- [将弹性 IP 地址与辅助私有 IPv4 地址关联 \(p. 463\)](#)
- [查看您的辅助私有 IPv4 地址 \(p. 463\)](#)
- [取消分配辅助私有 IPv4 地址 \(p. 464\)](#)

分配辅助私有 IPv4 地址

您可以在启动实例时或在实例运行后为实例的网络接口分配辅助私有 IPv4 地址。本节包括以下过程。

- [在 EC2-VPC 中启动实例时分配辅助私有 IPv4 地址 \(p. 462\)](#)
- [使用命令行在启动期间分配辅助 IPv4 地址 \(p. 462\)](#)
- [为网络接口分配辅助私有 IPv4 地址 \(p. 462\)](#)

- 使用命令行为现有实例分配辅助私有 IPv4 (p. 463)

在 EC2-VPC 中启动实例时分配辅助私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 选择一个 AMI，然后选择实例类型并选择 Next: Configure Instance Details。
4. 在配置实例详细信息页面中，为网络选择一个 VPC，为子网选择一个子网。
5. 在 Network Interfaces 部分中，执行以下操作，然后选择 Next: Add Storage：
 - 要添加其他网络接口，请选择添加设备。当您启动实例时，控制台允许您指定最多两个网络接口。启动实例后，选择导航窗格中的 Network Interfaces 以添加其他网络接口。您可以连接的网络接口总数因实例类型而有所差异。有关更多信息，请参阅 [每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。

Important

当您添加第二个网络接口时，系统将无法再自动分配公有 IPv4 地址。除非您将弹性 IP 地址分配给主网络接口 (eth0)，否则将无法通过 IPv4 连接到实例。您可在完成启动向导后分配弹性 IP 地址。有关更多信息，请参阅 [使用弹性 IP 地址 \(p. 469\)](#)。

- 对于每个网络接口，在辅助 IP 地址下，选择添加 IP，然后输入一个处于子网范围内的私有 IP 地址，或接受默认值 Auto-assign，从而让 Amazon 选择一个地址。
6. 在接下来的 Add Storage 页面上，除了 AMI 指定的卷 (如根设备卷) 外，您可指定要挂载到实例的卷，然后选择 Next: Add Tags。
 7. 在 Add Tags 页面上，为实例指定标签 (例如，便于用户识别的名称)，然后选择 Next: Configure Security Group。
 8. 在 Configure Security Group (配置安全组) 页面上，选择一个现有安全组或创建新安全组。选择 Review and Launch。
 9. 在 Review Instance Launch 页面上，检查您的设置，然后选择 Launch 以选择一个密钥对并启动您的实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

Important

向网络接口添加辅助私有 IP 地址后，您必须连接到实例并在该实例上配置辅助私有 IP 地址。有关更多信息，请参阅 [在您的实例上配置操作系统以识别辅助私有 IPv4 地址 \(p. 463\)](#)。

使用命令行在启动期间分配辅助 IPv4 地址

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - 用于 `--secondary-private-ip-addresses` 的 [run-instances 命令 \(AWS CLI\)](#) 选项
 - 使用 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 定义 `-NetworkInterface` 并指定 `PrivateIpAddresses` 参数。

为网络接口分配辅助私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces，然后选择附加到实例的网络接口。
3. 依次选择 Actions、Manage IP Addresses。
4. 在 IPv4 Addresses 下，选择 Assign new IP。
5. 输入一个处于实例子网范围内的特定 IPv4 地址，或者将该字段留空，以便让 Amazon 为您选择一个 IP 地址。
6. (可选) 选择 Allow reassignment，以允许已分配到另一个网络接口的辅助私有 IP 地址能够重新分配。
7. 选择是，请更新。

或者，您也可以为实例分配辅助私有 IPv4 地址。在导航窗格中选择 Instances，选择实例，然后依次选择 Actions、Networking、Manage IP Addresses。您可以按上述步骤进行操作，以配置相同的内容。该 IP 地址将分配给实例的主网络接口 (eth0)。

使用命令行为现有实例分配辅助私有 IPv4

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - `assign-private-ip-addresses` (AWS CLI)
 - `Register-EC2PrivateIpAddress` (适用于 Windows PowerShell 的 AWS 工具)

在您的实例上配置操作系统以识别辅助私有 IPv4 地址

为实例分配辅助私有 IPv4 地址后，您需要在实例上配置操作系统，以识别辅助私有 IP 地址。

- 如果您使用的是 Amazon Linux，`ec2-net-utils` 包可以在此步骤上为您提供帮助。它能在实例运行期间配置您附加的其他网络接口，在 DHCP 租约续订期间更新辅助 IPv4 地址，并更新相关的路由规则。您可以使用 `sudo service network restart` 命令立即刷新接口列表，然后使用 `ip addr li` 查看最新列表。如果您需要手动控制网络配置，可以删除 `ec2-net-utils` 包。有关更多信息，请参阅 [使用 ec2-net-utils 配置网络接口 \(p. 478\)](#)。
- 如果您正在使用其他 Linux 分配，请参阅有关 Linux 分配的文档。您可以搜索有关配置其他网络接口和辅助 IPv4 地址的信息。如果实例在同一子网中有两个或更多接口，请搜索有关利用路由规则解决非对称路由的信息。

有关配置 Windows 实例的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [为 VPC 中的 Windows 实例配置辅助私有 IP 地址](#)。

将弹性 IP 地址与辅助私有 IPv4 地址关联

在 EC2-VPC 中将弹性 IP 地址与辅助私有 IPv4 地址关联

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Actions，然后选择 Associate address。
4. 对于 Network interface，选择网络接口，然后从 Private IP 列表中选择辅助 IP 地址。
5. 选择 Associate。

使用命令行将弹性 IP 地址与辅助私有 IPv4 地址关联

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - `associate-address` (AWS CLI)
 - `Register-EC2Address` (适用于 Windows PowerShell 的 AWS 工具)

查看您的辅助私有 IPv4 地址

在 EC2-VPC 中查看分配给网络接口的私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择您要查看其私有 IP 地址的网络接口。
4. 在详细信息窗格中的 Details 选项卡上，查看 Primary private IPv4 IP 和 Secondary private IPv4 IP 字段，了解分配给该网络接口的主要私有 IPv4 地址和任何辅助私有 IPv4 地址。

查看分配给实例的私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择要查看其私有 IP 地址的实例。
4. 在详细信息窗格的 Description 选项卡上，查看 Private IPs 和 Secondary private IPs 字段，了解通过实例的网络接口分配给实例的主要私有 IPv4 地址和任何辅助私有 IPv4 地址。

取消分配辅助私有 IPv4 地址

如果您不再需要辅助私有 IPv4 地址，则可取消分配给实例或网络接口的这类地址。当取消分配给网络接口的辅助私有 IPv4 地址后，弹性 IP 地址（如果存在）也会断开相关联系。

取消分配给实例的辅助私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，然后依次选择 Actions、Networking、Manage IP Addresses。
4. 在 IPv4 Addresses 下，选择要取消分配的 IPv4 地址对应的 Unassign。
5. 选择是，请更新。

取消分配给网络接口的辅助私有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv4 Addresses 下，选择要取消分配的 IPv4 地址对应的 Unassign。
5. 选择是，请更新。

使用命令行取消分配辅助私有 IPv4 地址

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - [unassign-private-ip-addresses \(AWS CLI\)](#)
 - [Unregister-EC2PrivateIpAddress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

使用多个 IPv6 地址

您可以将多个 IPv6 地址分配给实例、查看分配给实例的 IPv6 地址以及取消分配给实例的 IPv6 地址。

内容

- [分配多个 IPv6 地址 \(p. 464\)](#)
- [查看您的 IPv6 地址 \(p. 466\)](#)
- [取消分配 IPv6 地址 \(p. 466\)](#)

分配多个 IPv6 地址

您可以在启动期间或之后将一个或多个 IPv6 地址分配给实例。要将 IPv6 地址分配给实例，您在其中启动实例的 VPC 和子网都必须有一个关联的 IPv6 CIDR 块。有关更多信息，请参阅 Amazon VPC 用户指南中的 [VPC 和子网](#)。

在启动期间分配多个 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板中，选择 Launch Instance。
3. 选择一个 AMI 和实例类型，然后选择 Next: Configure Instance Details。请确保您选择的实例类型支持 IPv6。有关更多信息，请参阅 [实例类型 \(p. 135\)](#)。
4. 在 Configure Instance Details (配置实例详细信息) 页上，从 Network (网络) 列表中选择一个 VPC，然后从 Subnet (子网) 列表中选择一个子网。
5. 在 Network Interfaces 部分中，执行以下操作，然后选择 Next: Add Storage：
 - 要将单个 IPv6 地址分配给主网络接口 (eth0)，请在 IPv6 IP 下选择 Add IP。要添加辅助 IPv6 地址，请再次选择 Add IP。您可以输入一个处于子网范围内的 IPv6 地址，或保留默认值 Auto-assign，从而让 Amazon 为您选择一个 IPv6 地址。
 - 选择 Add Device，以添加另一个网络接口，并重复上述步骤，将一个或多个 IPv6 地址添加到该网络接口。当您启动实例时，控制台允许您指定最多两个网络接口。启动实例后，选择导航窗格中的 Network Interfaces 以添加其他网络接口。您可以连接的网络接口总数因实例类型而有所差异。有关更多信息，请参阅 [每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。
6. 按照向导中的后续步骤将卷和标记挂载到您的实例。
7. 在 Configure Security Group (配置安全组) 页面上，选择一个现有安全组或创建新安全组。如果您想让实例可通过 IPv6 访问，请确保您的安全组拥有允许从 IPv6 地址访问的规则。有关更多信息，请参阅 [安全组规则引用 \(p. 361\)](#)。选择 Review and Launch。
8. 在 Review Instance Launch 页面上，检查您的设置，然后选择 Launch 以选择一个密钥对并启动您的实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

您可以使用实例 屏幕 Amazon EC2 控制台将多个 IPv6 地址分配给现有实例。该做法可将 IPv6 地址分配给实例的主网络接口 (eth0)。要将特定 IPv6 地址分配给实例，请确保 IPv6 地址尚未分配给其他实例或网络接口。

将多个 IPv6 地址分配给现有实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择您要添加的每个 IPv6 地址对应的 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择是，请更新。

或者，您可以将多个 IPv6 地址分配给现有网络接口。网络接口必须是在具有关联的 IPv6 CIDR 块的子网中创建的。要将特定 IPv6 地址分配给网络接口，请确保该 IPv6 地址尚未分配给其他网络接口。

将多个 IPv6 地址分配给网络接口

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择您的网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择您要添加的每个 IPv6 地址对应的 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择是，请更新。

CLI 概述

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- 在启动期间分配 IPv6 地址：
 - 将 `--ipv6-addresses` 或 `--ipv6-address-count` 选项与 `run-instances` 命令 (AWS CLI) 结合使用。
 - 使用 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 定义 `-NetworkInterface` 并指定 `Ipv6Addresses` 或 `Ipv6AddressCount` 参数。
- 将 IPv6 地址分配给网络接口：
 - `assign-ipv6-addresses` (AWS CLI)
 - `Register-EC2Ipv6AddressList` (适用于 Windows PowerShell 的 AWS 工具)

查看您的 IPv6 地址

您可以查看实例或网络接口的 IPv6 地址。

查看分配给实例的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。在详细信息窗格中，查看 IPv6 IPs 字段。

查看分配给网络接口的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择您的网络接口。在详细信息窗格中，查看 IPv6 IPs 字段。

CLI 概述

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- 查看实例的 IPv6 地址：
 - `describe-instances` (AWS CLI)
 - `Get-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)。
- 查看网络接口的 IPv6 地址：
 - `describe-network-interfaces` (AWS CLI)
 - `Get-EC2NetworkInterface` (适用于 Windows PowerShell 的 AWS 工具)

取消分配 IPv6 地址

您可以取消分配给实例主网络接口的 IPv6 地址，也可以取消分配给网络接口的 IPv6 地址。

取消分配给实例的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择要取消分配的 IPv6 地址对应的 Unassign。
5. 选择是，请更新。

取消分配给网络接口的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Network Interfaces。
3. 选择您的网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择要取消分配的 IPv6 地址对应的 Unassign。
5. 选择 Save。

CLI 概述

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [unassign-ipv6-addresses \(AWS CLI\)](#)
- [Unregister-EC2Ipv6AddressList \(适用于 Windows PowerShell 的 AWS 工具\)](#)。

弹性 IP 地址

弹性 IP 地址 是专为动态云计算设计的静态 IPv4 地址。弹性 IP 地址与您的 AWS 账户关联。借助弹性 IP 地址，您可以快速将地址重新映射到您的账户中的另一个实例，从而屏蔽实例故障。

弹性 IP 地址是公有 IPv4 地址，可通过 Internet 访问。如果您的实例没有公有 IPv4 地址，则可以将弹性 IP 地址与您的实例关联以启用与 Internet 的通信；例如，从本地计算机连接到您的实例。

我们目前不支持对 IPv6 使用弹性 IP 地址。

主题

- [弹性 IP 地址基础信息 \(p. 467\)](#)
- [EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别 \(p. 468\)](#)
- [使用弹性 IP 地址 \(p. 469\)](#)
- [将反向 DNS 用于电子邮件应用程序 \(p. 472\)](#)
- [弹性 IP 地址限额 \(p. 473\)](#)

弹性 IP 地址基础信息

下面是弹性 IP 地址的基本特征：

- 要使用弹性 IP 地址，您应首先向您的账户分配这样一个地址，然后将其与您的实例或网络接口关联。
- 当您将弹性 IP 地址与实例或其主网络接口关联时，实例的公有 IPv4 地址（如果有）将释放回 Amazon 的公有 IPv4 地址池中。您无法重复使用公有 IPv4 地址。有关更多信息，请参阅 [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。
- 您可以取消弹性 IP 地址与资源的关联，然后重新将此地址与其他资源关联。
- 取消关联的弹性 IP 地址保持分配到您的账户，直至您明确释放它。
- 为确保弹性 IP 地址的有效使用，如果弹性 IP 地址未与正在运行的实例关联，或者它已与停止的实例或未连接的网络接口关联，我们将强制收取小额的小时费用。当您的实例正在运行时，您无需为与该实例关联的某个弹性 IP 地址付费，但需为与该实例关联的所有其他弹性 IP 地址付费。有关更多信息，请参阅 [Amazon EC2 定价](#)。
- 弹性 IP 地址只能在一个特定区域中使用。
- 在将弹性 IP 地址与之前具有公有 IPv4 地址的实例关联时，该实例的公有 DNS 主机名将发生更改以匹配弹性 IP 地址。
- 我们会将公有 DNS 主机名解析为实例所在网络外部的该实例的公有 IPv4 地址或弹性 IP 地址，以及实例所在网络内部的该实例的私有 IPv4 地址。

如果您的账户支持 EC2-Classic，则 EC2-Classic 与 EC2-VPC 的弹性 IP 地址的使用和行为可能有所不同。有关更多信息，请参阅 [EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别 \(p. 468\)](#)。

EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别

如果您的账户支持 EC2-Classic，则其中一个弹性 IP 地址池可与 EC2-Classic 平台配合使用，而另一个可与 EC2-VPC 平台配合使用。您不能将已分配与 VPC 配合使用的弹性 IP 地址与 EC2-Classic 中的实例相关联，反之亦然。但是，您可将已分配在 EC2-Classic 平台中使用的弹性 IP 地址迁移至 EC2-VPC 平台。您不能将弹性 IP 地址迁移到另一个区域。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 435\)](#)。

当您将弹性 IP 地址与 EC2-Classic（默认 VPC）中的实例或与您在启动时为 eth0 网络接口分配了公有 IPv4 的非默认 VPC 中的实例关联时，该实例的当前公有 IPv4 地址会释放回公有 IP 地址池。如果您取消弹性 IP 地址与实例的关联，系统会在几分钟内自动为该实例分配新的公有 IPv4 地址。但是，如果将第二个网络接口连接到 VPC 中的实例，则系统不会自动为该实例分配新的公有 IPv4 地址。有关公有 IPv4 地址的更多信息，请参阅[公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。

有关对 VPC 中的实例使用弹性 IP 地址的信息，请参阅 Amazon VPC 用户指南 中的[弹性 IP 地址](#)。

下表列出了 EC2-Classic 和 EC2-VPC 上的弹性 IP 地址之间的区别。有关私有 IP 地址和公有 IP 地址之间的区别的更多信息，请参阅 [EC2-Classic 和 EC2-VPC 之间的 IP 地址区别 \(p. 455\)](#)。

| 性能 | EC2-Classic | EC2-VPC |
|-----------------------------|--|---|
| 分配弹性 IP 地址 | 在分配弹性 IP 地址后，它将在 EC2-Classic 中使用；但是，您可将弹性 IP 地址迁移到 EC2-VPC 平台。有关更多信息，请参阅 将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 469) 。 | 在分配弹性 IP 地址后，它将只能在 VPC 中使用。 |
| 分配弹性 IP 地址 | 将弹性 IP 地址与实例相关联。 | 弹性 IP 地址是网络接口的一个属性。您可以通过更新附加到实例的网络接口，将弹性 IP 地址与该实例关联起来。有关更多信息，请参阅 弹性网络接口 (p. 473) 。 |
| 取消关联弹性 IP 地址 | 如果您试图关联已与其他实例关联的弹性 IP 地址，该地址会自动与新实例关联。 | 如果您的账户仅支持 EC2-VPC，并且您尝试关联已与其他实例相关联的弹性 IP 地址，则该地址会自动与新实例关联。如果您在 EC2-Classic 账户中使用 VPC，并且您尝试关联已与其他实例相关联的弹性 IP 地址，则仅当您允许重新关联时才会成功。 |
| 将弹性 IP 地址与具有现有弹性 IP 地址的目标关联 | 虽然将解除现有弹性 IP 地址与实例的关联，但仍会将其分配给您的账户。 | 如果您的账户仅支持 EC2-VPC，将解除现有弹性 IP 地址与实例的关联，但仍会将其分配给您的账户。如果您在 EC2-Classic 账户中使用 VPC，则无法将弹性 IP 地址与网络接口或具有现有弹性 IP 地址的实例关联。 |
| 停止实例 | 如果您停止某个实例，则其弹性 IP 地址将取消关联；在您重新启动该实例时，必须重新关联该弹性 IP 地址。 | 如果您停止某个实例，其弹性 IP 地址会保持关联。 |
| 分配多个 IP 地址 | 实例仅支持一个私有 IPv4 地址和一个相应的弹性 IP 地址。 | 实例支持多个 IPv4 地址，并且每个 IPv4 地址都可拥有相应的弹性 IP 地址。有关更多信息，请参阅 多个 IP 地址 (p. 460) 。 |

将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC

如果您的账户支持 EC2-Classic，则可将已分配为在 EC2-Classic 平台中使用的弹性 IP 地址迁移至同一区域中的 EC2-VPC 平台。这可帮助您将资源从 EC2-Classic 迁移到 VPC；例如，您可在 VPC 中启动新的 Web 服务器，然后将 EC2-Classic 中您的 Web 服务器所使用的弹性 IP 地址用于新的 VPC Web 服务器。

在将弹性 IP 地址迁移至 EC2-VPC 后，您将无法在 EC2-Classic 平台中使用该地址；不过，如果需要，您可以将该地址还原至 EC2-Classic。在将弹性 IP 地址还原至 EC2-Classic 后，您将无法在 EC2-VPC 中使用该地址，直至您重新迁移它。只能将弹性 IP 地址从 EC2-Classic 迁移至 EC2-VPC。不能将本来分配为在 EC2-VPC 中使用的弹性 IP 地址迁移至 EC2-Classic。

要迁移弹性 IP 地址，则不得将该地址与实例关联。有关解除弹性 IP 地址与实例的关联的更多信息，请参阅取消关联弹性 IP 地址，并将它与其他实例重新关联 (p. 470)。

您可以迁移您账户中拥有的数量的 EC2-Classic 弹性 IP 地址。但是，在将弹性 IP 地址迁移到 EC2-VPC 时，该地址会计入 EC2-VPC 的弹性 IP 地址限制。如果某个弹性 IP 地址将导致您超出限制，则不能迁移该地址。同样，在将弹性 IP 地址还原到 EC2-Classic 时，该地址会计入 EC2-Classic 的弹性 IP 地址限制。有关更多信息，请参阅弹性 IP 地址限额 (p. 473)。

您不能迁移在 24 小时之前分配给您的账户弹性 IP 地址。

有关更多信息，请参阅移动弹性 IP 地址 (p. 471)。

使用弹性 IP 地址

以下部分介绍如何使用弹性 IP 地址。

主题

- 分配弹性 IP 地址 (p. 469)
- 描述您的弹性 IP 地址 (p. 470)
- 将弹性 IP 地址与正在运行的实例关联起来 (p. 470)
- 取消关联弹性 IP 地址，并将它与其他实例重新关联 (p. 470)
- 移动弹性 IP 地址 (p. 471)
- 释放弹性 IP 地址 (p. 472)

分配弹性 IP 地址

您可以使用 Amazon EC2 控制台或命令行分配弹性 IP 地址。如果您的账户支持 EC2-Classic，则可分配一个地址来在 EC2-Classic 或 EC2-VPC 中使用。

使用控制台分配用于 EC2-VPC 的弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. (EC2-Classic 账户) 选择 VPC，然后选择 Allocate。关闭确认屏幕。
5. (仅限 VPC 账户) 选择 Allocate，然后关闭确认屏幕。

使用控制台分配可在 EC2-Classic 中使用的弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. 选择 Classic，然后选择 Allocate。关闭确认屏幕。

使用命令行分配弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [allocate-address \(AWS CLI\)](#)
- [New-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

描述您的弹性 IP 地址

您可以使用 Amazon EC2 或命令行描述弹性 IP 地址。

使用控制台描述您的弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 从“Resource Attribute (资源属性)”列表中选择筛选条件以开始搜索。可以在单个搜索中使用多个筛选条件。

使用命令行描述您的弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-addresses \(AWS CLI\)](#)
- [Get-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

将弹性 IP 地址与正在运行的实例关联起来

您可以使用 Amazon EC2 控制台或命令行将弹性 IP 地址关联到实例。

(仅限 VPC) 如果要将弹性 IP 地址与您的实例关联以启用与 Internet 的通信，您还必须确保您的实例在公有子网中。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 Internet 网关。

使用控制台将弹性 IP 地址与实例关联

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Associate address。
4. 从 Instance 中选择实例，然后选择 Associate。

使用命令行关联弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [associate-address \(AWS CLI\)](#)
- [Register-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

取消关联弹性 IP 地址，并将它与其他实例重新关联

您可以使用 Amazon EC2 控制台或命令行取消关联弹性 IP 地址并将它重新关联。

使用控制台取消关联并重新关联弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Disassociate address。
4. 选择 Disassociate address。
5. 选择您在之前的步骤中取消关联的地址。对于 Actions，选择 Associate address。
6. 从 Instance 中选择新实例，然后选择 Associate。

使用命令行取消关联弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行关联弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

移动弹性 IP 地址

您可使用 Amazon EC2 控制台或 Amazon VPC 控制台将弹性 IP 地址从 EC2-Classic 移动到 EC2-VPC。此选项仅在您的账户支持 EC2-Classic 时可用。

使用 Amazon EC2 控制台将弹性 IP 地址移动到 EC2-VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Move to VPC scope。
4. 在确认对话框中，选择 Move Elastic IP。

您可以使用 Amazon EC2 控制台或 Amazon VPC 控制台将弹性 IP 地址还原到 EC2-Classic。

使用 Amazon EC2 控制台将弹性 IP 地址还原到 EC2-Classic

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Restore to EC2 scope。
4. 在确认对话框中，选择 Restore。

在您执行相关命令来移动或还原弹性 IP 地址后，弹性 IP 地址的迁移过程可能需要花费几分钟时间。使用 [describe-moving-addresses](#) 命令可查看您的弹性 IP 地址是仍在移动还是已完成移动。

将弹性 IP 地址移动到 EC2-VPC 后，您可以在 Elastic IPs 页面上的 Allocation ID 字段中查看其分配 ID。

如果弹性 IP 地址处于移动状态超过 5 分钟，请联系 <https://aws.amazon.com/premiumsupport/>。

使用 Amazon EC2 查询 API 或 AWS CLI 移动弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [move-address-to-vpc](#) (AWS CLI)

- [MoveAddressToVpc](#) (Amazon EC2 查询 API)
- [Move-EC2AddressToVpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 Amazon EC2 查询 API 或 AWS CLI 将弹性 IP 地址还原到 EC2-Classic

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [restore-address-to-classic](#) (AWS CLI)
- [RestoreAddressToClassic](#) (Amazon EC2 查询 API)
- [Restore-EC2AddressToClassic](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 Amazon EC2 查询 API 或 AWS CLI 描述移动中的地址的状态

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-moving-addresses](#) (AWS CLI)
- [DescribeMovingAddresses](#) (Amazon EC2 查询 API)
- [Get-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

在 EC2-VPC 中检索已迁移的弹性 IP 地址的分配 ID

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-addresses](#) (AWS CLI)
- [DescribeAddresses](#) (Amazon EC2 查询 API)
- [Get-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

释放弹性 IP 地址

如果您不再需要弹性 IP 地址，我们建议您解除此弹性 IP 地址（地址不可与实例相关联）。对于已分配用于 EC2-Classic 但未与实例关联的所有弹性 IP 地址，您也需要承担相应费用。

您可以使用 Amazon EC2 控制台或命令行释放弹性 IP 地址。

使用控制台释放弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Release addresses。系统提示时，请选择 Release。

使用命令行释放弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [release-address](#) (AWS CLI)
- [Remove-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

将反向 DNS 用于电子邮件应用程序

如果您打算从实例向第三方发送电子邮件，我们建议您调配一个或多个弹性 IP 地址，并将它们提供给我们。AWS 与 ISP 以及国际反垃圾电子邮件组织合作，减少从这些地址发送的电子邮件被标记为垃圾电子邮件的机率。

此外，还向您用于发送电子邮件的弹性 IP 地址分配了静态反向 DNS 记录，有助于避免电子邮件被一些反垃圾电子邮件组织标记为垃圾电子邮件。请注意，必须要先有指向您的弹性 IP 地址的对应的正向 DNS 记录（记录类型 A），然后我们才能创建反向 DNS 记录。

如果反向 DNS 记录与弹性 IP 地址关联，则该弹性 IP 地址将锁定到您的账户中且无法从您的账户中释放，直至删除记录。

要删除电子邮件发送限制，或向我们提供您的弹性 IP 地址和反向 DNS 记录，请前往[请求删除电子邮件发送限制](#)页面。

弹性 IP 地址限额

在默认情况下，所有 AWS 账户在每个区域最多可拥有 5 个弹性 IP 地址，因为公有 (IPv4) Internet 地址是稀缺的公共资源。我们大大鼓励您主要使用弹性 IP 地址，以便在实例发生故障的情况下能够将该地址映射到另一实例，并能够将 DNS 主机名用于所有其他节点间通信。

如果您认为您的架构需要额外的弹性 IP 地址，请填写[Amazon EC2 弹性 IP 地址申请表](#)。我们会要求您描述您的使用案例，让我们能够了解您对额外地址的需求。

弹性网络接口

弹性网络接口（在本文档中称为网络接口）是一种虚拟网络接口，可以附加到 VPC 中的实例。网络接口只能用于在 VPC 中运行的实例。

网络接口可以包含以下属性：

- 一个主要私有 IPv4 地址
- 一个或多个辅助私有 IPv4 地址
- 每个私有 IPv4 地址一个弹性 IP 地址 (IPv4)。
- 一个公有 IPv4 地址
- 一个或多个 IPv6 地址
- 一个或多个安全组
- 一个 MAC 地址
- 一个源/目标检查标记
- 一个描述

您可以创建一个网络接口，将其连接到某个实例，将其与实例分离，再连接到另一个实例。将网络接口附加到一个实例或者从一个实例分离并重新附加到另一实例时，网络接口的属性不会变化。当您将一个网络接口从一个实例移动到另一个实例时，网络流量也会重导向到新的实例。

VPC 中的每个实例都有一个默认网络接口，称为主网络接口 (eth0)。您无法从实例断开主网络接口。您可以创建并连接额外的网络接口。您可以使用的网络接口的数量上限因实例类型而不同。有关更多信息，请参阅[每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。

网络接口的私有 IPv4 地址

实例的主网络接口会分配到一个处于 VPC 的 IPv4 地址范围内的主要私有 IPv4 地址。您可以将其他私有 IPv4 地址分配给网络接口。

网络接口的公有 IPv4 地址

在 VPC 中，所有子网都有一个可以修改的属性，该属性可以确定在子网中创建的网络接口（以及在该子网中启动的实例）是否会分配到一个公有 IPv4 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的[子网的 IP 寻址行为](#)。公有 IPv4 地址从 Amazon 的公有 IPv4 地址池分配。当您启动一个实例时，IP 地址会被分配给创建的主网络接口 (eth0)。

当您创建一个网络接口时，它会继承子网的公有 IPv4 寻址属性。如果您日后修改了子网的公有 IPv4 寻址属性，网络接口仍会继续使用在其创建时生效的设置。如果您启动了一个实例并将一个现有网络接口指定为 eth0 接口，则公有 IPv4 寻址属性由网络接口决定。

有关更多信息，请参阅 [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。

网络接口的 IPv6 地址

您可以将一个 IPv6 CIDR 块与您的 VPC 和子网关联，并将子网范围的一个或多个 IPv6 地址分配给一个网络接口。

所有子网都有一个可以修改的属性，该属性可以确定在子网中创建的网络接口（以及在该子网中启动的实例）是否会自动分配到一个处于子网范围内的 IPv6 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的 [子网的 IP 寻址行为](#)。当您启动一个实例时，IPv6 地址会被分配给创建的主网络接口（eth0）。

有关更多信息，请参阅 [IPv6 地址 \(p. 455\)](#)。

内容

- [每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)
- [网络接口的使用场景 \(p. 477\)](#)
- [网络接口最佳配置实践 \(p. 477\)](#)
- [使用 ec2-net-utils 配置网络接口 \(p. 478\)](#)
- [使用网络接口 \(p. 479\)](#)

每个实例类型的每个网络接口的 IP 地址

下表列出了每个实例类型的网络接口的最大数量，以及每个网络接口的私有 IPv4 地址和 IPv6 地址的最大数量。每个网络接口的 IPv6 地址与私有 IPv4 地址有不同的限制并且分别列出。并非所有实例类型都支持 IPv6 寻址。网络接口、多个私有 IPv4 地址和 IPv6 地址仅适用于在 VPC 中运行的实例。有关更多信息，请参阅 [多个 IP 地址 \(p. 460\)](#)。有关 VPC 中的 IPv6 的更多信息，请参阅 Amazon VPC 用户指南中的 [IP Addressing in Your VPC](#)。

| 实例类型 | 最大网络接口数 | 每个接口的 IPv4 地址数 | 每个接口的 IPv6 地址数 |
|------------|---------|----------------|----------------|
| c1.medium | 2 | 6 | 不支持 IPv6 |
| c1.xlarge | 4 | 15 | 不支持 IPv6 |
| c3.large | 3 | 10 | 10 |
| c3.xlarge | 4 | 15 | 15 |
| c3.2xlarge | 4 | 15 | 15 |
| c3.4xlarge | 8 | 30 | 30 |
| c3.8xlarge | 8 | 30 | 30 |
| c4.large | 3 | 10 | 10 |
| c4.xlarge | 4 | 15 | 15 |
| c4.2xlarge | 4 | 15 | 15 |
| c4.4xlarge | 8 | 30 | 30 |
| c4.8xlarge | 8 | 30 | 30 |

| 实例类型 | 最大网络接口数 | 每个接口的 IPv4 地址数 | 每个接口的 IPv6 地址数 |
|-------------|---------|----------------|----------------|
| cc2.8xlarge | 8 | 30 | 不支持 IPv6 |
| cg1.4xlarge | 8 | 30 | 不支持 IPv6 |
| cr1.8xlarge | 8 | 30 | 不支持 IPv6 |
| d2.xlarge | 4 | 15 | 15 |
| d2.2xlarge | 4 | 15 | 15 |
| d2.4xlarge | 8 | 30 | 30 |
| d2.8xlarge | 8 | 30 | 30 |
| g2.2xlarge | 4 | 15 | 不支持 IPv6 |
| g2.8xlarge | 8 | 30 | 不支持 IPv6 |
| hi1.4xlarge | 8 | 30 | 不支持 IPv6 |
| hs1.8xlarge | 8 | 30 | 不支持 IPv6 |
| i2.xlarge | 4 | 15 | 15 |
| i2.2xlarge | 4 | 15 | 15 |
| i2.4xlarge | 8 | 30 | 30 |
| i2.8xlarge | 8 | 30 | 30 |
| i3.large | 3 | 10 | 10 |
| i3.xlarge | 4 | 15 | 15 |
| i3.2xlarge | 4 | 15 | 15 |
| i3.4xlarge | 8 | 30 | 30 |
| i3.8xlarge | 8 | 30 | 30 |
| i316xlarge | 15 | 50 | 50 |
| m1.small | 2 | 4 | 不支持 IPv6 |
| m1.medium | 2 | 6 | 不支持 IPv6 |
| m1.large | 3 | 10 | 不支持 IPv6 |
| m1.xlarge | 4 | 15 | 不支持 IPv6 |
| m2.xlarge | 4 | 15 | 不支持 IPv6 |
| m2.2xlarge | 4 | 30 | 不支持 IPv6 |
| m2.4xlarge | 8 | 30 | 不支持 IPv6 |
| m3.medium | 2 | 6 | 不支持 IPv6 |
| m3.large | 3 | 10 | 不支持 IPv6 |

| 实例类型 | 最大网络接口数 | 每个接口的 IPv4 地址数 | 每个接口的 IPv6 地址数 |
|-------------|---------|----------------|----------------|
| m3.xlarge | 4 | 15 | 不支持 IPv6 |
| m3.2xlarge | 4 | 30 | 不支持 IPv6 |
| m4.large | 2 | 10 | 10 |
| m4.xlarge | 4 | 15 | 15 |
| m4.2xlarge | 4 | 15 | 15 |
| m4.4xlarge | 8 | 30 | 30 |
| m4.10xlarge | 8 | 30 | 30 |
| m4.16xlarge | 8 | 30 | 30 |
| p2.xlarge | 4 | 15 | 15 |
| p2.8xlarge | 8 | 30 | 30 |
| p2.16xlarge | 8 | 30 | 30 |
| r3.large | 3 | 10 | 10 |
| r3.xlarge | 4 | 15 | 15 |
| r3.2xlarge | 4 | 15 | 15 |
| r3.4xlarge | 8 | 30 | 30 |
| r3.8xlarge | 8 | 30 | 30 |
| r4.large | 3 | 10 | 10 |
| r4.xlarge | 4 | 15 | 15 |
| r4.2xlarge | 4 | 15 | 15 |
| r4.4xlarge | 8 | 30 | 30 |
| r4.8xlarge | 8 | 30 | 30 |
| r4.16xlarge | 15 | 50 | 50 |
| t1.micro | 2 | 2 | 不支持 IPv6 |
| t2.nano | 2 | 2 | 2 |
| t2.micro | 2 | 2 | 2 |
| t2.small | 2 | 4 | 4 |
| t2.medium | 3 | 6 | 6 |
| t2.large | 3 | 12 | 12 |
| t2.xlarge | 3 | 15 | 15 |
| t2.2xlarge | 3 | 15 | 15 |

| 实例类型 | 最大网络接口数 | 每个接口的 IPv4 地址数 | 每个接口的 IPv6 地址数 |
|-------------|---------|----------------|----------------|
| x1.16xlarge | 8 | 30 | 30 |
| x1.32xlarge | 8 | 30 | 30 |

网络接口的使用场景

当您想执行以下操作时，将多个网络接口连接至一个实例很有帮助：

- 创建管理网络。
- 在您的 VPC 中使用网络和安全性设备。
- 创建双归属实例，并在不同子网间分配工作负载/任务。
- 创建低预算、高可用性的解决方案。

创建一个管理网络

您可以使用网络接口创建管理网络。在这种情况下，实例上的次要网络接口处理面向公众的通信，主要网络接口处理后端管理通信并会与您的有较多限制性访问控制的 VPC 中单独的子网相连接。面向公众的接口可能处于或不处于负载均衡器之后，它有一个关联的安全组来控制从 Internet 对服务器访问（例如，允许来自 0.0.0.0/0 或负载均衡器的 TCP 端口 80 和 443 的访问），而面向私人的接口的相关安全组只能允许来自 VPC 或 Internet 中允许的 IP 地址范围以及 VPC 或虚拟专用网关内的私有子网的 SSH 访问。

为确保故障转移功能，可以考虑针对网络接口上的传入流量使用辅助私有 IPv4。在某个实例失效时，您可以将接口和/或辅助私有 IPv4 地址移动到备用实例中。

使用您的 VPC 中的网络和安全设备

负载均衡器、网络地址转换 (NAT) 服务器和代理服务器等网络和安全设备更偏向于配置多个网络接口。您可以创建并附加次要网络接口至 VPC 中正在运行这些类型的应用程序的实例中，并用实例自己的公用和私有 IP 地址、安全组和源/目标检查设置其它接口。

通过不同子网的工作负荷/角色创建双主机实例。

您可以将网络接口放置到每一个与承载应用程序服务器的中间层网络相连接的 Web 服务器。应用程序服务器也可以用双主机连接至承载数据库服务器的后端网络（子网）。每一个双主机实例都在前端接收和处理请求、启动与后端的连接，然后将请求发送至后端网络上的服务器，而不是通过双主机实例路由网络数据包。

创建一个低成本、高可用性解决方案

如果您的一个提供特定功能的实例失效，则其网络接口可连接至一个针对同一种角色预配置的替代或热备用实例，以快速恢复服务。例如，您可以将一个网络接口用作连接数据库实例或 NAT 实例等关键服务的主要或辅助网络接口。如果实例失效，您（或更有可能是代表您运行的代码）可以将网络接口附加到热备用实例。由于接口保持其私有 IP 地址、弹性 IP 地址和 MAC 地址，因此只要您将网络接口附加到替代实例，网络流量就会立即开始流向备用实例。在实例失效之后、网络接口附加到备用实例之前，用户会暂时失去连接，但不需要更改 VPC 路由表或您的 DNS 服务器。

网络接口最佳配置实践

- 您可以在实例运行时（热连接）、实例停止时（暖连接）或实例启动时（冷连接）将网络接口连接至实例。

- 您可以在实例运行时或停止时分离次要 (ethN) 网络接口。但您不能分离主要 (eth0) 接口。
- 您可以在同一个 VPC 中将一个子网中的网络接口附加到另一个子网中的实例；但该网络接口和实例必须处于同一个可用区内。
- 通过 CLI 或 API 启动实例时，您可以针对主要 (eth0) 网络接口和其他网络接口指定要连接至实例的网络接口。
- 启动具有多个网络接口的 Amazon Linux 或 Windows Server 实例会自动在该实例的操作系统上配置接口、私有 IPv4 地址和路由表。
- 如果要通过暖附加或热附加方式附加一个额外的网络接口，您可能需要手动添加第二个接口、配置私有 IPv4 地址并相应修改路由表。运行 Amazon Linux 或 Windows Server 的实例会自动识别暖挂载或热挂载，并自行进行配置。
- 将另一个网络接口附加到实例（例如一种网卡绑定配置）不会增加或加倍双主机实例的网络带宽。
- 如果将来自同一子网的两个或多个网络接口连接到一个实例，可能会遇到非对称路由等联网问题。请尽可能在主网络接口上改用辅助私有 IPv4 地址。有关更多信息，请参阅 [分配辅助私有 IPv4 地址 \(p. 461\)](#)。

使用 ec2-net-utils 配置网络接口

Amazon Linux AMI 可能包含由 AWS 安装的其他脚本，它们称为 ec2-net-utils。这些脚本可以选择性地自动配置您的网络接口。这些脚本仅适用于 Amazon Linux。

使用以下命令可在 Amazon Linux 上安装该程序包（如果尚未安装）或对其进行更新（如果已安装且存在可用的其他更新）：

```
$ yum install ec2-net-utils
```

以下组件属于 ec2-net-utils 的一部分：

udev 规则 (/etc/udev/rules.d)

在网络接口连接、分离或重新连接正在运行的实例时识别它们，并确保 hotplug 脚本运行 (53-ec2-network-interfaces.rules)。将 MAC 地址映射到设备名称（生成 70-persistent-net.rules 的 75-persistent-net-generator.rules）。

hotplug 脚本

生成一个适用于 DHCP 的接口配置文件 (/etc/sysconfig/network-scripts/ifcfg-ethN)。并生成一个路由配置文件 (/etc/sysconfig/network-scripts/route-ethN)。

DHCP 脚本

每当网络接口收到一个新的 DHCP 租约时，此脚本会查询弹性 IP 地址的实例元数据。对于每个弹性 IP 地址，它会为路由策略数据库添加一个规则，确保来自该地址的出站流量使用正确的网络接口。它还会将每个私有 IP 地址作为次要地址添加至网络接口。

ec2ifup ethN

拓展标准 ifup 的功能。在此脚本重写配置文件 ifcfg-ethN 和 route-ethN 之后，它将运行 ifup。

ec2ifdown ethN

拓展标准 ifdown 的功能。当此脚本从路由策略数据库中删除网络接口的任何规则后，它将运行 ifdown。

ec2ifscan

检查尚未配置的网络接口并对它们进行配置。

请注意，此脚本在初始版本的 ec2-net-utils 中不可用。

要列出任何由 ec2-net-utils 生成的配置文件，请使用以下命令：

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

要针对每个实例禁用自动化，您可以将 `EC2SYNC=no` 添加至相应的 `ifcfg-ethN` 文件。例如，您可以使用以下命令为 `eth1` 接口禁用自动化：

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

如果您希望彻底禁用自动化，则可以使用以下命令删除该包：

```
$ yum remove ec2-net-utils
```

使用网络接口

您可以通过 Amazon EC2 控制台来使用网络接口。

内容

- [创建网络接口 \(p. 479\)](#)
- [删除网络接口 \(p. 480\)](#)
- [查看有关网络接口的详细信息 \(p. 480\)](#)
- [监控 IP 流量 \(p. 481\)](#)
- [在启动实例时连接网络接口 \(p. 481\)](#)
- [将网络接口连接至已停止的实例或正在运行的实例 \(p. 482\)](#)
- [将网络接口与实例分离 \(p. 482\)](#)
- [更改安全组 \(p. 483\)](#)
- [更改源/目标检查 \(p. 483\)](#)
- [关联弹性 IP 地址 \(IPv4\) \(p. 484\)](#)
- [取消关联弹性 IP 地址 \(IPv4\) \(p. 484\)](#)
- [分配 IPv6 地址 \(p. 485\)](#)
- [取消分配 IPv6 地址 \(p. 485\)](#)
- [更改终止行为 \(p. 485\)](#)
- [添加或编辑描述 \(p. 486\)](#)
- [添加或编辑标签 \(p. 486\)](#)

创建网络接口

您可以使用 Amazon EC2 控制台或命令行创建网络接口。

使用控制台创建网络接口

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择 Create Network Interface。
4. 对于 Description，输入一个描述性名称。
5. 对于 Subnet，选择子网。请注意，您不能在创建网络接口之后将其移动至另一子网，而且您只能将该接口附加到同一可用区中的实例。
6. 对于私有 IP (或 IPv4 私有 IP)，请输入主要私有 IPv4 地址。如果您未指定 IPv4 地址，我们将在所选子网中选择一个可用的 IPv4 地址。

7. (仅限 IPv6) 如果您选择了一个拥有相关联的 IPv6 CIDR 块的子网，那么可以选择性地在 IPv6 IP 字段中指定一个 IPv6 地址。
8. 对于 Security groups，选择一个或多个安全组。
9. 选择 Yes, Create。

使用命令行创建网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-network-interface](#) (AWS CLI)
- [New-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

删除网络接口

在删除网络接口之前，您必须先将其与实例分离。删除网络接口之后，所有与该接口关联的属性都会被释放，而且所有私有 IP 地址或弹性 IP 地址也都会被释放以供另一个实例使用。

您可以使用 Amazon EC2 控制台或命令行删除网络接口。

使用控制台删除网络接口

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择一个网络接口，然后选择删除。
4. 在 Delete Network Interface 对话框中，选择 Yes, Delete。

使用命令行删除网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [delete-network-interface](#) (AWS CLI)
- [Remove-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

查看有关网络接口的详细信息

您可以使用 Amazon EC2 控制台或命令行描述网络接口。

使用控制台描述网络接口

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口。
4. 在 Details (详细信息) 选项卡上查看详细信息。

使用命令行描述网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-network-interfaces](#) (AWS CLI)
- [Get-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行描述网络接口属性

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-network-interface-attribute](#) (AWS CLI)
- [Get-EC2NetworkInterfaceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

监控 IP 流量

您可以在网络接口上启用 VPC 流日志，以便收集有关出入该接口的 IP 流量的信息。创建流日志后，您可以在 Amazon CloudWatch Logs 中查看和检索其数据。

有关更多信息，请参阅 Amazon VPC 用户指南 中的 [VPC 流日志](#)。

在启动实例时连接网络接口

启动实例时，您可以指定一个现有的网络接口或连接其他网络接口。您可以使用 Amazon EC2 控制台或命令行执行此操作。

Note

如果在将网络接口连接至实例时发生错误，则会导致实例启动失效。

使用控制台在启动实例时连接网络接口

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 选择一个 AMI 和实例类型，然后选择 Next: Configure Instance Details。
4. 在 Configure Instance Details 页面上，为 Network 选择一个 VPC，为 Subnet 选择一个子网。
5. 在网络接口部分，控制台让您可以在启动实例时指定最多两个网络接口（新接口、现有接口或二者的组合）。对于任何新接口，您还可以输入一个主要 IPv4 地址和一个或多个辅助 IPv4 地址。

启动实例后，您可以将更多网络接口添加到该实例。您可以连接的网络接口总数因实例类型而有所差异。有关更多信息，请参阅 [每个实例类型的每个网络接口的 IP 地址 \(p. 474\)](#)。

Note

如果您指定了多个网络接口，则无法将公有 IPv4 地址自动分配给您的实例。

6. (仅限 IPv6) 如果您正在拥有相关联的 IPv6 CIDR 块的子网中启动实例，则可以为您附加的任何网络接口指定 IPv6 地址。在 IPv6 IPs 下，选择 Add IP。要添加一个辅助 IPv6 地址，请再次选择 Add IP。您可以输入子网范围内的 IPv6 地址，或保留默认值 Auto-assign，这样 Amazon 会从子网中为您选择一个 IPv6 地址。
7. 选择 Next: Add Storage。
8. 在 Add Storage 页面上，除了 AMI 指定的卷（如根设备卷）外，您可指定要挂载到实例的卷，然后选择 Next: Add Tags。
9. 在 Add Tags 页面上，为实例指定标签（例如，便于用户识别的名称），然后选择 Next: Configure Security Group。
10. 在 Configure Security Group 页面上，您可以选择一个安全组，也可以创建新的安全组。选择 Review and Launch。

Note

如果您在第 5 步指定了一个现有网络接口，实例将与该网络接口的安全组关联，无论您在此步骤中选择哪个选项。

11. Review Instance Launch (查看实例启动) 页面上会显示有关主要网络接口和其他网络接口的详细信息。检查设置，然后选择 Launch 以选择密钥对并启动实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

使用命令行在启动实例时连接网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

将网络接口连接至已停止的实例或正在运行的实例

您可以通过 Amazon EC2 控制台的 Instances (实例) 页面或 Network Interfaces (网络接口) 页面将网络接口连接至您的 VPC 中的任何一个已停止或正在运行的实例。

Note

如果您的实例上的公有 IPv4 地址已释放，并且有多个网络接口附加到实例，那么该实例不会收到新地址。有关公有 IPv4 地址行为的更多信息，请参阅 [公有 IPv4 地址和外部 DNS 主机名 \(p. 454\)](#)。

使用实例页面将网络接口连接到实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择 Actions、Networking、Attach Network Interface。
4. 在附加网络接口对话框中，选择网络接口，然后选择附加。

使用网络接口页面将网络接口连接到实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后选择附加。
4. 在 Attach Network Interface 对话框中，选择实例，然后选择 Attach。

使用命令行将网络接口连接到实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [attach-network-interface](#) (AWS CLI)
- [Add-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

将网络接口与实例分离

您可以随时使用 Amazon EC2 控制台的实例或网络接口页面，或使用命令行界面分离辅助网络接口。

使用实例页面将网络接口与实例断开

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择 Actions、Networking、Detach Network Interface。
4. 在分离网络接口对话框中，选择网络接口，然后选择分离。

使用网络接口页面将网络接口与实例断开

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后选择分离。
4. 在 Detach Network Interface 对话框中，选择 Yes, Detach。如果网络接口未能与实例分离，请选择 Force detachment，然后重试。

使用命令行断开网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [detach-network-interface](#) (AWS CLI)
- [Dismount-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

更改安全组

您可以更改与网络接口相关联的安全组。当您创建安全组时，请确保指定相同的 VPC 作为该接口的子网。

您可以使用 Amazon EC2 控制台或命令行更改网络接口的安全组。

Note

要更改其他服务（如 Elastic Load Balancing）所拥有的接口的安全组成员身份，请使用该服务的控制台或命令行界面。

使用控制台更改网络接口的安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和更改安全组。
4. 在 Change Security Groups 对话框中，选择要使用的安全组，然后选择 Save。

使用命令行更改网络接口的安全组

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

更改源/目标检查

源/目标检查属性用于控制源/目标检查是否已在实例上启用。禁用此属性后，实例会处理并未明确指定至该实例的网络通信。例如，运行网络地址转换、路由或防火墙等服务的实例应将此值设置为 disabled。默认值为 enabled。

您可以使用 Amazon EC2 控制台或命令行更改源/目标检查。

使用控制台更改网络接口的源/目标检查

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和 Change Source/Dest Check。
4. 在该对话框中，选择 Enabled（如果要启用）或 Disabled（如果要禁用），然后选择 Save。

使用命令行更改网络接口的源/目标检查

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

关联弹性 IP 地址 (IPv4)

如果您有弹性 IP 地址 (IPv4)，则可将其与网络接口的一个私有 IPv4 地址关联起来。您可以为每个私有 IPv4 地址关联一个弹性 IP 地址。

您可以使用 Amazon EC2 控制台或命令行关联弹性 IP 地址。

使用控制台关联弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和关联地址。
4. 在 Associate Elastic IP Address (关联弹性 IP 地址) 对话框中，从 Address (地址) 列表中选择弹性 IP 地址。
5. 对于 Associate to private IP address，选择要与弹性 IP 地址关联的私有 IPv4 地址。
6. 选择 Allow reassociation 以允许弹性 IP 地址在已与另一个实例或网络接口相关联的情况下与指定网络接口关联，然后选择 Associate Address。

使用命令行关联弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

取消关联弹性 IP 地址 (IPv4)

如果网络接口有一个与之关联的弹性 IP 地址 (IPv4)，您可以取消此地址的关联，然后将其与另一个网络接口关联或释放回地址池中。请注意，要通过网络接口将弹性 IP 地址与不同子网或 VPC 中的实例关联起来，这是唯一的方法，因为网络接口特定于每个单独的子网。

您可以使用 Amazon EC2 控制台或命令行取消关联弹性 IP 地址。

使用控制台取消关联弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和取消关联地址。
4. 在 Disassociate IP Address 对话框中，选择 Yes, Disassociate。

使用命令行取消关联弹性 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [disassociate-address](#) (AWS CLI)

- [Unregister-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

分配 IPv6 地址

您可以将一个或多个 IPv6 地址分配给一个网络接口。网络接口必须处于具有一个关联的 IPv6 CIDR 块的子网中。要将特定 IPv6 地址分配给网络接口，请确保该 IPv6 地址尚未分配给其他网络接口。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择网络接口，然后选择网络接口。
3. 依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择 Assign new IP。指定子网范围内的一个 IPv6 地址，或保留 Auto-assign 值，让 Amazon 为您选择。
5. 选择 Yes, Update。

使用命令行将 IPv6 地址分配给网络接口

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - [assign-ipv6-addresses](#) (AWS CLI)
 - [Register-EC2Ipv6AddressList](#) (适用于 Windows PowerShell 的 AWS 工具)

取消分配 IPv6 地址

您可以使用 Amazon EC2 控制台取消分配给网络接口 IPv6 地址。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择网络接口，然后选择网络接口。
3. 依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择要移动的 IPv6 地址对应的 Unassign。
5. 选择 Yes, Update。

使用命令行取消分配给网络接口的 IPv6 地址

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。
 - [unassign-ipv6-addresses](#) (AWS CLI)
 - [Unregister-EC2Ipv6AddressList](#) (适用于 Windows PowerShell 的 AWS 工具)

更改终止行为

您可设置附加到实例的网络接口的终止行为，以便在您删除其附加到的实例时自动删除该接口。

Note

默认情况下，使用控制台自动创建和连接至实例的网络接口会被设置为在实例终止时终止。但是使用命令行界面创建的网络接口不会被设置为在实例终止时终止。

您可以使用 Amazon EC2 控制台或命令行更改网络接口的终止行为。

使用控制台更改网络接口的终止行为

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和 Change Termination Behavior。
4. 如果您希望在您终止实例时删除网络接口，请在 Change Termination Behavior (更改终止操作) 对话框中选中 Delete on termination (终止时删除) 复选框。

使用命令行更改网络接口的终止行为

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

添加或编辑描述

您可以使用 Amazon EC2 控制台或命令行更改网络接口的描述。

使用控制台更改网络接口的描述

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后依次选择操作和 Change Description。
4. 在 Change Description 对话框中，输入对网络接口的描述，然后选择保存。

使用命令行更改网络接口的描述

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

添加或编辑标签

标签是您可以添加到网络接口的元数据。标签是私有的，只有您的账户可见。每一个标签都包含一个密钥和一个可选值。有关标签的更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 626\)](#)。

您可以使用 Amazon EC2 控制台或命令行标记资源。

使用控制台编辑或添加网络接口的标签

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口。
4. 在详细信息窗格中，选择 Tags、Add/Edit Tags。
5. 在 Add/Edit Tags 对话框中，对于每个要创建的标签选择 Create Tag，然后输入键和可选值。完成此操作后，选择 Save。

使用命令行添加或编辑网络接口的标签

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-tags](#) (AWS CLI)

- [New-EC2Tag](#) (适用于 Windows PowerShell 的 AWS 工具)

置放群组

置放群组是单个可用区中的实例的逻辑分组。建议将置放群组用于可受益于低网络延迟、高网络吞吐量或两者的应用程序。要为置放群组提供最低延迟和最高每秒数据包数的网络性能，请选择支持增强联网的实例类型。有关更多信息，请参阅[增强联网 \(p. 492\)](#)。

首先，您可创建置放群组，然后可将多个实例启动到该置放群组中。我们建议您在单个启动请求中启动置放群组中需要数量的实例，并对置放群组中的所有实例使用相同的实例类型。如果您以后尝试将更多实例添加到置放群组，或者如果您尝试在置放群组中启动多个实例类型，都会增大发生容量不足错误的可能性。

创建置放群组无需支付费用。

如果您停止置放群组中的某个实例，然后重启该实例，则其仍将在该置放群组中运行。但是，如果没有足够容量可用于该实例，则启动将会失败。

如果您在已有正在运行的实例的置放群组中启动实例时接收到容量错误信息，请在该置放群组中停止并启动所有实例，然后尝试再次启动。重启实例可能会将实例迁移至具有针对所有请求实例的容量的硬件。

内容

- [置放群组的限制 \(p. 487\)](#)
- [将实例启动到置放群组中 \(p. 488\)](#)
- [删除置放群组 \(p. 489\)](#)

置放群组的限制

置放群组有以下限制：

- 置放群组不可跨越多个可用区。
- 您为置放群组指定的名称在您的 AWS 账户中必须是唯一的。
- 将实例启动到置放群组中时，仅可使用以下实例类型：
 - 通用型: m4.large | m4.xlarge | m4.2xlarge | m4.4xlarge | m4.10xlarge | m4.16xlarge
 - 计算优化: c4.large | c4.xlarge | c4.2xlarge | c4.4xlarge | c4.8xlarge | c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge | cc2.8xlarge
 - 内存优化: cr1.8xlarge | r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge | r4.large | r4.xlarge | r4.2xlarge | r4.4xlarge | r4.8xlarge | r4.16xlarge | x1.16xlarge | x1.32xlarge
 - 存储优化: d2.xlarge | d2.2xlarge | d2.4xlarge | d2.8xlarge | hi1.4xlarge | hs1.8xlarge | i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge | i3.large | i3.xlarge | i3.2xlarge | i3.4xlarge | i3.8xlarge | i3.16xlarge
 - 加速的计算 : cg1.4xlarge | g2.2xlarge | g2.8xlarge | p2.xlarge | p2.8xlarge | p2.16xlarge
- 放置组中的两个实例之间的最大网络吞吐量流速受两个实例的较慢者限制。对于具有高吞吐量要求的应用程序，请选择具有 10 Gbps 或 20 Gbps 网络连接的实例类型。有关实例类型网络性能的更多信息，请参阅[Amazon EC2 实例类型矩阵](#)。
- 虽然可以将多个实例类型启动到一个置放群组中，但这会减小提供成功启动所需容量的可能性。我们建议对一个置放群组中的所有实例使用相同的实例类型。
- 不能合并置放群组。您必须在一个置放群组中终止相关实例，然后在另一个置放群组中重新启动这些实例。
- 置放群组可跨越多个对等 VPC，但是，您不会在对等 VPC 实例之间获取全部的等分带宽。有关 VPC 对等连接的更多信息，请参阅[Amazon VPC Peering Guide](#)。

- 您不能将现有实例移动到置放群组中。您可以从现有实例创建 AMI，然后通过该 AMI 在置放群组中启动新实例。
- 预留实例可为可用区中的 EC2 实例提供容量预留。容量预留可供置放群组中分配到同一可用区的实例使用。但是，您无法为置放群组显式预留容量。
- 为确保网络流量处于置放群组内，置放群组的成员必须通过其私有 IPv4 地址或 IPv6 地址（如果适用）相互寻址。如果成员使用公有 IPv4 地址相互寻址，则吞吐量将降到 5Gbps 或更低。
- 置放群组外部资源间的网络流量限制为 5 Gbps。

将实例启动到置放群组中

我们建议您专门为要启动到置放群组中的实例创建一个 AMI。

使用控制台将实例启动到置放群组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 为您的实例创建一个 AMI。
 - a. 从 Amazon EC2 控制面板中，选择 Launch Instance。在完成向导后，选择 Launch。
 - b. 连接到您的实例。（有关更多信息，请参阅[连接到您的 Linux 实例 \(p. 252\)](#)。）
 - c. 在实例上安装软件和应用程序、复制数据或附加更多 Amazon EBS 卷。
 - d. （可选）如果您的实例类型支持增强联网，请通过执行[Linux 上的增强联网 \(p. 492\)](#)中的过程确保启用此功能。
 - e. 在导航窗格中，选择 Instances，选择您的实例，然后选择 Actions、Image、Create Image。提供 Create Image 对话框所请求的信息，然后选择 Create Image。
 - f. （可选）如果您无需进一步使用，则可终止该实例。
3. 创建置放群组。
 - a. 在导航窗格中，选择 Placement Groups。
 - b. 选择 Create Placement Group。
 - c. 在 Create Placement Group 对话框中，提供置放群组名称（该名称在您使用的 AWS 账户中是唯一的），然后选择 Create。

当置放群组的状态为 available 时，您可将实例启动到该置放群组中。

4. 将您的实例启动到置放群组。
 - a. 在导航窗格中，选择 Instances。
 - b. 选择 Launch Instance。按指示完成向导，注意执行以下操作：
 - 在 Choose an Amazon Machine Image (AMI) 页面上，选择 My AMIs 选项卡，然后选择创建的 AMI。
 - 在 Choose an Instance Type 页面上，选择可以启动到置放群组中的实例类型。
 - 在 Configure Instance Details 页面上，输入您需要放在此置放群组中的实例总数，因为您以后可能无法将实例添加到置放群组。
 - 在 Configure Instance Details 页面上，选择您从 Placement group 创建的置放群组。如果您在此页面上没有看到 Placement group 列表，请确保您选择了可启动到置放群组的实例类型，否则该选项会不可用。

使用命令行将实例启动到置放群组

1. 使用以下命令之一为实例创建 AMI：

- `create-image` (AWS CLI)

- [New-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)
2. 使用以下命令之一创建置放群组：
 - [create-placement-group](#) (AWS CLI)
 - [New-EC2PlacementGroup](#) (适用于 Windows PowerShell 的 AWS 工具)
 3. 使用以下选项之一将实例启动到置放群组：
 - `--placement` 与 [run-instances](#) (AWS CLI)
 - `-PlacementGroup` 与 [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

删除置放群组

如果您需要替换或不再需要置放群组，您可以删除置放群组。在删除置放群组前，您必须终止启动到该置放群组中的所有实例。

使用控制台删除置放群组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择并终止置放群组中的所有实例。(在终止实例前，您可通过检查详细信息窗格中的 Placement Group 值来验证该实例是否位于相关置放群组中。)
4. 在导航窗格中，选择 Placement Groups。
5. 选择置放群组，然后选择 Delete Placement Group。
6. 当系统提示进行确认时，选择 Yes, Delete。

使用命令行删除置放群组

您可以使用以下任一命令集。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [terminate-instances](#) 和 [delete-placement-group](#) (AWS CLI)
- [Stop-EC2Instance](#) 和 [Remove-EC2PlacementGroup](#); (适用于 Windows PowerShell 的 AWS 工具)

EC2 实例的网络最大传输单位 (MTU)

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小 (以字节为单位)。连接的 MTU 越大，可在单个数据包中传递的数据越多。以太网数据包由帧 (或您发送的实际数据) 和围绕它的网络开销信息组成。

以太网帧有不同的格式，最常见的格式是标准以太网 v2 帧格式。它支持 1500 MTU，它是通过大部分 Internet 支持的最大以太网数据包大小。实例支持的最大 MTU 取决于其实例类型。所有 Amazon EC2 实例类型都支持 1500 MTU，并且当前很多实例大小都支持 9001 MTU 或极大帧。

内容

- [极大帧 \(9001 MTU\) \(p. 490\)](#)
- [路径 MTU 发现 \(p. 490\)](#)
- [查看两台主机之间的路径 MTU \(p. 490\)](#)
- [在您的 Amazon EC2 实例上检查并设置 MTU \(p. 491\)](#)
- [故障排除 \(p. 492\)](#)

极大帧 (9001 MTU)

极大帧通过增加每个数据包的负载大小，从而增加数据包中不属于数据包开销的百分比来支持 1500 个字节以上的数据。发送等量的可用数据所需要的数据包更少。但在给定 AWS 区域 (EC2-Classic)、单一 VPC 或 VPC 对等连接的外部，您将遇到的最大路径为 1500 MTU。VPN 连接和通过 Internet 网关发送的流量限制为 1500 MTU。如果数据包大于 1500 字节，则对数据包进行分片；如果在 IP 标头中设置了 `Don't Fragment` 标志，则丢弃数据包。

不应将极大帧用于 Internet 绑定的流量或离开 VPC 的任何流量。中间系统会对数据包进行分片，从而减缓此流量。要使用 VPC 中的极大帧而不减慢 VPC 外部的绑定流量的速度，您可按路由配置 MTU 大小，或者将弹性网络接口与不同 MTU 大小和不同路由结合使用。

对于在一个置放群组中并置的实例，极大帧可帮助达到可能的最大网络吞吐量，因此建议在这种情况下使用。有关更多信息，请参阅 [置放群组 \(p. 487\)](#)。

以下实例支持极大帧：

- 计算已优化：C3、C4、CC2
- 通用型：M3、M4、T2
- 加速计算：CG1、G2、P2
- 内存优化型：CR1、R3、R4、X1
- 存储已优化：D2、HI1、HS1、I2、I3

路径 MTU 发现

路径 MTU 发现用于确定两台设备之间的路径 MTU。路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机或设备将返回以下 ICMP 消息：`Destination Unreachable: Fragmentation Needed and Don't Fragment was Set`(类型 3，代码 4)。这指示原始主机调整 MTU，直到可以传输数据包。

默认情况下，安全组不允许任何入站 ICMP 流量。要确保您的实例可以收到此消息并且数据包不会丢失，您必须将具有无法访问目标协议的自定义 ICMP 规则添加到您实例的入站安全组规则。有关更多信息，请参阅 Amazon EC2 安全组主题中的 [向安全组添加规则 \(p. 359\)](#) 和 [API 和命令概览 \(p. 360\)](#) 部分。

Important

将您实例的安全组修改为允许路径 MTU 发现不能保证极大帧不会被某些路由器忽略。您 VPC 中的 Internet 网关仅将转发最多 1500 字节的数据包。建议对 Internet 流量使用 1500 MTU 数据包。

查看两台主机之间的路径 MTU

您可使用 `tracepath` 命令查看两台主机之间的路径 MTU，此命令是许多 Linux 分发默认情况下提供的 `iputils` 数据包的一部分，包括您可从 <http://www.elifulkerson.com/projects/mturoute.php> 下载并安装的 Amazon Linux。

使用 `tracepath` 查看路径 MTU

- 使用以下命令查看您的 Amazon EC2 实例和另一台主机之间的路径 MTU。您可以使用 DNS 名称或 IP 地址作为目标；此示例将查看 EC2 实例和 `amazon.com` 之间的路径 MTU。

```
[ec2-user ~]$ tracepath amazon.com
 1?: [LOCALHOST]      pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)    0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
```

```
4: 100.64.16.241 (100.64.16.241)          0.574ms
5: 72.21.222.221 (72.21.222.221)          84.447ms asymm 21
6: 205.251.229.97 (205.251.229.97)        79.970ms asymm 19
7: 72.21.222.194 (72.21.222.194)          96.546ms asymm 16
8: 72.21.222.239 (72.21.222.239)          79.244ms asymm 15
9: 205.251.225.73 (205.251.225.73)        91.867ms asymm 16
...
31: no reply
    Too many hops: pmtu 1500
    Resume: pmtu 1500
```

在此示例中，路径 MTU 为 1500。

Note

如果要对另一个 Amazon EC2 实例使用 `tracepath`，您可能需要检查该实例的安全组规则是否允许入站 UDP 流量。

在您的 Amazon EC2 实例上检查并设置 MTU

一些 AMI 配置为在实例上使用支持 AMI 的极大帧，另一些 AMI 配置为使用标准帧大小。您可能希望将极大帧用于您的 VPC 内的网络流量，或希望将标准帧用于 Internet 流量。无论您的使用案例如何，我们建议验证您的实例是否会按您的预期运行。您可以使用本部分中的过程查看您的网络接口的 MTU 设置并按需对其进行修改。

查看 Linux 实例上的 MTU 设置

- 如果您的实例使用的是 Linux 操作系统，则可使用 `ip` 命令查看 MTU 值。运行以下命令可确定当前 MTU 值：

```
[ec2-user ~]$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
    DEFAULT group default qlen 1000
        link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

在以上示例中，输出中的 `mtu 9001` 指示此实例使用极大帧。

在 Linux 实例上设置 MTU 值

- 如果您的实例使用的是 Linux 操作系统，则可使用 `ip` 命令设置 MTU 值。运行以下命令以设置所需的 MTU 值。此过程将 MTU 设置为 1500，9001 的设置过程与此相同。

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

- (可选) 要在重启后保留您的网络 MTU 设置，请根据您的操作系统类型修改配置文件。此过程适用于 Amazon Linux 和 Ubuntu；对于其他分发版本，请参阅其特定文档。

- 对于 Amazon Linux，请将下列行添加到您的 `/etc/dhcp/dhclient-eth0.conf` 文件。

```
interface "eth0" {
    supersede interface-mtu 1500;
}
```

- 对于 Ubuntu，请将下列行添加到 `/etc/network/interfaces.d/eth0.cfg`。

```
post-up /sbin/ifconfig eth0 mtu 1500
```

- (可选) 重启实例并验证 MTU 设置是否正确。

故障排除

如果在使用极大顿时您的 EC2 实例和 Amazon Redshift 群集之间出现连接问题，请参阅 Amazon Redshift Cluster Management Guide 中的[查询挂起](#)

Linux 上的增强联网

增强联网使用单个根 I/O 虚拟化 (SR-IOV) 在[支持的实例类型 \(p. 492\)](#)上提供高性能的联网功能。SR-IOV 是一种设备虚拟化方法，与传统虚拟化网络接口相比，它不仅能提高 I/O 性能，还能降低 CPU 利用率。增强联网可以提高带宽，提高每秒数据包数 (PPS) 性能，并不断降低实例间的延迟。使用增强联网不收取任何额外费用。

内容

- [增强联网类型 \(p. 492\)](#)
- [在实例上启用增强联网 \(p. 492\)](#)
- [在 VPC 中的 Linux 实例上启用 Intel 82599 VF 接口增强联网 \(p. 492\)](#)
- [在 VPC 中的 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 501\)](#)
- [对 Elastic Network Adapter \(ENA\) 进行故障排除 \(p. 509\)](#)

增强联网类型

根据您的实例类型，可以使用以下机制之一启用增强联网：

Intel 82599 虚拟功能 (VF) 接口

对于受支持的实例类型，Intel 82599 虚拟功能接口支持高达 10 Gbps 的网络速度。

C3、C4、D2、I2、R3、和 M4 (`m4.16xlarge` 除外) 实例使用 Intel 82599 VF 接口实现增强联网。要了解哪些实例类型支持 10 Gbps 网络速度，请参阅[实例类型矩阵](#)。

Elastic Network Adapter (ENA)

对于支持的实例类型，弹性网络适配器 (ENA) 支持高达 20 Gbps 的网络速度。

I3、P2、R4、X1 和 `m4.16xlarge` 实例使用 Elastic Network Adapter 实现增强联网。要了解哪些实例类型支持 20 Gbps 网络速度，请参阅[实例类型矩阵](#)。

在实例上启用增强联网

如果您的实例类型支持使用 Intel 82599 VF 接口实现增强联网，请执行[在 VPC 中的 Linux 实例上启用 Intel 82599 VF 接口增强联网 \(p. 492\)](#)中的步骤。

如果您的实例类型支持使用 Elastic Network Adapter 实现增强联网，请执行[在 VPC 中的 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 501\)](#)中的步骤。

在 VPC 中的 Linux 实例上启用 Intel 82599 VF 接口增强联网

Amazon EC2 通过使用 Intel `ixgbevf` 驱动程序的 Intel 82599 VF 接口向 C3、C4、D2、I2、R3、和 M4 (`m4.16xlarge` 除外) 实例提供增强联网功能。

要准备 Intel 82599 VF 接口增强联网，请按如下方式设置您的实例：

- 从使用 Linux 内核版本 2.6.32 或更高版本的 HVM AMI 启动实例。最新的 Amazon Linux HVM AMI 安装有增强联网所需的模块，并已设置所需的属性。因此，如果使用最新的 Amazon Linux HVM AMI 启动由 Amazon EBS 提供支持且支持增强联网的实例，则已为您的实例启用增强联网。
- 在 VPC 中启动实例。(如果实例在 EC2-Classic 中，则您不能启用增强联网功能。)
- 将 [AWS CLI](#) 或 [适用于 Windows PowerShell 的 AWS 工具](#) 安装到您选择的任意计算机上(最好是您的本地台式计算机或笔记本电脑)并进行配置。有关更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留，则应立即从您的实例创建 AMI，来备份这些数据。更新内核和内核模块以及启用 `sriovNetSupport` 属性可能会导致实例不兼容或操作系统无法访问；如果您有最新备份，则可在发生这种情况时保留数据。

内容

- [测试是否启用了 Intel 82599 VF 接口增强联网 \(p. 493\)](#)
- [在 Amazon Linux 上启用 Intel 82599 VF 接口增强联网 \(p. 495\)](#)
- [在 Ubuntu 上启用 Intel 82599 VF 接口增强联网 \(p. 496\)](#)
- [在其他 Linux 发行版上启用 Intel 82599 VF 接口增强联网 \(p. 499\)](#)
- [排除连接问题 \(p. 501\)](#)

测试是否启用了 Intel 82599 VF 接口增强联网

要测试是否已启用 Intel 82599 VF 接口增强联网，请验证实例上已安装 `ixgbevf` 模块，且设置了 `sriovNetSupport` 属性。如果实例满足这两个条件，则 `ethtool -i ethn` 命令应显示该模块已在网络接口上使用。

内核模块 (`ixgbevf`)

若要验证是否已安装 `ixgbevf` 模块以及版本是否与增强联网兼容，请使用 `modinfo` 命令，如下所示：

```
[ec2-user ~]$ modinfo ixgbevf
filename:      /lib/modules/3.10.48-55.140.amzn1.x86_64/kernel/drivers/amazon/ixgbevf/
ixgbevf.ko
version:       2.14.2
license:        GPL
description:   Intel(R) 82599 Virtual Function Driver
author:         Intel Corporation, <linux.nics@intel.com>
srcversion:    50CBF6F36B99FE70E56C95A
alias:          pci:v00008086d00001515sv*sd*bc*sc*i*
alias:          pci:v00008086d000010EDsv*sd*bc*sc*i*
depends:
intree:        Y
vermagic:      3.10.48-55.140.amzn1.x86_64 SMP mod_unload modversions
parm:          InterruptThrottleRate:Maximum interrupts per second, per vector,
(956-488281, 0=off, 1=dynamic), default 1 (array of int)
```

在以上 Amazon Linux 示例中，`ixgbevf` 模块已安装，并为推荐的最低版本 (2.14.2)。

```
ubuntu:~$ modinfo ixgbevf
filename:      /lib/modules/3.13.0-29-generic/kernel/drivers/net/ethernet/intel/ixgbevf/
ixgbevf.ko
version:       2.11.3-k
license:        GPL
description:   Intel(R) 82599 Virtual Function Driver
author:         Intel Corporation, <linux.nics@intel.com>
srcversion:    0816EA811025C8062A9C269
alias:          pci:v00008086d00001515sv*sd*bc*sc*i*
alias:          pci:v00008086d000010EDsv*sd*bc*sc*i*
```

```
depends:  
intree: Y  
vermagic: 3.13.0-29-generic SMP mod_unload modversions  
signer: Magrathea: Glacier signing key  
sig_key: 66:02:CB:36:F1:31:3B:EA:01:C4:BD:A9:65:67:CF:A7:23:C9:70:D8  
sig_hashalgo: sha512  
parm: debug:Debug level (0=none,...,16=all) (int)
```

在以上 Ubuntu 实例中，该模块已安装，但版本是 2.11.3-k，该版本不包含推荐版本 2.14.2 所包含的最新错误修复。在这种情况下，虽然 ixgbevf 模块会正常运行，但仍可以在实例上安装并加载新版本以获得最佳体验。

实例属性 (srivNetSupport)

要检查实例是否设置了增强联网 srivNetSupport 属性，请使用以下任一命令：

- [describe-instance-attribute](#) (AWS CLI)

```
aws ec2 describe-instance-attribute --instance-id instance-id --attribute srivNetSupport
```

- [Get-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute srivNetSupport
```

如果此属性未设置，则 SrivNetSupport 为空；否则，设置如下：

```
"SrivNetSupport": {  
    "Value": "simple"  
},
```

映像属性 (srivNetSupport)

要检查 AMI 是否设置了增强联网 srivNetSupport 属性，请使用以下任一命令：

- [describe-image-attribute](#) (AWS CLI)

```
aws ec2 describe-image-attribute --image-id ami-id --attribute srivNetSupport
```

请注意，此命令仅适用于您拥有的映像。对于不属于您账户的映像，您会收到 AuthFailure 错误。

- [Get-EC2ImageAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Get-EC2ImageAttribute -ImageId ami-id -Attribute srivNetSupport
```

如果此属性未设置，则 SrivNetSupport 为空；否则，设置如下：

```
"SrivNetSupport": {  
    "Value": "simple"  
},
```

网络接口驱动程序

使用以下命令验证模块是否在特定接口上使用 (替换为要检查的接口的名称)。如果您使用单个接口 (默认设置)，则它是 eth0。

```
[ec2-user ~]$ ethtool -i eth0
```

```
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

在上例中，ixgbevf 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 2.14.2
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

在此例中，ixgbevf 模块进行加载并具有推荐的最低版本。此实例正确配置了增强联网。

在 Amazon Linux 上启用 Intel 82599 VF 接口增强联网

最新的 Amazon Linux HVM AMI 安装有增强联网所需的 ixgbevf 模块，并已设置所需的 sriovNetSupport 属性。因此，如果您使用最新的 Amazon Linux HVM AMI 启动 C3、C4、D2、I2、R3、或 M4 (m4.16xlarge 除外) 实例，则您的实例已经支持增强联网功能。有关更多信息，请参阅 [测试是否启用了 Intel 82599 VF 接口增强联网 \(p. 493\)](#)。

如果您使用较旧的 Amazon Linux AMI 启动了实例，并且实例尚未启用增强联网，请通过以下步骤启用增强联网。

启用增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 从实例运行以下命令以使用最新内核和内核模块（包括 ixgbevf）更新实例：

```
[ec2-user ~]$ sudo yum update
```

3. 使用 Amazon EC2 控制台或以下任一命令从本地计算机重新启动实例：[reboot-instances](#) (AWS CLI)，[Restart-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。
4. 再次连接到您的实例，并使用 [测试是否启用了 Intel 82599 VF 接口增强联网 \(p. 493\)](#) 中的 modinfo ixgbevf 命令验证 ixgbevf 模块是否已安装并具有推荐的最低版本。
5. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：[stop-instances](#) (AWS CLI)，[Stop-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续启用增强联网（[实例存储支持的实例](#)）(p. 496)。

6. 使用以下任一命令从本地计算机启用增强联网属性。

Warning

增强联网属性启用之后将无法禁用。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute \(AWS CLI\)](#)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

- [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (可选) 从实例创建 AMI , 如 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 中所述。该 AMI 从实例继承增强联网属性。因此 , 您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。
8. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例 : [start-instances \(AWS CLI\)](#) , [Start-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)。如果您的实例由 AWS OpsWorks 管理 , 则应在 AWS OpsWorks 控制台中启动该实例 , 以便使实例状态保持同步。
9. 连接到您的实例 , 并使用[测试是否启用了 Intel 82599 VF 接口增强联网 \(p. 493\)](#)中的 `ethtool -i ethn` 命令验证是否在网络接口上安装并加载了 `ixgbevf` 模块。

启用增强联网 (实例存储支持的实例)

如果实例是实例存储支持的实例 , 请执行上一过程中的 [Step 1 \(p. 495\)](#) 到 [Step 4 \(p. 495\)](#) , 然后创建新 AMI (如 [创建由实例存储支持的 Linux AMI \(p. 78\)](#) 中所述)。在注册 AMI 时 , 请确保启用增强联网属性。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --sriov-net-support simple ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

在 Ubuntu 上启用 Intel 82599 VF 接口增强联网

以下过程提供在 Ubuntu 实例上启用 Intel 82599 VF 接口增强联网时将执行的一般步骤。

在 Ubuntu 上启用增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 更新包缓存和包。

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y
```

Important

如果在更新过程中系统提示您安装 grub , 请使用 `/dev/xvda` 安装 grub , 然后选择保留当前版本的 `/boot/grub/menu.lst`。

3. 安装 dkms 包 , 以便每次更新内核时都会重建 `ixgbevf` 模块。

```
ubuntu:~$ sudo apt-get install -y dkms
```

4. 将 ixgbevf 模块的版本 2.16.4 源代码从 Sourceforge (<http://sourceforge.net/projects/e1000/files/ixgbevf%20stable/>) 下载到您的实例上。

请注意，ixgbevf 的早期版本（包括最低推荐版本 2.14.2）在某些 Ubuntu 版本上构建不正确。Ubuntu 实例应使用 ixgbevf 2.16.4 版。

```
ubuntu:~$ wget "sourceforge.net/projects/e1000/files/ixgbevf_stable/2.16.4/ixgbevf-2.16.4.tar.gz"
```

5. 解压缩并解档 ixgbevf 包。

```
ubuntu:~$ tar -xzf ixgbevf-2.16.4.tar.gz
```

6. 将 ixgbevf 包移动到 /usr/src/ 目录，以便 dkms 可以在每次内核更新中找到并构建该模块。

```
ubuntu:~$ sudo mv ixgbevf-2.16.4 /usr/src/
```

7. 使用以下值创建 dkms 配置文件（替换为您的 ixgbevf 版本）。

- a. 创建文件。

```
ubuntu:~$ sudo touch /usr/src/ixgbevf-2.16.4/dkms.conf
```

- b. 编辑文件并添加以下值。

```
ubuntu:~$ sudo vim /usr/src/ixgbevf-2.16.4/dkms.conf
PACKAGE_NAME="ixgbevf"
PACKAGE_VERSION="2.16.4"
CLEAN="cd src/; make clean"
MAKE="cd src/; make BUILD_KERNEL=${kernelver}"
BUILT_MODULE_LOCATION[0]="/src/"
BUILT_MODULE_NAME[0]="ixgbevf"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ixgbevf"
AUTOINSTALL="yes"
```

8. 使用 dkms 在实例上添加、构建并安装 ixgbevf 模块。

- a. 将该模块添加到 dkms。

```
ubuntu:~$ sudo dkms add -m ixgbevf -v 2.16.4
```

- b. 使用 dkms 构建该模块。

```
ubuntu:~$ sudo dkms build -m ixgbevf -v 2.16.4
```

- c. 使用 dkms 安装该模块。

```
ubuntu:~$ sudo dkms install -m ixgbevf -v 2.16.4
```

9. 重新构建 initramfs，以便在启动时加载正确的模块。

```
ubuntu:~$ sudo update-initramfs -c -k all
```

10. 使用## modinfo ixgbevf 命令验证 ixgbevf 测试是否启用了 Intel 82599 VF 接口增强联网 (p. 493) 模块是否已安装并具有推荐的最低版本。

```
ubuntu:~$ modinfo ixgbevf
```

```
filename:      /lib/modules/3.13.0-74-generic/updates/dkms/ixgbevf.ko
version:       2.16.4
license:        GPL
description:   Intel(R) 10 Gigabit Virtual Function Network Driver
author:        Intel Corporation, <linux.nics@intel.com>
srcversion:    759A432E3151C8F9F6EA882
alias:         pci:v00008086d0001515sv*sd*bc*sc*i*
alias:         pci:v00008086d000010EDsv*sd*bc*sc*i*
depends:
vermagic:     3.13.0-74-generic SMP mod_unload modversions
parm:          InterruptThrottleRate:Maximum interrupts per second, per vector,
(956-488281, 0=off, 1=dynamic), default 1 (array of int)
```

11. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例 : [stop-instances](#) (AWS CLI) , [Stop-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续在 [Ubuntu 上启用增强联网 \(实例存储支持的实例\) \(p. 498\)](#)。

12. 使用以下任一命令从本地计算机启用增强联网 `sriovNetSupport` 属性。请注意，此属性启用之后将无法禁用。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

13. (可选) 从实例创建 AMI，如 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 中所述。该 AMI 从实例继承增强联网 `sriovNetSupport` 属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。
14. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例 : [start-instances](#) (AWS CLI) , [Start-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
15. (可选) 连接到实例并确认已安装模块。

在 Ubuntu 上启用增强联网 (实例存储支持的实例)

如果实例是实例存储支持的实例，请执行上一过程中的 [Step 1 \(p. 496\)](#) 到 [Step 10 \(p. 497\)](#)，然后创建新 AMI (如[创建由实例存储支持的 Linux AMI \(p. 78\)](#)中所述)。在注册 AMI 时，请确保启用增强联网属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --sriov-net-support simple ...
```

- Register-EC2Image (适用于 Windows PowerShell 的 AWS 工具)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

在其他 Linux 发行版上启用 Intel 82599 VF 接口增强联网

下面的过程提供在 Amazon Linux 或 Ubuntu 之外的 Linux 发行版上启用 Intel 82599 VF 接口增强联网时将执行的一般步骤。有关更多信息 (如命令的详细语法、文件位置或包和工具支持)，请参阅您的 Linux 分发版的特定文档。

在 Linux 上启用增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 将 ixgbevf 模块的版本 2.14.2 源代码从 Sourceforge (<http://sourceforge.net/projects/e1000/files/ixgbevf%20stable/>) 下载到您的实例上。这是为增强联网推荐的最低版本。

早期版本的 ixgbevf (包括最低推荐版本 2.14.2) 在某些 Linux 发行版 (包括某些 Ubuntu 版本) 上构建不正确。如果您收到构建错误，可以尝试较新版本，如 2.16.4 (该版本修复了受影响的 Ubuntu 版本上的构建问题)。

3. 在实例上编译并安装 ixgbevf 模块。

如果您的分发版支持 dkms，则应考虑配置 dkms 以便在每次更新系统内核时重新编译 ixgbevf 模块。如果您的分发版自身不支持 dkms，则可以在用于 Red Hat Enterprise Linux 各版本的 EPEL 存储库 (<https://fedoraproject.org/wiki/EPEL>) 中找到它，也可以到 <http://linux.dell.com/dkms/> 下载该软件。使用 [在 Ubuntu 上启用增强联网 \(EBS 支持的实例\) \(p. 496\)](#) 中 Step 6 (p. 497) 到 Step 8 (p. 497) 帮助配置 dkms。

Warning

如果您为当前内核编译 ixgbevf 模块，然后升级内核而不为新内核重建驱动程序，则系统会在下次重新启动时恢复为特定于分发版的 ixgbevf 模块，这可能会在特定于分发版的版本与增强联网不兼容时使您的系统无法访问。

4. 运行 sudo depmod 命令以更新模块依赖项。
5. 在实例上更新 initramfs 以确保在启动时加载新模块。
6. 确定您的系统是否默认使用可预测的网络接口名称。使用 systemd 或 udev 版本 197 或更高版本的系统可以重命名以太网设备，它们不保证单个网络接口将命名为 eth0。此行为可能导致连接到实例时出现问题。要获取更多信息并查看其他配置选项，请参阅 freedesktop.org 网站上的[可预测的网络接口名称](#)。

- a. 您可以使用以下命令在基于 RPM 的系统上检查 systemd 或 udev 版本：

```
[ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]+\+|^udev-[0-9]+\+'  
systemd-208-11.el7_0.2.x86_64
```

在以上 Red Hat 7 示例中，systemd 版本是 208，因此必须禁用可预测的网络接口名称。

- b. 通过将 net.ifnames=0 选项添加到 GRUB_CMDLINE_LINUX/etc/default/grub ## 行，禁用可预测的网络接口名称。

```
[ec2-user ~]$ sudo sed -i '/^GRUB_CMDLINE_LINUX/s/^$/ net.ifnames=0/' /etc/default/grub
```

- c. 重新构建 grub 配置文件。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例 : [stop-instances](#) (AWS CLI) , [Stop-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续启用增强联网 (实例存储支持的实例) ([p. 500](#))。

8. 使用以下任一命令从本地计算机启用增强联网属性。请注意，联网属性启用之后将无法禁用。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

9. (可选) 从实例创建 AMI，如 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 中所述。该 AMI 从实例继承增强联网属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。

Important

如果您的实例操作系统包含 `/etc/udev/rules.d/70-persistent-net.rules` 文件，在创建 AMI 前必须将其删除。此文件包含原始实例的以太网适配器 MAC 地址。如果其他实例使用此文件启动，操作系统将找不到设备，`eth0` 会失败，从而导致启动问题。此文件将在下次启动过程中重新生成，从 AMI 启动的任意实例都会创建这个文件的自有版本。

10. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例 : [start-instances](#) (AWS CLI) , [Start-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
11. (可选) 连接到实例并确认已安装模块。

启用增强联网 (实例存储支持的实例)

如果实例是实例存储支持的实例，请执行上一过程中的 [Step 1 \(p. 499\)](#) 到 [Step 5 \(p. 499\)](#)，然后创建新 AMI (如 [创建由实例存储支持的 Linux AMI \(p. 78\)](#) 中所述)。在注册 AMI 时，请确保启用增强联网属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --sriov-net-support simple ...
```

- [Register-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

排除连接问题

如果您在启用增强联网期间丢失连接，则 `ixgbevf` 模块可能与内核不兼容。请尝试安装用于您实例的 Linux 分发版所附带的 `ixgbevf` 模块版本。

如果您为半虚拟化实例或 AMI 启用增强网络，则这可能会使您的实例无法访问。

在 VPC 中的 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网

要准备 ENA 网络适配器增强联网，请按如下方式设置您的实例：

- 从使用 Linux 内核版本 3.2 或更高版本的 HVM AMI 启动实例。最新的 Amazon Linux HVM AMI 安装有增强联网所需的模块，并已设置所需的属性。因此，如果使用最新的 Amazon Linux HVM AMI 启动由 Amazon EBS 提供支持且支持增强联网的实例，则已为您的实例启用 ENA 增强联网。
- 在 VPC 中启动实例。(如果实例在 EC2-Classic 中，则您不能启用增强联网功能。)
- 将 [AWS CLI](#) 或 [适用于 Windows PowerShell 的 AWS 工具](#) 安装到您选择的任意计算机上(最好是您的本地台式计算机或笔记本电脑)并进行配置。有关更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留，则应立即从您的实例创建 AMI，来备份这些数据。更新内核和内核模块以及启用 `enaSupport` 属性可能会导致实例不兼容或操作系统无法访问；如果您有最新备份，则可在发生这种情况时保留数据。

内容

- [测试是否启用了 ENA 增强联网 \(p. 501\)](#)
- [在 Amazon Linux 上启用 ENA 增强联网 \(p. 503\)](#)
- [在 Ubuntu 上启用 ENA 增强联网 \(p. 504\)](#)
- [在其他 Linux 发行版上启用 ENA 增强联网 \(p. 507\)](#)
- [故障排除 \(p. 509\)](#)

测试是否启用了 ENA 增强联网

要测试是否已启用 ENA 增强联网，请验证实例上已安装 `ena` 模块，且设置了 `enaSupport` 属性。如果实例满足这两个条件，则 `ethtool -i ethn` 命令应显示该模块已在网络接口上使用。

内核模块 (`ena`)

要验证是否已安装 `ena` 模块，请使用 `modinfo` 命令，如下所示：

```
[ec2-user ~]$ modinfo ena
filename:      /lib/modules/4.4.11-23.53.amzn1.x86_64/kernel/drivers/amazon/net/ena/ena.ko
version:       0.6.6
license:        GPL
description:   Elastic Network Adapter (ENA)
author:        Amazon.com, Inc. or its affiliates
srcversion:    3141E47566402C79D6B8284
alias:         pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:         pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:         pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:         pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
intree:
```

```
vermagic:      4.4.11-23.53.amzn1.x86_64 SMP mod_unload modversions
parm:          debug:Debug level (0=none,...,16=all) (int)
parm:          push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:          enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:          enable_missing_tx_detection:Enable missing Tx completions. (default=1)
    (int)
parm:          numa_node_override_array:Numa node override map
    (array of int)
parm:          numa_node_override:Enable/Disable numa node override (0=disable)
    (int)
```

在上述 Amazon Linux 情况中，ena 模块已安装。

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

在上述 Ubuntu 实例中，此模块未安装，因此您必须首先安装它。有关更多信息，请参阅 [在 Ubuntu 上启用 ENA 增强联网 \(p. 504\)](#)。

实例属性 (enaSupport)

要检查实例是否设置了增强联网 enaSupport 属性，请使用以下任一命令。如果该属性已设置，则响应为 true。

- [describe-instances](#) (AWS CLI)

```
aws ec2 describe-instances --instance-id instance_id --query
'Reservations[].[Instances[]].EnaSupport'
```

- [Get-EC2Instance](#) (Windows PowerShell 工具)

```
(Get-EC2Instance -InstanceId instance_id).Instances.EnaSupport
```

映像属性 (enaSupport)

要检查 AMI 是否设置了增强联网 enaSupport 属性，请使用以下任一命令。如果该属性已设置，则响应为 true。

- [describe-images](#) (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query 'Images[].[EnaSupport]'
```

- [Get-EC2Image](#) (Windows PowerShell 工具)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

网络接口驱动程序

使用以下命令验证 ena 模块是否在特定接口上使用 (替换为要检查的接口的名称)。如果您使用单个接口 (默认设置)，则它是 eth0。

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
```

```
version:  
firmware-version:  
bus-info: vif-0  
supports-statistics: yes  
supports-test: no  
supports-eeprom-access: no  
supports-register-dump: no  
supports-priv-flags: no
```

在上例中，ena 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0  
driver: ena  
version: 0.6.6  
firmware-version:  
bus-info: 0000:00:03.0  
supports-statistics: yes  
supports-test: no  
supports-eeprom-access: no  
supports-register-dump: no  
supports-priv-flags: no
```

在此例中，加载的 ena 模块具有推荐的最低版本。此实例正确配置了增强联网。

在 Amazon Linux 上启用 ENA 增强联网

最新的 Amazon Linux HVM AMI 安装有 ENA 增强联网所需的模块，并已设置所需的 `enaSupport` 属性。因此，如果使用最新的 Amazon Linux HVM AMI 在支持的实例类型上启动实例，则已为您的实例启用 ENA 增强联网。有关更多信息，请参阅 [测试是否启用了 ENA 增强联网 \(p. 501\)](#)。

如果您使用较旧的 Amazon Linux AMI 启动了实例，并且实例尚未启用增强联网，请通过以下步骤启用增强联网。

启用 ENA 增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 从实例运行以下命令，以使用最新内核和内核模块（包括 ena）更新实例：

```
[ec2-user ~]$ sudo yum update
```

3. 使用 Amazon EC2 控制台或以下任一命令从本地计算机重新启动实例：[reboot-instances](#) (AWS CLI)，[Restart-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。
4. 再次连接到您的实例，并根据 [测试是否启用了 ENA 增强联网 \(p. 501\)](#) 使用 `modinfo ena` 命令验证 ena 模块是否已安装并具有推荐的最低版本。
5. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：[stop-instances](#) (AWS CLI)，[Stop-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续启用 ENA 增强联网 ([实例存储支持的实例 \(p. 504\)](#))。

6. 使用以下任一命令从本地计算机启用增强联网属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute \(AWS CLI\)](#)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute \(Windows PowerShell 工具\)](#)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

7. (可选) 从实例创建 AMI , 如[创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#)中所述。该 AMI 从实例继承增强联网 enaSupport 属性。因此 , 您可以使用该 AMI 来启动默认情况下启用了 ENA 增强联网的另一个实例。
8. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例 : [start-instances \(AWS CLI\)](#) , [Start-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)。如果您的实例由 AWS OpsWorks 管理 , 则应在 AWS OpsWorks 控制台中启动该实例 , 以便使实例状态保持同步。
9. 连接到您的实例 , 并根据[测试是否启用了 ENA 增强联网 \(p. 501\)](#) 使用 ethtool -i ethn 命令验证是否在网络接口上安装并加载了 ena 模块。

如果您在启用 ENA 增强联网之后无法连接到实例 , 请参阅[对 Elastic Network Adapter \(ENA\) 进行故障排除 \(p. 509\)](#)。

启用 ENA 增强联网 (实例存储支持的实例)

如果您的实例是实例存储支持的实例 , 请按照上述过程中的[Step 1 \(p. 503\)](#) 到[Step 4 \(p. 503\)](#) 操作 , 然后创建新的 AMI , 如[创建实例存储支持的 Linux AMI](#) 中所述。在注册 AMI 时 , 请确保启用增强联网 enaSupport 属性。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Register-EC2Image -EnaSupport $true ...
```

在 Ubuntu 上启用 ENA 增强联网

以下过程提供您在 Ubuntu 实例上启用 ENA 增强联网时执行的一般步骤。

在 Ubuntu 上启用 ENA 增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 更新包缓存和包。

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y
```

Important

如果在更新过程中系统提示您安装 grub , 请使用 /dev/xvda 安装 grub , 然后选择保留当前版本的 /boot/grub/menu.lst。

3. 安装 build-essential 包以编译内核模块和 dkms 包 , 这样每次更新内核时都会重建 ena 模块。

```
ubuntu:~$ sudo apt-get install -y build-essential dkms
```

- 从 GitHub 克隆您实例上的 ena 模块的源代码，网址为：<https://github.com/amzn/amzn-drivers>。

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

- 将 amzn-drivers 包移动到 /usr/src/ 目录，以便 dkms 可以在每次内核更新中找到并构建该模块。将源代码的版本号（您可在发行说明中找到当前版本号）附加到目录名称。例如，版本 1.0.0 显示在以下示例中。

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

- 使用以下值创建 dkms 配置文件（替换您的 ena 版本）。

- 创建文件。

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

- 编辑文件并添加以下值。

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

- 使用 dkms 在实例上添加、构建并安装 ena 模块。

- 将该模块添加到 dkms。

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

- 使用 dkms 构建该模块。

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

- 使用 dkms 安装该模块。

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

- 重新构建 initramfs，以便在启动时加载正确的模块。

```
ubuntu:~$ sudo update-initramfs -c -k all
```

- 根据 [测试是否启用了 ENA 增强联网 \(p. 501\)](#)，使用 modinfo ena 命令验证是否安装了 ena 模块。

```
ubuntu:~$ modinfo ena
filename:      /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:       1.0.0
license:        GPL
description:   Elastic Network Adapter (ENA)
author:        Amazon.com, Inc. or its affiliates
srcversion:    9693C876C54CA64AE48F0CA
alias:         pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:         pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:         pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
```

```
alias:          pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:      3.13.0-74-generic SMP mod_unload modversions
parm:          debug:Debug level (0=none,...,16=all) (int)
parm:          push_mode:Descriptor / header push mode
(0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:          enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1)
(int)
parm:          enable_missing_tx_detection:Enable missing Tx completions. (default=1)
(int)
parm:          numa_node_override_array:Numa node override map
(array of int)
parm:          numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

10. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例 : [stop-instances](#) (AWS CLI) , [Stop-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续在 Ubuntu 上启用 ENA 增强联网 ([实例存储支持的实例](#) (p. 506))。

11. 从本地计算机中，使用以下命令启用增强联网属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Windows PowerShell 工具)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

12. (可选) 从实例创建 AMI，如 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 中所述。该 AMI 从实例继承增强联网属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。
13. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例 : [start-instances](#) (AWS CLI) , [Start-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
14. (可选) 连接到实例并确认已安装模块。

如果您在启用 ENA 增强联网之后无法连接到实例，请参阅[对 Elastic Network Adapter \(ENA\) 进行故障排除 \(p. 509\)](#)。

在 Ubuntu 上启用 ENA 增强联网 (实例存储支持的实例)

如果实例是实例存储支持的实例，请执行上一过程中的 Step 1 (p. 504) 到 Step 9 (p. 505)，然后创建新 AMI (如[创建由实例存储支持的 Linux AMI \(p. 78\)](#)中所述)。在注册 AMI 时，请确保启用增强联网 enaSupport 属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Register-EC2Image -EnaSupport $true ...
```

在其他 Linux 发行版上启用 ENA 增强联网

下面的过程提供在 Amazon Linux 或 Ubuntu 之外的 Linux 发行版上启用 ENA 增强联网时将执行的一般步骤。有关更多信息 (如命令的详细语法、文件位置或包和工具支持)，请参阅您的 Linux 分发版的特定文档。

在 Linux 上启用 ENA 增强联网 (EBS 支持的实例)

1. 连接到您的实例。
2. 从 GitHub 克隆您实例上的 ena 模块的源代码，网址为：<https://github.com/amzn/amzn-drivers>。

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

3. 在实例上编译并安装 ena 模块。

如果您的分发版支持 dkms，则应考虑配置 dkms 以便在每次更新系统内核时重新编译 ena 模块。如果您的分发版自身不支持 dkms，则可以在用于 Red Hat Enterprise Linux 各版本的 EPEL 存储库 (<https://fedoraproject.org/wiki/EPEL>) 中找到它，也可以到 <http://linux.dell.com/dkms/> 下载该软件。使用 [在 Ubuntu 上启用 ENA 增强联网 \(EBS 支持的实例\) \(p. 504\)](#) 中 Step 5 (p. 505) 到 Step 7 (p. 505) 帮助配置 dkms。

4. 运行 sudo depmod 命令以更新模块依赖项。
5. 在实例上更新 initramfs 以确保在启动时加载新模块。
6. 确定您的系统是否默认使用可预测的网络接口名称。使用 systemd 或 udev 版本 197 或更高版本的系统可以重命名以太网设备，它们不保证单个网络接口将命名为 eth0。此行为可能导致连接到实例时出现问题。要获取更多信息并查看其他配置选项，请参阅 freedesktop.org 网站上的[可预测的网络接口名称](#)。

- a. 您可以使用以下命令在基于 RPM 的系统上检查 systemd 或 udev 版本：

```
[ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]+\+|udev-[0-9]+\+'  
systemd-208-11.el7_0.2.x86_64
```

在以上 Red Hat 7 示例中，systemd 版本是 208，因此必须禁用可预测的网络接口名称。

- b. 通过将 net.ifnames=0 选项添加到 GRUB_CMDLINE_LINUX/etc/default/grub ## 行，禁用可预测的网络接口名称。

```
[ec2-user ~]$ sudo sed -i '/^GRUB_CMDLINE_LINUX/s/$/\ net.ifnames=0/' /etc/default/grub
```

- c. 重新构建 grub 配置文件。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：[stop-instances \(AWS CLI\)](#)，[Stop-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续启用 ENA 增强联网 (实例存储支持的实例) (p. 508)。

8. 使用以下任一命令从本地计算机启用增强联网 `enaSupport` 属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [modify-instance-attribute \(AWS CLI\)](#)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute \(Windows PowerShell 工具\)](#)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

9. (可选) 从实例创建 AMI，如 [创建 Amazon EBS 支持的 Linux AMI \(p. 75\)](#) 中所述。该 AMI 从实例继承增强联网 `enaSupport` 属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。

Important

如果您的实例操作系统包含 `/etc/udev/rules.d/70-persistent-net.rules` 文件，在创建 AMI 前必须将其删除。此文件包含原始实例的以太网适配器 MAC 地址。如果其他实例使用此文件启动，操作系统将找不到设备，`eth0` 会失败，从而导致启动问题。此文件将在下次启动过程中重新生成，从 AMI 启动的任意实例都会创建这个文件的自有版本。

10. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：[start-instances \(AWS CLI\)](#)，[Start-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
11. (可选) 连接到实例并确认已安装模块。

如果您在启用 ENA 增强联网之后无法连接到实例，请参阅[对 Elastic Network Adapter \(ENA\) 进行故障排除 \(p. 509\)](#)。

启用 ENA 增强联网 (实例存储支持的实例)

如果您的实例是实例存储支持的实例，请执行上述过程中的[Step 1 \(p. 507\)](#) 到[Step 5 \(p. 507\)](#)，然后创建新的 AMI (如[创建由实例存储支持的 Linux AMI \(p. 78\)](#) 中所述)。在注册 AMI 时，请确保启用增强联网 `enaSupport` 属性。

Warning

仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Register-EC2Image -EnaSupport ...
```

故障排除

有关对 ENA 适配器进行故障排除的其他信息，请参阅对 Elastic Network Adapter (ENA) 进行故障排除 (p. 509)。

对 Elastic Network Adapter (ENA) 进行故障排除

Elastic Network Adapter (ENA) 旨在改进操作系统运行状况和降低因意外硬件行为或故障而导致长期中断的几率。ENA 架构保持设备或驱动程序故障对系统尽可能透明。本主题提供了关于 ENA 的故障排除信息。

如果您不能连接到实例，请先从[排除连接问题 \(p. 509\)](#)部分开始。

如果您能连接到实例，则可以使用本主题后面部分中涵盖的故障检测和恢复机制收集诊断信息。

内容

- [排除连接问题 \(p. 509\)](#)
- [保持活动机制 \(p. 510\)](#)
- [注册表读取超时 \(p. 511\)](#)
- [统计数据 \(p. 511\)](#)
- [syslog 中的驱动程序错误日志 \(p. 513\)](#)

排除连接问题

如果您在启用增强联网时丢失连接，则 ena 模块可能与您实例当前运行的内核不兼容。如果您为特定内核版本安装该模块（不使用 dkms，或使用配置错误的 dkms.conf 文件），然后更新您的实例内核，则会发生这种情况。如果在启动时加载的实例内核未正确安装 ena 模块，则您的实例将无法识别网络适配器，并且您的实例将变得无法访问。

如果您为 PV 实例或 AMI 启用增强联网，这也会使您的实例无法访问。

如果在启用 ENA 增强联网后您的实例变得无法访问，可以为您的实例禁用 `enaSupport` 属性，这将回退到库存网络适配器。

禁用 ENA 增强联网 (EBS 支持的实例)

1. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：`stop-instances` (AWS CLI)，`Stop-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

Important

如果您使用的是实例存储支持的实例，则不能停止实例，而应继续禁用 ENA 增强联网 ([实例存储支持的实例 \(p. 510\)](#))。

2. 从本地计算机中，使用以下命令禁用增强联网属性。

- [modify-instance-attribute](#) (AWS CLI)

```
$ aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

3. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：`start-instances` (AWS CLI)，`Start-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)。如果您的实例由 AWS OpsWorks 管理，则应在 AWS OpsWorks 控制台中启动该实例，以便使实例状态保持同步。

4. (可选) 连接到您的实例，并按照[在 VPC 中的 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 501\)](#)中的步骤尝试重新安装具有当前内核版本的 ena 模块。

禁用 ENA 增强联网 (实例存储支持的实例)

如果您的实例是实例存储支持的实例，则创建新的 AMI，如[创建由实例存储支持的 Linux AMI \(p. 78\)](#) 中所述。在注册 AMI 时，请确保禁用增强联网 enaSupport 属性。

- [register-image \(AWS CLI\)](#)

```
$ aws ec2 register-image --no-ena-support ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

保持活动机制

ENAs 按固定速度（通常每秒一次）发布保持活动事件。ENAs 驱动程序实施一种监视机制，用于检查是否存在这些保持活动消息。如果存在一条或多条消息，则重新启动监视，否则此驱动程序将认为设备出现故障，然后执行以下操作：

- 将当前统计数据转储到 syslog
- 重置 ENA 设备
- 重置 ENA 驱动程序状态

上述重置过程可能会在短时间内导致一些流量丢失（TCP 连接应该能恢复），但应该不会影响到用户。

例如，如果 ENA 设备在加载无法恢复的配置后进入未知状态，ENAs 设备也可能会间接请求设备重置过程，而不发送保持活动通知。

下面是重置过程示例：

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.....
.....
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date [Wed Apr 6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
```

```
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset process
is complete
```

注册表读取超时

ENA 架构建议使用有限的内存映射的 I/O (MMIO) 读取操作。ENA 设备驱动程序仅在其初始化过程中访问 MMIO 注册表。

如果驱动程序日志 (在 dmesg 输出中可用) 指示读取操作失败，这可能是由驱动程序不兼容或编译错误、硬件设备繁忙或硬件故障所导致的。

指示读取操作失败的间歇性日志条目不应视为问题；在这种情况下，驱动程序将重试读取操作。但是，一系列包含读取失败的日志条目则指示驱动程序或硬件问题。

下面是指示读取操作因超时而失败的驱动程序日志条目示例：

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

统计数据

如果您遇到网络性能差或延迟问题，您应该检索设备统计数据并检查这些数据。可以使用 ethtool 获取这些统计数据，如下所示：

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
    tx_timeout: 0
    io_suspend: 0
    io_resume: 0
    wd_expired: 0
    interface_up: 1
    interface_down: 0
    admin_q_pause: 0
    queue_0_tx_cnt: 4329
    queue_0_tx_bytes: 1075749
    queue_0_tx_queue_stop: 0
    ...
```

命令输出参数如下所述：

tx_timeout: *N*

Netdev 监视的激活次数。

io_suspend: *N*

不支持。此值应始终为零。

io_resume: *N*

不支持。此值应始终为零。

`wd_expired: N`

驱动程序在过去的 3 秒内未收到保持活动事件的次数。

`interface_up: N`

ENAs 接口启动的次数。

`interface_down: N`

ENAs 接口关闭的次数。

`admin_q_pause: N`

管理队列处于不稳定状态。此值应始终为零。

`queue_N_tx_cnt: N`

为队列 `N` 传输的数据包数。

`queue_N_tx_bytes: N`

为队列 `N` 传输的字节数。

`queue_N_tx_queue_stop: N`

队列 `N` 已满并停止的次数。

`queue_N_tx_queue_wakeup: N`

队列 `N` 在停止后恢复的次数。

`queue_N_tx_dma_mapping_err: N`

直接内存访问错误计数。如果此值不为 0，则表示系统资源不足。

`queue_N_tx_napi_comp: N`

napi 处理程序为队列 `N` 调用 `napi_complete` 的次数。

`queue_N_tx_poll: N`

为队列 `N` 计划 napi 处理程序的次数。

`queue_N_tx_doorbells: N`

队列 `N` 的传输门铃数。

`queue_N_tx_linearize: N`

对队列 `N` 尝试 SKB 线性化处理的次数。

`queue_N_tx_linearize_failed: N`

队列 `N` 的 SKB 线性化处理失败的次数。

`queue_N_tx_prepare_ctx_err: N`

队列 `N` 的 `ena_com_prepare_tx` 失败的次数。此值应始终为零；否则，请查看驱动程序日志。

`queue_N_tx_missing_tx_comp: N`

队列 `N` 剩下未完成的数据包数。此值应始终为零。

`queue_N_tx_bad_req_id: N`

队列 `N` 的无效 `req_id`。有效的 `req_id` = 0 - `queue_size` - 1。

`queue_N_rx_cnt: N`

为队列 `N` 接收的数据包数。

`queue_N_rx_bytes: N`

为队列 `N` 接收的字节数。

queue_ **N**_rx_refil_partial: **N**

驱动程序未成功使用队列 **N** 的缓冲区重填空的 rx 队列部分的次数。如果此值不为零，则表示内存资源不足。

queue_ **N**_rx_bad_csum: **N**

rx 队列具有队列 **N** 的错误校验和的次数 (仅当支持 rx 校验和卸载时)。

queue_ **N**_rx_page_alloc_fail: **N**

队列 **N** 的页分配失败的次数。如果此值不为零，则表示内存资源不足。

queue_ **N**_rx_skb_alloc_fail: **N**

队列 **N** 的 SKB 分配失败的次数。如果此值不为零，则表示系统资源不足。

queue_ **N**_rx_dma_mapping_err: **N**

直接内存访问错误计数。如果此值不为 0，则表示系统资源不足。

queue_ **N**_rx_bad_desc_num: **N**

每个数据包使用的缓冲区太多。如果此值不为 0，则表示使用的缓冲区非常小。

queue_ **N**_rx_small_copy_len_pkt: **N**

优化：对于小于此阈值 (由 sysfs 设置) 的数据包，将数据包直接复制到堆栈中以避免分配新页面。

ena_admin_q_aborted_cmd: **N**

已中止的管理命令数。这通常发生在自动恢复过程中。

ena_admin_q_submitted_cmd: **N**

管理队列门铃数。

ena_admin_q_completed_cmd: **N**

管理队列完成数。

ena_admin_q_out_of_space: **N**

驱动程序尝试提交新管理命令但队列已满的次数。

ena_admin_q_no_completion: **N**

驱动程序未获得命令的管理完成的次数。

syslog 中的驱动程序错误日志

ENA 驱动程序会在系统启动期间将日志消息写入到 syslog 中。如果您遇到问题，则可以查看这些日志以检查错误。下面是 ENA 驱动程序在系统启动期间记录在 syslog 中的信息示例以及一些选择消息注释。

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.416939] [ENA_COM: ena_com_validate_version]
ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.420915] [ENA_COM: ena_com_validate_version]
ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.256831] ena 0000:00:03.0: Device watchdog is
Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.672947] ena 0000:00:03.0: creating 8 io
queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.680885] [ENA_COM:
ena_com_init_interrupt_moderation] Feature 20 isn't supported // Interrupt moderation is
not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.691609] [ENA_COM: ena_com_get_feature_ex]
Feature 10 isn't supported // RSS HASH function configuration is not supported by the
device
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.694583] [ENA_COM: ena_com_get_feature_ex]  
Feature 18 isn't supported //RSS HASH input source configuration is not supported by the  
device  
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.697433] [ENA_COM:  
ena_com_set_host_attributes] Set host attribute isn't supported  
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.701064] ena 0000:00:03.0 (unnamed  
net_device) (uninitialized): Cannot set host attributes  
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.704917] ena 0000:00:03.0: Elastic Network  
Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8  
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 480.805037] EXT4-fs (xvdal): re-mounted. Opts:  
(null)  
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 481.025842] NET: Registered protocol family 10
```

可以忽略哪些错误？

可以忽略以下可能出现在系统错误日志中的关于 Elastic Network Adapter 的警告：

Set host attribute isn't supported

此设备不支持主机属性。

failed to alloc buffer for rx queue

这是可恢复的错误，引发此错误时，表示可能存在内存压力问题。

Feature **X** isn't supported

Elastic Network Adapter 不支持引用的功能。**X** 的可能值包括：

- 10：此设备不支持 RSS 哈希函数配置。
- 12：此设备不支持 RSS 间接表配置。
- 18：此设备不支持 RSS 哈希输入配置。
- 20：此设备不支持中断裁决。

Failed to config AENQ

Elastic Network Adapter 不支持 AENQ 配置。

Trying to set unsupported AENQ events

此错误表示尝试设置 Elastic Network Adapter 不支持的 AENQ 事件组。

存储

Amazon EC2 为您的实例提供了灵活、经济且易于使用的数据存储选项。各选项都具有独特的性能和耐久性。这些存储选项既可以单独使用，也可以组合使用，以便满足您的需求。

阅读本部分后，您应该会对如何使用 Amazon EC2 支持的数据存储选项来满足特定要求有很好的了解。这些存储选项包含以下产品：

- [Amazon Elastic Block Store\(Amazon EBS\) \(p. 516\)](#)
- [Amazon EC2 实例存储 \(p. 591\)](#)
- [Amazon Elastic File System \(Amazon EFS\) \(p. 602\)](#)
- [Amazon Simple Storage Service \(Amazon S3\) \(p. 605\)](#)

下图显示了这些不同存储类型之间的关系。

Amazon EBS

Amazon EBS 提供数据块级别的持久存储卷，您可将这些卷连接到正在运行的实例。您可以将 Amazon EBS 用作需要频繁和细粒度更新的数据的主存储设备。例如，如果在实例上运行数据库，则建议选用 Amazon EBS 作为存储设备。

EBS 卷就像原始未经格式化的外部数据块储存设备，可连接到单个实例。卷始终不受实例运行时间的影响。将 EBS 卷连接到实例后，您可以像使用其他物理硬盘一样使用它。如上图所示，可以将多个卷连接到一个实例。您也可以将 EBS 卷从实例中断开，并将其连接到另一个实例。您可以动态更改附加到实例的卷的配置。还可以使用 Amazon EBS 加密功能以加密卷的形式创建 EBS 卷。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 568\)](#)。

为保留您的数据的备份副本，您可以创建 EBS 卷的快照，该快照存储在 Amazon S3 中。您可以从快照创建 EBS 卷，并将其连接到另一个实例。有关更多信息，请参阅 [Amazon Elastic Block Store\(Amazon EBS\) \(p. 516\)](#)。

Amazon EC2 实例存储

很多实例可以访问物理连接到主机的磁盘中的存储。此磁盘存储称为实例存储。实例存储可为实例提供临时性块级存储。实例存储卷上的数据仅在关联实例的生命周期内保留；如果您停止或终止实例，则实例存储卷上的任何数据都会丢失。有关更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#)。

Amazon EFS 文件系统

Amazon EFS 提供可扩展文件存储以供和 Amazon EC2 一起使用。您可以创建 EFS 文件系统并配置实例来安装文件系统。您可以使用 EFS 文件系统作为在多个实例上运行的工作负载和应用程序的通用数据源。有关更多信息，请参阅 [Amazon Elastic File System \(Amazon EFS\) \(p. 602\)](#)。

Amazon S3

Amazon S3 为您提供可靠的廉价数据存储基础设施。它的设计理念是通过支持您随时从 Amazon EC2 内部或从网络上的任何地方存储和检索任何数量的数据，从而简化整个网络计算。例如，您可以使用 Amazon S3 来存储数据和应用程序的备份副本。Amazon EC2 使用 Amazon S3 存储 EBS 快照和实例存储支持的 AMI。有关更多信息，请参阅 [Amazon Simple Storage Service \(Amazon S3\) \(p. 605\)](#)。

添加存储

您每次从 AMI 启动实例时，系统都会为该实例创建一个根存储设备。根存储设备中包含启动实例所需的全部信息。当您创建 AMI 或使用块储存设备映射启动实例时，除了根设备外，您还可以指定存储卷。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。

您还可以将 EBS 卷连接到运行中的实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

Amazon Elastic Block Store(Amazon EBS)

Amazon Elastic Block Store (Amazon EBS) 提供数据块级存储卷以用于 EC2 实例。EBS 卷是高度可用和可靠的存储卷，可以挂载到同一可用区中任何正在运行的实例。挂载到 EC2 实例的 EBS 卷公开为独立于实例生命周期存在的存储卷。使用 Amazon EBS，您可以按实际用量付费。有关 Amazon EBS 定价的更多信息，请参阅 [Amazon Elastic Block Store 页](#) 的“预计费用”部分。

如果数据必须能够快速访问且需要长期保存，建议使用 Amazon EBS。EBS 卷特别适合用作文件系统和数据库的主存储，还适用于任何需要细粒度更新及访问原始的、未经格式化的数据块级存储的应用程序。Amazon EBS 非常适合依赖随机读写操作的数据库式应用程序以及执行长期持续读写操作的吞吐量密集型应用程序。

要使用简化的数据加密，可将 EBS 卷作为加密卷进行启动。Amazon EBS 加密 提供了用于 EBS 卷的简单加密解决方案，您无需构建、管理和保护自己的密钥管理基础设施。创建加密 EBS 卷并将它连接到支持的实例类型时，该卷上静态存储的数据、磁盘 I/O 和通过该卷创建的快照都会进行加密。加密在托管 EC2 实例的服务器上进行，从而为从 EC2 实例传输到 EBS 存储的数据提供加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 568\)](#)。

Amazon EBS 加密在创建加密卷以及通过加密卷创建任何快照时，使用 AWS Key Management Service (AWS KMS) 主密钥。首次在区域中创建加密的 EBS 卷时，将自动为您创建一个默认主密钥。此密钥将用于 Amazon EBS 加密，除非您选择采用 AWS Key Management Service 单独创建的客户主密钥 (CMK)。创建您自己的 CMK 可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥的能力。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

您可以将多个卷连接到同一实例，但是不能超过 AWS 账户指定的限额。您的账户对您可以使用的 EBS 卷数量和总存储量有相应的限制。如要了解有关限制的更多信息，以及如何申请提高限额，请参阅 [请求提高 Amazon EBS 卷限制](#)。

内容

- [Amazon EBS 的功能 \(p. 517\)](#)
- [Amazon EBS 卷 \(p. 517\)](#)
- [Amazon EBS 快照 \(p. 559\)](#)
- [Amazon EBS 优化实例 \(p. 564\)](#)
- [Amazon EBS Encryption \(p. 568\)](#)
- [Linux 实例上的 Amazon EBS 卷性能 \(p. 571\)](#)
- [Amazon EBS 的 Amazon CloudWatch Events \(p. 586\)](#)

Amazon EBS 的功能

- 您可以创建大小高达 16TiB 的 EBS 通用型 SSD (gp2)、预配置 IOPS SSD (io1)、吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷。您可以将这些卷作为设备装载在您的 Amazon EC2 实例上。您可以在同一实例上安装多个卷，但每个卷一次只能连接到一个实例。您可以动态更改附加到实例的卷的配置。有关更多信息，请参阅 [创建 Amazon EBS 卷 \(p. 527\)](#)。
- 通过 通用型 SSD (gp2) 卷，基本性能可以达到 3 IOPS/GiB，并能突增至 3000 IOPS 并保持一段时间。gp2 卷适用于多种使用案例，例如引导卷、中小型数据库以及开发和测试环境。gp2 卷最高可支持 10000 的 IOPS 和 160MB/s 的吞吐量。有关更多信息，请参阅 [通用型 SSD \(gp2\) 卷 \(p. 521\)](#)。
- 通过 预配置 IOPS SSD (io1) 卷，您可以预配置特定级别的 I/O 性能。io1 卷最高可支持 20000 IOPS 和 320 MB/s 吞吐量。因此，您可预见性地将每个 EC2 实例扩展到数万 IOPS。有关更多信息，请参阅 [预配置 IOPS SSD \(io1\) 卷 \(p. 522\)](#)。
- 吞吐优化 HDD (st1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。这种卷的吞吐量高达 500MB/s，非常适合大型顺序工作负载，例如 Amazon EMR、ETL、数据仓库和日志处理。有关更多信息，请参阅 [吞吐优化 HDD \(st1\) 卷 \(p. 522\)](#)。
- Cold HDD (sc1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。sc1 的吞吐量高达 250MB/s，是大型顺序冷数据工作负载的理想选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的数据块存储。有关更多信息，请参阅 [Cold HDD \(sc1\) 卷 \(p. 524\)](#)。
- EBS 卷的行为类似于原始、未格式化的块储存设备。您可基于这些卷来创建文件系统，或以任何其他块储存设备（如硬盘）使用方式使用这些卷。有关创建文件系统和安装卷的更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 531\)](#)。
- 您可以使用加密 EBS 卷为监管/审核的数据和应用程序实现各种静态数据加密要求。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 568\)](#)。
- 您可以创建持久保存到 Amazon S3 的 EBS 卷的时间点快照。快照可为数据提供保护以获得长期持久性，可用作新 EBS 卷的起点。您随心所欲地用相同快照对任意多的卷进行实例化。可以跨多个 AWS 区域复制这些快照。有关更多信息，请参阅 [Amazon EBS 快照 \(p. 559\)](#)。
- EBS 卷在特定可用区中创建，随后可以挂载到同一可用区内的任何实例。若要在可用区外部提供某个卷，您可以创建快照并将该快照还原到该区域任何位置处的新卷。您可以将快照复制到其他区域，再将它们还原到那里的新卷，这样可更方便地利用多个 AWS 区域以实现地理扩展、数据中心迁移和灾难恢复。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 559\)](#)、[从快照还原 Amazon EBS 卷 \(p. 529\)](#) 和 [复制 Amazon EBS 快照 \(p. 561\)](#)。
- 可以将公用数据集快照的大型存储库还原到 EBS 卷，并无缝集成到基于 AWS 云的应用程序中。有关更多信息，请参阅 [使用公用数据集 \(p. 617\)](#)。
- 带宽、吞吐量、延迟和平均队列长度等性能指标是通过 AWS 管理控制台提供的。通过 Amazon CloudWatch 提供的这些指标，您可以监视卷的性能，确保为应用程序提供足够性能，又不会为不需要的资源付费。有关更多信息，请参阅 [Linux 实例上的 Amazon EBS 卷性能 \(p. 571\)](#)。

Amazon EBS 卷

Amazon EBS 卷是一种耐用的数据块级存储设备，可以连接到单个 EC2 实例。您可以将 EBS 卷用作需要频繁更新的数据的主存储，例如实例的系统驱动器或数据库应用程序的存储，也可以用于执行持续硬盘扫描的吞吐量密集型应用程序。EBS 卷始终不受 EC2 实例运行时间的影响。将卷连接到实例后，您可以像使用其他物理硬盘一样使用它。EBS 卷非常灵活。您可以在实时生产卷上动态增长卷、修改预配置 IOPS 容量和更改卷类型。Amazon EBS 提供以下卷类型：通用型 SSD (gp2)、预配置 IOPS SSD (io1)、吞吐优化 HDD (st1)、Cold HDD (sc1) 和 磁介质 (standard)。它们的性能特点和价格不同，您可根据应用程序要求定制您所需的存储性能和相应费用。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

内容

- [使用 EBS 卷的优势 \(p. 518\)](#)
- [Amazon EBS 卷类型 \(p. 519\)](#)
- [创建 Amazon EBS 卷 \(p. 527\)](#)

- [从快照还原 Amazon EBS 卷 \(p. 529\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)
- [使 Amazon EBS 卷可用 \(p. 531\)](#)
- [查看卷信息 \(p. 533\)](#)
- [监控您的卷状态 \(p. 534\)](#)
- [从实例断开 Amazon EBS 卷 \(p. 541\)](#)
- [删除 Amazon EBS 卷 \(p. 542\)](#)
- [在 Linux 上修改 EBS 卷的大小、IOPS 或类型 \(p. 543\)](#)
- [扩展 Linux 分区 \(p. 551\)](#)

使用 EBS 卷的优势

EBS 卷可提供实例存储卷不支持的多种优势。

- **数据可用性**

当您在可用区域内创建 EBS 卷时，系统会在该区域内自动复制该卷，以防止因任何一个硬件组件故障而导致数据丢失。在您创建卷后，可将其连接到同一可用区域内的任何 EC2 实例。连接后，该卷显示为类似于硬盘或其他物理设备的本机块设备。这时，实例就像与本地硬盘交互一样与该卷相互；实例还可以使用文件系统（如 ext3）将 EBS 卷格式化，然后安装应用程序。

一个 EBS 卷一次只能连接到同一可用区域中的一个实例。但是，可将多个卷连接到同一实例。如果您将多个卷连接到您指定的一个设备，则可以在卷内将数据条带化，以增强 I/O 性能和吞吐量。

您可以获取针对 EBS 卷的监控数据，而无需额外付费（其中包含 EBS 支持的实例根设备卷的数据）。有关更多信息，请参阅 [使用 CloudWatch 监控卷 \(p. 534\)](#)。

- **数据持久性**

EBS 卷是一种实例外存储，其数据的保存期限不受实例使用寿命的影响。只要数据存在，您就要继续支付卷的使用费用。

在默认情况下，当实例终止时，连接到该实例的 EBS 卷会自动断开连接，同时完整地保留数据。然后，可将卷重新连接到新的实例，从而快速恢复数据。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其连接的卷中保存的数据。在从停止到启动的整个周期中，该卷均为已连接状态。这使您能够无限期地在卷上处理和存储数据，并只在需要时使用处理和存储资源。数据将一直保存在该卷上，直至将其显式删除。已删除的 EBS 卷使用的物理数据块存储先由零覆盖，然后分配给其他账户。如果要处理敏感数据，应考虑手动加密数据或将数据存储在由 Amazon EBS 加密保护的卷上。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 568\)](#)。

在默认情况下，当实例终止时，在启动时创建并连接的 EBS 卷也会被删除。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `false`。修改值后，即使实例终止，也可将该卷保留下并连接到其他实例。

- **数据加密**

为简化数据加密，您可以使用 Amazon EBS 加密功能创建加密 EBS 卷。所有 EBS 卷类型都支持加密。您可以使用加密 EBS 卷为监管/审核的数据和应用程序实现各种静态数据加密要求。Amazon EBS 加密使用 256 位高级加密标准算法（AES-256）和 Amazon 托管密钥基础设施。加密在托管 EC2 实例的服务器上进行，从而为从 EC2 实例传输到 Amazon EBS 存储的数据提供加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 568\)](#)。

Amazon EBS 加密在创建加密卷以及通过加密卷创建任何快照时，使用 AWS Key Management Service (AWS KMS) 主密钥。首次在区域中创建加密的 EBS 卷时，将自动为您创建一个默认主密钥。此密钥用于 Amazon EBS 加密，除非您选择采用 AWS KMS 单独创建的客户主密钥 (CMK)。创建您自己的 CMK 可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥的能力。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

- 快照

Amazon EBS 提供为任何 EBS 卷创建快照 (备份) 并将卷中数据的副本写入 Amazon S3 (其中数据以冗余方式存储在多个可用区中) 的功能。不必将该卷连接到运行中的实例，也可以拍摄快照。因为您不断向卷写入数据，则可定期创建该卷的快照，以用作创建新卷的基线。也可利用这些快照创建多个新的 EBS 卷或在可用区间移动卷的位置。加密 EBS 卷的快照会自动加密。

从快照创建新卷时，新卷是拍摄快照时的原始卷的精确副本。从加密快照还原的 EBS 卷会自动加密。通过指定不同的可用区 (可选)，您可以使用此功能在该区域中创建重复的卷。可与特定的 AWS 账户共享这些卷或使其公开可用。当您创建快照时，您需根据卷的总大小支付 Amazon S3 费用。对于连续的卷快照，您只需支付任何超过卷原始大小的附加数据的费用。

快照是增量备份，这意味着仅保存卷上在最新快照之后更改的数据块。如果您的卷中有 100 GiB 的数据，但自上次快照以来只更改了 5 GiB 的数据，则只有这 5 GiB 经过修改的数据会写入 Amazon S3。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

为了便于对卷和快照进行分类和管理，您可以使用选择的元数据对它们加以标记。有关更多信息，请参阅[标记 Amazon EC2 资源 \(p. 626\)](#)。

- 弹性

EBS 卷支持生产期间的实时配置更改。您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。

Amazon EBS 卷类型

Amazon EBS 提供以下卷类型，各种类型性能特点和价格不同，因此您可根据应用程序要求定制您所需的存储性能和相应成本。卷类型归入两大类别：

- 支持 SSD 的卷针对涉及小型 I/O 的频繁读/写操作的事务性工作负载进行了优化，其中管理性能属性为 IOPS
- 支持 HDD 的卷针对吞吐量 (以 MiB/s 为单位) 是优于 IOPS 的性能指标的大型流式处理工作负载进行了优化

下表列出了每个卷类型的使用案例和性能特点：

| | 固态硬盘 (SSD) | | 硬盘 (HDD) | |
|------|---|--|---|---|
| 卷类型 | 通用型 SSD (gp2)* | 预配置 IOPS SSD (io1) | 吞吐优化 HDD (st1) | Cold HDD (sc1) |
| 描述 | 平衡价格和性能的通用 SSD 卷，可用多种事务性工作负载 | 为任务关键型应用程序设计的最高性能 SSD 卷 | 为频繁访问的吞吐量密集型工作负载设计的低成本 HDD 卷 | 为不常访问的工作负载设计的最低成本 HDD 卷 |
| 使用案例 | <ul style="list-style-type: none">建议用于大多数工作负载系统启动卷虚拟桌面低延迟交互式应用程序开发和测试环境 | <ul style="list-style-type: none">需要持续 IOPS 性能或每卷高于 10000 IOPS 或 160 MiB/s 吞吐量的关键业务应用程序大型数据库工作负载，如：<ul style="list-style-type: none">MongoDBCassandraMicrosoft SQL Server | <ul style="list-style-type: none">以低成本流式处理需要一致、快速的吞吐量的工作负载大数据数据仓库日志处理不能是启动卷 | <ul style="list-style-type: none">适合大量不常访问的数据、面向吞吐量的存储最低存储成本至关重要的情形不能是启动卷 |

| | 固态硬盘 (SSD) | | 硬盘 (HDD) | |
|--------------|----------------|---|------------------|------------------|
| | | <ul style="list-style-type: none"> • MySQL • PostgreSQL • Oracle | | |
| API 名称 | gp2 | io1 | st1 | sc1 |
| 卷大小 | 1 GiB - 16 TiB | 4 GiB - 16 TiB | 500 GiB - 16 TiB | 500 GiB - 16 TiB |
| 最大 IOPS**/卷† | 10000 | 20000 | 500 | 250 |
| 最大吞吐量/卷† | 160 MiB/s | 320 MiB/s | 500 MiB/s | 250 MiB/s |
| 最大 IOPS/实例 | 65000 | 65000 | 65000 | 65000 |
| 最大吞吐量/实例 | 1,250 MiB/s | 1,250 MiB/s | 1,250 MiB/s | 1,250 MiB/s |
| 管理性能属性 | IOPS | IOPS | MiB/s | MiB/s |

*默认卷类型

** gp2/io1 基于 16KiB I/O 大小，st1/sc1 基于 1 MiB I/O 大小

† 要达到此吞吐量，您必须要有支持该吞吐量的实例，如 r3.8xlarge 或 x1.32xlarge。

下表列出了上一代 EBS 卷类型。如果您需要比上一代卷更高的性能或性能一致性，建议您考虑使用通用型 SSD (gp2) 或其他最新卷类型。有关更多信息，请参阅[上一代卷](#)。

| 上一代卷 | |
|------------|---------------|
| 卷类型 | EBS 磁介质 |
| 描述 | 上一代 HDD |
| 使用案例 | 数据不常访问的工作负载 |
| API 名称 | standard |
| 卷大小 | 1 GiB - 1 TiB |
| 最大 IOPS/卷 | 40 – 200 |
| 最大吞吐量/卷 | 40-90 MiB/s |
| 最大 IOPS/实例 | 48000 |
| 最大吞吐量/实例 | 1,250 MiB/s |
| 管理性能属性 | IOPS |

Note

Linux AMI 需要将 GPT 分区表和 GRUB 2 用于 2 TiB (2048 GiB) 或更大的引导卷。现在的许多 Linux AMI 都使用 MBR 分区方案，此方案仅支持最高 2047 GiB 的引导卷。如果您的实例不通过 2 TiB 或更大的引导卷启动，您要使用的 AMI 会限制为 2047 GiB 引导卷大小。非引导卷对 Linux 实例没有这种限制。

有多种因素会影响 EBS 卷的性能，如实例配置、I/O 特性和工作负载需求。有关充分利用 EBS 卷的更多信息，请参阅[Linux 实例上的 Amazon EBS 卷性能 \(p. 571\)](#)。

有关这些卷类型的定价的更多信息，请参阅 [Amazon EBS 定价](#)。

通用型 SSD (`gp2`) 卷

通用型 SSD (`gp2`) 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷可以提供几毫秒的延迟，能够突增至 3000 IOPS 并维持一段较长的时间。在最小 100 IOPS (以 33.33 GiB 及以下) 和最大 10,000 IOPS (以 3334 GiB 及以上) 之间，基准性能以每 GiB 卷大小 3 IOPS 的速度线性扩展。`gp2` 卷的大小范围为 1 GiB 到 16 TiB。

I/O 点数和突增性能

`gp2` 卷的性能与卷大小关联，卷大小确定卷的基准性能水平以及积累 I/O 点数的速度；卷越大，基准性能级别就越高，I/O 点数积累速度也越快。I/O 点数表示您的`gp2` 卷在需求超过基准性能时可用来突增大量 I/O 的可用带宽。您的卷拥有的 I/O 点数越多，它在需要更高性能时可以超过其基准性能水平的突增时间就越长，表现也越好。下图显示 `gp2` 的突增存储桶行为。

每个卷都有 540 万 I/O 点的初始 I/O 点数余额，这足以维持 3000 IOPS 的最大突增性能 30 分钟。设计初始点数余额的目的是为启动卷提供快速初始启动循环，并为其他应用程序提供良好的引导过程。卷以每 GiB 卷大小 3 IOPS 的基准性能率的速度获得 I/O 点数。例如，一个 100 GiB 的`gp2` 卷具有 300 IOPS 的基准性能。

当卷的需求超出了基准性能 I/O 水平时，它会使用点数余额中的 I/O 点数突增到所需的性能水平，最大为 3000 IOPS。大于 1000 GiB 的卷的基准性能等于或大于最大突增性能，并且其 I/O 点数余额永远不会耗尽。如果卷在一秒内使用的 I/O 点数少于它所赚取的点数，未使用的 I/O 点数会加到 I/O 点数余额中。卷的最大 I/O 点数余额等于初始点数余额 (540 万 I/O 点数)。

下表列出了几种卷大小以及卷的相关基准性能 (也就是它积累 I/O 点数的速度)、在最大 3000 IOPS 时的突增持续时间 (从完整点数余额开始时) 以及卷重新填满空点数余额所需的秒数。

| 卷大小 (GiB) | 基准性能 (IOPS) | 最大突增持续时间 @ 3000 IOPS (秒数) | 填满空点数余额的秒数 |
|----------------------|-------------|---------------------------|------------|
| 1 | 100 | 1862 | 54000 |
| 100 | 300 | 2000 | 18000 |
| 214 (最大吞吐量的最小大小) | 642 | 2290 | 8412 |
| 250 | 750 | 2400 | 7200 |
| 500 | 1500 | 3600 | 3600 |
| 750 | 2250 | 7200 | 2400 |
| 1000 | 3000 | 不适用* | 不适用* |
| 3334 (最大 IOPS 的最小大小) | 10000 | 不适用* | 不适用* |
| 16384 (16 TiB，最大卷大小) | 10000 | 不适用* | 不适用* |

* 突增和 I/O 点数仅与低于 1000 GiB 的卷有关，此时突增性能超出了基准性能。

卷的突增持续时间取决于卷的大小、所需的突增 IOPS 以及突增开始时的点数余额。如下面的等式所示：

(Credit balance)

| |
|--|
| Burst duration = ----- (Burst IOPS) - 3(Volume size in GiB) |
|--|

如果我清空我的 I/O 点数余额，会发生什么情况？

如果您的 gp2 卷使用其所有 I/O 点数余额，则该卷的最大 IOPS 性能将保持在基准 IOPS 性能水平（亦即您的卷获得点数的速率），并且该卷的最大吞吐量将降低到最大 I/O 大小乘以基准 IOPS。吞吐量不能超过 160 MiB/s。当 I/O 需求下降到基准水平以下并且未使用的点数添加到 I/O 点数余额中时，该卷的最大 IOPS 性能将不再超出基准。例如，点数余额为空的 100 GiB gp2 卷具有 300 IOPS 的基准性能和 75 MiB/s 的吞吐量限制（每秒 300 个 I/O 操作 * 每个 I/O 操作 256 KiB = 75 MiB/s）。卷越大，基准性能就越高，补充点数余额的速度也越快。有关如何测量 IOPS 的详细信息，请参阅 [I/O 特性](#)。

如果您注意到卷性能常常受限于基准水平（由于空 I/O 点数余额），则应考虑使用较大的 gp2 卷（具有较高基准性能水平），或对需要大于 10000 IOPS 的持续 IOPS 性能的工作负载改用 io1 卷。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅 [监控 gp2、st1 和 sc1 卷的突增存储桶余额 \(p. 527\)](#)。

吞吐量性能

gp2 卷的吞吐量限制对于小于或等于 170 GiB 的卷是 128 MiB/s，对于大于 170 GiB 的卷是 160 MiB/s。

预配置 IOPS SSD (io1) 卷

预配置 IOPS SSD (io1) 卷旨在满足 I/O 密集型工作负载（尤其是数据库工作负载）的需要，这些工作负载对存储性能和一致性非常敏感。io1 卷不使用存储桶和信用模型计算性能，它允许您在创建卷时指定一致的 IOPS 速率，Amazon EBS 在指定年份的超过 99.9% 的时间里可提供 10% 以内的预配置 IOPS 性能。

io1 卷的大小范围为 4 GiB 到 16 TiB，您可以为每卷预配置 100 到 20,000 IOPS。预配置 IOPS 与请求的卷大小（以 GiB 为单位）的最大比率为 50:1。例如，100 GiB 卷可以预配置为最高 5,000 IOPS。任何大小为 400 GiB 或更大的卷可以预配置为最大值 20,000 IOPS。

对于预配置的每个 IOPS，io1 卷的吞吐量限制为 256 KiB，最高可达 320 MiB/s（在 1280 IOPS 情况下）。

您的每 I/O 延迟体验取决于预配置 IOPS 以及您的工作负载模式。要获得最佳的每 I/O 延迟体验，我们建议您将 IOPS 与 GiB 的比率预配置为大于 2:1。例如，2,000 IOPS 卷应该小于 1,000 GiB。

Note

2012 年以前创建的部分 AWS 账户可能可以访问 us-west-1 或 ap-northeast-1 中不支持 预配置 IOPS SSD (io1) 卷的可用区。如果您无法在其中一个区域中创建 io1 卷（或在其块储存设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

吞吐优化 HDD (st1) 卷

吞吐优化 HDD (st1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。此卷类型是大型顺序工作负载（如 Amazon EMR、ETL、数据仓库和日志处理）的理想之选。不支持可启动的 st1 卷。

Note

此卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅 [HDD 上的小型读/写效率低下问题 \(p. 527\)](#)。

吞吐量点数和突增性能

与 gp2 类似，st1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量点数的速度。卷大小还决定卷的突增吞吐量，即有点数可用时消耗点数的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的点数越多，它以突增水平驱动 I/O 的时间就越长。

下图显示 st1 的突增存储桶行为。

st1 卷的可用吞吐量受吞吐量和吞吐量点数上限的约束，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

对于 1 TiB st1 卷，突增吞吐量限制为 250 MiB/s，存储桶以 40 MiB/s 的速度填充，最多可容纳 1 TiB 点数。

较大卷以线性扩展这些限制，吞吐量上限为最大 500 MiB/s。存储桶耗尽后，吞吐量限制为每 TiB 40 MiB/s 的基准速率。

在从 0.5 到 16 TiB 的卷大小范围内，基准吞吐量从 20 到上限 500 MiB/s 变化，12.5 TiB 时达到上限，因为

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

突增吞吐量从 125 MiB/s 到上限 500 MiB/s 变化，2 TiB 时达到上限，因为

$$2 \text{ TiB} \times \frac{250 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

下表列出了 st1 基准和突增吞吐量值的完整范围：

| 卷大小 (TiB) | ST1 基准吞吐量 (MiB/s) | ST1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 0.5 | 20 | 125 |
| 1 | 40 | 250 |
| 2 | 80 | 500 |
| 3 | 120 | 500 |
| 4 | 160 | 500 |
| 5 | 200 | 500 |
| 6 | 240 | 500 |
| 7 | 280 | 500 |
| 8 | 320 | 500 |
| 9 | 360 | 500 |
| 10 | 400 | 500 |
| 11 | 440 | 500 |
| 12 | 480 | 500 |
| 12.5 | 500 | 500 |
| 13 | 500 | 500 |
| 14 | 500 | 500 |

| 卷大小 (TiB) | ST1 基准吞吐量 (MiB/s) | ST1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 15 | 500 | 500 |
| 16 | 500 | 500 |

下图绘制了表值：

Note

如果创建 吞吐优化 HDD (st1) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅[监控 gp2、st1 和 sc1 卷的突增存储桶余额 \(p. 527\)](#)。

Cold HDD (sc1) 卷

Cold HDD (sc1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。sc1 的吞吐量限制比 st1 更低，是大型顺序冷数据工作负载的理想选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的数据块存储。不支持可启动的 sc1 卷。

Note

此卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅[HDD 上的小型读/写效率低下问题 \(p. 527\)](#)。

吞吐量点数和突增性能

与 gp2 类似，sc1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量点数的速度。卷大小还决定卷的突增吞吐量，即有点数可用时消耗点数的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的点数越多，它以突增水平驱动 I/O 的时间就越长。

sc1 卷的可用吞吐量受吞吐量和吞吐量点数上限的约束，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

对于 1 TiB sc1 卷，突增吞吐量限制为 80 MiB/s，存储桶以 12 MiB/s 的速度填充，最多可容纳 1 TiB 点数。

较大卷以线性扩展这些限制，吞吐量上限为最大 250 MiB/s。存储桶耗尽后，吞吐量限制为每 TiB 12 MiB/s 的基准速率。

在从 0.5 到 16 TiB 的卷大小范围内，基准吞吐量从 6 MiB/s 到最大 192 MiB/s 变化，16 TiB 时达到上限，因为

$$\frac{12 \text{ MiB/s}}{16 \text{ TiB}} \times \frac{1}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

突增吞吐量从 40 MiB/s 到上限 250 MiB/s 变化，3.125 TiB 时达到上限，因为

$$\frac{80 \text{ MiB/s}}{3.125 \text{ TiB}} \times \frac{1}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

下表列出了 sc1 基准和突增吞吐量值的完整范围：

| 卷大小 (TiB) | SC1 基准吞吐量 (MiB/s) | SC1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 0.5 | 6 | 40 |
| 1 | 12 | 80 |
| 2 | 24 | 160 |
| 3 | 36 | 240 |
| 3.125 | 37.5 | 250 |
| 4 | 48 | 250 |
| 5 | 60 | 250 |
| 6 | 72 | 250 |
| 7 | 84 | 250 |
| 8 | 96 | 250 |
| 9 | 108 | 250 |
| 10 | 120 | 250 |
| 11 | 132 | 250 |
| 12 | 144 | 250 |
| 13 | 156 | 250 |
| 14 | 168 | 250 |
| 15 | 180 | 250 |
| 16 | 192 | 250 |

下图绘制了表值：

Note

如果创建 Cold HDD (sc1) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅[监控 gp2、st1 和 sc1 卷的突增存储桶余额 \(p. 527\)](#)。

磁介质 (standard)

磁介质卷由磁盘驱动器支持，适用于不经常访问数据的工作负载以及小型卷大小的低成本存储非常重要的场景。这些卷平均提供大约 100 IOPS，突增能力最大可达数百 IOPS，大小范围是 1 GiB 到 1 TiB。

Note

磁介质是上一代卷。对于新应用程序，我们建议使用较新的卷类型。有关更多信息，请参阅[上一代卷](#)。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅[监控 gp2、st1 和 sc1 卷的突增存储桶余额 \(p. 527\)](#)。

使用 HDD 卷时的性能注意事项

为了使用 HDD 卷获得最优的吞吐量结果，请根据以下注意事项计划您的工作负载。

吞吐优化 HDD 与 Cold HDD

`st1` 和 `sc1` 存储桶大小因卷大小而异，满的存储桶包含充足的令牌用于完整卷扫描。不过，因为每实例和每卷的吞吐量限制，更大的 `st1` 和 `sc1` 卷需要更长的时间完成卷扫描。附加到较小实例的卷被限制在每实例吞吐量上，而不是 `st1` 或 `sc1` 吞吐量限制。

`st1` 和 `sc1` 的设计都可以在 99% 的时间内提供 90% 的突增吞吐量性能一致性。不合规时间近似均匀分配，目标是达到 99% 的每小时预计总吞吐量。

下表列出了不同大小卷的理想扫描时间，假设存储桶是满的并且有充足的实例吞吐量。

一般来说，扫描时间可由此公式表示：

$$\frac{\text{Volume size}}{\text{Throughput}} = \frac{\text{Scan time}}{\text{Throughput}}$$

例如，考虑到性能一致性保证和其他优化，拥有 5 TiB 卷的 `st1` 客户预计在 2.91 到 3.27 小时内完成整卷扫描。

$$\begin{aligned} \frac{5 \text{ TiB}}{500 \text{ MiB/s}} &= \frac{5 \text{ TiB}}{0.00047684 \text{ TiB/s}} = 10,486 \text{ s} = 2.91 \text{ hours (optimal)} \\ 2.91 \text{ hours} + \frac{2.91 \text{ hours}}{(0.90)(0.99)} &= 3.27 \text{ hours (minimum expected)} \\ &\quad \text{-- From expected performance of 90% of burst 99% of the time} \end{aligned}$$

同样，拥有 5 TiB 卷的 `sc1` 客户预计在 5.83 到 6.54 小时内完成整卷扫描。

$$\begin{aligned} \frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} &= 20972 \text{ s} = 5.83 \text{ hours (optimal)} \\ 5.83 \text{ hours} + \frac{5.83 \text{ hours}}{(0.90)(0.99)} &= 6.54 \text{ hours (minimum expected)} \end{aligned}$$

| 卷大小 (TiB) | 带突增的 ST1 扫描时间 (小时)* | 带突增的 SC1 扫描时间 (小时)* |
|-----------|---------------------|---------------------|
| 1 | 1.17 | 3.64 |
| 2 | 1.17 | 3.64 |
| 3 | 1.75 | 3.64 |
| 4 | 2.33 | 4.66 |
| 5 | 2.91 | 5.83 |
| 6 | 3.50 | 6.99 |
| 7 | 4.08 | 8.16 |

| 卷大小 (TiB) | 带突增的 ST1 扫描时间 (小时)* | 带突增的 SC1 扫描时间 (小时)* |
|-----------|---------------------|---------------------|
| 8 | 4.66 | 9.32 |
| 9 | 5.24 | 10.49 |
| 10 | 5.83 | 11.65 |
| 11 | 6.41 | 12.82 |
| 12 | 6.99 | 13.98 |
| 13 | 7.57 | 15.15 |
| 14 | 8.16 | 16.31 |
| 15 | 8.74 | 17.48 |
| 16 | 9.32 | 18.64 |

* 这些扫描时间在执行 1 MiB 顺序 I/O 时采取平均队列深度 (四舍五入到最近的整数) 四或更多。

因此，如果您有面向吞吐量的工作负载需要快速完成扫描 (最快 500 MiB/s) 或一天查询几个整卷，请使用 `st1`。如果您针对成本进行了优化，数据访问相对不频繁，而且不需要超过 250 MiB/s 的扫描性能，请使用 `sc1`。

HDD 上的小型读/写效率低下问题

`st1` 和 `sc1` 卷的性能模型针对顺序 I/O 进行了优化，支持高吞吐量工作负载，对具有混合 IOPS 和吞吐量的工作负载提供可接受的性能，不建议使用具有小型随机 I/O 的工作负载。

例如，1 MiB 或更小的 I/O 请求计为 1 MiB I/O 点数。但是，如果是顺序 I/O，则会合并为 1 MiB I/O 数据块，并且只计为 1 MiB I/O 点数。

每实例吞吐量限制

`st1` 和 `sc1` 卷的吞吐量始终由以下限制中较小的决定：

- 卷的吞吐量限制
- 实例的吞吐量限制

对于所有 Amazon EBS 卷，我们建议选择适当的 EBS 优化的 EC2 实例来避免网络瓶颈。有关更多信息，请参阅 [Amazon EBS 优化实例](#)。

监控 `gp2`、`st1` 和 `sc1` 卷的突增存储桶余额

您可以使用 Amazon CloudWatch 中提供的 EBS `BurstBalance` 指标来监控 `gp2`、`st1` 和 `sc1` 卷的突增存储桶水平。这个指标显示突增存储桶中剩余的 I/O 点数百分比 (对于 `gp2`) 或吞吐量点数 (对于 `st1` 和 `sc1`)。有关 `BurstBalance` 指标和与 I/O 相关的其他指标的更多信息，请参阅 [I/O 特性和监控](#)。CloudWatch 还允许您设置警报以便在 `BurstBalance` 值小于某一水平时通知您。有关 CloudWatch 警报的更多信息，请参阅 [创建 Amazon CloudWatch 警报](#)。

创建 Amazon EBS 卷

您可以创建一个 Amazon EBS 卷，然后将它连接到同一可用区内的任何 EC2 实例。您可以选择创建加密 EBS 卷，但是加密卷只能连接到所选的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。

您可以使用 IAM 策略对新卷进行加密。有关更多信息，请参阅 [4：使用卷 \(p. 400\)](#) 和 [5：启动实例 \(RunInstances\) \(p. 403\)](#) 中的示例 IAM 策略。

如果通过指定块储存设备映射启动实例，也可以创建并连接 EBS 卷。有关更多信息，请参阅 [启动实例 \(p. 244\)](#) 和 [块储存设备映射 \(p. 609\)](#)。您可基于先前创建的快照来还原卷。有关更多信息，请参阅 [从快照还原 Amazon EBS 卷 \(p. 529\)](#)。

您可以在创建时向 EBS 卷应用标签。借助标记，您可以简化对 Amazon EC2 资源清单的跟踪工作。可以将创建时标记与 IAM 策略结合起来，在新卷上强制实施标记。有关更多信息，请参阅[标记您的成员资源](#)。

如果您要针对一种高性能存储情形来创建卷，应确保使用 预配置 IOPS SSD (io1) 卷并将它连接到一个具有足够带宽支持您的应用程序的实例，如 EBS 优化实例或具有 10 GiB 网络连接的实例。对吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷也是同样的建议。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 573\)](#)。

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。访问数据完毕后，性能随之恢复。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 578\)](#)。

使用控制台创建 EBS 卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中，选择您想创建卷的区域。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 在导航窗格中的 ELASTIC BLOCK STORE 下，选择 Volumes。
4. 在上方窗格上，选择 Create Volume。
5. 在 Create Volume 对话框中，对于 Volume Type，选择 通用型 SSD (GP2)、预配置 IOPS SSD (IO1)、吞吐优化 HDD (ST1)、Cold HDD (SC1) 或 磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

Note

2012 年以前创建的部分 AWS 账户可能可以访问 us-west-1 或 ap-northeast-1 中不支持 预配置 IOPS SSD (io1) 卷的可用区。如果您无法在其中一个区域中创建 io1 卷（或在其块储存设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

6. 对于 Size，输入卷大小，以 GiB 为单位。
7. 对于 io1 卷，在 IOPS 字段中输入该卷应支持的每秒输入/输出操作 (IOPS) 的最大值。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。
9. (可选) 要创建加密卷，请选中 Encrypted (已加密) 框，然后选择您希望在加密卷时所使用的主密钥。您可以选择自己账户的默认主密钥，也可以选择此前使用 AWS Key Management Service 创建的任何客户主密钥 (CMK)。Master Key (主密钥) 菜单中显示了可用的密钥，或者您可以粘贴您能访问的任何密钥的完整 ARN。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

Note

加密卷只能连接到所选的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。

10. 选择 Yes, Create。

使用命令行创建 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-volume \(AWS CLI\)](#)
- [New-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

从快照还原 Amazon EBS 卷

您可以使用存储在 Amazon S3 中的快照的数据还原 Amazon EBS 卷。您需要知道您希望用来还原卷的快照的 ID，还需要拥有对该快照的访问权限。有关快照的更多信息，请参阅 [Amazon EBS 快照 \(p. 559\)](#)。

基于现有 EBS 快照创建的新卷在后台延时加载。也就是说，通过快照创建卷之后，无需等待所有数据从 Amazon S3 传输到 EBS 卷，连接的实例即可开始访问该卷及其所有数据。如果您的实例访问还没有加载的数据，卷会立即从 Amazon S3 下载请求的数据，并在后台继续加载剩余数据。

从加密快照还原的 EBS 卷会自动加密。加密卷只能连接到所选的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。

由于存在安全限制，您不可以从不属于您的共享加密快照直接还原 EBS 卷。您必须首先创建属于您的快照副本。之后，您便可以从该副本还原卷。有关更多信息，请参阅 [Amazon EBS 加密](#)。

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。访问数据完毕后，性能随之恢复。

对于大部分应用程序，可将此初始化成本分摊到卷的整个使用期限。如果您需要确保您的存储卷始终能在生产高峰期正常工作，可使用 dd 或 fio 对整个卷强制实施即时初始化。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 578\)](#)。

使用控制台从快照还原 EBS 卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航栏中，选择快照所处的区域。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅 [资源位置 \(p. 619\)](#)。如果您需要将快照还原到在不同区域的某个卷，则您可以将快照复制到该新区域，然后将它还原到该区域的一个卷。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 561\)](#)。
3. 在导航窗格中，选择 Volumes、Create Volume。
4. 在 Create Volume 对话框中，对于 Volume Type 选择 通用型 SSD、预配置 IOPS SSD 或 磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

Note

2012 年以前创建的部分 AWS 账户可能可以访问 us-west-1 或 ap-northeast-1 中不支持 预配置 IOPS SSD (`io1`) 卷的可用区。如果您无法在其中一个区域中创建 `io1` 卷（或在其块储存设备映射中启动具有 `io1` 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB `io1` 卷来验证该可用区是否支持 `io1` 卷。

5. 对于 Snapshot，开始键入您要用于还原卷的快照的 ID 或描述，并从所建议的选项列表中选择该快照。

Note

从加密快照还原的卷只能连接到支持 Amazon EBS 加密的实例。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。

6. 对于 Size，输入卷的大小（以 GiB 为单位），或验证快照的默认大小是否足够。

如果您指定卷大小和快照 ID，其大小必须等于或大于快照的大小。当您选择一种卷类型和一个快照 ID 时，最小和最大卷大小将显示在 Size (大小) 列表旁边。任何来自快照的 AWS Marketplace 产品代码都会传送到该卷。

7. 对于 `io1` 卷，在 IOPS 字段中输入该卷可支持的每秒输入/输出操作 (IOPS) 的最大值。
8. 在 Availability Zone (可用区) 列表中，选择要在其中创建卷的可用区。EBS 卷只能挂载到同一可用区中的 EC2 实例。
9. 选择 Yes, Create。

Important

如果将一个快照还原到了超过该快照默认大小的一个较大的卷，则需要扩展卷上的文件系统以利用额外的空间。有关更多信息，请参阅 [在 Linux 上修改 EBS 卷的大小、IOPS 或类型 \(p. 543\)](#)。

从快照恢复某个卷后，您可以将其挂载到实例上并开始使用。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

使用命令行还原 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-volume \(AWS CLI\)](#)
- [New-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

将 Amazon EBS 卷连接到实例

您可以将 EBS 卷连接到与该卷处于同一可用区中的任一实例。

先决条件

- 确定您将使用的设备名称。有关更多信息，请参阅 [Linux 实例上的设备命名 \(p. 608\)](#)。
- 确定您可以将多少个卷连接到您的实例。有关更多信息，请参阅 [实例卷限制 \(p. 607\)](#)。
- 如果卷是加密的，则只能将它连接到支持 Amazon EBS 加密的实例。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。
- 如果某个卷有 AWS Marketplace 产品代码：
 - 卷只能连接到已停止的实例。
 - 您必须订阅卷上的 AWS Marketplace 代码。
 - 实例的配置(实例类型、操作系统)必须支持这一特定的 AWS Marketplace 代码。例如，您不能从 Windows 实例取用卷，然后将其连接到 Linux 实例。
 - AWS Marketplace 产品代码从卷复制到实例。

使用控制台将 EBS 卷连接到实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择卷，然后选择 Actions、Attach Volume。
4. 在 Attach Instance 对话框中，开始在 Instance 中键入要将卷挂载到的实例的名称或 ID，并从建议的选项(只显示与卷处于相同可用区中的实例)的列表中选择它。
5. 您可以保留推荐的设备名称，也可以输入其他受支持的设备名称。

Important

该实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的不同。

6. 选择 Attach。
7. 连接到您的实例并将卷置于可用状态。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 531\)](#)。

使用命令行将 EBS 卷连接到实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [attach-volume \(AWS CLI\)](#)
- [Add-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

使 Amazon EBS 卷可用

将某个 Amazon EBS 卷连接到您的实例后，该卷将显示为块储存设备。您可以使用任何文件系统将卷格式化，然后进行安装。在使 EBS 卷可供使用后，您可以像访问其他所有卷一样访问该卷。任何写入此文件系统的数据均写入 EBS 卷，并且对使用该设备的应用程序是透明的。

请注意，您可以拍摄 EBS 卷的快照以进行备份或在您创建其他卷时作为基线。有关更多信息，请参阅 [Amazon EBS 快照 \(p. 559\)](#)。

使卷可在 Linux 上使用

按照以下过程使卷可用。请注意，您可以从 Amazon EC2 用户指南（适用于 Windows 实例）中的[使卷可在 Windows 上使用](#)，获得有关 Windows 实例上的卷的指示。

使 EBS 卷可在 Linux 上使用

1. 使用 SSH 连接到您的实例。有关更多信息，请参阅 [步骤 2：连接到您的实例 \(p. 22\)](#)。
2. 根据内核的块储存设备驱动程序，附加的设备所采用的名称可能与您指定的名称不同。例如，如果您指定设备名称 /dev/sdh，内核可能将该设备重命名为 /dev/xvdh 或 /dev/hdh；在大多数情况下，尾部字母保持不变。在某些版本的 Red Hat Enterprise Linux（及其变体，例如，CentOS）中，尾部字母也可能发生变化（例如 /dev/sda 可能变为 /dev/xvde）。在这些情况下，设备名称各尾部字母都会递增相同次数。例如，/dev/sdb 将变为 /dev/xvdf，/dev/sdc 将变为 /dev/xvdg。Amazon Linux AMI 会使用您在启动时指定的名称创建指向重命名设备路径的符号链接，但是其他 AMI 的工作方式可能不同。

使用 lsblk 命令可查看可用磁盘设备及其安装点（如果适用），以帮助您确定要使用的正确设备名称。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvdf  202:80    0 100G  0 disk
xvda1 202:1     0   8G  0 disk /
```

lsblk 的输出移除了完整设备路径中的 /dev/ 前缀。在此示例中，/dev/xvda1 安装为根设备（请注意 MOUNTPOINT 被列为 /，即 Linux 文件系统层次结构的根），且连接了 /dev/xvdf，但它还未安装。

3. 确定是否需要在卷上创建文件系统。新卷为原始的块储存设备，您需要先在这种设备上创建文件系统，然后才能够安装并使用它们。从快照还原的卷可能已经含有文件系统；如果您在现有的文件系统上创建新的文件系统，则该操作将覆盖您的数据。使用 sudo file -s **device** 命令可列出特殊信息，例如文件系统类型。

```
[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data
```

如果前面的命令的输出仅显示该设备的 data，则说明设备上没有文件系统，您需要创建一个文件系统。您可继续[Step 4 \(p. 531\)](#)。如果您在包含文件系统的设备上运行此命令，则您的输出将有所不同。

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-
a14c-8c64d6819362 (needs journal recovery) (extents) (large files) (huge files)
```

在以上示例中，该设备包含 Linux rev 1.0 ext4 filesystem data，因此，此卷无需创建文件系统（如果您的输出中显示文件系统数据，则可以跳过[Step 4 \(p. 531\)](#)）。

4. （有条件）使用以下命令在卷上创建 ext4 文件系统。用设备名称（例如，/dev/xvdf）替换 **device_name**。根据应用程序的要求或操作系统的限制，您可以选择其他文件系统类型，如 ext3 或 XFS。

Warning

此步骤假定您在安装空的卷。如果要安装已包含数据的卷(如，从快照还原的卷)，请勿在安装卷之前使用 mkfs(而应跳到下一步)。否则，您会格式化卷并删除现有数据。

```
[ec2-user ~]$ sudo mkfs -t ext4 device_name
```

5. 使用以下命令创建卷的安装点目录。安装点是卷在文件系统树中的位置，以及您在安装卷之后读写文件的位置。替换 **mount_point** 的位置，如 /data。

```
[ec2-user ~]$ sudo mkdir mount_point
```

6. 使用以下命令在您刚才创建的位置安装卷。

```
[ec2-user ~]$ sudo mount device_name mount_point
```

7. (可选) 要在每一次系统重启时安装此 EBS 卷，可在 /etc/fstab 文件中为该设备添加一个条目。

- a. 创建 /etc/fstab 文件的备份，当您进行编辑时意外损坏或删除了此文件的情况下，可以使用该备份。

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

- b. 使用任意文本编辑器(如 nano 或 vim) 打开 /etc/fstab 文件。

Note

需要将该文件作为 root 打开或使用 sudo 命令打开。

- c. 使用以下格式在卷文件的末尾添加一行：

```
device_name mount_point file_system_type fs_mntops fs_freq fs_passno
```

该行上的最后三个字段是文件系统装载选项、文件系统的转储频率和引导时完成的文件系统顺序检查。如果您不知道这些值应该是什么值，请使用下面的示例中的值 (defaults,nofail 0 2)。有关 /etc/fstab 条目的更多信息，请参阅 fstab 手册页面(通过在命令行上输入 man fstab)。

您可以使用系统的当前设备名称(/dev/sda1、/dev/xvda1等)在 /etc/fstab 中，我们建议使用设备的 128 位通用唯一标识符(UUID)代替。系统声明的块设备名称可能会在各种情况下更改，但是格式化时 UUID 会分配给卷分区，并在整个分区的使用寿命期间保留。通过使用 UUID，您可以减少 /etc/fstab 中块设备映射的机会，使系统在硬件重新配置后无法引导。

要查找设备的 UUID，请首先显示可用设备：

```
[ec2-user ~]$ df
```

这会产生类似下面的列表：

| Filesystem | 1K-blocks | Used | Available | Use% | Mounted on |
|------------|-----------|---------|-----------|------|------------|
| /dev/xvda1 | 8123812 | 1876888 | 6146676 | 24% | / |
| devtmpfs | 500712 | 56 | 500656 | 1% | /dev |
| tmpfs | 509724 | 0 | 509724 | 0% | /dev/shm |

接下来，继续本示例，检查两个命令中任意一个的输出，以找到 /dev/xvda1 的 UUID：

- **sudo file -s /dev/xvda1**
- **ls -al /dev/disk/by-uuid/**

假设您找到具有 UUID de9a1ccd-a2dd-44f1-8be8-0123456abcdef 的 /dev/xvda1，您可以将以下条目添加到 /etc/fstab 以在装载点装载 ext4 文件系统 /data：

```
UUID=de9a1ccd-a2dd-44f1-8be8-0123456abcdef      /data    ext4    defaults,nofail
0          2
```

Note

如果您要在未连接此卷的情况下启动实例（例如，以便此卷可以在不同实例之间向后和向前移动），则应添加 nofail 安装选项，该选项允许实例即使在卷安装过程中出现错误时也可启动。Debian 衍生物（包括早于 16.04 的 Ubuntu 版本）还必须添加 nobootwait 挂载选项。

- d. 将新条目添加到 /etc/fstab 后，需要检查条目是否有效。运行 sudo mount -a 命令，以便安装 /etc/fstab 中的所有文件系统。

```
[ec2-user ~]$ sudo mount -a
```

如果上述命令未产生错误，说明您的 /etc/fstab 文件正常，您的文件系统会在下次启动时自动安装。如果该命令产生了任何错误，请检查这些错误并尝试更正 /etc/fstab。

Warning

/etc/fstab 文件中的错误可能导致系统无法启动。请勿关闭 /etc/fstab 文件中有错误的系统。

- e.（可选）如果您无法确定如何更正 /etc/fstab 错误，则始终可以使用以下命令还原您的备份 /etc/fstab 文件。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

8. 检查新卷安装的文件权限，确保您的用户和应用程序可以向该卷写入数据。有关文件权限的更多信息，请参阅 Linux 文档项目 [文件安全性](#)。

查看卷信息

您可以在 AWS 管理控制台中同时查看所选区域中 Amazon EBS 卷的描述性信息。您还可以查看有关单个卷的详细信息，包括大小、卷类型、卷是否加密、加密卷所用的主密钥以及卷所连接的特定实例。

使用控制台查看有关 EBS 卷的信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 要查看有关卷的更多信息，请选择该选项。在详细信息窗格中，您可以检查所提供的关于卷的信息。

了解某个 Amazon EC2 实例附加了哪些 EBS（或其他）卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 要查看有关某个实例的更多信息，请选择该实例。
4. 在详细信息窗格中，您可以检查所提供的关于根设备和块储存设备的信息。

使用命令行查看有关 EBS 卷的信息

您可以使用以下命令之一查看卷属性。有关更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volumes \(AWS CLI\)](#)
- [Get-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

监控您的卷状态

Amazon Web Services (AWS) 自动提供数据，如 Amazon CloudWatch 指标和卷状态检查，您可以使用这些数据来监控您的 Amazon Elastic Block Store (Amazon EBS) 卷。

内容

- [使用 CloudWatch 监控卷 \(p. 534\)](#)
- [使用状态检查来监控卷 \(p. 536\)](#)
- [监控卷事件 \(p. 537\)](#)
- [使用一个受损卷工作 \(p. 538\)](#)
- [使用 AutoEnableIO 卷属性 \(p. 540\)](#)

使用 CloudWatch 监控卷

CloudWatch 指标是统计数据，您可以使用这些指标来查看、分析和设置有关卷操作行为的警报。

下表描述适用于您的 Amazon EBS 卷的监控数据的类型。

| 类型 | 说明 |
|----|--|
| 基本 | 数据在 5 分钟期间内自动可用，无需收费。该数据包括 EBS 支持的实例的根设备卷数据。 |
| 明细 | 预配置 IOPS SSD (io1) 卷向 CloudWatch 自动发送一分钟指标。 |

当您从 CloudWatch 得到数据时，您可以列入一个 `Period` 请求参数来指定返回数据的粒度。这不同于我们收集数据时所用的时间（5 分钟时间）。我们建议您在您的请求中指定的时间大于或等于收集时间，从而确保返回数据有效。

获取数据时，您可以使用 CloudWatch API 或 Amazon EC2 控制台。控制台从 CloudWatch API 中获取原始数据并根据数据显示一系列图表。根据您的需要，您既可以选择使用从 API 中获得的数据也可以选择使用控制台中的图表。

Amazon EBS 指标

Amazon Elastic Block Store (Amazon EBS) 可将若干指标的数据点发送到 CloudWatch。Amazon EBS 通用型 SSD (gp2)、吞吐优化的 HDD (st1)、冷数据 HDD (sc1) 和磁盘 (标准) 卷自动将 5 分钟指标发送到 CloudWatch。预配置的 IOPS SSD (io1) 卷会自动向 CloudWatch 发送 1 分钟指标。有关如何监控 Amazon EBS 的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 [监控您的卷状态](#)。

AWS/EBS 命名空间包括以下指标。

| 指标 | 说明 |
|-------------------------------|--|
| <code>VolumeReadBytes</code> | 提供有关指定时段内的 I/O 操作的信息。 <code>Sum</code> 统计数据将报告该时段内传输的总字节数。 <code>Average</code> 统计数据将报告指定时段内每个 I/O 操作的平均大小。 <code>SampleCount</code> 统计数据将报告指定时段内的 I/O 操作总数。 <code>Minimum</code> 和 <code>Maximum</code> 统计数据与该指标无关，卷处于活动状态时，数据仅报告给 Amazon |
| <code>VolumeWriteBytes</code> | |

| 指标 | 说明 |
|---|---|
| | <p>CloudWatch。如果卷处于空闲状态，则不会向 Amazon CloudWatch 报告任何数据。</p> <p>单位：字节</p> |
| VolumeReadOps VolumeWriteOps | <p>在指定时间的 I/O 操作总数。</p> <p>Note</p> <p>要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。</p> <p>单位：计数</p> |
| VolumeTotalReadTime VolumeTotalWriteTime | <p>指定时间段中所有操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 5 分钟 (300 秒) 的时间段：如果该时间段内完成了 700 个操作，每个操作耗时 1 秒，值便是 700 秒。</p> <p>单位：秒</p> |
| VolumeIdleTime | <p>未提交读取或写入操作的指定时间段中的总秒数。</p> <p>单位：秒</p> |
| VolumeQueueLength | <p>指定时间段中等待完成的读取和写入操作请求的数量。</p> <p>单位：计数</p> |
| VolumeThroughputPercent | <p>仅用于预配置 IOPS SSD 卷。每秒传输的 I/O 操作数 (IOPS) 在为 Amazon EBS 卷预配置的总 IOPS 中所占的百分比。预配置 IOPS SSD 卷在指定年份的超过 99.9% 的时间里可提供预配置 IOPS 的 10%。</p> <p>Note</p> <p>写入过程中，如果一分钟内没有其他待处理的 I/O 请求，指标值就会是 100%。另外，卷的 I/O 性能可能由于您已执行的操作而暂时降低 (例如：在使用高峰期创建卷的快照、在非 EBS 优化的实例上运行卷，首次访问你卷上的数据)。</p> <p>单位：百分比</p> |
| VolumeConsumedReadWriteOps | <p>仅用于预配置 IOPS SSD 卷。指定时间段内使用的读取和写入操作的总量 (规格化为 256K 容量单位)。</p> <p>每个小于 256K 的 I/O 操作算作使用了 1 IOPS。大于 256K 的 I/O 操作按 256K 容量单位计算。例如，1024K I/O 算作使用了 4 IOPS。</p> <p>单位：计数</p> |
| BurstBalance | <p>仅用于通用型 SSD (gp2)、吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷。提供有关突增存储桶中剩余的 I/O 点数百分比 (对于 gp2) 或吞吐量点数 (对于 st1 和 sc1) 的信息。仅在卷处于活动状态时，数据才报告给 CloudWatch。如果未挂载卷，则不会报告任何数据。</p> <p>单位：百分比</p> |

Amazon EBS 指标的维度

Amazon EBS 发送到 CloudWatch 的唯一维度是卷 ID。这表示所有可用统计数据会通过卷 ID 进行筛选。

Amazon EC2 控制台中的图表

创建一个卷后，您可以在 Amazon EC2 控制台中查看该卷的监控图表。在控制台的 Volumes 页面上选择一个卷，然后选择 Monitoring。下表列出了显示的图表。右列说明如何使用从 CloudWatch API 中获得的原始数据指标来生成每一个图表。所有的图表周期都是 5 分钟。

| 图表 | 使用原始指标描述 |
|-----------------|----------------------------------|
| 读取带宽 (KiB/s) | 总和(VolumeReadBytes) / 周期 / 1024 |
| 写入带宽 (KiB/s) | 总和(VolumeWriteBytes) / 周期 / 1024 |
| 读取吞吐量 (Ops/s) | 总和(VolumeReadOps) / 周期 |
| 写入吞吐量 (Ops/s) | 总和(VolumeWriteOps) / 周期 |
| 平均队列长度 (ops) | 平均 (VolumeQueueLength) |
| 空闲花费时间百分比 | 总和 (VolumedIdleTime) / 周期 * 100 |
| 平均读取大小 (KiB/op) | 平均 (VolumeReadBytes) / 1024 |
| 平均写入大小 (KiB/op) | 平均 (VolumeWriteBytes) / 1024 |
| 平均读取延迟 (ms/op) | 平均 (VolumeTotalReadTime) * 1000 |
| 平均写入延迟 (ms/op) | 平均 (VolumeTotalWriteTime) * 1000 |

对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

使用状态检查来监控卷

通过卷状态检查，您可以更好地了解、追踪和管理 Amazon EBS 卷上数据的潜在不一致性。它们的作用是在您需要确定 Amazon EBS 卷是否损坏的时候为您提供信息，帮助您控制处理潜在不一致卷的方式。

卷状态检查为自动执行的测试，该测试每隔 5 分钟运行一次并返回通过或故障状态。如果所有的检查都通过，则卷的状态为 `ok`。如果一个检查返回故障，则卷的状态为 `impaired`。如果状态为 `insufficient-data`，那么该检查将在该卷上继续进行。您可以查看卷状态检查的结果来识别任意受损卷并进行所需操作。

当 Amazon EBS 判定一个卷中的数据具有潜在不一致性时，默认禁用从任何连接的 EC2 实例到该卷的 I/O，以此来防止数据损坏。禁用 I/O 后，下一个卷状态检查故障，并且卷状态为 `impaired`。此外，您还会看到一个通知您 I/O 被禁用的事件，并且您可以通过使能该卷的 I/O 来解决卷的损坏状态。我们将一直等待，直至您启用 I/O 以便您能够决定是继续让实例使用该卷，还是使用命令（例如 `fsck`（Linux）或 `chkdsk`（Windows））来运行一致性检查。

Note

卷状况以卷状况检查为依据，并不反映卷状态。因此，卷状态并不表示卷处于 `error` 状态（例如，卷无法接受 I/O 时）。

如果某一个卷的一致性对您无关重要，您可以立即使该卷可用，如果该卷受损，您可以配置该卷为自动使能 I/O 来覆盖默认行为，如果您使能了 `AutoEnableIO` 这一属性，那么该卷的状态检查将一直保持为通过。此外，您将会看到一个通知您该卷具有潜在不一致性的事件，但它的 I/O 不会自动使能。这使您能够检查卷的一致性或随后替换它。

I/O 性能状态检查将实际卷性能与卷的预期性能进行比较，并在卷性能低于预期时向您发出警示。此状态检查只适用于附加到实例的 `io1` 卷，对于通用型 SSD (`gp2`)、吞吐优化 HDD (`st1`)、Cold HDD (`sc1`) 或 磁介质 (`standard`) 卷无效。I/O 性能状态检查每分钟执行一次，CloudWatch 每 5 分钟收集一次这些数据，因此在将 `io1` 卷附加到实例之后，最多可能要到 5 分钟后此检查才会报告 I/O 性能状态。

Important

在初始化已从快照还原的 `io1` 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O Performance 状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 `io1` 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 578\)](#)。

下表列出了 Amazon EBS 卷的状态。

| 卷状态 | I/O 使能状态 | I/O 性能状态 (只适用于预配置 IOPS 卷) |
|--------------------------------|--|--|
| <code>ok</code> | 使能 (I/O 使能或 I/O 自动使能) | 正常 (卷的期望性能) |
| <code>warning</code> | 使能 (I/O 使能或 I/O 自动使能) | 降级 (卷的性能低于期望性能) 严重降级 (卷的性能大大低于期望性能) |
| <code>impaired</code> | 使能 (I/O 使能或 I/O 自动使能) 禁用 (卷脱机和挂起恢复，或等待用户使能 I/O) | 停滞 (卷性能受到严重影响) 不可用 (由于 I/O 被禁用，所以不能确定 I/O 性能) |
| <code>insufficient-data</code> | 使能 (I/O 使能或 I/O 自动使能) 数据不足 | 数据不足 |

您可以使用 Amazon EC2 控制台、API 或命令行界面来查看和使用状态检查。

在控制台中查看状态检查

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 在 EBS Volumes 页面上，使用 Volume Status 列列出每个卷的运行状态。
4. 要查看某个卷的状态，请选中该卷，然后选择 Status Checks。
5. 如果您的卷状态检查返回故障 (状态是 `impaired`)，请参阅 [使用一个受损卷工作 \(p. 538\)](#)。

另外，您还可以使用“Events”窗格来查看一个单一窗格中的实例和卷所有的事件。有关更多信息，请参阅 [监控卷事件 \(p. 537\)](#)。

使用命令行查看卷状态信息

您可以使用以下命令之一查看 Amazon EBS 卷的状态。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `describe-volume-status` (AWS CLI)
- `Get-EC2VolumeStatus` (适用于 Windows PowerShell 的 AWS 工具)

监控卷事件

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何连接的 EC2 实例对该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来查明故障的原因。

想要自动使能具有潜在不一致性卷上的 I/O，您可以改变 `AutoEnableIO` 卷属性的设置。更多关于改变这些属性的信息，请参阅 [使用一个受损卷工作 \(p. 538\)](#)。

每一个事件都包括一个开始时间，该时间指明事件发生的时间，和一个持续时间，该时间会指明该卷 I/O 会被禁用多久。当该卷的 I/O 被使能时，将会为该事件添加结束时间。

卷状态事件包括下列描述中的一个：

等待操作：使能 IO

卷数据具有潜在一致性。在您明确的使能它之前，将一直禁用 I/O。您明确使能 I/O 后，事件描述变为“IO Enabled”。

IO 使能

明确地使能这些卷的 I/O 操作。

IO 自动使能

事件发生后，自动使能这些卷上的 I/O 操作。我们建议您在继续使用数据前，先检查数据的不一致性。

普通

仅限 io1 卷。卷执行其期望性能。

降级

仅限 io1 卷。卷性能低于期望性能。

严重降级

仅限 io1 卷。卷性能大大地低于期望性能。

停滞

仅限 io1 卷。卷的性能受到严重影响。

您可以使用 Amazon EC2 控制台、API 或命令行界面来查看您的卷事件。

在控制台中查看卷的事件

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Events。
3. 列出具有事件的所有实例和卷。可以按卷进行筛选以便仅查看卷状态。您也可以过滤指定的状态类型。
4. 选择一个卷以查看其特定事件。

如果您的卷 I/O 被禁用，请参阅[使用一个受损卷工作 \(p. 538\)](#)。如果您的卷 I/O 性能低于正常值，这可能是因为您之前的操作（例如，在使用高峰期间创建卷快照、在无法支持所需 I/O 带宽的实例上运行卷、第一次访问卷上的数据，等等）而造成的暂时状况。

使用命令行查看卷的事件

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volume-status](#) (AWS CLI)
- [Get-EC2VolumeStatus](#) (适用于 Windows PowerShell 的 AWS 工具)

使用一个受损卷工作

本节讨论了如果因为您的卷中数据具有潜在不一致性而导致一个卷受损时您可以进行的选择。

选项

- 选择 1：在附加到它的实例上的卷上进行一次一致性检查。 (p. 539)
- 选择 2：使用其他实例在该卷上进行一次一致性检查 (p. 539)
- 选择 3：如果您不再需要它，请删除该卷 (p. 540)

选择 1：在附加到它的实例上的卷上进行一次一致性检查。

最简单的选择是使能 I/O，然后在卷上进行一次数据一致性检查，但该卷仍附加到它的 Amazon EC2 实例。

想要在一个附加的卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 在该卷上使能 I/O。
 - a. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
 - b. 在导航窗格中，选择 Volumes。
 - c. 选择要使能 I/O 操作的卷。
 - d. 在详细信息窗格中，选择 Enable Volume IO。
3. 检查卷上数据。
 - a. 运行 fsck (Linux) 或 chkdsk (Windows) 命令。
 - b. (可选) 查看所有适用的应用程序或系统日志以了解相关错误消息。
 - c. 如果卷受损时间超过 20 分钟，您可以联系支持。选择 Troubleshoot，然后在 Troubleshoot Status Checks 对话框上选择 Contact Support 提交一个支持案例。

使用命令行启用卷的 I/O

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [enable-volume-io \(AWS CLI\)](#)
- [Enable-EC2VolumeIO \(适用于 Windows PowerShell 的 AWS 工具\)](#)

选择 2：使用其他实例在该卷上进行一次一致性检查

按照以下程序在您的产品环境外检查该卷。

Important

当卷 I/O 被禁用时，这些程序可能会导致挂起的写入 I/O 丢失。

想要在一个隔离环境中在一个卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 将该卷从实例中分离。
 - a. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
 - b. 在导航窗格中，选择 Volumes。
 - c. 选择要分离的卷。
 - d. 选择 Actions、Force Detach Volume。系统会提示您进行确认。
3. 在该卷上使能 I/O。
 - a. 在导航窗格中，选择 Volumes。

- b. 选择您在之前的步骤中分离的卷。
 - c. 在详细信息窗格中，选择 Enable Volume IO。
 - d. 在 Enable Volume IO 对话框中选择 Yes, Enable。
4. 将该卷附加到另一个实例。有关信息，请参阅 [启动实例 \(p. 243\)](#) 和 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
5. 检查卷上数据。
- a. 运行 fsck (Linux) 或 chkdsk (Windows) 命令。
 - b. (可选) 查看所有适用的应用程序或系统日志以了解相关错误消息。
 - c. 如果卷受损时间超过 20 分钟，您可以联系支持。选择 Troubleshoot，然后在故障排除对话框中选择 Contact Support 以提交支持案例。

使用命令行启用卷的 I/O

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [enable-volume-io \(AWS CLI\)](#)
- [Enable-EC2VolumeIO \(适用于 Windows PowerShell 的 AWS 工具\)](#)

选择 3：如果您不再需要它，请删除该卷

如果您想将该卷从您的环境中去除，只需删除它即可。关于删除一个卷的信息，请查阅 [删除 Amazon EBS 卷 \(p. 542\)](#)。

如果您有在该卷上备份的近期快照，那么您可以从快照中创建一个新卷。关于从一个快照中新建一个卷的信息，请查阅 [从快照还原 Amazon EBS 卷 \(p. 529\)](#)。

使用 AutoEnableIO 卷属性

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何连接的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来智明故障的原因。如果特定卷的一致性无关紧要，并且您希望在其为 impaired 的情况下该卷立即可用，可通过将该卷配置为自动启用 I/O 来覆盖默认行为。如果您启用 AutoEnableIO 卷属性，则会自动重新启用该卷与实例之间的 I/O，该卷的状态检查会通过。此外，您将会看到一个通知您该卷具有潜在不一致状态的事件，但它的 I/O 不会自动启用。如果发生此事件，您应该检查该卷的一致性，如有必要，可对其进行更换。有关更多信息，请参阅 [监控卷事件 \(p. 537\)](#)。

本部分介绍如何使用 Amazon EC2 控制台、命令行界面或 API 来查看和修改卷的 AutoEnableIO 属性。

在控制台中查看卷的 AutoEnableIO 属性

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 在下方窗格中，选择 Status Checks。
5. 在“Status Checks”标签中，“Auto-Enable IO”显示了您选中卷的当前设置，是 Enabled 或 Disabled。

在控制台中修改卷的 AutoEnableIO 属性

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 在 Volumes 页面顶部，选择 Actions。
5. 选择 Change Auto-Enable IO Setting。
6. 在 Change Auto-Enable IO Setting (更改自动启用 IO 设置) 对话框中，选择 Auto-Enable Volume IO (自动启用卷 IO) 选项为受损卷自动启用 IO。想要禁用该功能，请清除该选项。
7. 选择 Save。

或者，不完成上一过程中的步骤 4-6，而是选择 Status Checks、Edit。

使用命令行查看或修改卷的 AutoEnableIO 属性

您可以使用以下命令之一查看 Amazon EBS 卷的 AutoEnableIO 属性。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volume-attribute \(AWS CLI\)](#)
- [Get-EC2VolumeAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

要修改卷的 AutoEnableIO 属性，您可以使用以下命令之一。

- [modify-volume-attribute \(AWS CLI\)](#)
- [Edit-EC2VolumeAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

从实例断开 Amazon EBS 卷

您可以明确地从实例断开 Amazon EBS 卷，或终止实例。但是，如果实例正在运行，您首先必须从实例卸载卷。;

如果 EBS 卷是实例的根设备，则在断开卷连接之前必须停止该实例。

如果具有 AWS Marketplace 产品代码的卷与实例断开，产品代码就不再与该实例关联。

Important

分离卷之后，只要存储量超出了 AWS 免费套餐的限额，您仍需为卷存储付费。您必须删除卷以避免产生更多费用。有关更多信息，请参阅 [删除 Amazon EBS 卷 \(p. 542\)](#)。

该示例卸载了卷，然后明确地将其从实例断开。当您要终止实例或将卷连接到其他实例时，这会非常有用。要验证该卷是否不再与该实例连接，可参阅 [查看卷信息 \(p. 533\)](#)。

注意，您可以重新连接断开的卷(无需卸载)，但可能不能获得相同安装点，如果断开时正在写入卷，那么卷上的数据可能不同步。

使用控制台断开 EBS 卷

1. 使用以下命令卸载 /dev/sdh 设备。

```
[ec2-user ~]$ umount -d /dev/sdh
```

2. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
3. 在导航窗格中，选择 Volumes。
4. 选择卷，然后选择 Actions、Detach Volume。
5. 在确认对话框中，选择 Yes, Detach。

使用命令行将 EBS 卷从实例断开

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [detach-volume \(AWS CLI\)](#)
- [Dismount-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

故障排除

本部分介绍在分离卷时遇到的常见问题并介绍如何解决这些问题。

Note

要防止出现数据丢失的可能性，请在尝试卸载之前为您的卷拍摄快照。强制分离一个状态卡住的卷可能对文件系统或其中包含的数据造成破坏，或者除非重启实例，否则无法使用同样的设备名称挂载新卷。

- 如果在通过 Amazon EC2 控制台分离卷时遇到问题，使用 `describe-volumes` CLI 命令诊断问题可能会有所帮助。有关更多信息，请参阅 [describe-volumes](#)。
- 如果您的卷处于 `detaching` 状态，您可以通过选择 Force Detach 强制执行分离操作。请将此选项仅用作在不得已的情况下从故障实例断开卷的方法，或是在要删除卷的情况下断开卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用此选项，则必须执行文件系统检查和修复流程。
- 如果在几分钟内多次尝试强制分离卷，并且该卷处于 `detaching` 状态，则可以向 [Amazon EC2 forum](#) 发布帮助请求。为了帮助加快解决问题，请提供卷 ID 并描述已采取的步骤。
- 如果尝试分离仍然安装着的卷，该卷可能在尝试分离时卡在 `busy` 状态。`describe-volumes` 的以下输出说明了这种情况：

```
[ec2-user ~]$ aws ec2 describe-volumes --region us-west-2 --volume-ids vol-1234abcd
{
    "Volumes": [
        {
            "AvailabilityZone": "us-west-2b",
            "Attachments": [
                {
                    "AttachTime": "2016-07-21T23:44:52.000Z",
                    "InstanceId": "i-fedc9876",
                    "VolumeId": "vol-1234abcd",
                    "State": "busy",
                    "DeleteOnTermination": false,
                    "Device": "/dev/sdf"
                }
            ...
        }
    ]
}
```

如果遇到这种状态，可能无限期延迟分离，直到您卸载卷，强制分离，重启实例，或者执行前述全部三项操作。

删除 Amazon EBS 卷

如果不再需要某个 Amazon EBS 卷，可以将其删除。删除后，卷上的数据都不复存在，并且再也不能连接到任何实例。然而，您可在删除之前，保存卷的快照，以便以后使用该快照重新创建该卷。

要删除卷，其必须处于 `available` 状态（未挂载到实例）。

使用控制台删除 EBS 卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Volumes。
3. 选择卷，然后选择 Actions、Delete Volume。
4. 在确认对话框中，选择 Yes, Delete。

使用命令行删除 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `delete-volume` (AWS CLI)
- `Remove-EC2Volume` (适用于 Windows PowerShell 的 AWS 工具)

在 Linux 上修改 EBS 卷的大小、IOPS 或类型

如果您的 Amazon EBS 卷连接到最新一代的 EC2 实例类型，您可以在不分离它的情况下增加其大小、更改其卷类型或 (对于 `io1` 卷) 调整其 IOPS 性能。您也可以将这些更改应用到已分离的卷。有关最新一代实例类型的更多信息，请参阅[最新一代实例](#)。

如果您使用的是上一代实例类型，或者如果您在尝试修改卷时遇到错误，请按照 [附录：启动和停止实例以修改 EBS 卷 \(p. 550\)](#) 中的步骤完成操作。

一般来说，修改卷涉及以下步骤：

1. 发出修改命令。有关更多信息，请参阅 [从控制台修改 EBS 卷 \(p. 543\)](#) 和 [从命令行修改 EBS 卷 \(p. 544\)](#)。
2. 监视修改进度。有关更多信息，请参阅 [监控卷修改的进度 \(p. 544\)](#)。
3. 如果修改了卷的大小，请扩展卷的文件系统以利用增加的存储容量。有关更多信息，请参阅[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。

此外，您还可以使用 [Amazon CloudWatch Events](#) 和 [AWS CloudFormation](#) 来自动化与卷修改相关联的操作。

修改卷配置是免费的。修改开始后，系统将按新卷配置价格计费。有关更多信息，请参阅 [Amazon EC2 定价](#) 页面上的 Amazon Elastic Block Store 部分。

有关更多信息，请参阅 [修改 EBS 卷的注意事项 \(p. 549\)](#)。

Important

在修改包含有用数据的卷之前，最佳实践是创建卷的快照 (如果您需要回滚您的更改)。有关 EBS 快照的信息，请参阅[创建 Amazon EBS 快照](#)。

从控制台修改 EBS 卷

下面的过程说明如何从 Amazon EC2 控制台应用可用的卷修改。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Volumes，选择要修改的卷，然后依次选择 Actions、Modify Volume。
3. Modify Volume 窗口显示卷 ID 和卷的当前配置，包括类型、大小和 IOPS。您可以在单个操作中更改任何或所有这些设置。设置新的配置值，如下所述：
 - 要修改类型，请为 Volume Type 选择一个值。
 - 要修改大小，请为 Size 输入一个允许的整数值。
 - 如果选择 Provisioned IOPS (IO1) 作为卷类型，请为 IOPS 输入一个允许的整数值。

4. 指定要应用的所有修改后，依次选择 Modify、Yes。

Note

在扩展卷的文件系统以使用新的存储容量之前，修改卷大小没有实际效果。有关更多信息，请参阅[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。

从命令行修改 EBS 卷

下面的示例演示如何使用 AWS CLI 从命令行修改 EBS 卷。根据默认配置，您可能需要指定区域和可用区等信息。要修改的源卷的 ID 是必需的，并且您必须具有适当的权限才能执行操作。当 io1 卷是修改目标时，您必须指定其预配置 IOPS 的级别。可以在单个命令中执行多个修改操作 (以更改容量、IOPS 或类型)。

例如，EBS 卷配置如下：

- 卷 ID: vol-11111111111111111111
- 卷大小：100 GiB
- 卷类型: gp2

您可以将卷配置更改为以下内容：

- 卷大小：200 GiB
- 卷类型: io1
- 配置级别：10000 IOPS

使用下面的命令应用上述修改：

```
aws ec2 modify-volume --region us-east-1 --volume-id vol-1111111111111111 --size 200 --volume-type io1 --iops 10000
```

此命令产生的输出与以下内容类似：

```
{  
    "VolumeModification": {  
        "TargetSize": 200,  
        "TargetVolumeType": "io1",  
        "ModificationState": "modifying",  
        "VolumeId": "vol-1111111111111111",  
        "TargetIops": 10000,  
        "StartTime": "2017-01-19T22:21:02.959Z",  
        "Progress": 0,  
        "OriginalVolumeType": "gp2",  
        "OriginalIops": 300,  
        "OriginalSize": 100  
    }  
}
```

Note

在扩展卷的文件系统以使用新的存储容量之前，修改卷大小没有实际效果。有关更多信息，请参阅[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。

监控卷修改的进度

被修改的 EBS 卷将经历一系列状态。当您从控制台、CLI、API 或软件开发工具包发出 `ModifyVolume` 指令后，卷首先进入 `Modifying` 状态，然后是 `optimizing` 状态，最后是 `Complete` 状态。此时，卷已准备好做

进一步的修改。在极少数情况下，暂时的 AWS 故障可能会导致 Failed 状态。如果发生这种情况，请重试修改。

大小更改通常需要几秒钟才能完成，并在卷处于 Optimizing 状态后生效。

性能 (IOPS) 更改可能需要几分钟到几小时才能完成，具体视所做的配置更改而定。

新配置最多可能需要 24 小时才能生效。通常，完全使用的 1 TiB 卷需要约 6 个小时才能迁移到新的性能配置。

当卷处于 optimizing 状态时，卷性能将介于源配置规范和目标配置规范之间。过渡卷的性能将不会低于源卷的性能。如果您降级 IOPS，则过渡卷的性能将不低于目标卷的性能。

您可以通过检查 AWS 管理控制台、使用 AWS EC2 API/CLI 查询卷的状态或访问发送到 Amazon CloudWatch Events 的指标来监控修改进度。以下过程说明了这些方法。

从控制台监控修改进度

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Volumes，然后选择要检查的卷。卷的状态显示在 State 列中。在下面的示例中，修改状态为 completed。此状态信息也显示在详细信息窗格的 State 字段中。
3. 打开 State 字段旁边的信息图标可显示有关最近一次修改操作完成前后的信息，如下所示。

从命令行监控修改进度

- 使用 [describe-volumes-modifications \(p. 544\)](#) 查看修改进度。本例调用了上面的卷 vol-1111111111111111 和另一个卷 vol-2222222222222222。

```
aws ec2 describe-volumes-modifications --region us-east-1 --volume-id vol-1111111111111111 vol-2222222222222222
```

此命令产生的输出与以下内容类似：

```
{  
    "VolumesModifications": [  
        {  
            "TargetSize": 200,  
            "TargetVolumeType": "io1",  
            "ModificationState": "modifying",  
            "VolumeId": "vol-1111111111111111",  
            "TargetIops": 10000,  
            "StartTime": "2017-01-19T22:21:02.959Z",  
            "Progress": 0,  
            "OriginalVolumeType": "gp2",  
            "OriginalIops": 300,  
            "OriginalSize": 100  
        },  
        {  
            "TargetSize": 2000,  
            "TargetVolumeType": "sc1",  
            "ModificationState": "modifying",  
            "VolumeId": "vol-2222222222222222",  
            "StartTime": "2017-01-19T22:23:22.158Z",  
            "Progress": 0,  
            "OriginalVolumeType": "gp2",  
            "OriginalIops": 300,  
            "OriginalSize": 1000  
        }  
    ]  
}
```

```
    ]  
}
```

`describe-volumes-modifications` 命令返回一个或多个 `VolumesModification` 对象。本示例中的第一个与上面显示的原始 `modify-volume` 命令的输出几乎相同。但是，它没有应用额外的修改。

下一个示例查询区域中修改状态为 `optimizing` 或 `completed` 的所有卷，然后筛选和格式化结果以只显示于 2017 年 2 月 1 日及之后做出的修改。

```
aws ec2 describe-volumes-modifications --filters Name=modification-state,Values="optimizing","completed" --region us-east-1 --query "VolumesModifications[?StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

在本例中，查询返回有关两个卷的信息：

```
[  
  {  
    "STATE": "optimizing",  
    "ID": "vol-06397e7a0eEXAMPLE"  
  },  
  {  
    "STATE": "completed",  
    "ID": "vol-bEXAMPLE"  
  }  
]
```

使用 CloudWatch Events 监控修改进度

借助 CloudWatch Events，您可以为卷修改事件创建通知规则，以发送文本消息或执行 Lambda 函数。

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 依次选择 Events、Create rule。
3. 对于 Build event pattern to match events by service，选择 Custom event pattern。
4. 对于 Build custom event pattern，将内容替换为以下代码：

```
{  
  "source": [  
    "aws.ec2"  
  ],  
  "detail-type": [  
    "EBS Volume Notification"  
  ],  
  "detail": {  
    "event": [  
      "modifyVolume"  
    ]  
  }  
}
```

完成后选择 Save。

典型的事件输出应与以下内容类似：

```
Body:  
{  
  "version": "0",  
  "id": "1ea2ace2-7790-46ed-99ab-d07a8bd68685",
```

```
"detail-type": "EBS Volume Notification",
"source": "aws.ec2",
"account": "065441870323",
"time": "2017-01-12T21:09:07Z",
"region": "us-east-1",
"resources": [
    "arn:aws:ec2:us-east-1:065441870323:volume/vol-03a55cf56513fa1b6"
],
"detail": {
    "result": "optimizing",
    "cause": "",
    "event": "modifyVolume",
    "request-id": "auto-58c08bad-d90b-11e6-a309-b51ed35473f8"
}
}
```

您可以使用规则生成有关 [Amazon SNS](#) 的通知消息，或调用 [AWS Lambda 函数](#)来响应匹配事件。

调整卷大小后扩展 Linux 文件系统

使用特定于文件系统的命令，将文件系统调整为更大的新卷大小。即使要扩展的卷是根卷，这些命令依然有效。对于 ext2、ext3 和 ext4 文件系统，此命令为 resize2fs。对于 XFS 文件系统，此命令为 xfs_growfs。对于其他文件系统，请参阅这些文件系统的特定文档以了解有关如何进行扩展的说明。

如果您不确定所使用的文件系统，可以使用 file -s 命令列出设备的文件系统数据。以下示例演示一个 Linux ext4 文件系统和一个 SGI XFS 文件系统。

```
[ec2-user ~]$ sudo file -s /dev/xvd*
/dev/xvda1: Linux rev 1.0 ext4 filesystem data ...
/dev/xvdf:  SGI XFS filesystem data ...
```

Note

如果您正扩展的卷已进行分区，那么，您需要在调整文件系统前，增加分区的大小。此时，您还可以分配其他分区。有关更多信息，请参阅 [扩展 Linux 分区 \(p. 551\)](#)。

一旦卷进入 Optimizing 状态，您就可以开始调整文件系统的大小。

Important

在扩展包含有用数据的文件系统之前，最佳实践是创建包含它的卷的快照（如果您需要回滚您的更改）。有关 EBS 快照的信息，请参阅 [创建 Amazon EBS 快照](#)。

检查您的卷分区是否需要调整大小

- 使用 lsblk 命令可列出连接到实例的块储存设备。下面的示例显示三个卷：`/dev/xvda`、`/dev/xvdb` 和 `/dev/xvdf`。

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0   30G  0 disk
##xvda1 202:1    0   30G  0 part /
xvdb     202:16   0   30G  0 disk /mnt
xvdf     202:80   0   35G  0 disk
##xvdf1 202:81   0    8G  0 part
```

根卷 `/dev/xvda1` 是 `/dev/xvda` 上的分区。请注意，两者大小都是 30 GiB。在这种情况下，分区会占用设备上的所有空间，因此无需调整大小。

卷 /dev/xvdb 尚未进行分区，因此无需调整大小。

然而，/dev/xvdf1 是一个 8 GiB 分区，位于一个 35 GiB 设备上，并且卷上没有其他分区。在这种情况下，分区必须调整大小，以便使用卷上的剩余空间。有关更多信息，请参阅 [扩展 Linux 分区 \(p. 551\)](#)。调整分区大小之后，您可以按照下一个过程扩展文件系统以占用分区上的所有空间。

扩展 Linux 文件系统

1. 使用 SSH 客户端登录到您的 Linux 实例。有关连接到 Linux 实例的更多信息，请参阅 [使用 SSH 连接到 Linux 实例 \(p. 252\)](#)。
2. 使用 df -h 命令可报告现有文件系统的磁盘空间使用率。在此示例中，/dev/xvda1 设备已扩展为 70 GiB，但操作系统仍只能看到原来的 7.9 GiB ext4 文件系统。与此类似，/dev/xvdf 设备已扩展为 100 GiB，但操作系统仍只能看到原来的 1.0 GiB XFS 文件系统。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       8.0G  943M  6.9G  12% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
/dev/xvdf      1014M   33M  982M   4% /mnt
```

3. 可使用特定于文件系统的命令将每个文件系统调整为新的卷容量。

对于 Linux ext2、ext3 或 ext4 文件系统，请使用以下命令并替换为要扩展的设备名称：

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
resize2fs 1.42.3 (14-May-2012)
Filesystem at /dev/xvda1 is mounted on /; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 5
Performing an on-line resize of /dev/xvda1 to 18350080 (4k) blocks.
The filesystem on /dev/xvda1 is now 18350080 blocks long.
```

对于 XFS 文件系统，请首先安装 XFS 用户空间工具：

```
[ec2-user ~]$ sudo yum install xfsprogs
```

然后，使用以下命令，替换文件系统的挂载点（必须挂载 XFS 文件系统才能调整其大小）：

```
[ec2-user ~]$ sudo xfs_growfs -d /mnt
meta-data=/dev/xvdf              isize=256    agcount=4, agsize=65536 blks
                                =          sectsz=512  attr=2
data                   =          bsize=4096   blocks=262144, imaxpct=25
                                =          sunit=0    swidth=0 blks
naming      =version 2          bsize=4096   ascii-ci=0
log         =internal           bsize=4096   blocks=2560, version=2
                                =          sectsz=512  sunit=0 blks, lazy-count=1
realtime   =none                extsz=4096   blocks=0, rtextents=0
data blocks changed from 262144 to 26214400
```

Note

如果您收到 xfsctl failed: Cannot allocate memory 错误，则可能需要更新实例上的 Linux 内核。有关更多信息，请参阅您的特定操作系统文档。

如果您收到 the filesystem is already nnnnnnn blocks long. Nothing to do! 错误，请参阅 [扩展 Linux 分区 \(p. 551\)](#)。

4. 使用 df -h 命令可报告现有文件系统磁盘空间使用率，现在应在 ext4 文件系统上显示完整的 70 GiB，在 XFS 文件系统上显示 100 GiB：

```
# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       70G  951M   69G   2% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
/dev/xvdf       100G   45M  100G   1% /mnt
```

Tip

如果您的卷中增加的可用空间在系统中仍不可见，请尝试重新初始化卷，具体说明请参阅[初始化 Amazon EBS 卷](#)。

修改 EBS 卷的注意事项

请注意影响卷修改的以下限制和特殊情况：

- 在某些情况下，您需要分离卷或停止实例才能继续进行修改。如果在尝试对 EBS 卷应用修改时遇到错误消息，或者如果要修改附加到上一代实例类型的 EBS 卷，请执行以下步骤之一：
 - 对于非根卷，将卷与实例分离，应用修改，然后重新附加卷。有关更多信息，请参阅[从实例中分离 Amazon EBS 卷](#)和[将 Amazon EBS 卷附加到实例](#)。
 - 对于根（引导）卷，停止实例，应用修改，然后重新启动实例。有关更多信息，请参阅[附录：启动和停止实例以修改 EBS 卷 \(p. 550\)](#)。
- 本主题中描述的卷修改方法不支持上一代 磁介质 卷类型。但是，您可以创建 磁介质 卷的快照并将其还原到采用不同配置的 EBS 卷。
- 不支持减小 EBS 卷的大小。但是，您可以创建较小的卷，然后使用应用程序级工具（如 rsync）将数据迁移到此卷。
- 修改卷后，您需要等待至少六个小时，然后再对同一个卷应用进一步的修改。
- Linux AMI 需要将 GPT 分区表和 GRUB 2 用于 2 TiB (2048 GiB) 或更大的引导卷。现在的许多 Linux AMI 都使用 MBR 分区方案，此方案仅支持最高 2047 GiB 的引导卷。如果您的实例不通过 2 TiB 或更大的引导卷启动，您要使用的 AMI 会限制为 2047 GiB 引导卷大小。非引导卷对 Linux 实例没有这种限制。
- 在 2016 年 11 月 1 日前附加到最新一代实例的卷需要执行以下操作之一来初始化本主题中描述的修改支持：
 - 停止并重启实例。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

- 分离然后重新附加卷。
这是一次性要求。

要确定卷的创建时间，请在 Amazon EC2 控制台中导航到卷详细信息页面并查看 Created 字段。要显示卷的最近附加时间（可能比创建时间更近），请使用 AWS CLI。下面的命令对在截止日期前最近附加的卷发出查询：

```
aws ec2 describe-volumes --region us-east-1 --query "Volumes[?Attachments[?AttachTime<='2016-11-01']]".{ID:VolumeId}" --output text
```

输出是需要注意的卷的 ID 的文本列表：

```
vol-0EXAMPLE
vol-5EXAMPLE
vol-4EXAMPLE
```

```
vol-bEXAMPLE
vol-0db1c57561EXAMPLE
vol-06f90d0c16EXAMPLE
```

- 最新一代的 m3.medium 实例完全支持卷修改。然而，某些 m3.large、m3.xlarge 和 m3.2xlarge 实例可能并不支持所有卷修改功能。如果遇到错误，请按照[附录：启动和停止实例以修改 EBS 卷 \(p. 550\)](#)中针对上一代实例类型的过程操作。

附录：启动和停止实例以修改 EBS 卷

如果您使用的是上一代 Amazon EC2 实例并且您需要修改根（引导）卷，则必须停止实例，应用修改，然后重新启动实例。此处描述的过程可用于修改任意实例类型上的任何 EBS 卷。

当您停止和启动实例时，需要注意以下事项：

- 如果您的实例在 VPC 中运行并具有公有 IPv4 地址，则我们会释放该地址并向实例提供一个新的公有 IPv4 地址。实例会保留其私有 IPv4 地址和任何弹性 IP 地址。
- 如果实例在 EC2-Classic 中运行，则我们会为其提供新的公有和私有 IPv4 地址，并取消该实例与任何弹性 IP 地址的关联。您在重新启动实例后，必须重新关联任何弹性 IP 地址。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。为预防这一问题，您可暂时挂起组的 Auto Scaling 进程。有关更多信息，请参阅 Auto Scaling 用户指南 中的[挂起和恢复 Auto Scaling 进程](#)。

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Instances，然后选择具有要扩展的卷的实例。
- 确保 Shutdown Behavior 设置为 Stop 而不是 Terminate。
 - 选择实例。
 - 从上下文菜单（右键单击）中依次选择 Instance Settings、Change Shutdown Behavior。
 - 如果 Shutdown behavior 设置为 Terminate，请选择 Stop，然后选择 Apply。

如果 Shutdown behavior 已经设置为 Stop，则选择 Cancel。

- 停止实例。有关更多信息，请参阅[停止和启动您的实例 \(p. 264\)](#)。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

- 按[从控制台修改 EBS 卷 \(p. 543\)](#)或[从命令行修改 EBS 卷 \(p. 544\)](#)中所述修改您的 EBS 卷。
- 重新启动实例。
 - 在导航窗格中，选择 Instances，然后选择要重新启动的实例。
 - 从上下文菜单（右键单击）中依次选择 Instance State、Start。
 - 在 Start Instances 对话框中，选择 Yes, Start。如果实例无法启动，并且扩展卷为根卷，请确认已使用与原始卷相同的设备名称连接了扩展卷，例如 /dev/sda1。

实例启动之后，可以检查文件系统大小，看实例是否识别这个更大的卷空间。在 Linux 上，请使用 df -h 命令检查文件系统大小。

```
[ec2-user ~]$ df -h
Filesystem      Size   Used  Avail Use% Mounted on
/dev/xvda1      7.9G  943M  6.9G  12% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
```

如果大小没有反映新扩展的卷，则必须扩展设备的文件系统，以便实例可以使用新的空间。有关更多信息，请参阅[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)。

扩展 Linux 分区

某些 Amazon EC2 根卷和从快照还原的卷包含实际保存文件系统和数据的分区。如果您将卷视为容器，则分区是卷中的另一个容器，并且数据位于分区上。增大卷大小并不会增大分区；要利用较大卷，分区必须扩展为新大小。

Note

并非所有从快照还原的卷都进行分区，此过程可能不适用于您的卷。您可能只需对卷上的文件系统调整大小，即可使所有空间可用。如果您不确定卷是否具有需要调整大小的分区，请参阅[检查您的卷分区是否需要调整大小 \(p. 547\)](#)了解更多信息。

如果要扩展的分区不是根分区，只需卸载它并通过实例本身调整分区大小。如果需要调整大小的分区是实例的根分区，则过程更复杂，因为您无法卸载正在运行的实例的根分区。您必须对其他实例（这称为辅助实例）执行以下过程。

Important

以下过程是针对 Amazon Linux 编写的并在其上进行了测试。具有不同工具集和工具版本的其他分发版的行为方式可能不同。

主题

- [为进行扩展准备 Linux 根分区 \(p. 551\)](#)
- [使用 parted 扩展 Linux 分区 \(p. 552\)](#)
- [使用 gdisk 扩展 Linux 分区 \(p. 555\)](#)
- [将扩展的分区恢复到其原始实例 \(p. 558\)](#)

为进行扩展准备 Linux 根分区

需要执行几个步骤来扩展实例的根分区。如果需要扩展的分区不是根分区，则此过程不是必需的。

为进行扩展准备 Linux 根分区

1. 如果您的主实例正在运行，请停止它。您无法对正在运行的实例执行此过程的其余部分。有关更多信息，请参阅[停止和启动您的实例 \(p. 263\)](#)。
2. 检查卷的完整性。如果快照选取损坏的文件系统，会导致恢复后的根卷无法引导。
3. 拍摄卷的快照。在以下过程中，可能容易损坏或丢失数据。如果您具有最新快照，则随时可以在出现错误时重新开始，数据仍是安全的。有关更多信息，请参阅[创建 Amazon EBS 快照 \(p. 559\)](#)。
4. 记录卷连接到的设备名称。您可以在实例详细信息窗格的 Root device (根设备) 字段中找到此信息。值可能是`/dev/sda1` 或 `/dev/xvda`。
5. 从主实例分离卷。有关更多信息，请参阅[从实例断开 Amazon EBS 卷 \(p. 541\)](#)。
6. 将卷连接到同一个可用区中的其他（辅助）实例。有关更多信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。如果您的 EBS 卷已加密，则必须使用支持 Amazon EBS 加密的辅助实例；否则，您可以在此过程使用`t2.micro` 实例。有关更多信息，请参阅[支持的实例类型 \(p. 569\)](#)。如果您还没有辅助实例，则需要启动一个。有关更多信息，请参阅[启动实例 \(p. 244\)](#)。

Important

在附加卷时，辅助实例必须在运行，并且您不应在附加了多个根卷时重新启动辅助实例；启动附加了多个根卷的实例可能会造成该实例启动至错误的卷。

7. 使用 SSH 登录辅助实例。有关更多信息，请参阅 [连接到您的 Linux 实例 \(p. 252\)](#)。继续执行下一个过程。

使用 parted 扩展 Linux 分区

parted 实用工具是一款分区编辑工具，大多数 Linux 分发版均会提供。它可以创建和编辑 MBR 分区表和 GPT 分区表。某些版本的 parted (高于版本 2.1) 对 GPT 分区表的支持有限，如果使用这些版本的 parted 修 改启动卷，则可能会导致启动问题。可以使用 `parted --version` 命令查看 parted 的版本。

如果要扩展的分区位于采用 GPT 分区设备上，则应选用 gdisk 实用工具。如果您不确定自己的卷所用的磁盘 标签类型，可以使用 `sudo fdisk -l` 命令查看。有关更多信息，请参阅 [使用 gdisk 扩展 Linux 分区 \(p. 555\)](#)。

使用 parted 扩展 Linux 分区

如果需要扩展的分区是根分区，请务必先执行[为进行扩展准备 Linux 根分区 \(p. 551\)](#)中的步骤。

1. 确定包含要扩展的分区的设备。使用 `lsblk` 命令列出附加到实例的所有设备和分区。

```
[ec2-user ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvdf    202:80   0 100G  0 disk 
##xvdf1 202:81   0     8G  0 part /mnt
xvda1   202:1    0   30G  0 disk /

```

在该示例中，`xvdf` 设备有 100 GiB 可用存储，包含一个 8 GiB 分区。

2. 如果该分区已装载，请卸载它。使用来自 `lsblk` 命令的 `MOUNTPOINT` 值运行 `umount` 命令。在此示例中， 分区的 `MOUNTPOINT` 值是 `/mnt`。

```
[ec2-user ~]$ sudo umount /mnt
```

3. 拍摄卷的快照 (除非您刚才在上一个过程中拍摄了一个快照)。在以下过程中，可能容易损坏或丢失数 据。如果您具有最新快照，则随时可以在出现错误时重新开始，数据仍是安全的。有关更多信息，请参 阅 [创建 Amazon EBS 快照 \(p. 559\)](#)。
4. 对设备 (而不是设备上的分区) 运行 `parted` 命令。请注意将 `/dev/` 前缀添加到 `lsblk` 输出的名称。

```
[ec2-user ~]$ sudo parted /dev/xvdf
GNU Parted 2.1
Using /dev/xvdf
Welcome to GNU Parted! Type 'help' to view a list of commands.
```

5. 将 `parted` 度量单位更改为扇区。

```
(parted) unit s
```

6. 运行 `print` 命令，列出设备上的分区。对于某些分区表类型，系统可能会提示您针对较大卷大小修复分 区表。对所有关于是否修复现有分区表的问题回答“Ignore”；之后开始创建新表。

```
(parted) print
```

- a. 如果收到以下消息，请输入“Ignore”以防止备份 GPT 位置更改。

```
Error: The backup GPT table is not at the end of the disk, as it should be. This
      might mean that another operating
      system believes the disk is smaller. Fix, by moving the backup to the end (and
      removing the old backup)?
Fix/Ignore/Cancel? Ignore
```

- b. 如果收到以下消息，请再次输入“Ignore”使驱动器上的空间保持不变。

```
Warning: Not all of the space available to /dev/xvdf appears to be used, you can
fix the GPT to use all of the
space (an extra 46137344 blocks) or continue with the current setting?
Fix/Ignore? Ignore
```

7. 检查输出以了解磁盘总大小、分区表类型、分区编号、分区起点和任何标志（如 boot）。对于 gpt 分区表，记下分区名称；对于 msdos 分区表，记下 Type 字段（primary 或 extended）。这些值将在后面的步骤中使用。

以下是 gpt 分区表示例。

```
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdf: 209715200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size      File system  Name           Flags
128     2048s  4095s   2048s    ext4        BIOS Boot Partition bios_grub
1       4096s  16777182s 16773087s  ext4        Linux
```

以下是 msdos 分区表示例。

```
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdg: 104857600s
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size      Type      File system  Flags
1       2048s  35649535s 35647488s  primary   ext3
```

8. 使用来自上一步的编号（1）删除分区的分区条目。

```
(parted) rm 1
```

9. 创建扩展到卷末尾的新分区。

（对于 gpt 分区表示例）记下上面的分区 1 的起点和名称。对于 gpt 示例，起点为 4096s，名称为 Linux。使用分区 1 的起点、名称和 100% 运行 mkpart 命令，以使用所有可用空间。

```
(parted) mkpart Linux 4096s 100%
```

（对于 msdos 分区表示例）记下上面的分区 1 的起点和分区类型。对于 msdos 示例，起点为 2048s，分区类型为 primary。使用主分区类型、分区 1 的起点和 100% 运行 mkpart 命令，以使用所有可用空间。

```
(parted) mkpart primary 2048s 100%
```

10. 再次运行 print 命令以验证分区。

（对于 gpt 分区表示例）

```
(parted) print
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdf: 209715200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size      File system  Name           Flags
1       4096s  16777182s 16773087s  ext4        Linux
```

| | | | | | |
|-----|-------|------------|------------|---------------------|-----------|
| 128 | 2048s | 4095s | 2048s | BIOS Boot Partition | bios_grub |
| 1 | 4096s | 209713151s | 209709056s | ext4 | Linux |

(对于 msdos 分区表示例)

```
(parted) print
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdd: 104857600s
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type      File system  Flags
 1      2048s  104857599s 104855552s primary    ext3
```

- 对于扩展的分区，检查以前存在的任何标志是否仍存在。有时 boot 标志可能会丢失。如果在扩展时分区丢弃了标志，请使用以下命令添加标志(替换为您的分区编号和标志名称)。例如，以下命令将 boot 标志添加到分区 1。

```
(parted) set 1 boot on
```

可以再次运行 print 命令以验证更改。

- 运行 quit 命令，退出 parted。

```
(parted) quit
```

Note

由于您删除了一个分区并添加了一个分区，因此parted 会警告您需要更新 /etc/fstab。仅当分区编号更改时，才需要此操作。

- 检查文件系统以确保没有错误(需要先执行此操作，然后才能扩展文件系统)。记录上一个 print 命令中的文件系统类型。根据您的文件系统类型选择以下命令之一；如果使用其他文件系统，请参阅该文件系统的文档以确定正确的检查命令。

(对于 ext3 或 ext4 文件系统)

```
[ec2-user ~]$ sudo e2fsck -f /dev/xvdf1
e2fsck 1.42.3 (14-May-2012)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/: 31568/524288 files (0.4% non-contiguous), 266685/2096635 blocks
```

(对于 xfs 文件系统)

```
[ec2-user ~]$ sudo xfs_repair /dev/xvdf1
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
```

```
- agno = 3
- process newly discovered inodes...
Phase 4 - check for duplicate blocks...
- setting up duplicate extent list...
- check for inodes claiming duplicate blocks...
- agno = 0
- agno = 1
- agno = 2
- agno = 3
Phase 5 - rebuild AG headers and trees...
- reset superblock...
Phase 6 - check inode connectivity...
- resetting contents of realtime bitmap and summary inodes
- traversing filesystem ...
- traversal finished ...
- moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

14. 后续步骤因扩展的分区是否属于当前实例或是否为另一个实例的根分区而异。

- 如果此分区属于当前实例，请在 MOUNTPOINT 中标识的 [Step 2 \(p. 552\)](#) 处重新装载分区。

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt
```

装载了分区之后，按照[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#) 中的过程扩展文件系统以使用新提供的空间。

- 如果此卷是另一个实例的根分区，请继续执行[将扩展的分区恢复到其原始实例 \(p. 558\)](#)中的过程。

使用 gdisk 扩展 Linux 分区

gdisk 实用工具(有时称为 GPT fdisk)是用于创建和编辑分区表的文本界面菜单驱动型工具，在某些分发版中对 GPT 分区表的支持比 parted 更好。许多常用 Linux 分发版(例如 Amazon Linux 和 Ubuntu)默认提供 gdisk。如果您的分发版不提供 gdisk 命令，则可以通过访问[获取 GPT fdisk](#)来了解如何获取它；在许多情况下，启动一个 Amazon Linux 实例并将其用作辅助实例要简单得多，因为已提供了 gdisk 命令。

使用 gdisk 扩展 Linux 分区

如果需要扩展的分区是根分区，请务必先执行[为进行扩展准备 Linux 根分区 \(p. 551\)](#)中的步骤。

1. 确定包含要扩展的分区的设备。使用 lsblk 命令列出附加到实例的所有设备和分区。

```
[ec2-user ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO MOUNTPOINT
xvdf    202:80   0 100G  0
##xvdf1 202:81   0  9.9G  0 /mnt
xvda1   202:1    0   30G  0 /
```

在此示例中，xvdf 设备有 100 GiB 可用存储，包含一个 9.9 GiB 分区。

2. 如果该分区已装载，请卸载它。使用来自 lsblk 命令的 MOUNTPOINT 值运行 umount 命令。在此示例中，分区的 MOUNTPOINT 值是 /mnt。

```
[ec2-user ~]$ sudo umount /mnt
```

3. 拍摄卷的快照(除非您刚才在上一个过程中拍摄了一个快照)。在以下过程中，可能容易损坏或丢失数据。如果您具有最新快照，则随时可以在出现错误时重新开始，数据仍是安全的。有关更多信息，请参阅[创建 Amazon EBS 快照 \(p. 559\)](#)。

4. 对设备(而不是设备上的分区)运行 gdisk 命令。请注意将 /dev/ 前缀添加到 lsblk 输出的名称。

```
[ec2-user ~]$ sudo gdisk /dev/xvdf
gdisk /dev/xvdf
GPT fdisk (gdisk) version 0.8.10

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
```

5. 运行 p 命令以打印设备的分区表。
6. 查看磁盘标识符、分区编号、起始扇区、分区代码和分区名称的输出。如果您的卷有多个分区，请记录所有分区。

```
Command (? for help): p
Disk /dev/xvdf: 209715200 sectors, 100.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 947F4655-F3BF-4A1F-8203-A7B30C2A4425
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 20705246
Partitions will be aligned on 2048-sector boundaries
Total free space is 2108 sectors (1.0 MiB)

Number  Start (sector)   End (sector)   Size            Code  Name
      1              2048          20705152   9.9 GiB        EF00  lxroot
```

在以上示例中，磁盘标识符是 947F4655-F3BF-4A1F-8203-A7B30C2A4425，分区编号是 1，起始扇区是 2048，代码是 EF00，名称是 lxroot。

7. 因为现有分区表最初是为较小卷创建的，所以您需要为较大卷创建新分区表。运行 o 命令以创建新的空分区表。

```
Command (? for help): o
This option deletes all partitions and creates a new protective MBR.
Proceed? (Y/N): Y
```

8. 使用 n 命令在设备上为各个分区创建新的分区条目。
 - 如果您的卷只有一个分区，请在每次出现提示时输入您之前记录的值。对于最后扇区值，使用默认值扩展为整个卷大小。

```
Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-209715166, default = 2048) or {+-}size{KMGTP}: 2048
Last sector (2048-209715166, default = 209715166) or {+-}size{KMGTP}: 209715166
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): EF00
Changed type of partition to 'EFI System'
```

- 如果您的卷有不止一个分区，可能是一个 BIOS 引导分区和一个主要数据分区。使用您之前记录的值为 BIOS 引导分区创建新的分区条目。使用您之前记录的值为主要数据分区创建另一个新分区条目，但对于最后一个扇区值，请使用默认值扩展为整个卷大小。

```
Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-209715166, default = 2048) or {+-}size{KMGTP}: 2048
Last sector (2048-209715166, default = 209715166) or {+-}size{KMGTP}: 4095
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): EF02
```

```
Changed type of partition to 'BIOS boot partition'

Command (? for help): n
Partition number (2-128, default 2): 2
First sector (34-209715166, default = 4096) or {+-}size{KMGTP}: 4096
Last sector (4096-209715166, default = 209715166) or {+-}size{KMGTP}: 209715166
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 0700
Changed type of partition to 'Microsoft basic data'
```

9. 使用 c 命令将各个分区的名称更改为前一个分区的名称。如果您的分区没有名称，按 Enter 即可。

```
Command (? for help): c
Using 1
Enter name: lxroot
```

10. 使用 x 命令进入专家命令菜单。

11. 使用 g 命令将磁盘标识符更改为原始值。

```
Expert command (? for help): g
Enter the disk's unique GUID ('R' to randomize): 947F4655-F3BF-4A1F-8203-A7B30C2A4425
The new disk GUID is 947F4655-F3BF-4A1F-8203-A7B30C2A4425
```

12. 使用 w 命令将更改写入设备并退出。

```
Expert command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): Y
OK; writing new GUID partition table (GPT) to /dev/xvdf.
The operation has completed successfully.
```

13. 检查文件系统以确保没有错误 (需要先执行此操作，然后才能扩展文件系统)。

- a. 替换您刚刚扩展的分区 (如果卷有多个分区，这可能是 `/dev/xvdf2`)，使用以下命令查找文件系统类型。

```
[ec2-user ~]$ sudo file -sL /dev/xvdf1
```

- b. 根据您的文件系统类型选择以下命令之一；如果使用其他文件系统，请参阅该文件系统的文档以确定正确的检查命令。

(对于 ext3 或 ext4 文件系统)

```
[ec2-user ~]$ sudo e2fsck -f /dev/xvdf1
e2fsck 1.42.3 (14-May-2012)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/: 31568/524288 files (0.4% non-contiguous), 266685/2096635 blocks
```

(对于 xfs 文件系统)

Note

您可能需要安装 xfsprogs 包以便使用 XFS 文件系统。使用以下命令向 Amazon Linux 实例中添加 XFS 支持。

```
[ec2-user ~]$ sudo yum install -y xfsprogs
```

```
[ec2-user ~]$ sudo xfs_repair /dev/xvdf1
Phase 1 - find and verify superblock...
Phase 2 - using internal log
    - zero log...
    - scan filesystem freespace and inode maps...
    - found root inode chunk
Phase 3 - for each AG...
    - scan and clear agi unlinked lists...
    - process known inodes and perform inode discovery...
    - agno = 0
    - agno = 1
    - agno = 2
    - agno = 3
    - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
    - setting up duplicate extent list...
    - check for inodes claiming duplicate blocks...
    - agno = 0
    - agno = 1
    - agno = 2
    - agno = 3
Phase 5 - rebuild AG headers and trees...
    - reset superblock...
Phase 6 - check inode connectivity...
    - resetting contents of realtime bitmap and summary inodes
    - traversing filesystem ...
    - traversal finished ...
    - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

14. 后续步骤因扩展的分区是否属于当前实例或是否为另一个实例的根分区而异。

- 如果此分区属于当前实例，请在 MOUNTPOINT 中标识的 [Step 2 \(p. 555\)](#) 处重新装载分区。

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt
```

装载了分区之后，按照[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)中的过程扩展文件系统以使用新提供的空间。

- 如果此卷是另一个实例的根分区，请继续执行[将扩展的分区恢复到其原始实例 \(p. 558\)](#)中的过程。

将扩展的分区恢复到其原始实例

如果您扩展另一个实例中的根分区，请按照本过程将卷恢复到其原始实例。

将扩展的根分区恢复到其原始实例

- 将扩展的分区与其辅助实例分离。有关更多信息，请参阅[从实例断开 Amazon EBS 卷 \(p. 541\)](#)。
- 使用[Step 4 \(p. 551\)](#)准备过程的 (p. 551)中标识的设备名称，将卷重新连接到主实例。有关更多信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
- 启动主实例。有关更多信息，请参阅[停止和启动您的实例 \(p. 263\)](#)。
- (可选) 如果您只是为了扩展分区而启动了辅助实例，则可以终止该实例以停止产生费用。有关更多信息，请参阅[终止您的实例 \(p. 267\)](#)。
- 按照[调整卷大小后扩展 Linux 文件系统 \(p. 547\)](#)中的过程连接到主实例并扩展文件系统以使用新提供的空间。

完成此文件系统扩展过程之后，您可以从可用于启动具有所需分区大小的新实例的实例创建 AMI。有关更多信息，请参阅 [Amazon 系统映像 \(AMI\) \(p. 58\)](#)。

Amazon EBS 快照

您可以通过拍摄时间点快照将 EBS 卷上的数据备份到 Amazon S3。快照属于增量备份，这意味着仅保存设备上在最新快照之后更改的数据块。这将最大程度地缩短创建快照所需的时间，且可以节省存储成本。删除快照时，只有该快照特有的数据会被删除。活动快照包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。

内容

- [快照概述 \(p. 559\)](#)
- [创建 Amazon EBS 快照 \(p. 559\)](#)
- [删除 Amazon EBS 快照 \(p. 560\)](#)
- [复制 Amazon EBS 快照 \(p. 561\)](#)
- [查看 Amazon EBS 快照信息 \(p. 563\)](#)
- [共享 Amazon EBS 快照 \(p. 563\)](#)

快照概述

创建 EBS 卷时，可基于现有快照创建。新卷此时为用于创建快照的原始卷的精确副本。从现有快照创建卷时，其在后台延时加载，因此可以立即开始使用它们。如果您访问尚未加载的一部分数据，则卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的剩余数据。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 559\)](#)。

通过修改其访问权限，您可以在不同 AWS 账户之间共享快照。您可以复制您拥有的快照以及与您共享的快照。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

EBS 快照广泛支持 EBS 加密：

- 加密卷的快照会自动加密。
- 通过加密快照创建的卷会自动加密。
- 在复制您拥有的未加密快照时，您可以在复制过程中对其进行加密。
- 在复制您拥有的加密快照时，您可在复制过程中使用其他密钥重新加密。

有关更多信息，请参阅 [Amazon EBS 加密](#)。

快照受限于在其中创建它们的区域。在您创建 EBS 卷的快照之后，可以在同一区域使用它来创建新卷。有关更多信息，请参阅 [从快照还原 Amazon EBS 卷 \(p. 529\)](#)。您还可以跨区域复制快照，从而能够更轻松地将多个区域用于地理扩展、数据中心迁移和灾难恢复。您可以复制具有 completed 状态的任何可访问快照。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 561\)](#)。

创建 Amazon EBS 快照

将数据写入 EBS 卷之后，您可以定期创建卷快照，以用作新卷的基线或用于数据备份。如果您定期为卷拍摄快照，则快照为增量快照，因此新快照中仅保存设备上在保存上次快照之后更改的数据块。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

快照是异步拍摄的；时间点快照是立即创建的，但在快照完成（当所有已修改数据块都已转移到 Amazon S3 时）之前，其状态为 pending，很多大型初始快照或后续快照（其中的数据块已更改）可能需要几个小时才能完成。执行期间，正在进行的快照不会受到同时发生的卷读写操作的影响。

Important

尽管您可以在某个卷的前一个快照处于 pending 状态时拍摄该卷的快照，但一个卷有多个 pending 快照可能会导致该卷的性能降低，直至这些快照完成。

一个 gp2、io1、或 磁介质 卷最多可有 5 张 pending 快照，而一个 st1 或 sc1 卷只能有 1 张 pending 快照。如果您在尝试给同一个卷创建多个并发快照时收到 ConcurrentSnapshotLimitExceeded 错误，请等待一个或多个 pending 快照完成，然后再为该卷创建另一个快照。

从加密卷拍摄的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷及所有关联快照中的数据在静态或传输过程中均受到保护。有关更多信息，请参阅 [Amazon EBS 加密](#)。

默认情况下，只有您可以从您拥有的快照创建卷。但是，您可以将未加密的快照将共享给特定 AWS 账户，还可通过将其设为公开来与整个 AWS 社区共享。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

您仅可以将加密快照共享给特定 AWS 账户。要让其他账户使用您共享的加密快照，您还必须与其共享用于加密该快照的 CMK 密钥。获取了您的加密快照访问权限的用户必须先自行创建该快照的副本，然后使用该副本还原卷。您还可以使用其他密钥重新加密您的共享加密快照的副本。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

在从具有 AWS Marketplace 产品代码的卷创建快照后，该卷的产品代码将会传送到该快照。

您可以拍摄正在使用的已连接卷的快照。但是，快照只能捕获发出快照命令时已经写入您的 Amazon EBS 卷的数据。其中可能不包括已由任何应用程序或操作系统缓存的任何数据。如果您可以将该卷的所有文件写入暂停足够长的时间以拍摄快照，则快照应该是完整的。但是，如果您无法暂停该卷的所有文件写入，则应该从实例中卸载该卷、发出快照命令，然后重新安装该卷，以确保获得一致且完整的快照。当快照状态为 pending 时，您可以重新安装并使用卷。

要为用作根设备的 Amazon EBS 卷创建快照，您应该在拍摄快照之前停止实例。

要在 Linux 中卸载卷，请使用以下命令：

```
umount -d device_name
```

其中 device_name 是设备名称 (如 /dev/sdh)。

创建快照后，您可以为其添加标记，以方便日后管理。例如，您可以添加类似以下内容的标记：描述该快照对应的原始卷，或用于将原始卷挂载到实例上的设备名称。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 626\)](#)。

使用控制台创建快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择 Create Snapshot。
4. 在 Create Snapshot 对话框中，选择要为其创建快照的卷，然后选择 Create。

使用命令行创建快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [create-snapshot \(AWS CLI\)](#)
- [New-EC2Snapshot\(适用于 Windows PowerShell 的 AWS 工具\)](#)

删除 Amazon EBS 快照

删除快照时，仅删除该快照专有的数据。删除卷之前的快照不会影响您使用该卷之后的快照还原卷的能力。

如果您定期为卷拍摄快照，则快照为增量快照，因此新快照上仅保存自上次快照后设备上新增加的块。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

请注意，您不能删除已注册 AMI 所用 EBS 卷的根设备的快照。您必须先取消注册 AMI，然后才能删除快照。有关更多信息，请参阅 [取消注册您的 AMI \(p. 121\)](#)。

如需使用控制台删除快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择快照，然后从 Actions 列表中选择 Delete。
4. 选择 Yes, Delete。

使用命令行删除快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [delete-snapshot](#) (AWS CLI)
- [Remove-EC2Snapshot](#) (适用于 Windows PowerShell 的 AWS 工具)

复制 Amazon EBS 快照

利用 Amazon EBS，您可以创建卷的时间点快照，我们为您将其存储在 Amazon Simple Storage Service (Amazon S3) 中。在创建快照并且已完成到 Amazon S3 的复制（快照状态为 completed 时）后，您可将快照从一个 AWS 区域复制到另一个 AWS 区域或复制到相同区域内。Amazon S3 服务器端加密 (256 位 AES) 可在复制过程中保护传输中的快照数据。快照副本将获得与原始快照 ID 不同的快照 ID。

Note

要复制 Amazon Relational Database Service (Amazon RDS) 快照，请参阅 Amazon Relational Database Service 用户指南 中的 [复制数据库快照](#)。

您可以通过以下方式使用快照副本：

- 地理扩展：在新的区域启动您的应用程序。
- 迁移：将应用程序迁移到新区域，以实现更好的可用性并最大限度地降低成本。
- 灾难恢复：在不同的地理位置定期备份您的数据和日志。为防止灾难发生，您可以使用辅助区域存储的时间点备份恢复您的应用程序。该操作能够让数据丢失和恢复时间降至最低。
- 加密：对之前未加密的快照进行加密、为加密快照或与您共享的加密快照更改密钥、为您拥有的快照创建副本以便从其中还原卷。
- 数据保留和审计要求：将您的加密 EBS 快照从一个 AWS 账户复制到其他 AWS 账户，以保留数据日志或其他文件，便于进行审计或数据保留。使用不同的账户有助于防止意外删除快照，并在您的主要 AWS 账户遭到泄露时为您提供保护。

Note

由 CopySnapshot 操作创建的快照具有一个不应用于任何用途的任意卷 ID。

用户定义的标签不会从源快照复制到新快照。复制操作完成后，您可将用户定义的标签应用于新的快照。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 626\)](#)。

每个账户最多可以同时进行到同一目的地的五个快照复制请求。您可以复制任何状态为 completed 的可访问快照，包括共享快照和您创建的快照。您也可以复制 AWS Marketplace、VM Import/Export 和 AWS Storage Gateway 快照，但必须确认目标区域支持该快照。

到另一个区域的第一个快照副本始终是完整副本。每个后续快照副本都是增量式的（可加快复制过程），这意味着只会传输在到同一目的地的最后一次快照复制以后发生更改的快照中的数据块。对增量快照的支持是

特定于某个区域对的，在该区域对中，源卷的上一个完整快照副本已在目标区域中可用，并且被限制为加密快照的默认 EBS CMK。例如，如果将未加密快照从 美国东部（弗吉尼亚北部）区域复制到 美国西部（俄勒冈）区域，则卷的第一个快照副本是完整副本，并且在相同区域间传输的相同卷的后续快照副本是增量副本。

Note

只要满足以下条件，单个账户和区域内的快照副本就完全不会复制任何数据，并且是免费的：

- 在复制操作过程中，快照副本的加密状态不会更改。
- 对于加密快照，源快照和副本都使用默认 EBS CMK 进行加密。

如果希望另一账户能够复制您的快照，您必须修改快照权限以允许访问该账户，或使快照公开可用，以便所有 AWS 账户均可复制它。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

有关跨区域和账户复制快照的定价信息，请参阅 [Amazon EBS 定价](#)。

加密快照

复制快照时，您可选择加密副本（如果原始快照未加密），也可以指定一个与原始快照不同的 CMK，这样，生成的快照副本将使用新 CMK。但是，在复制操作过程中更改快照的加密状态或使用非默认 EBS CMK 总是会生成完整副本（非增量），这可能产生更多的数据传输和存储费用。

要通过其他账户复制加密快照，您必须拥有使用该快照以及用于加密原始快照的客户主密钥（CMK）的权限。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 563\)](#)。

Note

如果要复制一个与您共享的加密快照，那么您应考虑在复制过程中使用您控制的其他密钥重新加密快照。这样，即使原始密钥泄露或拥有者出于任何原因撤销了密钥，您也不会失去对您创建的卷的访问权限。

使用 Amazon EC2 控制台复制快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择要复制的快照，然后从 Actions 列表中选择 Copy。
4. 在 Copy Snapshot (复制快照) 对话框中，根据需要进行以下更新：
 - Destination region (目标区域)：选择要在其中写入快照副本的区域。
 - Description (描述)：默认情况下，描述包括源快照的相关信息，以便您能区别副本和原始内容。必要时，您可以更改此描述。
 - 加密：如果源快照未加密，则可选择对副本进行加密。您无法解密已加密快照。
 - 主密钥：将用于对此快照进行加密的客户主密钥（CMK）。您可以从您账户的主密钥中选择或从一个不同的账户中键入/粘贴密钥 ARN。您可在 IAM 控制台中创建新的加密主密钥。
5. 选择 Copy。
6. 在 Copy Snapshot 确认对话框中，选择 Snapshots 转至指定区域的 Snapshots 页面，或选择 Close。

要在稍后查看复制过程的进度，请切换到目标区域，然后刷新 Snapshots (快照) 页面。该页面的顶部将列出正在进行的复制。

检查是否失败

如果您在未获得加密密钥使用权限的情况下试图复制加密快照，则操作将失败，且系统不会提示。您刷新页面后，控制台才会显示错误状态。您还可以通过命令行检查快照的状态。例如：

```
$ aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

如果复制因密钥权限不足而失败，您将看到以下消息：

```
"StateMessage": "Given key ID is not accessible"
```

Note

在复制加密的快照时，您必须对默认 CMK 具有描述权限。显式拒绝这些权限将导致复制失败。

使用命令行复制快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [copy-snapshot](#) (AWS CLI)
- [Copy-EC2Snapshot](#) (适用于 Windows PowerShell 的 AWS 工具)

查看 Amazon EBS 快照信息

您可以查看有关您的快照的详细信息。

使用控制台查看快照信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 要减少列表内容，请从 Filter 列表中选择一个选项。例如，要仅查看您的快照，请选择 Owned By Me。您可以使用高级搜索选项来进一步筛选您的快照。选择搜索栏可查看可用筛选条件。
4. 要查看有关某个快照的更多信息，请选择该快照。

使用命令行查看快照信息

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-snapshots](#) (AWS CLI)
- [Get-EC2Snapshot](#) (适用于 Windows PowerShell 的 AWS 工具)

共享 Amazon EBS 快照

您可以通过修改快照权限，与同事或 AWS 社区中的其他人共享未加密的快照。您授权的用户可以使用您的未加密共享快照为基础，快速创建其自己的 EBS 卷。如选择，您也可使您的未加密快照对所有 AWS 用户公开可用。

您可与特定 AWS 账户共享加密快照，但是您无法将其设为公开。要让其他账户使用快照，您还必须共享用于加密快照的自定义 CMK 密钥。跨账户权限可以在创建自定义密钥时应用于该密钥，也可以在创建之后应用于该密钥。获得访问权限的用户可以复制您的快照，并可基于您的快照创建自己的 EBS 卷，而您的原始快照不会受到影响。

Important

当您共享快照时（无论是将其与其他 AWS 账户共享，或使其公开可用），即表示您向他人授予了访问快照上所有数据的权限。仅与您要与其分享所有快照数据的人分享快照。

共享快照受到多种技术和策略限制：

- 快照受限于在其中创建它们的区域。如果要与另一个区域共享快照，则需要将快照复制到该区域。有关复制快照的更多信息，请参阅[复制 Amazon EBS 快照 \(p. 561\)](#)。
- 如果您的快照使用较长资源 ID 格式，则只能将其与支持较长 ID 的账户共享。有关更多信息，请参阅[资源 ID](#)。

- AWS 会阻止您共享使用您的默认 CMK 加密的快照。您打算共享的快照必须使用自定义 CMK 加密。有关创建密钥的更多信息，请参阅[创建密钥](#)。
- 与您共享 CMK 的用户如要访问您的加密快照，还必须获得 `DescribeKey` 和 `ReEncrypt` 权限。有关管理和共享 CMK 密钥的更多信息，请参阅[控制客户主密钥的访问权限](#)。
- 如果您拥有共享加密快照的访问权限，并且您希望从该快照还原卷，则必须自行创建该快照的一个副本，然后使用副本还原卷。我们建议您在复制过程中，使用您控制的其他密钥重新加密快照。这样，即使原始密钥遭到泄露或拥有者出于任何原因撤销了密钥，您也不会失去对卷的访问权限。

使用控制台修改快照权限

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 `Snapshots`。
3. 选择快照，然后从 `Actions` 列表中选择 `Modify Permissions`。
4. 选择是否公开快照或与特定 AWS 账户共享：
 - 要使快照公开可用，请选择 `Public`。
该选项不适用于加密快照或具有 AWS Marketplace 产品代码的快照。
 - 要仅向特定的 AWS 账户显示快照，请选择 `Private`，在 `AWS Account Number` 字段中输入 AWS 账户的 ID (无连字符)，然后选择 `Add Permission`。重复以上操作，直至您添加完所有需要 AWS 账户。
5. 选择 `Save`。

Important

如果您的快照已加密，请确保满足以下条件：

- 快照使用自定义 CMK 加密，而不是默认 CMK。如果您尝试更改使用默认 CMK 进行加密的快照的权限，控制台将显示一条错误消息。
- 您与享有您的快照访问权限的账户共享了自定义 CMK。

使用命令行查看和修改快照权限

要查看快照的 `createVolumePermission` 属性，您可以使用以下命令之一。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- `describe-snapshot-attribute` (AWS CLI)
- `Get-EC2SnapshotAttribute` (适用于 Windows PowerShell 的 AWS 工具)

要修改快照的 `createVolumePermission` 属性，您可以使用以下命令之一。

- `modify-snapshot-attribute` (AWS CLI)
- `Edit-EC2SnapshotAttribute` (适用于 Windows PowerShell 的 AWS 工具)

Amazon EBS 优化实例

Amazon EBS 优化的实例使用优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过尽可能减少 Amazon EBS I/O 与来自实例的其他流量之间的争用提供最好的 EBS 卷性能。

EBS 优化实例为 Amazon EBS 提供了专用带宽，根据您使用的实例类型，此带宽可在 500 Mbps 到 12,000 Mbps 的范围内选择。当挂载到 EBS 优化实例时，通用型 SSD (`gp2`) 卷可在所指定一年 99% 的时间内提供其 10% 以内的基准性能和突增性能，而 预配置 IOPS SSD (`io1`) 卷可在所指定一年 99.9% 的时间内提供其

10% 以内的预置性能。吞吐优化 HDD (`st1`) 和 Cold HDD (`sc1`) 都可确保所指定一年 99% 的时间内 90% 的突增性能一致。不合规时间近似均匀分配，目标是达到 99% 的每小时预计总吞吐量。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

当您对默认情况下不会进行 EBS 优化的实例启用 EBS 优化时，您需为专用容量支付一笔较小的按小时计算的额外费用。有关定价信息，请参阅 Amazon EC2 按需定价页中的 [EBS 优化实例](#)。

内容

- [支持 EBS 优化的实例类型 \(p. 565\)](#)
- [在启动时启用 EBS 优化 \(p. 567\)](#)
- [为正在运行的实例修改 EBS 优化 \(p. 567\)](#)

支持 EBS 优化的实例类型

下表显示了支持 EBS 优化实例类型、针对 Amazon EBS 的专用带宽、实例可以支持的最大 IOPS 量（如果使用的是 16 KB I/O 大小）以及在具有流式处理读取工作负载和 128 KiB I/O 大小的连接上可实现的典型最大聚合吞吐量（以 MB/s 为单位）。请选择提供的专用 EBS 吞吐量大于应用程序所需的 EBS 优化实例；否则，Amazon EBS 与 Amazon EC2 的连接将成为性能障碍。

请注意，某些实例类型在默认情况下会进行 EBS 优化。对于默认情况下为会进行 EBS 优化的实例，无需启用 EBS 优化，并且使用 CLI 或 API 禁用 EBS 优化也不会有影响。您可以在启动实例时对支持 EBS 优化的其他实例类型启用 EBS 优化，或在实例已在运行后启用 EBS 优化。

| 实例类型 | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB)** |
|-------------------------|---------------|--------------|----------------|--------------------------|
| <code>c1.xlarge</code> | | 1000 | 125 | 8000 |
| <code>c3.xlarge</code> | | 500 | 62.5 | 4000 |
| <code>c3.2xlarge</code> | | 1000 | 125 | 8000 |
| <code>c3.4xlarge</code> | | 2000 | 250 | 16000 |
| <code>c4.large</code> | 是 | 500 | 62.5 | 4000 |
| <code>c4.xlarge</code> | 是 | 750 | 93.75 | 6000 |
| <code>c4.2xlarge</code> | 是 | 1000 | 125 | 8000 |
| <code>c4.4xlarge</code> | 是 | 2000 | 250 | 16000 |
| <code>c4.8xlarge</code> | 是 | 4000 | 500 | 32000 |
| <code>d2.xlarge</code> | 是 | 750 | 93.75 | 6000 |
| <code>d2.2xlarge</code> | 是 | 1000 | 125 | 8000 |
| <code>d2.4xlarge</code> | 是 | 2000 | 250 | 16000 |
| <code>d2.8xlarge</code> | 是 | 4000 | 500 | 32000 |
| <code>g2.2xlarge</code> | | 1000 | 125 | 8000 |
| <code>i2.xlarge</code> | | 500 | 62.5 | 4000 |
| <code>i2.2xlarge</code> | | 1000 | 125 | 8000 |
| <code>i2.4xlarge</code> | | 2000 | 250 | 16000 |

| 实例类型 | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB)** |
|-------------|---------------|--------------|----------------|--------------------------|
| i3.large | 是 | 425 | 50 | 3000 |
| i3.xlarge | 是 | 850 | 100 | 6000 |
| i3.2xlarge | 是 | 1,700 | 200 | 12000 |
| i3.4xlarge | 是 | 3,500 | 400 | 16000 |
| i3.8xlarge | 是 | 7,000 | 850 | 32,500 |
| i3.16xlarge | 是 | 14,000 | 1,750 | 65000 |
| m1.large | | 500 | 62.5 | 4000 |
| m1.xlarge | | 1000 | 125 | 8000 |
| m2.2xlarge | | 500 | 62.5 | 4000 |
| m2.4xlarge | | 1000 | 125 | 8000 |
| m3.xlarge | | 500 | 62.5 | 4000 |
| m3.2xlarge | | 1000 | 125 | 8000 |
| m4.large | 是 | 450 | 56.25 | 3600 |
| m4.xlarge | 是 | 750 | 93.75 | 6000 |
| m4.2xlarge | 是 | 1000 | 125 | 8000 |
| m4.4xlarge | 是 | 2000 | 250 | 16000 |
| m4.10xlarge | 是 | 4000 | 500 | 32000 |
| m4.16xlarge | 是 | 10000 | 1250 | 65000 |
| p2.xlarge | 是 | 750 | 93.75 | 6000 |
| p2.8xlarge | 是 | 5000 | 625 | 32,500 |
| p2.16xlarge | 是 | 10000 | 1250 | 65000 |
| r3.xlarge | | 500 | 62.5 | 4000 |
| r3.2xlarge | | 1000 | 125 | 8000 |
| r3.4xlarge | | 2000 | 250 | 16000 |
| r4.large | 是 | 400 | 50 | 3000 |
| r4.xlarge | 是 | 800 | 100 | 6000 |
| r4.2xlarge | 是 | 1600 | 200 | 12000 |
| r4.4xlarge | 是 | 3000 | 375 | 16000 |
| r4.8xlarge | 是 | 6000 | 750 | 32000 |
| r4.16xlarge | 是 | 12000 | 1500 | 65000 |

| 实例类型 | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB)** |
|-------------|---------------|--------------|----------------|--------------------------|
| x1.16xlarge | 是 | 5000 | 625 | 32,500 |
| x1.32xlarge | 是 | 10000 | 1250 | 65000 |

* 必须将这些实例类型作为 EBS 优化实例启动，才能始终实现此级别的性能。

** 此值是基于 100% 只读工作负载的舍入近似值，作为基线配置帮助提供。EBS 优化连接是全双工连接，可以在同时使用两个通信通道的 50/50 读/写工作负载中驱动更多吞吐量和 IOPS。在某些情况下，网络、文件系统和 Amazon EBS 加密的开销可能会降低可用的最大吞吐量和 IOPS。

请注意，某些带 10 Gb 网络接口的实例（例如，i2.8xlarge 和 r3.8xlarge）不提供 EBS 优化，因此它们没有可用的专用 EBS 带宽且未在此处列出。在这些实例上，将在同一个 10 Gb 网络接口上共享网络流量和 Amazon EBS 流量。其他一些 10 Gb 网络实例（例如，c4.8xlarge 和 d2.8xlarge）提供专用 EBS 带宽以及专门用于网络流量的 10 Gb 接口。

在启动时启用 EBS 优化

您可以通过设置某个实例的 EBS 优化属性来对该实例启用 EBS 优化。

在启动实例时使用控制台启用 EBS 优化

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 单击 Launch Instance。在步骤 1：选择 Amazon 系统映像 (AMI) 中，选择 AMI。
3. 在 Step 2: Choose an Instance Type 中，选择作为支持性 EBS 优化列出的实例类型。
4. 在步骤 3：配置实例详细信息中，填写所需的字段并选择作为 EBS 优化实例启动。如果您在上一个步骤中选择的实例类型不支持 EBS 优化，此选项将不存在。如果您选择的实例类型在默认情况下会进行 EBS 优化，则会选择此选项，并且无法取消选择。
5. 按照说明来完成向导和启动实例。

在启动实例时使用命令行启用 EBS 优化

您可以将以下选项之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--ebs-optimized` 与 `run-instances` (AWS CLI)
- `-EbsOptimized` 与 `New-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

为正在运行的实例修改 EBS 优化

您可以修改正在运行的实例的 EBS 优化实例属性，以便为该实例启用或禁用 EBS 优化。

使用控制台为正在运行的实例启用 EBS 优化

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，单击 Instances，然后选择实例。
3. 单击 Actions (操作)，选择 Instance State (实例状态)，然后单击 Stop (停止)。

Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，单击 Yes, Stop。停止实例可能需要几分钟时间。

5. 在实例仍处于选中状态下，单击 Actions (操作)，选择 Instance Settings (实例设置)，然后单击 Change Instance Type (更改实例类型)。
6. 在 Change Instance Type 对话框中，执行下列操作之一：
 - 如果您的实例默认情况下为经过 EBS 优化的实例类型，则 EBS-optimized 已被选择，您无法取消选择。您可以单击 Cancel，因为该实例已启用 EBS 优化。
 - 如果您的实例的实例类型支持 EBS 优化，请选择 EBS-optimized，然后单击 Apply。
 - 如果您的实例的实例类型不支持 EBS 优化，则 EBS-optimized 已取消选择，您无法选择它。您可以从支持 EBS 优化的 Instance Type 中选择一个实例类型，选择 EBS-optimized，然后单击 Apply。
7. 单击 Actions (操作)，选择 Instance State (实例状态)，然后单击 Start (启动)。

使用命令行为正在运行的实例启用 EBS 优化

您可以将以下选项之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--ebs-optimized` 与 [modify-instance-attribute](#) (AWS CLI)
- `-EbsOptimized` 与 [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

Amazon EBS Encryption

Amazon EBS 加密提供了用于 EBS 卷的简单加密解决方案，您无需构建、维护和保护自己的密钥管理基础设施。在创建加密的 EBS 卷并将其连接到支持的实例类型后，将对以下类型的数据进行加密：

- 卷中的静态数据
- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照

加密在托管 EC2 实例的服务器上进行，对从 EC2 实例传输到 EBS 存储的数据进行加密。

Amazon EBS 加密在创建加密卷及其快照时，使用 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK)。首次在某个区域中创建加密卷时，将自动为您创建一个默认 CMK。除非您选择了使用 AWS KMS 单独创建的 CMK，否则此密钥将用于 Amazon EBS 加密。创建您自己的 CMK 可以实现更高的灵活性，让您可以创建、轮换、禁用密钥以定义访问控制，并审核用于保护数据的加密密钥。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

所有 EBS 卷类型 (通用型 SSD [gp2]、预配置 IOPS SSD [io1]、吞吐优化 HDD [st1]、Cold HDD [sc1] 和磁介质 [standard]) 都支持此功能，加密卷对延迟的影响极小，其 IOPS 性能与未加密卷一样。您可以通过与访问未加密卷相同的方式来访问加密卷；加密和解密以透明方式处理，您的 EC2 实例或您的应用程序都无需执行其他任何操作。

从加密卷拍摄的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷的快照无法公开，但是如果执行以下步骤，您可以与特定账户共享加密快照：

1. 使用自定义 CMK 而非默认 CMK 对您的卷进行加密。
2. 允许特定账户访问自定义 CMK。
3. 创建快照。
4. 允许特定账户访问该快照。

有关更多信息，请参阅 [共享 Amazon EBS 快照](#)。

Amazon EBS 加密仅对特定实例类型可用。加密卷和未加密卷都可以连接到支持的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 569\)](#)。

内容

- [加密密钥管理 \(p. 569\)](#)
- [支持的实例类型 \(p. 569\)](#)
- [更改数据的加密状态 \(p. 569\)](#)
- [Amazon EBS 加密和 CloudWatch Events \(p. 571\)](#)

加密密钥管理

Amazon EBS 加密 为您处理密钥管理。每个新创建的卷都使用一个唯一的 256 位密钥加密；此卷的所有快照以及从这些快照创建的后续卷也共享该密钥。这些密钥受我们自己的密钥管理基础设施的保护，这将实施强逻辑和物理安全控制以防止未经授权的访问。您的数据和关联的密钥使用行业标准的 AES-256 算法进行加密。

您无法更改与现有快照或加密卷关联的 CMK。然而，您可在快照复制操作（包括加密未加密快照的副本）期间关联另一个 CMK，而生成的已复制快照将使用新的 CMK。

Amazon 的整体密钥管理基础设施使用联邦信息处理标准 (FIPS) 140-2 批准的加密算法，符合美国国家标准与技术研究院 (NIST) 800-57 建议。

每个 AWS 账户都具有一个唯一的主密钥，该密钥与数据完全分开，存储在一个受严格的物理和逻辑安全控制保护的系统上。每个加密卷（及其后续的快照）使用唯一卷加密密钥来加密，然后使用特定于区域的安全主密钥加密。卷加密密钥在托管您的 EC2 实例的服务器的内存中使用，永远不会以纯文本格式存储在磁盘上。

支持的实例类型

Amazon EBS 加密 适用于下表中所列的实例类型。这些实例类型利用 Intel AES 新指令 (AES-NI) 指令集提供更快且更简单的数据保护。您可以同时将加密卷和未加密卷连接到这些实例类型。

| 实例系列 | 支持 Amazon EBS 加密 的实例类型 |
|-------|--|
| 通用型 | m3.medium m3.large m3.xlarge m3.2xlarge m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge |
| 计算优化 | c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge |
| 内存优化 | cr1.8xlarge r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge r4.large r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge x1.16xlarge x1.32xlarge |
| 存储优化 | d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge i3.large i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge |
| 加速的计算 | g2.2xlarge g2.8xlarge p2.xlarge p2.8xlarge p2.16xlarge |

有关这些实例类型的更多信息，请参阅[实例类型详细信息](#)。

更改数据的加密状态

不能直接对现有的未加密卷加密或对加密卷删除加密。但是，您可以在加密卷与未加密卷之间迁移数据。您也可以在复制快照时应用新的加密状态：

- 在复制未加密卷的未加密快照时，您可以将副本加密。从该加密副本还原的卷也将被加密。

- 在复制加密卷的加密快照时，您可以使用不同的 CMK 将副本重新加密。从该加密副本还原的卷只能使用新应用的 CMK 进行访问。

在加密卷与未加密卷之间迁移数据

当您对加密卷和未加密卷都可以访问时，就可以在它们之间自由传输数据了。EC2 透明地执行加密和解密操作。

在加密卷与未加密卷之间迁移数据

- 按照 [创建 Amazon EBS 卷 \(p. 527\)](#) 中的程序创建您的目标卷（是否加密取决于您的需求）。
- 将目标卷挂载到托管待迁移数据的实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
- 按照 [使 Amazon EBS 卷可用 \(p. 531\)](#) 中的过程使目标卷可用。对于 Linux 实例，您可以在 `/mnt/destination` 创建安装点，然后在此处安装目标卷。
- 将数据从您的源目录复制到目标卷。使用批量复制实用工具执行此任务可能最为方便。

Linux

按如下所示使用 `rsync` 命令将数据从源复制到目标卷。在此示例中，源数据位于 `/mnt/source` 中，目标卷安装在 `/mnt/destination`。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

Windows

在命令提示符处，使用 `robocopy` 命令将数据从源复制到目标卷。在此示例中，源数据位于 `D:\` 中，目标卷安装在 `E:\`。

```
PS C:\Users\Administrator> robocopy D:\ E:\ /e /copyall /eta
```

在复制快照时应用加密

因为可以在复制快照时对快照应用加密，所以复制数据的另一种途径步骤如下。

通过快照复制对卷数据加密

- 创建未加密 EBS 卷的快照。此快照也未加密。
- 复制快照的同时应用加密参数。生成的目标快照是加密的。
- 将加密快照还原到新卷，也还是加密的。

有关更多信息，请参阅 [复制 Amazon EBS 快照](#)。

使用新的 CMK 重新加密快照

由于能够在复制过程中加密快照，您可以重新加密您拥有的已加密过的快照。进行这一操作时，系统会使用您提供的新 CMK 对快照的纯文本进行加密。从生成的副本还原的卷只能使用新的 CMK 进行访问。

在相关的场景中，您可以选择对与您共享的快照进行重新加密。从共享的加密快照还原某个卷之前，您必须创建属于您自己的共享加密快照副本。默认情况下，系统会使用快照所有者共享的密钥对该副本进行加密。不过，我们建议您在复制过程中，使用您控制的其他密钥重新加密快照。这样，即使原始密钥遭到泄露或拥有者出于任何原因撤销了密钥，您也不会失去对卷的访问权限。

以下程序演示了如何重新加密您的快照。

使用控制台重新加密快照

1. 创建自定义 CMK。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。
2. 创建用您的默认 CMK (仅针对本示例) 加密的 EBS 卷。
3. 创建加密 EBS 卷的快照。此快照也使用您的默认 CMK 进行加密。
4. 在 Snapshots 页面，选择 Actions，然后选择 Copy。
5. 在 Copy Snapshot 窗口中，在 Master Key 字段中输入您自定义的 CMK 的完整 ARN (以 arn:aws:kms:**us-east-1:012345678910:key/abcd1234-a123-456a-a12b-a123b4cd56ef** 的形式)，或从菜单中选择该 ARN。单击“Copy”。

生成的快照副本以及从其还原的所有卷都将使用您自定义的 CMK 进行加密。

以下程序演示了如何在复制过程中重新加密共享的加密快照。要进行这一操作，您需要拥有共享加密快照及用于对其进行加密的 CMK 的访问权限。

使用控制台复制并重新加密共享快照

1. 在 Snapshots 页面选择共享的加密快照，选择 Actions，然后选择 Copy。
2. 在 Copy Snapshot 窗口中，在 Master Key 字段中输入您拥有的 CMK 的完整 ARN (以 arn:aws:kms:**us-east-1:012345678910:key/abcd1234-a123-456a-a12b-a123b4cd56ef** 的形式)，或从菜单中选择该 ARN。单击“Copy”。

生成的快照副本以及从其还原的所有卷都将使用您提供的 CMK 进行加密。原始共享快照、其加密状态或共享 CMK 的更改不会对您的副本产生影响。

有关更多信息，请参阅 [复制 Amazon EBS 快照](#)。

Amazon EBS 加密和 CloudWatch Events

在与加密相关的某些特定情景下，EBS 支持 Amazon CloudWatch Events。有关更多信息，请参阅 [Amazon CloudWatch Events for Amazon EBS](#)。

Linux 实例上的 Amazon EBS 卷性能

几个因素 (包括 I/O 特性以及实例和卷的配置) 会对 Amazon EBS 的性能造成影响。客户如按照 Amazon EBS 和 Amazon EC2 产品详细信息页面上的指导操作，通常能获得很好的性能。但是，在某些情况下，您可能需要进行一些调整才能在此平台上获得最好的性能。本主题讨论特定于某些使用案例的一般最佳实践和性能调整。除了基准测试之外，我们建议您根据实际工作负载信息来调整性能，以确定最佳配置。当您学习了使用 EBS 卷的基础知识后，最好了解一下所需的 I/O 性能，以及可用于提升 Amazon EBS 性能以满足这些要求的选项。

内容

- [Amazon EBS 性能提示 \(p. 571\)](#)
- [Amazon EC2 实例配置 \(p. 573\)](#)
- [I/O 特性和监控 \(p. 576\)](#)
- [初始化 Amazon EBS 卷 \(p. 578\)](#)
- [Linux 上的 RAID 配置 \(p. 579\)](#)
- [对 EBS 卷进行基准测试 \(p. 582\)](#)

Amazon EBS 性能提示

这些提示代表了在各种用户场景下能够获得最佳 EBS 卷性能的最佳实践。

使用 EBS 优化的实例

对于不支持 EBS 优化吞吐量的实例，网络流量可能会与实例和 EBS 卷之间的流量产生冲突；而在 EBS 优化实例中，这两种流量相互独立。部分 EBS 优化实例配置（如 C3、R3 和 M3）会产生额外成本，另一些实例（如 M4、C4 和 D2）始终可进行 EBS 优化而不会产生额外成本。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 573\)](#)。

了解如何计算性能

度量 EBS 卷的性能时，应了解所需采用的度量单位以及如何计算性能，这十分重要。有关更多信息，请参阅 [I/O 特性和监控 \(p. 576\)](#)。

了解您的工作负载

EBS 卷的最高性能、I/O 操作的大小和数量，以及完成每个操作所需时间之间存在着某种关系。这些因素（性能、I/O 和延迟）相互影响，不同应用程序对各个因素的敏感程度也不同。有关更多信息，请参阅 [对 EBS 卷进行基准测试 \(p. 582\)](#)。

请注意，在从快照初始化卷时，可能会有性能损失

当您首次访问从快照还原的新 EBS 卷上的每个数据块时，延迟会大大增加。您可以在将卷用于生产之前访问每个数据块，以避免这种性能影响。此过程称为初始化（以前称为预热）。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 578\)](#)。

可能降低 HDD 性能的因素

如果创建吞吐优化 HDD (`st1`) 或 Cold HDD (`sc1`) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。这种情况是这些卷类型特有的。其他可能会限制性能的因素包括迫使吞吐量超过实例的支持能力，在初始化从快照还原的卷时损失性能，以及卷上的小型随机 I/O 过多。有关计算 HDD 卷的吞吐量的更多信息，请参阅 [Amazon EBS 卷类型](#)。

如果您的应用程序没有发送足够的 I/O 请求，性能可能也会受影响。这可通过查看卷的队列长度和 I/O 大小来监控。队列长度是您的应用程序向卷发起的待处理 I/O 请求的数量。为实现最大程度的一致性，在执行 1 MiB 的顺序 I/O 时，HDD 卷必须保持 4 或更大的队列长度（四舍五入为最近的整数）。有关确保卷的性能一致的更多信息，请参阅 [I/O 特性和监控 \(p. 576\)](#)

为 `st1` 和 `sc1` 上高吞吐量、读取操作量大的工作负载增大预读取值

一些工作负载读取操作量大，并会访问操作系统页缓存中的块储存设备（例如，从文件系统访问）。在这种情况下，为了实现最大的吞吐量，我们建议您将预读取设置配置为 1 MiB。每个块储存设备的设置不同，应该只应用于您的 HDD 卷。以下示例假设您在使用 Amazon Linux 实例。

要检查您的块储存设备的当前预读数值，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

块储存设备信息采用以下格式返回：

| RO | RA | SSZ | BSZ | StartSec | Size | Device |
|----|-----|-----|------|----------|------------|---------------|
| rw | 256 | 512 | 4096 | 4096 | 8587820544 | /dev/<device> |

以上显示的设备报告预读取值为 256（默认值）。将此数字乘以扇区大小（512 字节）就可获得预读取缓冲区的大小，在此例中为 128 KiB。要将缓冲区值设置为 1 MiB，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

再次运行第一个命令，验证预读取设置现在显示 2048。

仅当您的工作负载包括大型顺序 I/O 时，才使用此设置。如果它主要包含的是小型随机 I/O，则此设置会降低性能。一般来说，如果工作负载主要包括小型随机 I/O，则应考虑使用通用型 SSD (gp2) 卷，而不是 st1 或 sc1。

使用现代 Linux 内核

借助对间接描述符的支持，使用现代 Linux 内核。所有 Linux 内核 3.11 及更高版本的内核上具有此支持，以及任何当代 EC2 实例。如果您的平均 I/O 大小达到或接近 44 KiB，则说明您可能是在不支持间接描述符的情况下使用实例或内核。有关根据 Amazon CloudWatch 指标得出平均 I/O 大小的信息，请参阅 [I/O 特性和监控 \(p. 576\)](#)。

对于所有 Linux Kernel 4.2 及以上版本的内核，要在 st1 或 sc1 卷上实现最大吞吐量，建议将 `xen_blkfront.max` 参数设置为 256。此参数可在操作系统 boot 命令行中设置。例如，在 Amazon Linux AMI 中，您可以将它添加到在 `/boot/grub/menu.lst` 中找到的 GRUB 配置的 kernel 行末尾：

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
xen_blkfront.max=256
```

重启实例，让此设置生效。

有关更多信息，请参阅[配置 GRUB](#)。对于其他 Linux 版本 (尤其是不使用 GRUB 引导加载程序的版本) 可能需要采用不同方法来调整 Kernel 参数。

有关 EBS I/O 特征的更多信息，请参阅本主题上的 [Amazon EBS：为性能而设计 re:Invent 演示文稿](#)。

使用 RAID 0 最大程度利用实例资源

某些实例类型可以实现的 I/O 吞吐量大于可以为单个 EBS 卷配置的量。可以将多个 gp2、io1、st1 或 sc1 卷一起加入到 RAID 0 配置中，以将可用带宽用于这些实例。有关更多信息，请参阅 [Linux 上的 RAID 配置 \(p. 579\)](#)。

使用 Amazon CloudWatch 跟踪性能

Amazon Web Services 提供了您可以使用 Amazon CloudWatch 来分析和查看的 Amazon EBS 性能指标，以及可以用于监控卷运行状况的状态检查。有关更多信息，请参阅 [监控您的卷状态 \(p. 534\)](#)。

Amazon EC2 实例配置

为应用程序规划和配置 EBS 卷时，需考虑将卷连接到的实例的配置，这十分重要。为了获得最高的 EBS 卷性能，您应该将这些卷连接到具有足够带宽以支持您的卷的实例，如 EBS 优化实例或具有 10 Gb 网络连接的实例。在 RAID 配置中将多个卷条带化时，这尤其重要。

使用 EBS 优化的实例或 10 Gb 网络实例

对于需要最少变化以及专用 Amazon EC2 到 Amazon EBS 流量的任何性能敏感型工作负载 (如生产数据库或业务应用程序)，均应使用连接到 EBS 优化实例或具有 10 Gb 网络连接的实例的卷。不符合此条件的 EC2 实例不提供网络资源保证。确保 EC2 实例与 EBS 卷之间的持续可靠网络带宽的唯一方法是将 EC2 实例作为 EBS 优化实例启动，或选择具有 10 Gb 网络连接的实例类型。要了解哪些实例类型包括 10 Gb 网络连接，请参阅[实例类型详细信息](#)。有关配置 EBS 优化实例的信息，请参阅 [Amazon EBS 优化的实例](#)。

选择具有足够带宽的 EC2 实例

启动进行了 EBS 优化的实例可为您提供 EC2 实例与 EBS 卷之间的专用连接。然而，仍可以为特定实例类型配置超过可用带宽的 EBS 卷，尤其是在 RAID 配置中将多个卷条带化时。下表显示了可以采用 EBS 优化形式启动的实例类型及其专用吞吐量、Amazon EBS 的专用带宽、实例可以支持的最大 IOPS 量 (如果您使用

的 I/O 大小为 16KB) 以及该连接上可用的 I/O 带宽近似值 (以 MB/s 为单位)。请务必选择提供的专用 EBS 吞吐量大于应用程序所需的 EBS 优化实例；否则，Amazon EBS 到 Amazon EC2 的连接将成为性能瓶颈。

Note

下表和以下示例仅出于说明目的使用 16 KB 作为 I/O 大小；您的应用程序 I/O 大小可能会有所不同 (Amazon EBS 将每秒的每个 I/O 操作 (即 256 KiB 或更小) 作为一个 IOPS 进行度量)。有关 IOPS 以及 I/O 大小和卷吞吐量限制之间的关系的更多信息，请参阅 [I/O 特性和监控 \(p. 576\)](#)。

| 实例类型 | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB)** |
|-------------|---------------|--------------|----------------|--------------------------|
| c1.xlarge | | 1000 | 125 | 8000 |
| c3.xlarge | | 500 | 62.5 | 4000 |
| c3.2xlarge | | 1000 | 125 | 8000 |
| c3.4xlarge | | 2000 | 250 | 16000 |
| c4.large | 是 | 500 | 62.5 | 4000 |
| c4.xlarge | 是 | 750 | 93.75 | 6000 |
| c4.2xlarge | 是 | 1000 | 125 | 8000 |
| c4.4xlarge | 是 | 2000 | 250 | 16000 |
| c4.8xlarge | 是 | 4000 | 500 | 32000 |
| d2.xlarge | 是 | 750 | 93.75 | 6000 |
| d2.2xlarge | 是 | 1000 | 125 | 8000 |
| d2.4xlarge | 是 | 2000 | 250 | 16000 |
| d2.8xlarge | 是 | 4000 | 500 | 32000 |
| g2.2xlarge | | 1000 | 125 | 8000 |
| i2.xlarge | | 500 | 62.5 | 4000 |
| i2.2xlarge | | 1000 | 125 | 8000 |
| i2.4xlarge | | 2000 | 250 | 16000 |
| i3.large | 是 | 425 | 50 | 3000 |
| i3.xlarge | 是 | 850 | 100 | 6000 |
| i3.2xlarge | 是 | 1,700 | 200 | 12000 |
| i3.4xlarge | 是 | 3,500 | 400 | 16000 |
| i3.8xlarge | 是 | 7,000 | 850 | 32,500 |
| i3.16xlarge | 是 | 14,000 | 1,750 | 65000 |
| m1.large | | 500 | 62.5 | 4000 |
| m1.xlarge | | 1000 | 125 | 8000 |
| m2.2xlarge | | 500 | 62.5 | 4000 |

| 实例类型 | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB)** |
|-------------|---------------|--------------|----------------|--------------------------|
| m2.4xlarge | | 1000 | 125 | 8000 |
| m3.xlarge | | 500 | 62.5 | 4000 |
| m3.2xlarge | | 1000 | 125 | 8000 |
| m4.large | 是 | 450 | 56.25 | 3600 |
| m4.xlarge | 是 | 750 | 93.75 | 6000 |
| m4.2xlarge | 是 | 1000 | 125 | 8000 |
| m4.4xlarge | 是 | 2000 | 250 | 16000 |
| m4.10xlarge | 是 | 4000 | 500 | 32000 |
| m4.16xlarge | 是 | 10000 | 1250 | 65000 |
| p2.xlarge | 是 | 750 | 93.75 | 6000 |
| p2.8xlarge | 是 | 5000 | 625 | 32,500 |
| p2.16xlarge | 是 | 10000 | 1250 | 65000 |
| r3.xlarge | | 500 | 62.5 | 4000 |
| r3.2xlarge | | 1000 | 125 | 8000 |
| r3.4xlarge | | 2000 | 250 | 16000 |
| r4.large | 是 | 400 | 50 | 3000 |
| r4.xlarge | 是 | 800 | 100 | 6000 |
| r4.2xlarge | 是 | 1600 | 200 | 12000 |
| r4.4xlarge | 是 | 3000 | 375 | 16000 |
| r4.8xlarge | 是 | 6000 | 750 | 32000 |
| r4.16xlarge | 是 | 12000 | 1500 | 65000 |
| x1.16xlarge | 是 | 5000 | 625 | 32,500 |
| x1.32xlarge | 是 | 10000 | 1250 | 65000 |

* 必须将这些实例类型作为 EBS 优化实例启动，才能始终实现此级别的性能。

** 此值是基于 100% 只读工作负载的舍入近似值，作为基线配置帮助提供。EBS 优化连接是全双工连接，可以在同时使用两个通信通道的 50/50 读/写工作负载中驱动更多吞吐量和 IOPS。在某些情况下，网络、文件系统和 Amazon EBS 加密的开销可能会降低可用的最大吞吐量和 IOPS。

请注意，某些带 10 Gb 网络接口的实例（如 i2.8xlarge、c3.8xlarge 和 r3.8xlarge）不提供 EBS 优化，因此它们没有可用的专用 EBS 带宽且未在此处列出。不过，如果您的应用程序不推送与 Amazon EBS 竞争的其他网络流量，则可以使用 Amazon EBS 流量的所有带宽。其他一些 10 GB 网络实例（例如，c4.8xlarge 和 d2.8xlarge）提供专用 Amazon EBS 带宽以及专门用于网络流量的 10 GB 接口。

m1.large 实例最大的 16 KB IOPS 值为 4000，但是，除非此实例类型作为 EBS 优化实例启动，否则该值只是理想情况下的值，且无法得到保证；要切实确保 16 KB IOPS 的值为 4000，您必须将此实例作为 EBS

优化实例启动。但是，如果 IOPS 为 4000 的 `io1` 卷挂载到 EBS 优化的 `m1.large` 实例，Amazon EC2 与 Amazon EBS 之间的连接带宽限制将使此卷无法提供它本可以实现的 320 MB/s 最大聚合吞吐量。在这种情况下，我们必须使用支持至少 320 MB/s 吞吐量的 EBS 优化 EC2 实例，如 `c4.8xlarge` 实例类型。

通用型 SSD (`gp2`) 类型的卷的吞吐量限制为 128 MB/s 到 160 MB/s 之间（具体取决于卷大小），这与 1000 Mbps 的 EBS 优化连接很相称。向 Amazon EBS 提供的吞吐量大于 1000 Mbps 的实例类型可以使用多个 `gp2` 卷来利用可用吞吐量。对于预配置的每个 IOPS，预配置 IOPS SSD (`io1`) 类型的卷的吞吐量限制为 256 KiB，最高可达 320 MiB/s (1280 IOPS 情况下)。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

具有 10 Gb 网络连接性的实例类型对于未加密的 Amazon EBS 卷支持最多 800 MB/s 吞吐量和 48000 16K IOPS，对于已加密的 Amazon EBS 卷，最多支持 25000 16K IOPS。由于 EBS 卷的最大 `io1` 值为 20,000 (对于 `io1` 卷) 和 10,000 (对于 `gp2` 卷)，您可以同时使用多个 EBS 卷来达到这些实例类型可实现的 I/O 性能水平。有关哪些实例类型具有 10 Gb 网络连接能力的更多信息，请参阅[实例类型详细信息](#)。

您应该使用 EBS 优化实例 (如可用) 以发挥 Amazon EBS `gp2` 和 `io1` 卷的全部性能优势。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。

I/O 特性和监控

在给定卷配置中，某些 I/O 特性会对 EBS 卷的性能表现造成影响。SSD 卷 (即通用型 SSD (`gp2`) 和预配置 IOPS SSD (`io1`)) 能够提供一致的性能，无论 I/O 操作是随机的还是顺序的。HDD 卷 (即吞吐优化 HDD (`st1`) 和 Cold HDD (`sc1`)) 仅当 I/O 操作是大型顺序操作时才能提供最佳性能。要了解 SSD 和 HDD 卷在您的应用程序中性能如何，务必要知道卷上的需求之间的联系、卷能支持的 IOPS 数量、完成 I/O 操作所需的时间，以及卷的吞吐量限制。

IOPS

IOPS 是表示每秒输入/输出操作数的度量单位。操作数以 KiB 来度量，底层驱动技术确定卷类型计算为单次 I/O 的最大数据量。SSD 卷的最大 I/O 大小为 256 KiB，HDD 卷的最大 I/O 大小为 1024 KiB，因为 SSD 卷比 HDD 卷处理小型或随机 I/O 的效率高很多。

当小型 I/O 操作在物理上连续进行时，Amazon EBS 会尝试将这些操作合并为单个 I/O，直至最大大小。例如，对于 SSD 卷，一个 1024 KiB 的 I/O 操作计为 4 个操作 ($1,024 \div 256 = 4$)，而 8 个 32 KiB 的连续 I/O 操作计为 1 个操作 ($8 \times 32 = 256$)。但是，8 个随机 32 KiB I/O 操作将被计为 8 个操作。每个低于 32 KiB 的 I/O 操作计为 1 个操作。

类似地，对于由 HDD 支持的卷，一个 1024 KiB 的 I/O 操作和 8 个顺序 128 KiB 操作将被计为一个操作。但是，8 个随机 128 KiB I/O 操作计为 8 个操作。

这样，当您创建支持 3000 IOPS (通过将 `io1` 配置为 3000 IOPS 或将 `gp2` 卷大小确定为 1000 GiB) 的 SSD 卷时，您就可以将它连接到一个 EBS 优化实例，该实例可以提供足够的带宽，您可以每秒传输最高 3000 次数据 I/O，其吞吐量由 I/O 大小决定。

卷队列长度和延迟

卷队列长度是指等待设备处理的 I/O 请求的数量。延迟为 I/O 操作的实际端到端客户端时间，也就是说，从将 I/O 发送到 EBS 到接收来自 EBS 的确认以表示 I/O 读取或写入完成所经过的时间。队列长度必须进行适当调整，以便与 I/O 大小和延迟匹配，避免在来宾操作系统上或在到 EBS 的网络链路上产生瓶颈。

每个工作负载的最佳队列长度不同，具体取决于您的特定应用程序对于 IOPS 和延迟的敏感程度。如果您的工作负载未提供足够的 I/O 请求来充分利用 EBS 卷的可用性能，则卷可能无法提供您预置的 IOPS 或吞吐量。

事务密集型应用程序对 I/O 延迟增加很敏感，很适合使用 SSD 支持的 `io1` 和 `gp2` 卷。您可以通过使卷保持较小的队列长度和较高的 IOPS 数量，来维持高 IOPS 和低延迟。持续迫使一个卷的 IOPS 高于它能够支持的 IOPS 可能增加 I/O 延迟。

吞吐量密集型应用程序对 I/O 延迟增加较不敏感，很适合使用 HDD 支持的 `st1` 和 `sc1` 卷。您可以在执行大型顺序 I/O 时维持大队列长度，从而对 HDD 卷保持高吞吐量。

I/O 大小和卷吞吐量限制

对于 SSD 卷，如果 I/O 大小非常大，由于达到卷的吞吐量限制，您的 IOPS 数可能会少于预配置数量。例如，对于具有可用突增额度的 1000 GiB 以下的 `gp2` 卷，IOPS 限制为 3000，卷吞吐量限制为 160 MiB/s。如果您正在使用 256 KiB 的 I/O 大小，则您的卷在 IOPS 为 640 时将达到其吞吐量限制 ($640 \times 256 \text{ KiB} = 160 \text{ MiB}$)。当 I/O 大小较小（如 16 KiB）时，这个卷可以支持 3000 IOPS，这是因为吞吐量远低于 160 MiB/s（这些例子都假设卷的 I/O 不会达到实例的吞吐量限制。）有关每种 EBS 卷类型吞吐量限制的更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。

对于较小的 I/O 操作，从实例内部进行度量时，您可能会看到 IOPS 值高于预配置值。当实例操作系统在将小型 I/O 操作传递到 Amazon EBS 之前将其合并为一个较大的操作时，会发生这种情况。

对于 HDD 支持的 `st1` 和 `sc1` 卷，如果您的工作负载使用顺序 I/O，则从实例内部进行度量时，您的 IOPS 值可能会高于预期数量。当实例操作系统将顺序 I/O 进行合并，并以 1024 KiB 大小为单位来对其进行计数时，会发生这种情况。如果您的工作负载使用小型随机 I/O，则吞吐量可能会低于您的预期。这是因为我们会将每个随机的非顺序 I/O 计入总的 IOPS 计数，这可能导致您比预期更快达到卷的 IOPS 限制。

无论您采用何种 EBS 卷类型，如果您的 IOPS 或吞吐量与您在配置中的预期不同，请确保 EC2 实例带宽并不是导致这种结果的限制因素。您应始终使用最新一代的 EBS 优化实例（或包含 10 Gb/s 网络连接的实例）以实现最佳性能。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 573\)](#)。未达到预期 IOPS 的另一个可能原因是未对 EBS 卷执行足够多的 I/O 操作。

使用 CloudWatch 监控 I/O 特性

您可以通过每个卷的 [CloudWatch 指标](#) 监控这些 I/O 特性。要考虑的重要指标包括：

- `BurstBalance`
- `VolumeReadBytes`
- `VolumeWriteBytes`
- `VolumeReadOps`
- `VolumeWriteOps`
- `VolumeQueueLength`

`BurstBalance` 以剩余余额百分比的形式显示 `gp2`, `st1`, and `sc1` 卷的突增存储桶余额。当您的突增存储桶耗尽时，卷 I/O 点数（对于 `gp2` 卷）或卷吞吐量点数（对于 `st1` 和 `sc1` 卷）会限制为基准。检查 `BurstBalance` 值以确定卷是否因为此原因而受限制。

HDD 支持的 `st1` 和 `sc1` 卷最适用于最大 I/O 为 1024KiB 的工作负载。要确定卷的平均 I/O 大小，请将 `volumeWriteBytes` 除以 `volumeWriteOps`。同样的计算也适用于读取操作。如果平均 I/O 大小低于 64 KiB，则提高发送到 `st1` 或 `sc1` 卷的 I/O 操作的大小应该能够提高性能。

Note

如果平均 I/O 大小达到或接近 44 KiB，说明您可能是在不支持间接描述符的情况下使用实例或内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，任何当代实例也具有此支持。

如果您的 I/O 延迟高于您的所需，请检查 `volumeQueueLength`，以确保应用程序尝试驱动的 IOPS 不会超过您的配置。如果您的应用程序需要的 IOPS 数量超出您的卷所能提供的数量，则应考虑使用基本性能水平较高的较大 `gp2` 卷，或使用预配置 IOPS 更高的 `io1` 卷，以实现更短的延迟。

有关 Amazon EBS I/O 特征的更多信息，请参阅本主题上的 [Amazon EBS：为性能而设计 re:Invent 演示文稿](#)。

初始化 Amazon EBS 卷

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。访问数据完毕后，性能随之恢复。

您可以通过在使用之前对卷上的所有数据块进行读取，在生产环境中避免这种性能冲击；此过程称为初始化。对于从快照创建的新卷，您应该在使用该卷前读取所有包含数据的块。

Important

在初始化已从快照还原的 `io1` 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O Performance 状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 `io1` 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅 [使用状态检查来监控卷 \(p. 536\)](#)。

在 Linux 上初始化 Amazon EBS 卷

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。对于已从快照还原的卷，请使用 `dd` 或 `fio` 实用程序读取卷上的所有数据块。卷上的所有现有数据都会保留。

在 Linux 上初始化从快照还原的卷

1. 将新还原的卷挂载到您的 Linux 实例。
2. 使用 `lsblk` 命令列出实例上的块储存设备。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0 30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

在此处可以看到新卷 `/dev/xvdf` 已连接，但是未安装（因为 `MOUNTPOINT` 列下没有列出任何路径）。

3. 使用 `dd` 或 `fio` 实用程序对设备上的所有数据块进行读取。默认情况下，`dd` 命令将安装在 Linux 系统上，但 `fio` 要快得多，因为它允许多线程读取。

Note

此步骤可能需要几分钟到几个小时，具体取决于 EC2 实例带宽、为卷配置的 IOPS 和卷的大小。

- 使用 `dd`：应将 `if`（输入文件）参数设置为要初始化的驱动器。应将 `of`（输出文件）参数设置为 Linux 空虚拟设备，`/dev/null`。`bs` 参数设置读取操作的数据块大小；要获得最佳性能，这应设置为 1 MB。

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

- 使用 `fio`：如果您在系统上安装了 `fio`，则可以复制并粘贴以下命令来初始化您的卷。应将 `--filename`（输入文件）参数设置为要初始化的驱动器。

Note

要在 Amazon Linux 上安装 `fio`，请使用以下命令：`sudo yum install -y fio`
要在 Ubuntu 上安装 `fio`，请使用以下命令：`sudo apt-get install -y fio`

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=128k --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

操作完成时，您会看到读取操作的报告。卷现在已准备就绪，可供使用。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 531\)](#)。

Linux 上的 RAID 配置

通过 Amazon EBS，您可以使用可与传统裸机服务器结合使用的任何标准 RAID 配置，只要实例的操作系统支持该特定 RAID 配置。这是因为，所有 RAID 都是在软件级别上实现的。为取得比通过单个卷取得的 I/O 性能更高的 I/O 性能，RAID 0 可将多个卷组合在一起；为取得实例上的冗余，RAID 1 可将两个卷镜像在一起。

Amazon EBS 卷的数据可在可用区内多个服务器间进行复制，以防由于任何单个组件发生故障导致数据丢失。此复制使得 Amazon EBS 卷的可靠程度比普通磁盘高 10 倍。更多信息，请参阅 Amazon EBS 产品详细信息页面中的 [Amazon EBS 可用性与持久性](#)。

Note

您应避免从 RAID 卷启动。Grub 通常只安装在 RAID 阵列中的一台设备上，如果某台镜像设备发生故障，您可能无法启动操作系统。

如果您需要在 Windows 实例上创建一个 RAID 阵列，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [Windows 上的 RAID 配置](#)。

内容

- [RAID 配置选项 \(p. 579\)](#)
- [在 Linux 上创建 RAID 阵列 \(p. 580\)](#)

RAID 配置选项

下表比较常见的 RAID 0 和 RAID 1 选项。

| 配置 | 使用 | 优点 | 缺点 |
|--------|---|---------------------------------|--|
| RAID 0 | 当 I/O 性能比容错能力更重要时；例如在频繁使用的数据库中（其中，已单独设置数据复制）。 | I/O 在卷内以条带状分布。如果您添加卷，则会直接增加吞吐量。 | 条带的性能受限于该集合中的最差的执行卷。丢失单个卷会导致完全丢失阵列的数据。 |
| RAID 1 | 当容错能力比 I/O 性能更重要时；例如在关键应用程序中。 | 在数据持久性方面更具安全性。 | 不提供写入性能改进；需要比非 RAID 配置更大的 Amazon EC2 到 Amazon EBS 带宽，因为数据将同时写入多个卷。 |

Important

不建议对 Amazon EBS 使用 RAID 5 和 RAID 6，因为这些 RAID 模式的奇偶校验写入操作会使用您的卷的一些可用 IOPS。根据您的 RAID 阵列配置，这些 RAID 模式提供的可用 IOPS 比 RAID 0 配置少 20-30%。成本增加也是与这些 RAID 模式有关的一个因素；在使用相同的卷大小和速度时，一个 2 卷 RAID 0 阵列明显胜过两倍成本的 4 卷 RAID 6 阵列。

相比在单个 Amazon EBS 卷上配置，通过创建 RAID 0 阵列，文件系统可以获得更高性能。为获得额外冗余性，RAID 1 阵列提供了数据的一个“镜像”。在执行此步骤之前，您需要确定 RAID 阵列的大小以及需要配置多少 IOPS。

RAID 0 阵列的最终大小是阵列中各个卷的大小之和，带宽是阵列中各个卷的可用带宽之和。RAID 1 阵列的最终大小和带宽等于阵列中各个卷的大小和带宽。例如，预配置 IOPS 为 4000 的两个 500 GiB Amazon EBS 卷将创建可用带宽为 8000 IOPS、吞吐量为 640 MB/s 的 1000 GiB RAID 0 阵列，或创建可用带宽为 4000 IOPS、吞吐量为 320 MB/s 的 500 GiB RAID 1 阵列。

本文档提供基本的 RAID 设置示例。有关 RAID 配置、性能和恢复的更多信息，请参阅 Linux RAID Wiki，网址为 https://raid.wiki.kernel.org/index.php/Linux_Raid。

在 Linux 上创建 RAID 阵列

使用以下过程创建 RAID 阵列。请注意，您可以从 Amazon EC2 用户指南（适用于 Windows 实例）中的[在 Windows 上创建 RAID 阵列](#)获得有关 Windows 实例的说明。

在 Linux 上创建 RAID 阵列

1. 为阵列创建 Amazon EBS 卷。有关更多信息，请参阅[创建 Amazon EBS 卷 \(p. 527\)](#)。

Important

为阵列创建具有相等大小和 IOPS 性能值的卷。确保不创建超过 EC2 实例的可用带宽的阵列。
有关更多信息，请参阅[Amazon EC2 实例配置 \(p. 573\)](#)。

2. 将 Amazon EBS 卷连接到要承载该阵列的实例。有关更多信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
3. 使用 mdadm 命令从新连接的 Amazon EBS 卷创建逻辑 RAID 设备。用阵列中的卷数替换 *number_of_volumes*，用阵列中每个卷的设备名称（例如 /dev/xvdf）替换 *device_name*。您还可以将 *MY_RAID* 替代为阵列的唯一名称。

Note

您可以使用 lsblk 命令列出实例上的设备以找到设备名称。

(仅限 RAID 0) 要创建 RAID 0 阵列，请执行以下命令（注意用于将阵列条带化的 --level=0 选项）：

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

(仅限 RAID 1) 要创建 RAID 1 阵列，请执行以下命令（注意用于将阵列镜像化的 --level=1 选项）：

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=1 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

4. 给 RAID 阵列一些时间进行初始化和同步。您可以借助下面的命令跟踪这些操作的进度：

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

这会产生类似下面的输出：

```
Personalities : [raid1]
md0 : active raid1 xvdg[1] xvdf[0]
      20955008 blocks super 1.2 [2/2] [UU]
      [======>.....]  resync = 46.8% (9826112/20955008) finish=2.9min
      speed=63016K/sec
```

通常，您可以通过下面的命令显示有关 RAID 阵列的详细信息：

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

这会产生类似下面的信息：

```
/dev/md0:
      Version : 1.2
      Creation Time : Mon Jun 27 11:31:28 2016
      Raid Level : raid1
      Array Size : 20955008 (19.98 GiB 21.46 GB)
      Used Dev Size : 20955008 (19.98 GiB 21.46 GB)
```

```
Raid Devices : 2
Total Devices : 2
Persistence : Superblock is persistent

Update Time : Mon Jun 27 11:37:02 2016
State : clean
...
...
...

Number  Major  Minor  RaidDevice State
0        202    80      0        active sync   /dev/sdf
1        202    96      1        active sync   /dev/sdg
```

5. 在您的 RAID 阵列上创建一个文件系统，并为该文件系统分配一个稍后在挂载该文件系统时使用的标签。例如，要创建带 **MY_RAID** 标签的 ext4 文件系统，请执行以下命令：

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

根据应用程序的要求或操作系统的限制，您可以使用不同的文件系统类型，例如 ext3 或 XFS (请参阅您的文件系统文档以了解相应的文件系统创建命令)。

6. 为 RAID 阵列创建装载点。

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

7. 最后，在已创建的安装点上安装 RAID 设备：

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

RAID 设备现已准备就绪，可供使用。

8. (可选) 要在每一次系统重启时安装该 Amazon EBS 卷，可将设备的条目添加到 /etc/fstab 文件中。
- 创建 /etc/fstab 文件的备份，当您进行编辑时意外损坏或删除了此文件的情况下，可以使用该备份。

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

- 使用您常用的文本编辑器(如 nano 或 vim) 打开 /etc/fstab 文件。
- 以 "UUID=" 开头为任意行添加评论，并使用以下格式在 RAID 卷文件的末尾添加新行：

```
device_label  mount_point  file_system_type  fs_mntops  fs_freq  fs_passno
```

该行中的最后三个字段是文件系统装载选项、文件系统的转储频率和启动时完成文件系统检查的顺序。如果您不知道这些值应该是什么值，请使用下面的示例中的值 (defaults, nofail 0 2)。有关 /etc/fstab 条目的更多信息，请参阅 fstab 手册页 (通过在命令行上输入 man fstab)。例如，要在设备上的挂载点 /mnt/raid 挂载带标签 MY_RAID 的 ext4 文件系统，请将以下条目添加到 /etc/fstab。

Note

如果您要在未连接此卷的情况下启动实例(例如，以便此卷可以在不同实例之间向后和向前移动)，则应添加 nofail 安装选项，该选项允许实例即使在卷安装过程中出现错误时也可启动。Debian 衍生物(如 Ubuntu)还必须添加 nobootwait 挂载选项。

| | | | | | |
|---------------|-----------|------|-----------------|---|---|
| LABEL=MY_RAID | /mnt/raid | ext4 | defaults,nofail | 0 | 2 |
|---------------|-----------|------|-----------------|---|---|

- d. 将新条目添加到 `/etc/fstab` 后，需要检查条目是否有效。运行 `sudo mount -a` 命令，以便安装 `/etc/fstab` 中的所有文件系统。

```
[ec2-user ~]$ sudo mount -a
```

如果上述命令未产生错误，说明您的 `/etc/fstab` 文件正常，您的文件系统会在下次启动时自动安装。如果该命令产生了任何错误，请检查这些错误并尝试更正 `/etc/fstab`。

Warning

`/etc/fstab` 文件中的错误可能导致系统无法启动。请勿关闭 `/etc/fstab` 文件中有错误的系统。

- e. (可选) 如果您无法确定如何更正 `/etc/fstab` 错误，则始终可以使用以下命令还原您的备份 `/etc/fstab` 文件。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

对 EBS 卷进行基准测试

本节介绍如何通过模拟 I/O 工作负载来测试 Amazon EBS 卷的性能。过程如下所述：

1. 启动 EBS 优化实例。
2. 创建新的 EBS 卷。
3. 将这些卷连接到您的 EBS 优化实例。
4. 配置并挂载块储存设备。
5. 安装工具以便测试 I/O 性能。
6. 测试卷的 I/O 性能。
7. 删除卷并终止实例，确保不会继续引发更改。

Important

本主题中描述的部分程序可能会对您进行基准测试的 EBS 卷上的现有数据造成破坏。基准测试程序适用于出于测试目的而特别创建的卷，并不适用于生产卷。

设置实例

为了获得最佳的 EBS 卷性能，我们建议您使用 EBS 优化实例。EBS 优化实例可在 Amazon EC2 和 Amazon EBS 之间提供实例专用吞吐量。EBS 优化实例可在 Amazon EC2 和 Amazon EBS 之间提供专用带宽，选择范围在 500 到 12,000 Mbps 之间，具体取决于实例类型。

要创建 EBS 优化实例，可在使用 Amazon EC2 控制台启动实例时选择 Launch as an EBS-Optimized instance，或在使用命令行时指定 `--ebs-optimized`。请确保您启动的实例是支持此选项的最新一代实例。要了解本主题中提到的测试示例，建议您启动一个 `c3.4xlarge` 实例。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 564\)](#)。

设置预配置 IOPS SSD (`io1`) 卷

要创建 `io1` 卷，请在使用 Amazon EC2 控制台创建卷时选择预配置 IOPS SSD，或在命令行中指定 `--type io1 --iops n`，其中 `n` 是 100 到 20000 之间的整数。有关创建 EBS 卷的信息，请参阅 [创建 Amazon EBS 卷 \(p. 527\)](#)。有关将这些卷挂载到实例的信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

要了解这些示例测试，我们建议您创建一个包含 6 个卷的高性能 RAID 阵列。因为您是按照预配置的 GB 数量以及为 `io1` 卷预配置 IOPS 的数量（而不是卷数）付费，因此创建多个较小卷并使用它们来创建条带集不会产生额外费用。如果您是使用 Oracle Orion 来测试卷的性能，则它可以模拟 Oracle ASM 的条带化操作，因

此我们建议您让 Orion 执行条带化分区。如果您使用的是其他基准测试工具，则需要自己对卷执行条带化分区。

要在 Amazon Linux 上创建 6 卷条带集，请使用与此类似的命令：

```
[ec2-user ~]$ sudo mdadm --create /dev/md0 --level=0 --chunk=64 --raid-devices=6 /dev/sdf /dev/sdg /dev/sdh /dev/sdi /dev/sdj /dev/sdk
```

在这个示例中，文件系统是 XFS。请使用符合您的要求的文件系统。使用以下命令安装 XFS 文件系统支持：

```
[ec2-user ~]$ sudo yum install -y xfsprogs
```

然后，使用这些命令创建、安装 XFS 文件系统并分配其的所有权：

```
[ec2-user ~]$ sudo mkdir -p /mnt/p_iops_volo && sudo mkfs.xfs /dev/md0
[ec2-user ~]$ sudo mount -t xfs /dev/md0 /mnt/p_iops_volo
[ec2-user ~]$ sudo chown ec2-user:ec2-user /mnt/p_iops_volo/
```

设置吞吐优化 HDD (st1) 或Cold HDD (sc1) 卷

要创建 st1 卷，可在使用 Amazon EC2 控制台创建卷时选择吞吐优化 HDD，或在使用命令行时指定 --type st1。要创建 sc1 卷，可在使用 Amazon EC2 控制台创建卷时选择Cold HDD，或在使用命令行时指定 --type sc1。有关创建 EBS 卷的信息，请参阅[创建 Amazon EBS 卷 \(p. 527\)](#)。有关将这些卷挂载到实例的信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

AWS 提供了一个 JSON 模板，以便与 AWS CloudFormation 配合使用来简化此设置过程。访问[模板](#)并将它另存为 JSON 文件。AWS CloudFormation 允许您配置自己的 SSH 密钥并提供了一种简单的方式来设置性能测试环境，以评估 st1 卷。此模板会创建一个最新一代的实例以及一个 2 TiB 的 st1 卷，然后将该卷挂载到 /dev/xvdf 处的实例。

使用模板创建 HDD 卷

1. 通过以下网址打开 AWS CloudFormation 控制台：<https://console.aws.amazon.com/cloudformation/>。
2. 选择 Create Stack。
3. 选择 Upload a Template to Amazon S3，然后选择之前获得的 JSON 模板。
4. 为您的堆栈提供名称（如“ebs-perf-testing”），然后选择实例类型（默认为 r3.8xlarge）和 SSH 密钥。
5. 选择 Next 两次，然后选择 Create Stack。
6. 新堆栈的状态从 CREATE_IN_PROGRESS 变为 COMPLETE 后，选择 Outputs 以获得新实例的公共 DNS 条目，新实例将挂载一个 2 TiB 的 st1 卷。
7. 以用户 `ec2-user` 的身份使用 SSH 连接到您的新堆栈（使用从上一步的 DNS 条目中获得的主机名）。
8. 继续执行[安装基准测试工具 \(p. 583\)](#)。

安装基准测试工具

下表列出了您可用于对 EBS 卷的性能进行基准测试的部分可用工具。

| 工具 | 说明 |
|---------------------|--|
| fio | 用于测试 I/O 性能。（请注意，fio 依赖于 libaio-devel。） 要在 Amazon Linux 上安装 fio，请执行以下命令： <pre>[ec2-user ~]\$ sudo yum install -y fio</pre> |

| 工具 | 说明 |
|-------------------|--|
| | 要在 Ubuntu 上安装 fio，请执行以下命令： \$ sudo apt-get install -y fio |
| Oracle Orion 校准工具 | 用于校准要与 Oracle 数据库搭配使用的存储系统的 I/O 性能。 |

这些基准测试工具可支持各种测试参数。您应该使用命令来测试您的卷支持的工作负载。下面提供的命令示例可帮助您入门。

选择卷队列长度

基于工作负载和卷类型选择最佳卷队列长度。

SSD 卷的队列长度

要确定 SSD 卷上工作负载的最佳队列长度，建议您将每 500 IOPS (gp2 卷的基准量，io1 卷的预配置量) 对应 1 个队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。

在达到预配置 IOPS、吞吐量或最佳系统队列长度值之前，增加队列长度有好处，当前队列长度设置为 32。举例来说，预配置 1000 IOPS 的卷应该将队列长度设置为 2。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

HDD 卷的队列长度

要确定 HDD 卷上工作负载的最佳队列长度，建议您在执行 1MiB 顺序 I/O 时以至少为 4 的队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。例如，突发吞吐量为 500 MiB/s、IOPS 为 500 的 2 TiB st1 卷在执行 1024 KiB、512 KiB 或 256 KiB 的顺序 I/O 时，分别应该将队列长度 4、8 或 16 作为目标。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

执行基准测试

以下步骤介绍各种 EBS 卷类型的基准测试命令。

对挂载了 EBS 卷的 EBS 优化实例运行以下命令。如果已从快照还原 EBS 卷，在执行基准测试之前，请确保初始化这些卷。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 578\)](#)。

完成对卷的测试后，可参阅以下主题来帮助清除卷：[删除 Amazon EBS 卷 \(p. 542\)](#) 和 [终止您的实例 \(p. 267\)](#)。

对 io1 卷进行基准测试

对创建的条带集运行 fio。

以下命令可执行 16 KB 随机写入操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_volo \
--name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G \
--numjobs=16 --time_based --runtime=180 --group_reporting --norandommap
```

以下命令可执行 16 KB 随机读取操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_volo \
```

```
--name fio_test_file --direct=1 --rw=randread --bs=16k --size=1G \
--numjobs=16 --time_based --runtime=180 --group_reporting --norandommap
```

有关解析结果的更多信息，请参阅以下教程：[使用 fio 检查磁盘 IO 性能](#)。

对 st1 和 sc1 卷进行基准测试

在 st1 或 sc1 卷上运行 fio。

Note

在执行这些测试之前，请按[为 st1 和 sc1 上高吞吐量、读取操作量大的工作负载增大预读取值 \(p. 572\)](#)所述在实例上设置缓冲 I/O。

以下命令针对挂载的 st1 块储存设备（例如 /dev/xvdf）执行 1 MiB 的顺序读取操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read
--randrepeat=0 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180
--name=fio_direct_read_test
```

以下命令针对挂载的 st1 块储存设备执行 1 MiB 的顺序写入操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write
--randrepeat=0 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180
--name=fio_direct_write_test
```

有些工作负载可对块储存设备的不同部分混合执行顺序读取和顺序写入操作。要对此类工作负载进行基准测试，我们建议您为读取和写入操作单独、同时使用 fio 作业，并为每个作业使用 `fio offset_increment` 选项将块储存设备的不同位置作为目标。

运行此类工作负载比顺序写入或顺序读取工作负载要复杂一些。使用文本编辑器创建一个 fio 作业文件，在此示例中名为 `fio_rw_mix.cfg`，包含以下内容：

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180
offset_increment=100g

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
```

然后运行以下命令：

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

有关如何解释结果的更多信息，请参阅 [Inspecting disk I/O performance with fio 教程](#)。

对于 `st1` 和 `sc1` 卷而言，通过多个 fio 作业来执行直接 I/O (即使使用顺序读入或写入操作) 可能会导致吞吐量小于预期数值。建议您使用一个直接 I/O 作业并使用 `iodepth` 参数来控制并发 I/O 操作的数量。

Amazon EBS 的 Amazon CloudWatch Events

Amazon EBS 根据 Amazon CloudWatch Events 发送通知，以告知一系列快照和加密状态的更改。借助 CloudWatch Events，您可以创建规则，以触发编程操作，从而响应快照或加密密钥状态的更改。例如，创建快照后，您可以触发 AWS Lambda 函数，以与其他账户共享已完成的快照，或将其复制到其他区域以便用于灾难恢复用途。

有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的[使用事件](#)。

事件定义和示例

此部分定义了受支持的 Amazon EBS 事件，并提供了特定情景的事件输出示例。CloudWatch 中的事件表示为 JSON 对象。有关事件对象的格式和内容的更多信息，请参阅 Amazon CloudWatch Events 用户指南中的[事件和事件模式](#)。

EBS 事件的独有字段包含在以下所示的 JSON 对象“详细信息”部分。“事件”字段包含事件名称。“结果”字段包含触发事件的操作的已完成状态。

创建快照 (`createSnapshot`)

当创建快照的操作完成后，系统会将 `createSnapshot` 事件发送至您的 AWS 账户。此事件的结果可能是 `succeeded` 或 `failed`。

事件数据

下面的列表是 EBS 为成功的 `createSnapshot` 事件发送的 JSON 对象示例。`source` 字段包含源卷的 ARN。`StartTime` 和 `EndTime` 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "StartTime": "yyyy-mm-ddThh:mm:ssZ",
    "EndTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

复制快照 (copySnapshot)

当复制快照的操作完成时，系统会将 copySnapshot 事件发送至您的 AWS 账户。此事件的结果可能是 succeeded 或 failed。

事件数据

下面的列表是 EBS 在 copySnapshot 事件失败后发送的 JSON 对象的示例。失败原因是源快照 ID 无效。snapshot_id 的值为失败快照的 ARN。source 的值为源快照的 ARN。StartTime 和EndTime 表示 copy-snapshot 操作何时开始以及何时结束。

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Snapshot Notification",  
    "source": "aws.ec2",  
    "account": "123456789012",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-west-2:snapshot/snap-01234567"  
    ],  
    "detail": {  
        "event": "copySnapshot",  
        "result": "failed",  
        "cause": "Source snapshot ID is not valid",  
        "request-id": "",  
        "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",  
        "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",  
        "StartTime": "yyyy-mm-ddThh:mm:ssZ",  
        "EndTime": "yyyy-mm-ddThh:mm:ssZ"  
    }  
}
```

共享快照 (shareSnapshot)

在其他与您的 AWS 账户共享快照时，系统会将 shareSnapshot 事件发送至您的 AWS 账户。结果始终是 succeeded。

事件数据

下面的列表是 EBS 在 shareSnapshot 事件完成后发送的 JSON 对象的示例。source 值是与您共享快照的用户的 AWS 账号。StartTime 和EndTime 表示 share-snapshot 操作何时开始以及何时结束。仅在与其他用户共享私有快照时，系统才会发送 shareSnapshot 事件。共享公有快照不会触发该事件。

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Snapshot Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-west-2:snapshot/snap-01234567"  
    ],  
    "detail": {  
        "event": "shareSnapshot",  
        "result": "succeeded",  
        "cause": "",  
        "request-id": "",  
        "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",  
        "target": "arn:aws:iam::123456789012:root"  
    }  
}
```

```
        "source": "012345678901",
        "StartTime": "yyyy-mm-ddThh:mm:ssZ",
        "EndTime": ""yyyy-mm-ddThh:mm:ssZ""
    }
}
```

挂载或重新挂载卷时加密密钥无效 (`attachVolume`、`reattachVolume`)

因 KMS 密钥无效而导致 `attachVolume` 事件无法将卷挂载或重新挂载到实例时，系统就会将该事件发送到您的 AWS 账户。

Note

您可以使用 KMS 密钥加密 EBS 卷。如果用于加密卷的密钥无效，则日后将该密钥用于创建、挂载或重新挂载卷时，EBS 将会发送该事件。

事件数据

下面的列表是 EBS 在 `attachVolume` 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥处于待删除状态。

Note

在对服务器进行日常维护后，AWS 可能会尝试重新挂载卷。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
        "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
    ],
    "detail": {
        "event": "attachVolume",
        "result": "failed",
        "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
        "request-id": ""
    }
}
```

下面的列表是 EBS 在 `reattachVolume` 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥处于待删除状态。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
        "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
    ],
    "detail": {

```

```
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
is pending deletion.",
    "request-id": ""
}
}
```

创建卷时加密密钥无效 (createVolume)

因 KMS 密钥无效而导致 `createVolume` 事件无法创建卷时，系统就会将该事件发送到您的 AWS 账户。

Note

您可以使用 KMS 密钥加密 EBS 卷。如果用于加密卷的密钥无效，则日后将该密钥用于创建、挂载或重新挂载卷时，EBS 将会发送该事件。

事件数据

下面的列表是 EBS 在 `createVolume` 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥被禁用。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

以下是 EBS 在 `createVolume` 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥正等待导入。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

使用 Amazon Lambda 处理 CloudWatch Events

您可以使用 Amazon EBS 和 CloudWatch Events 自动执行数据备份工作流。这需要您创建 IAM 策略、用于处理事件的 AWS Lambda 函数，以及与传入事件匹配并能将传入事件路由到 Lambda 函数的 Amazon CloudWatch Events 规则。

以下步骤使用 `createSnapshot` 事件自动将已完成的快照复制到其他区域，以用于灾难恢复。

将已完成的快照复制到其他区域

1. 创建 IAM 策略 (例如以下示例中显示的策略)，以便提供执行 `CopySnapshot` 操作和对 CloudWatch Events 日志执行写入操作的权限。将策略分配给要处理 CloudWatch 事件的 IAM 用户。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "logs>CreateLogGroup",  
                "logs>CreateLogStream",  
                "logs:PutLogEvents"  
            ],  
            "Resource": "arn:aws:logs:*:*:  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CopySnapshot"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

2. 在 Lambda 中定义一个可在 CloudWatch 控制台中使用的函数。在 Amazon EBS 发送匹配的 `createSnapshot` 事件时 (表示快照已完成)，CloudWatch 会调用下例中的在 Node.js 中编写的 Lambda 函数。该函数被调用后，它会将快照从 `us-east-2` 复制到 `us-east-1`。

```
// Sample Lambda function to copy an EBS snapshot to a different region  
  
var AWS = require('aws-sdk');  
var ec2 = new AWS.EC2();  
  
// define variables  
var destinationRegion = 'us-east-1';  
var sourceRegion = 'us-east-2';  
console.log ('Loading function')  
  
//main function  
exports.handler = (event, context, callback) => {  
  
    // Get the EBS snapshot ID from the CloudWatch event details  
    var snapshotArn = event.detail.snapshot_id.split('/');  
    const snapshotId = snapshotArn[1];  
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;  
    console.log ("snapshotId:", snapshotId);  
  
    // Load EC2 class and update the configuration to use destination region to  
    // initiate the snapshot.  
    AWS.config.update({region: destinationRegion});  
    var ec2 = new AWS.EC2();
```

```
// Prepare variables for ec2.modifySnapshotAttribute call
const copySnapshotParams = {
  Description: description,
  DestinationRegion: destinationRegion,
  SourceRegion: sourceRegion,
  SourceSnapshotId: snapshotId
};

// Execute the copy snapshot and log any errors
ec2.copySnapshot(copySnapshotParams, (err, data) => {
  if (err) {
    const errorMessage = `Error copying snapshot ${snapshotId} to region
${destinationRegion}.`;
    console.log(errorMessage);
    console.log(err);
    callback(errorMessage);
  } else {
    const successMessage = `Successfully started copy of snapshot ${snapshotId}
to region ${destinationRegion}.`;
    console.log(successMessage);
    console.log(data);
    callback(null, successMessage);
  }
});
```

为确保您的 Lambda 函数在 CloudWatch 控制台中可用，请在将发生 CloudWatch 事件的区域创建该函数。有关更多信息，请参阅 [AWS Lambda 开发人员指南](#)。

3. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
4. 依次选择事件、创建规则、选择事件源以及 Amazon EBS 快照。
5. 对于特定事件，请选择 `createSnapshot`，对于特定结果，请选择 `succeeded`。
6. 有关规则目标，请查找并选择您之前创建的示例函数。
7. 选择目标、添加目标。
8. 有关 Lambda 功能，请选择您之前创建的 Lambda 功能并选择配置详细信息。
9. 在配置规则详细信息页面，请键入名称和描述的值。选择状态复选框激活功能（将其设置为已启用）。
10. 选择 `Create rule`。

现在，您的规则应该会显示在规则选项卡中。在所示的示例中，当您下次复制快照时，EBS 应该会发送您所配置的事件。

Amazon EC2 实例存储

实例存储 为您的实例提供临时性块级存储。此存储位于已物理连接到主机的磁盘上。实例存储是一种理想的临时存储解决方案，非常适合存储需要经常更新的信息，如缓存、缓冲、临时数据和其他临时内容，或者存储从一组实例上复制的数据，如 Web 服务器的负载均衡池。

实例存储由一个或多个显示为块储存设备的实例存储卷组成。实例存储的大小以及可用设备的数量因实例类型而异。尽管实例存储专用于特定实例，但是磁盘子系统是在主机上的实例间共享的。

实例存储卷的虚拟设备为 `ephemeral[0-23]`。支持一个实例存储卷的实例类型具有 `ephemeral0`。支持两个实例存储卷的实例类型有 `ephemeral0` 和 `ephemeral1` 等。

NVMe 实例存储卷的虚拟设备为 `/dev/nvme[0-7]n1`。支持一个 NVMe 实例存储卷的实例类型具有 `/dev/nvme0n1`。支持两个 NVMe 实例存储卷的实例类型具有 `/dev/nvme0n1` 和 `/dev/nvme1n1`，依此类推。

内容

- [实例存储生命周期 \(p. 592\)](#)
- [实例存储卷 \(p. 592\)](#)
- [将实例存储卷添加到您的 EC2 实例 \(p. 595\)](#)
- [SSD 实例存储卷 \(p. 597\)](#)
- [实例存储交换卷 \(p. 599\)](#)
- [优化实例存储卷的磁盘性能 \(p. 601\)](#)

实例存储生命周期

您只能在启动实例时指定实例的实例存储卷。您无法将实例存储卷与一个实例分离并将该卷挂载到另一个实例。

实例存储内的数据仅在与关联的实例的生命周期内保留。如果实例重启(无论是故意还是意外)，实例存储内的数据都会保留下。然而，在以下情况下，实例存储中的数据会丢失：

- 底层磁盘驱动器发生故障
- 实例停止
- 实例终止

因此，切勿依赖实例存储来存储珍贵且需要长期保存的数据。应使用更持久的数据存储，如 Amazon S3、Amazon EBS 或 Amazon EFS。

当您停止或终止一个实例时，将重置实例存储中的每个存储数据块。因此，无法通过另一实例的实例存储访问您的数据。

如果您从实例创建 AMI，则从此 AMI 中启动实例时，实例存储卷上的数据不能保存且不会出现在实例存储卷上。

实例存储卷

实例类型决定了可用的实例存储的大小以及用于实例存储卷的硬件类型。实例存储卷包含在实例小时成本中。您必须指定在启动实例时要使用的实例存储卷(NVMe 实例存储卷除外，因为它们在默认情况下可用)，再设置这些卷的格式并挂载这些卷，然后再进行使用。您无法在启动实例后使实例存储卷可用。有关更多信息，请参阅[将实例存储卷添加到您的 EC2 实例 \(p. 595\)](#)。

某些实例类型使用基于 NVMe 或 SATA 的固态硬盘(SSD)来提供非常高的随机 I/O 性能。如果您需要延迟非常低的存储，且实例终止时不需要保留数据或可以使用容错架构，则可以选择这种实例。有关更多信息，请参阅[SSD 实例存储卷 \(p. 597\)](#)。

下表列出了每种支持的实例类型可以使用的实例存储卷的数量、大小、类型和性能优化。有关实例类型的完整列表，包括仅 EBS 类型，请参阅[Amazon EC2 实例类型](#)。

| 实例类型 | 实例存储卷 | 类型 | 需要初始化 * | TRIM Support** |
|------------|----------------------|-----|---------|----------------|
| c1.medium | 1 x 350 GB† | HDD | ✓ | |
| c1.xlarge | 4 x 420 GB (1680 GB) | HDD | ✓ | |
| c3.large | 2 x 16 GB (32 GB) | SSD | ✓ | |
| c3.xlarge | 2 x 40 GB (80 GB) | SSD | ✓ | |
| c3.2xlarge | 2 x 80 GB (160 GB) | SSD | ✓ | |

| 实例类型 | 实例存储卷 | 类型 | 需要初始化 * | TRIM Support** |
|-------------|-----------------------|----------|---------|----------------|
| c3.4xlarge | 2 x 160 GB (320 GB) | SSD | ✓ | |
| c3.8xlarge | 2 x 320 GB (640 GB) | SSD | ✓ | |
| cc2.8xlarge | 4 x 840 GB (3360 GB) | HDD | ✓ | |
| cg1.4xlarge | 2 x 840 GB (1680 GB) | HDD | ✓ | |
| cr1.8xlarge | 2 x 120 GB (240 GB) | SSD | ✓ | |
| d2.xlarge | 3 x 2000 GB (6 TB) | HDD | | |
| d2.2xlarge | 6 x 2000 GB (12 TB) | HDD | | |
| d2.4xlarge | 12 x 2000 GB (24 TB) | HDD | | |
| d2.8xlarge | 24 x 2000 GB (48 TB) | HDD | | |
| g2.2xlarge | 1 x 60 GB | SSD | ✓ | |
| g2.8xlarge | 2 x 120 GB (240 GB) | SSD | ✓ | |
| hi1.4xlarge | 2 x 1024 GB (2048 GB) | SSD | | |
| hs1.8xlarge | 24 x 2000 GB (48 TB) | HDD | ✓ | |
| i2.xlarge | 1 x 800 GB | SSD | | ✓ |
| i2.2xlarge | 2 x 800 GB (1600 GB) | SSD | | ✓ |
| i2.4xlarge | 4 x 800 GB (3200 GB) | SSD | | ✓ |
| i2.8xlarge | 8 x 800 GB (6400 GB) | SSD | | ✓ |
| i3.large | 1 x 475 GB | NVMe SSD | | ✓ |
| i3.xlarge | 1 x 950 GB | NVMe SSD | | ✓ |
| i3.2xlarge | 1 x 1,900 GB | NVMe SSD | | ✓ |
| i3.4xlarge | 2 x 1,900 GB (3.8 TB) | NVMe SSD | | ✓ |

| 实例类型 | 实例存储卷 | 类型 | 需要初始化 * | TRIM Support** |
|-------------|------------------------|----------|---------|----------------|
| i3.8xlarge | 4 x 1,900 GB (7.6 TB) | NVMe SSD | | ✓ |
| i3.16xlarge | 8 x 1,900 GB (15.2 TB) | NVMe SSD | | ✓ |
| m1.small | 1 x 160 GB† | HDD | ✓ | |
| m1.medium | 1 x 410 GB | HDD | ✓ | |
| m1.large | 2 x 420 GB (840 GB) | HDD | ✓ | |
| m1.xlarge | 4 x 420 GB (1680 GB) | HDD | ✓ | |
| m2.xlarge | 1 x 420 GB | HDD | ✓ | |
| m2.2xlarge | 1 x 850 GB | HDD | ✓ | |
| m2.4xlarge | 2 x 840 GB (1680 GB) | HDD | ✓ | |
| m3.medium | 1 x 4 GB | SSD | ✓ | |
| m3.large | 1 x 32 GB | SSD | ✓ | |
| m3.xlarge | 2 x 40 GB (80 GB) | SSD | ✓ | |
| m3.2xlarge | 2 x 80 GB (160 GB) | SSD | ✓ | |
| r3.large | 1 x 32 GB | SSD | | ✓ |
| r3.xlarge | 1 x 80 GB | SSD | | ✓ |
| r3.2xlarge | 1 x 160 GB | SSD | | ✓ |
| r3.4xlarge | 1 x 320 GB | SSD | | ✓ |
| r3.8xlarge | 2 x 320 GB (640 GB) | SSD | | ✓ |
| x1.16xlarge | 1 x 1,920 GB | SSD | | |
| x1.32xlarge | 2 x 1920 GB (3840 GB) | SSD | | |

* 如果挂载到特定实例上的卷没有初始化，则会遭受初始写入惩罚。有关更多信息，请参见[优化实例存储卷的磁盘性能 \(p. 601\)](#)。

** 支持 TRIM 指令的基于 SSD 的实例存储卷不会预先经过任何文件系统的格式化处理。然而，您可以在启动实例后，使用您选择的文件系统将卷格式化。有关更多信息，请参阅[实例存储卷 TRIM 支持 \(p. 598\)](#)。

† c1.medium 和 m1.small 实例类型还包括一个不会在启动时自动启用的 900 MB 实例存储交换卷。有关更多信息，请参阅[实例存储交换卷 \(p. 599\)](#)。

将实例存储卷添加到您的 EC2 实例

使用块储存设备映射为您的实例指定 EBS 卷和实例存储卷。块储存设备映射中的每个条目均包括设备名称和映射到其上的卷。默认块储存设备映射由使用的 AMI 指定。或者，您可在启动实例时为实例指定块储存设备映射。请注意，实例类型所支持的所有 NVMe 实例存储卷将在实例启动时自动添加；您无需将这些卷添加到 AMI 或实例的块储存设备映射。有关更多信息，请参阅 [块储存设备映射 \(p. 609\)](#)。

块储存设备映射始终指定实例的根卷。根卷是一个 Amazon EBS 卷或实例存储卷。有关更多信息，请参阅 [根设备存储 \(p. 60\)](#)。将自动安装根卷。对于根卷的具有实例存储卷的实例，此卷的大小因 AMI 而异，但最大大小为 10 GB。

您可在启动实例时使用块储存设备映射来指定额外的 EBS 卷，或者可在实例运行后挂载额外的 EBS 卷。有关更多信息，请参阅 [Amazon EBS 卷 \(p. 517\)](#)。

您只能在启动实例时为您的实例指定实例存储卷。无法在启动实例后将实例存储卷挂载到该实例。

对您的实例可用的实例存储卷的数量和大小因实例类型而异。一些实例类型不支持实例存储卷。有关每种实例类型支持的实例存储卷的更多信息，请参阅 [实例存储卷 \(p. 592\)](#)。如果为您的实例选择的实例类型支持实例存储卷，则您必须在启动实例时将这些卷添加到实例的块储存设备映射。在启动实例后，您必须先确保已格式化和安装实例的实例存储卷，然后才能使用这些存储卷。请注意，将自动安装实例存储所支持的实例的根卷。

内容

- [将实例存储卷添加到 AMI \(p. 595\)](#)
- [将实例存储卷添加到实例 \(p. 596\)](#)
- [使实例存储卷在您的实例上可用 \(p. 596\)](#)

将实例存储卷添加到 AMI

您可创建带包括实例存储卷的块储存设备映射的 AMI。将实例存储卷添加到 AMI 后，您从该 AMI 启动的所有实例都会包含这些实例存储卷。请注意，在启动实例时，可忽略 AMI 块储存设备映射中指定的卷，并添加新卷。

Important

对于 M3 实例，请在实例而不是 AMI 的块储存设备映射中指定实例存储卷。Amazon EC2 可能会忽略仅在 AMI 的块储存设备映射中指定的实例存储卷。

使用控制台向 Amazon EBS 支持的 AMI 添加实例存储卷

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Image 和 Create Image。
4. 在 Create Image 对话框中，为您的映像添加一个有意义的名称和描述。
5. 对于要添加的每个实例存储卷，请选择 Add New Volume，从 Type 中选择实例存储卷，然后从 Device 中选择设备名称。（有关更多信息，请参阅 [Linux 实例上的设备命名 \(p. 608\)](#)。）可用的实例存储卷数量取决于实例类型。请注意，对于具有 NVMe 实例存储卷的实例，这些卷的设备映射取决于操作系统枚举这些卷的顺序。
6. 选择 Create Image。

使用命令行向 AMI 添加实例存储卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `create-image` 或 `register-image` (AWS CLI)

- [New-EC2Image](#) 和 [Register-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

将实例存储卷添加到实例

启动实例时，指定的 AMI 将提供默认块储存设备映射。如果需要额外的实例存储卷，您必须在启动实例时将这些卷添加到实例。请注意，您还可忽略 AMI 块储存设备映射中指定的设备。

Important

对于 M3 实例，即使您未在实例的块储存设备映射中指定实例存储卷，您也可能收到这些卷。

Important

对于 HS1 实例，无论您在 AMI 的块储存设备映射中指定了多少个实例存储卷，从 AMI 中启动的实例的块储存设备映射都会自动包括最大数目的支持的实例存储卷。您必须先从块储存设备映射中显式删除不需要的实例存储卷，然后再启动该映射。

使用控制台更新实例的块储存设备映射

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择 Launch Instance。
3. 在 Step 1: Choose an Amazon Machine Image (AMI) 中，选择要使用的 AMI，然后选择 Select。
4. 按照向导说明操作以完成 Step 1: Choose an Amazon Machine Image (AMI)、Step 2: Choose an Instance Type 和 Step 3: Configure Instance Details。
5. 在 Step 4: Add Storage 中，根据需要修改现有条目。对于要添加的每个实例存储卷，请单击 Add New Volume，从 Type 中选择实例存储卷，然后从 Device 中选择设备名称。可用的实例存储卷数量取决于实例类型。
6. 完成向导以启动实例。

使用命令行更新实例的块储存设备映射

您可将下列选项命令之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--block-device-mappings` 与 `run-instances` (AWS CLI)
- `-BlockDeviceMapping` 与 [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

使实例存储卷在您的实例上可用

启动实例后，该实例可使用实例存储卷，但是必须先安装该卷，然后再使用。对于 Linux 实例，实例类型决定应为您挂载哪种实例存储卷，以及哪些存储卷可由您自行挂载。对于 Windows 实例，EC2Config 服务可为实例挂载实例存储卷。该实例的块储存设备驱动程序会在安装卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的名称不同。

许多实例存储卷都预先经过 ext3 文件系统的格式化处理。支持 TRIM 指令的基于 SSD 的实例存储卷不会预先经过任何文件系统的格式化处理。然而，您可以在启动实例后，使用您选择的文件系统将卷格式化。有关更多信息，请参阅 [实例存储卷 TRIM 支持 \(p. 598\)](#)。对于 Windows 实例，EC2Config 服务可利用 NTFS 文件系统重新格式化实例存储卷。

您可以确认，可以从使用自身元数据的实例内使用实例存储设备。有关更多信息，请参阅 [查看实例存储卷的实例块储存设备映射 \(p. 616\)](#)。

对于 Windows 实例，您还可以使用 Windows 磁盘管理来查看实例存储卷。有关更多信息，请参阅 [使用 Windows 磁盘管理列出磁盘](#)。

对于 Linux 实例，您可按照以下过程所述操作来查看和挂载实例存储卷。

使实例存储卷在 Linux 上可用

1. 使用 SSH 客户端连接到实例。
2. 使用 `df -h` 命令查看已格式化并安装的卷。使用 `lsblk` 查看在启动时已映射但未格式化和安装的所有卷。
3. 要格式化并挂载仅映射的实例存储卷，请执行以下操作：
 - a. 使用 `mkfs` 命令在设备上创建文件系统。
 - b. 使用 `mkdir` 命令创建要将设备挂载到的目录。
 - c. 使用 `mount` 命令在新建目录上挂载设备。

SSD 实例存储卷

以下实例支持使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能的实例存储卷：

C3、G2、H1、I2、I3、M3、R3 和 X1。有关每种实例类型支持的实例存储卷的更多信息，请参阅[实例存储卷 \(p. 592\)](#)。

为确保 Linux 上的您的 SSD 实例存储卷实现最佳 IOPS 性能，我们建议您使用 [Amazon Linux AMI](#) 的最新版本，或者内核版本为 3.8 或更高版本的其他 Linux AMI。如果您使用的 Linux AMI 的内核版本不是 3.8 或更高版本，则您的实例将无法实现这些实例类型可获得的最大 IOPS 性能。

像其他实例存储卷一样，您必须在启动实例时映射实例的 SSD 实例存储卷，而且 SSD 实例卷上的数据仅可在其关联的实例的生命周期内保留。有关更多信息，请参阅[将实例存储卷添加到您的 EC2 实例 \(p. 595\)](#)。

NVMe SSD 卷

I3 实例提供非易失性存储规范 (NVMe) SSD 实例存储卷。要访问 NVMe 卷，您必须使用支持 NVMe 的操作系统。以下是最低操作系统要求：

- 最新的 Amazon Linux AMI
- Ubuntu 版本 16.10 或版本 16.04 LTS。请注意，版本 14.04 具有我们建议您不使用的早期版本的 NVMe。
- CentOS 版本 7
- SUSE Linux Enterprise Server 版本 12 或版本 11 (带 SP3)
- Windows Server 2016、Windows Server 2012 R2 或 Windows Server 2008 R2。请注意，不支持 Windows Server 2012 和 Windows Server 2008。

连接到实例后，您可以使用 `lspci` 命令列出 NVMe 设备。以下是支持 4 台 NVMe 设备的 `i3.8xlarge` 实例的示例输出。

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

如果您使用了受支持的操作系统但未看到 NVMe 设备，请使用以下 `lsmod` 命令验证是否已加载 NVMe 模块。

```
[ec2-user ~]$ lsmod | grep nvme
nvme           48813   0
```

NVMe 卷符合 NVMe 1.0a 规范。您可以对 NVMe 卷使用 NVMe 命令。利用 Amazon Linux AMI，您可以用 yum install 命令从存储库安装 nvme-cli 包。利用其他受支持的 Linux 版本，您可以下载 nvme-cli 包（如果包在映像中不可用）。

实例存储卷 TRIM 支持

以下实例支持带 TRIM 的 SSD 卷：I2、I3 和 R3。

利用支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关使用 TRIM 命令的更多信息，请参阅您的实例的操作系统文档。

支持 TRIM 的实例存储卷先经全面删减，然后再分配到您的实例。这些卷在实例启动时未经过文件系统的格式化处理，因此，您必须先进行格式化，而后才能装载和使用。为快速访问这些卷，在格式化卷时您应当指定特定于文件系统的选项以跳过 TRIM 操作。在 Linux 上，您还应当在支持 TRIM 的设备的装载命令或 /etc/fstab 文件条目中添加 discard 选项，以便设备有效使用此功能。在 Windows 上，使用以下命令：fsutil behavior set DisableDeleteNotify 1。

使支持 TRIM 的实例存储卷在 Linux 上可用

1. 在启动实例时映射实例存储卷。有关更多信息，请参阅 [将实例存储卷添加到您的 EC2 实例 \(p. 595\)](#)。
2. 在实例中，使用 lsblk 命令列出可用设备或 [使用实例元数据查看实例存储卷 \(p. 616\)](#)。
3. 使用以下命令验证您的操作系统和设备是否支持 TRIM (将 xvdb 替换为您设备的名称)：

```
[ec2-user ~]$ sudo cat /sys/block/xvdb/queue/discard_max_bytes
322122547200
```

如果此命令返回 0 之外的值，则表示您的操作系统和设备支持 TRIM。

4. 使用您选择的文件系统格式化卷。
 - (EXT4) 要使用 ext4 文件系统格式化卷，请使用以下命令 (将 xvdc 替换为您设备的名称)：

```
[ec2-user ~]$ sudo mkfs.ext4 -E nodiscard /dev/xvdc
```

- (XFS) 要使用 xfs 文件系统格式化卷，请使用以下命令 (将 xvdb 替换为您设备的名称)：

```
[ec2-user ~]$ sudo mkfs.xfs -K /dev/xvdb
```

Note

您可能需要在您的操作系统上安装 XFS 文件系统支持，然后此命令才起效。对于 Amazon Linux，可使用 sudo yum install -y xfsprogs 命令。

5. 使用 discard 选项装载设备。请务必指定卷的设备名称。您可选择现有目录，也可使用 mkdir 命令创建新目录。

```
[ec2-user ~]$ sudo mount -o discard /dev/xvdb /mnt/my-data
```

6. (可选) 如果您希望设备在启动时装载，可以在 /etc/fstab 文件中添加或修改包含 discard 选项的条目。

```
/dev/xvdb    /mnt/xvdb    xfs    defaults,nofail,discard    0    2
/dev/xvdc    /mnt/xvdc    ext4   defaults,nofail,discard    0    2
```

Important

在编辑 `/etc/fstab` 文件之后，确认运行 `sudo mount -a` 命令时未出错。如果此文件中存在任何错误，系统可能无法正常启动或根本不启动。

HI1 SSD 存储

在 HI1 实例上采用 SSD 存储：

- 原始数据源是采用 SSD 存储的实例存储。
- 读取性能始终如一，写入性能可能会有所波动。
- 可能会发生写入放大问题。
- 目前不支持 TRIM 命令。

采用 SSD 存储的实例存储

`hi1.4xlarge` 实例使用由 Amazon EBS 支持的根设备。但是，它们的原始数据存储由实例存储中的 SSD 卷提供。像其他实例存储卷一样，这些实例存储卷只在实例生命周期内存在。由于 `hi1.4xlarge` 实例的根设备由 Amazon EBS 支持，因此您仍然可以启动和停止实例。当您停止实例时，应用程序仍会存留，但是实例存储中的生产数据则不会保留。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#)。

可变动的写入性能

写入性能受应用程序利用逻辑块寻址 (LBA) 空间的方式的影响。如果您的应用程序使用总 LBA 空间，则写入性能可能会下降约 90%。测试您的应用程序并监控队列长度 (卷的待处理 I/O 请求数量) 和 I/O 大小。

写入放大

写入放大是指与闪存和 SSD 相关的不良情况，在这种情况下，实际写入的物理信息量是计划写入的符合逻辑的信息量的几倍。因为对闪存执行重新写入操作前，必须先执行擦除操作，而执行这些操作的过程会导致用户数据和元数据遭到多次移动 (或覆盖)。放大影响会在 SSD 的使用期限内增加必须写入次数，而这会缩短稳定运行的时间。`hi1.4xlarge` 实例的设计自带调配模式，以用于最大程度上减少写入放大问题的影响。

比起顺序写入操作，随机写入在写入放大方面的影响更为严重。如果您担心写入放大问题，可为您的应用程序分配少于 1 TiB 的存储 (也称为预留空间)。

TRIM 命令

TRIM 命令支持操作系统通知 SSD，之前保存的数据块被认为已废止。TRIM 限制写入放大的影响。

HI1 实例不提供 TRIM 支持。有关支持 TRIM 的实例的信息，请参阅 [实例存储卷 TRIM 支持 \(p. 598\)](#)。

实例存储交换卷

当系统所需内存超过实际分配内存时，可以在 Linux 中使用交换空间。在启用交换空间时，Linux 系统可以频繁地将正在使用的内存页面从物理内存交换至交换空间 (无论是现有文件系统的专用分区还是交换文件)，而且可以为需要快速访问速度的内存页面释放空间。

Note

使用交换空间进行内存分页并不像使用 RAM 那样快速高效。如果您的工作负载定期将内存分页为交换空间，您应考虑迁移到具有更多 RAM 的较大实例类型。有关更多信息，请参阅 [调整您的实例大小 \(p. 156\)](#)。

c1.medium 和 m1.small 实例类型的可用物理内存数量有限，且启动时作为 Linux AMI 虚拟内存的是 900 MiB 交换卷。尽管 Linux 内核将此交换空间看作根设备的一部分，但是它实际上是一个独立的实例存储卷，与根设备的类型无关。

Amazon Linux AMI 可以自动启用和使用此交换空间，但是您的 AMI 可能需要一些额外的步骤来识别和使用此交换空间。要查看您的实例是否正在使用交换空间，可以使用 swapon -s 命令。

```
[ec2-user ~]$ swapon -s
Filename                                Type      Size   Used   Priority
/dev/xvda3                               partition 917500  0       -1
```

上述实例拥有一个已挂载并启用的 900 MiB 交换卷。如果您没有通过此命令看到列出的交换卷，则可能需要启用该设备的交换空间。使用 lsblk 命令检查您的可用磁盘。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M 0 disk
```

在这里，交换卷 xvda3 对该实例可用，但是尚未启用（请注意 MOUNTPOINT 字段为空）。您可以使用 swapon 命令启用交换卷。

Note

您需要在 lsblk 列出的设备名称前加上 /dev/。设备的命名可能不同，例如 sda3、sde3 或 xvde3。在以下命令中使用系统的设备名称。

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

现在交换空间应该显示在 lsblk 和 swapon -s 输出中。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M 0 disk [SWAP]
[ec2-user@ip-12-34-56-78 ~]$ swapon -s
Filename                                Type      Size   Used   Priority
/dev/xvda3                               partition 917500  0       -1
```

您还需要编辑您的 /etc/fstab 文件，以在每次启动系统时自动启用此交换空间。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

将以下行附加到您的 /etc/fstab 文件中（使用系统的交换设备名称）：

```
/dev/xvda3      none     swap     sw   0     0
```

使用实例存储卷作为交换空间

所有实例存储卷都可用作交换空间。例如，m3.medium 实例类型包含一个适用于交换空间的 4 GB SSD 实例存储卷。如果您的实例存储卷大很多（例如 350GB），则可以考虑将卷分区为一个较小的 4-8GB 交换分区，其余部分用作数据卷。

Note

此过程仅适用于支持实例存储的实例类型。有关受支持实例类型的列表，请参阅[实例存储卷 \(p. 592\)](#)。

1. 列出连接到您的实例的块储存设备以获取实例存储卷的设备名称。

```
[ec2-user ~]$ lsblk -p
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0    4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0    8G  0 disk /
```

在此示例中，实例存储卷为 /dev/xvdb。因为这是 Amazon Linux 实例，所以实例存储卷在 /media/ephemeral0 格式化并安装；并不是所有 Linux 操作系统都自动执行这一操作。

2. (可选) 如果您安装了实例存储卷 (它将在 MOUNTPOINTlsblk 命令输出中列出)，您需要使用以下命令卸载它。

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. 使用 mkswap 命令在设备上设置一个 Linux 交换区域。

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swap space version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. 启用新的交换空间。

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. 验证所使用的新交换空间。

```
[ec2-user ~]$ swapon -s
Filename      Type  Size Used Priority
/dev/xvdb            partition 4188668 0 -1
```

6. 编辑您的 /etc/fstab 文件，以在每次系统启动时自动启用此交换空间。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

如果您的 /etc/fstab 文件拥有 /dev/xvdb (或 /dev/sdb) 条目，请将其更改为与下面的行匹配；如果没有针对此设备的条目，请将以下行附加到您的 /etc/fstab 文件 (使用您系统的交换设备名称)：

```
/dev/xvdb      none      swap      sw  0      0
```

Important

当实例停止后，实例存储卷数据将丢失；这包括在 Step 3 (p. 601) 中创建的实例存储交换空间格式设置。如果您停止并重新启动已配置为使用实例存储交换空间的实例，则必须在新的实例存储卷上重复 Step 1 (p. 601) 到 Step 5 (p. 601)。

优化实例存储卷的磁盘性能

由于 Amazon EC2 采用特殊方式将磁盘虚拟化，所以第一次在大多数实例存储卷上执行写入操作的速度会比之后的写入操作慢。对于大部分应用程序，可将此成本分摊到实例的整个使用期限。然而，如果您需要较高的磁盘性能，我们建议您在生产使用之前对每个磁盘位置执行一次性写入操作，以此来实现硬盘初始化。

Note

某些实例类型使用直接连接的固态硬盘 (SSD) 并支持 TRIM，可以在启动时提供最大性能，且无需初始化。有关每种实例类型的实例存储的信息，请参阅 [实例存储卷 \(p. 592\)](#)。

如果您需要在延迟或吞吐量方面具有更大灵活性，我们建议您使用 Amazon EBS。

要初始化实例存储卷，请使用以下 dd 命令，具体取决于您要对哪个存储（例如，/dev/sdb 或 /dev/name[0-7]n1）进行初始化。

Note

请确保先卸载硬盘，然后再执行此命令。

初始化可能需要很长一段时间（对于超大型实例，约为 8 小时）。

要将实例存储卷初始化，可使用 m1.large、m1.xlarge、c1.xlarge、m2.xlarge、m2.2xlarge 和 m2.4xlarge 实例类型上的以下命令：

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

要同时对所有实例存储卷执行初始化，可使用以下命令：

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

配置硬盘以便通过对每个硬盘位置执行写入操作将它们初始化。当配置基于软件的 RAID 时，请务必更改最低重建速度：

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Amazon Elastic File System (Amazon EFS)

Amazon EFS 提供可扩展文件存储以供和 Amazon EC2 一起使用。您可以创建 EFS 文件系统并配置实例来安装文件系统。您可以使用 EFS 文件系统作为在多个实例上运行的工作负载和应用程序的通用数据源。有关更多信息，请参阅 [Amazon Elastic File System 产品页](#)。

在本教程中，您创建一个 EFS 文件系统和两个可以使用该文件系统共享数据的 Linux 实例。

Important

Amazon EFS 在 Windows 实例上不受支持。

任务

- [先决条件 \(p. 602\)](#)
- [步骤 1：创建 EFS 文件系统 \(p. 603\)](#)
- [步骤 2：挂载文件系统 \(p. 603\)](#)
- [步骤 3：测试文件系统 \(p. 604\)](#)
- [步骤 4：清除 \(p. 605\)](#)

先决条件

- 创建安全组（例如，efs-sg）并添加以下规则：
 - 允许来自您的计算机的入站 SSH 连接（源是您的网络的 CIDR 块）
 - 允许来自与组关联的 EC2 实例的入站 NFS 连接（源是安全组自身）
- 创建密钥对。您必须在配置您的实例时指定密钥对，否则无法连接到它们。有关更多信息，请参阅 [创建密钥对 \(p. 17\)](#)。

步骤 1：创建 EFS 文件系统

Amazon EFS 能让您创建一个可供多个实例同时安装并访问的文件系统。有关更多信息，请参阅 Amazon Elastic File System 用户指南 中的[为 Amazon EFS 创建资源](#)。

创建文件系统

1. 通过 <https://console.aws.amazon.com/efs/> 打开 Amazon Elastic File System 控制台。
2. 选择 Create file system。
3. 在 Configure file system access 页面上，执行以下操作：
 - a. 对于 VPC，选择用于您的实例的 VPC。
 - b. 对于 Create mount targets，选择所有可用区。
 - c. 对于每可用区，确保 Security group 的值是您在[先决条件 \(p. 602\)](#)中创建的安全组。
 - d. 选择 Next Step。
4. 在 Configure optional settings 页面上，执行以下操作：
 - a. 对于具有 Key=Name 的标签，在 Value 中键入文件系统的名称。
 - b. 对于 Choose performance mode，保留默认选项 General Purpose。
 - c. 选择 Next Step。
5. 在 Review and create 页面上，选择 Create File System。
6. 在创建文件系统后，请记下文件系统 ID，因为您将在本教程中稍后部分使用它。

步骤 2：挂载文件系统

使用以下步骤启动两个 t2.micro 实例。用户数据脚本在启动时将文件系统挂载到实例并且在实例重启之后更新 /etc/fstab 以确保重新挂载文件系统。请注意，必须在子网中启动 T2 实例。您可以使用默认的 VPC 或非默认的 VPC。

Note

还有其他挂载卷的方式（例如，在已运行的实例上）。有关更多信息，请参阅 Amazon Elastic File System 用户指南 中的[挂载文件系统](#)。

启动两个实例并挂载 EFS 文件系统

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在 Choose an Amazon Machine Image 页面上，选择一个具有 HVM 虚拟化类型的 Amazon Linux AMI。
4. 在 Choose an Instance Type 页面上，保留默认的实例类型 t2.micro，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中，执行以下操作：
 - a. 对于 Number of instances，键入 2。
 - b. [默认 VPC] 如果您有默认 VPC，则它是 Network 的默认值。保留默认 VPC 和 Subnet 的默认值以便在 Amazon EC2 为您的实例选择的可用区中使用默认子网。

[非默认 VPC] 为 Network 选择您的 VPC，并从 Subnet 中选择一个公有子网。

- c. [非默认 VPC] 对于 Auto-assign Public IP，选择 Enable。否则，您的实例将不会得到公有 IP 地址或公有 DNS 名称。

- d. 在 Advanced Details 下方，将以下脚本粘贴到 User data 中。用您的文件系统 ID 更新 EFS_ID，用您的文件系统的区域代码更新 EFS_REGION。您可以选择用您挂载的文件系统的一个目录更新 EFS_MOUNT_DIR。

```
#!/bin/bash
yum update -y
yum install -y nfs-utils
EFS_ID=fs-xxxxxxxxx
EFS_REGION=region-code
EFS_MOUNT_DIR=/mnt/efs
mkdir -p ${EFS_MOUNT_DIR}
chown ec2-user:ec2-user ${EFS_MOUNT_DIR}
echo $(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone).${EFS_ID}.efs.${EFS_REGION}.amazonaws.com:/ ${EFS_MOUNT_DIR} nfs4
    nfsvers=4.1,rsize=1048576,wszie=1048576,hard,timeo=600,retrans=2 >> /etc/fstab
mount -a
```

- e. 转到向导的步骤 6。
6. 在 Configure Security Group 页面上，选择 Select an existing security group，选择您的安全组，然后选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 在 Select an existing key pair or create a new key pair 对话框中，选择 Choose an existing key pair，然后选择您的密钥对。选择确认复选框，然后选择 Launch Instances。
9. 在导航窗格中，选择 Instances 以查看您的实例的状态。最初，其状态是 pending。在状态变为 running 后，您的实例即准备就绪，可以使用。

步骤 3：测试文件系统

您可以连接到您的实例并验证文件系统是否已挂载到您指定的目录（例如，/mnt/efs）。

验证文件系统是否已挂载

1. 连接到您的实例。有关更多信息，请参阅 [连接到您的 Linux 实例 \(p. 252\)](#)。
2. 从每个实例的终端窗口，运行 df -T 命令以验证 EFS 文件系统是否已挂载。

```
$ df -T
Filesystem      Type            1K-blocks      Used   Available Use% Mounted on
/dev/xvda1      ext4           8123812  1949800       6073764  25% /
devtmpfs        devtmpfs        4078468       56       4078412   1% /dev
tmpfs          tmpfs           4089312       0       4089312   0% /dev/shm
efs-dns         nfs4          9007199254740992       0     9007199254740992   0% /mnt/efs
```

请注意，文件系统的名称（在示例输出中显示为 **efs-dns**）具有以下格式：

```
availability-zone.filesystem-id.efs.region.amazonaws.com:/
```

3. (可选) 从一个实例在文件系统中创建一个文件，然后验证您是否可以从另一实例查看该文件。
 - a. 从第一个实例，运行以下命令来创建文件：

```
$ sudo touch /mnt/efs/test-file.txt
```

- b. 从第二个实例，运行以下命令来查看文件：

```
$ ls /mnt/efs
```

test-file.txt

步骤 4：清除

当您完成本教程后，您可以终止这些实例并删除文件系统。

终止实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择要终止的实例。
4. 依次选择 Actions、Instance State 和 Terminate。
5. 当系统提示您确认时，选择 Yes, Terminate。

删除文件系统

1. 通过 <https://console.aws.amazon.com/efs/> 打开 Amazon Elastic File System 控制台。
2. 选择要删除的文件系统。
3. 选择 Actions、Delete file system。
4. 在提示确认时，键入文件系统的 ID 并选择 Delete File System。

Amazon Simple Storage Service (Amazon S3)

Amazon S3 是 Internet 数据的存储库。Amazon S3 提供了可靠、快速和廉价的数据存储基础设施。它的目的是通过支持您随时从 Amazon EC2 内部或从网络上的任何地方存储和检索任何数量的数据来简化整个网络计算。Amazon S3 以冗余方式跨多个设施在多个设备上存储数据元，允许多个不同的客户端或应用程序线程同时对这些数据元进行读或写操作。您可以使用存储在 Amazon S3 中的冗余数据快速、可靠地恢复实例或应用程序故障。

Amazon EC2 使用 Amazon S3 来存储 Amazon Machine Images (AMIs)。您可以使用 AMI 启动 EC2 实例。万一实例发生故障，您可以使用已存储的 AMI 立即启动其他实例，从而实现快速故障恢复和确保业务的连续性。

Amazon EC2 还使用 Amazon S3 来存储数据卷的快照 (备份副本)。在应用程序或系统发生故障的情况下，您可以使用快照来快速、可靠地恢复数据。您也可以将快照用作基线来创建多个数据卷，扩展现有数据卷的大小，或者跨多个可用区域移动数据，因此使您的数据使用具有高度的可扩展性。有关使用数据卷和快照的更多信息，请参阅 [Amazon Elastic Block Store \(p. 516\)](#)。

数据元是 Amazon S3 中存储的基本实体。Amazon S3 中存储的每个数据元都包含在存储段中。存储段在最高级别上组织管理 Amazon S3 命名空间，并指定负责该存储的账户。Amazon S3 存储段类似于 Internet 域名。存储在存储段中的数据元具有唯一的密钥值，可以使用 HTTP URL 地址进行检索。例如，如果密钥值为 /photos/mygarden.jpg 的对象存储在 myawsbucket 存储桶中，则可以使用 <http://myawsbucket.s3.amazonaws.com/photos/mygarden.jpg>。

有关 Amazon S3 功能的更多信息，请参阅 [Amazon S3 产品页](#)。

Amazon S3 和 Amazon EC2

凭借 Amazon S3 的存储优势，您可以选择使用此服务存储文件和数据集以用于 EC2 实例。有几种方法可在 Amazon S3 和您的实例间移动数据。除下面所讨论的示例外，您还可以使用其他人编写的各种工具从您的计算机或实例访问您在 Amazon S3 中的数据。AWS 论坛中对其中一些常见工具进行了讨论。

如果您有权限，就可以使用以下某种方法在 Amazon S3 和您的实例之间复制文件。

GET 或 wget

wget 实用工具是 HTTP 和 FTP 客户端，可用于从 Amazon S3 下载公有对象。该实用工具在 Amazon Linux 和大多数其他分发版中均为默认安装，可在 Windows 上下载安装。要下载 Amazon S3 对象，请使用以下命令（替换要下载的对象的 URL）。

```
wget https://s3.amazonaws.com/my_bucket/my_folder/my_file.ext
```

此方法要求您请求的数据元是公用数据元；如果数据元不是公用的，您会收到一条 `ERROR 403: Forbidden` 消息。如果您收到此错误，请打开 Amazon S3 控制台并将该对象的权限更改为公用。有关更多信息，请参阅 [Amazon Simple Storage Service 开发人员指南](#)。

AWS 命令行界面

AWS 命令行界面 (AWS CLI) 是用于管理 AWS 服务的统一工具。只通过一个工具进行下载和配置，您就可以使用命令行控制多个 AWS 服务并利用脚本来自动执行这些服务。AWS CLI 允许用户对自己进行身份验证，从 Amazon S3 下载受限制的项目和上传项目。有关更多信息，例如如何安装和配置这些工具，请参阅 [AWS 命令行界面详细信息页](#)。

`aws s3 cp` 命令类似于 Unix `cp` 命令（语法是：`aws s3 cp source destination`）。您可以将文件从 Amazon S3 复制到您的实例，从您的实例复制到 Amazon S3，甚至可以将文件从一个 Amazon S3 位置复制到另一个位置。

使用以下命令可将一个对象从 Amazon S3 复制到您的实例。

```
$ aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

使用以下命令可将一个对象从您的实例重新复制到 Amazon S3。

```
$ aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

使用以下命令可将一个对象从一个 Amazon S3 位置复制到另一个位置。

```
$ aws s3 cp s3://my_bucket/my_folder/my_file.ext s3://my_bucket/my_folder/my_file2.ext
```

`aws s3 sync` 命令可以将整个 Amazon S3 存储桶同步到本地目录位置。这可以用于下载数据集并使本地副本随远程集保持更新。命令语法是：`aws s3 sync source destination`。如果您对 Amazon S3 存储桶拥有合适权限，则当您最后在命令中将源与目标位置反转时，可以将本地目录备份推送到云。

使用以下命令可将整个 Amazon S3 存储桶下载到实例上的本地目录。

```
$ aws s3 sync s3://remote_S3_bucket local_directory
```

适用于 Windows PowerShell 的 AWS 工具

Windows 实例有图形浏览器优势，您可以用图形浏览器直接访问 Amazon S3 控制台；不过，出于脚本编写目的，Windows 用户也可以使用 [适用于 Windows PowerShell 的 AWS 工具](#) 在实例与 Amazon S3 之间移动对象。

使用以下命令可将一个 Amazon S3 对象复制到您的 Windows 实例。

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key my_folder/my_file.ext -  
LocalFile my_copied_file.ext
```

Amazon S3 API

如果您是一名开发人员，则可以使用 API 访问 Amazon S3 中的数据。有关更多信息，请参阅 [Amazon Simple Storage Service 开发人员指南](#)。您可以使用此 API 及其示例帮助开发应用程序并将其与其他 API 和 SDK（例如 boto Python 接口）集成。

实例卷限制

您的实例可以连接的卷的最大数量取决于操作系统。考虑应将多少个卷添加到实例时，应考虑是否需要增加 I/O 带宽或存储容量。

内容

- [特定于 Linux 的卷限制 \(p. 607\)](#)
- [特定于 Windows 的卷限制 \(p. 607\)](#)
- [带宽与容量 \(p. 608\)](#)

特定于 Linux 的卷限制

连接的卷数超出 40 会导致启动失败。请注意，此数字包括根卷以及所有连接的实例存储卷和 EBS 卷。如果连接了大量卷的实例出现启动问题，请停止该实例，断开所有在启动过程中不必要的卷，然后在实例运行之后重新连接这些卷。

Important

如果将 40 个以上的卷连接到 Linux 实例，系统只会尽力支持，不对此进行保证。

特定于 Windows 的卷限制

下表基于所使用的驱动程序显示 Windows 实例的卷限制。请注意，这些数字包括根卷以及所有连接的实例存储卷和 EBS 卷。

Important

如果连接到 Windows 实例的卷的数量超过下面的数字，系统只会尽力支持，不对此提供保证。

| 驱动程序 | 卷限制 |
|-----------------|-----|
| AWS 半虚拟化驱动程序 | 26 |
| Citrix 半虚拟化驱动程序 | 26 |
| Red Hat 半虚拟化 | 17 |

建议 Windows 实例连接的使用 AWS 半虚拟化或 Citrix 半虚拟化驱动程序的卷不要超过 26 个，否则可能导致性能问题。

要确定您的实例所使用的半虚拟化驱动程序，或是要将 Windows 实例从 Red Hat 升级到 Citrix 半虚拟化驱动程序，请参阅[在 Windows 实例上升级半虚拟化驱动程序](#)。

有关设备名称与卷如何相关的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[将磁盘映射到 Windows EC2 实例上的卷](#)。

带宽与容量

为获得一致且可预测的带宽使用案例，请使用 EBS 优化或 10 GiB 网络连接实例并预配置通用型 SSD 或预配置 IOPS SSD 卷。按照 [Amazon EC2 实例配置 \(p. 573\)](#) 中的指导，使您为卷预配置的 IOPS 与实例提供的带宽匹配，以获得最大性能。对于 RAID 配置，许多管理员发现大于 8 个卷的阵列由于 I/O 开销提高而降低了性能回报。测试您的各个应用程序性能并根据需要优化。

Linux 实例上的设备命名

当您将卷连接到实例时，需要为卷提供设备名称。该设备名称由 Amazon EC2 使用。实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 使用的名称不同。

内容

- 可用设备名称 (p. 608)
- 设备名称注意事项 (p. 609)

有关 Windows 实例上的设备名称的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [Windows 实例上的设备命名](#)。

可用设备名称

下表列出了 Linux 实例的可用设备名称。您可以连接到实例的卷的数量取决于操作系统。有关更多信息，请参阅 [实例卷限制 \(p. 607\)](#)。

| 虚拟化类型 | 可用 | 根预留 | 建议用于 EBS 卷 | 用于实例存储卷 | 用于 NVMe 实例存储卷 |
|-------|------------------------|--------------------------|-----------------------------------|--|--------------------|
| 半虚拟化 | /dev/sd[a-z] | /dev/sda1 | /dev/sd[f-p] /dev/sd[f-p][1-6] | /dev/sd[b-e] /dev/sd[b-y] (hs1.8xlarge) | 不可用 |
| | /dev/sd[a-z] [1-15] | | | | |
| | /dev/hd[a-z] | | | | |
| | /dev/hd[a-z] [1-15] | | | | |
| 全虚拟化 | /dev/sd[a-z] | 不同的 AMI | /dev/sd[f-p] | /dev/sd[b-e] /dev/sd[b-y] (d2.8xlarge) | /dev/nvme[0-7]n1 * |
| | /dev/xvd[b-c] [a-z] | /dev/sda1 或 /dev/xvda | | /dev/sd[b-y] (hs1.8xlarge) /dev/sd[b-i] (i2.8xlarge) | |
| | | | | | |
| | | | | | |

* 将自动枚举 NVMe 卷并为其分配设备名称。无需在块储存设备映射中指定 NVMe 卷。

请注意，您可以使用以下 AWS CLI 命令确定您的特定 AMI 的根设备名称：

```
aws ec2 describe-images --image-ids image_id --query 'Images[].RootDeviceName'
```

有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 591\)](#)。有关根设备存储的信息，请参阅 [Amazon EC2 根设备卷 \(p. 11\)](#)。

设备名称注意事项

在选择设备名称时请记住以下原则：

- 尽管您可以使用用于连接实例存储卷的设备名连接 EBS 卷，我们还是强烈建议您不要这样做，因为这种操作具有不可预测性。
- 根据内核的块储存设备驱动程序，附加的设备所采用的名称可能与您指定的名称不同。例如，如果您指定设备名称 /dev/sdh，内核可能将该设备重命名为 /dev/xvdh 或 /dev/hdh；在大多数情况下，尾部字母保持不变。在某些版本的 Red Hat Enterprise Linux（及其变体，例如，CentOS）中，尾部字母也可能发生变化（例如 /dev/sda 可能变为 /dev/xvde）。在这些情况下，设备名称各尾部字母都会递增相同次数。例如，/dev/sdb 将变为 /dev/xvdf，/dev/sdc 将变为 /dev/xvdg。Amazon Linux AMI 会使用您在启动时指定的名称创建指向重命名设备路径的符号链接，但是其他 AMI 的工作方式可能不同。
- 实例的 NVMe 实例存储卷数取决于该实例的大小。设备名称为 /dev/nvme0n1、/dev/nvme1n1，依此类推。
- 对 Linux 实例提供两种类型的虚拟化：半虚拟化 (PV) 和硬件虚拟机 (HVM)。实例的虚拟化类型由用于启动实例的 AMI 确定。一些实例类型支持 PV 和 HVM，一些实例类型仅支持 HVM，其他一些仅支持 PV。请务必注意您的 AMI 的虚拟化类型，因为推荐的和您可以使用的可用设备名称取决于您的实例的虚拟化类型。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 62\)](#)。
- 您不能连接共享相同设备字母的卷，无论是否带有尾部数字都是如此。例如，如果您将一个卷连接为 /dev/sdc，将另一个卷连接为 /dev/sdc1，则只有 /dev/sdc 对实例可见。要在设备名称中使用尾部数字，您必须对所有基础字母相同的设备名称使用尾部数字（如 /dev/sdc1、/dev/sdc2、/dev/sdc3）。
- 硬件虚拟机 (HVM) AMI 不支持在设备名称中使用尾部数字。
- 一些自定义内核可能会限制使用 /dev/sd[f-p] 或 /dev/sd[f-p][1-6]。如果您使用 /dev/sd[q-z] 或 /dev/sd[q-z][1-6] 时遇到问题，可以尝试 /dev/sd[f-p] 或 /dev/sd[f-p][1-6]。

块储存设备映射

您启动的每个实例都有一个关联根设备卷，它是 Amazon EBS 卷或实例存储卷。您可以使用块储存设备映射来指定实例启动时要连接的其他 EBS 卷或实例存储卷。您还可以将其他 EBS 卷连接到运行中的实例，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。然而，将实例存储卷连接到实例的唯一办法是，在实例启动时，使用块储存设备映射来进行连接。

有关根设备卷的更多信息，请参阅 [将根设备卷更改为持久保留 \(p. 13\)](#)。

内容

- [块储存设备映射的概念 \(p. 609\)](#)
- [AMI 块储存设备映射 \(p. 611\)](#)
- [实例块储存设备映射 \(p. 613\)](#)

块储存设备映射的概念

块储存设备是一种以字节或位（块）为单位移动数据的储存设备。这些设备支持随机访问和广泛使用缓存 I/O。例如，包括硬盘、CD-ROM 盘和闪存盘。块储存设备可以实际连接到计算机，或者就像实际连接到计算机一样对进行远程访问。Amazon EC2 支持两种类型的块储存设备：

- 实例存储卷 (虚拟设备，其底层硬件实际连接到该实例的主机)
- EBS 卷 (远程存储设备)

块储存设备映射 定义了挂载到某个实例的块储存设备 (实例存储卷和 EBS 卷)。您可以指定块储存设备映射作为创建 AMI 的一部分，以便使从该 AMI 启动的所有实例均可使用该映射。或者，您还可以在启动实例时指定块储存设备映射，这样该映射会覆盖您在启动实例的 AMI 中指定的块储存设备映射。请注意，实例类型所支持的所有 NVMe 实例存储卷将在实例启动时自动添加；您无需将这些卷添加到 AMI 或实例的块储存设备映射。

内容

- [块储存设备映射条目 \(p. 610\)](#)
- [块储存设备映射实例存储注意事项 \(p. 610\)](#)
- [块储存设备映射示例 \(p. 611\)](#)
- [如何使设备在操作系统可用 \(p. 611\)](#)

块储存设备映射条目

当您创建块储存设备映射时，可以为需要挂载到该实例的每个块储存设备指定以下信息：

- 在 Amazon EC2 内使用的设备名称。该实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的不同。有关更多信息，请参阅 [Linux 实例上的设备命名 \(p. 608\)](#)。
- [实例存储卷] 虚拟设备：`ephemeral[0-23]`。请注意，对您的实例可用的实例存储卷的数量和大小因实例类型而异。
- [NVMe 实例存储卷] 这些卷将自动映射为 `/dev/nvme[0-7]n1`。您无需指定块储存设备映射中的实例类型所支持的 NVMe 卷。
- [EBS 卷] 用于创建块储存设备的快照的 ID (`snap-xxxxxxxx`)。只要您指定卷大小，此值为可选。
- [EBS 卷] 卷的大小，以 GiB 计算。所指定的大小必须大于或等于指定快照的大小。
- [EBS 卷] 是否在实例终止时删除卷 (`true` 或 `false`)。根设备卷的默认值为 `true`，挂载的卷的默认值为 `false`。当您创建 AMI 时，其块储存设备映射会从该实例继承此设置。当您启动某个实例时，该实例会从 AMI 继承此设置。
- [EBS 卷] 卷类型。对于通用型 SSD 卷是 `gp2`，对于预配置 IOPS SSD 卷是 `io1`，对于吞吐优化 HDD 卷是 `st1`，对于 Cold HDD 卷是 `sc1`，对于磁介质卷是 `standard`。在 Amazon EC2 控制台中，默认值为 `gp2`；在 AWS 开发工具包和 AWS CLI 中，默认值为 `standard`。
- [EBS 卷] 该卷支持的每秒输入/输出操作 (IOPS) 次数。(不适用于 `gp2`、`st1`、`sc1` 或 `standard` 卷。)

块储存设备映射实例存储注意事项

使用在其块储存设备映射中具有实例存储卷的 AMI 启动实例时，要考虑一些注意事项。

- 有些实例类型包含的实例存储卷多于其他类型，而有些实例类型根本不包含实例存储卷。如果实例类型支持一个实例存储卷，而且 AMI 具有用于两个实例存储卷的映射，则实例会在启动时带有一个实例存储卷。
- 实例存储卷只能在启动时进行映射。不能停止没有实例存储卷的实例 (如 `t2.micro`)，将实例更改为支持实例存储卷的类型，然后重新启动带有实例存储卷的实例。但是，您可以从实例创建 AMI 并以支持实例存储卷的实例类型启动它，然后将这些实例存储卷映射到实例。
- 如果您启动映射了实例存储卷的实例，然后停止实例，将它更改为具有较少实例存储卷的实例类型并重新启动它，则来自初始启动的实例存储卷映射会出现在实例元数据中。但是，实例使用的实例存储卷不能超出该实例类型支持的最大数量。

Note

实例停止时，实例存储卷上的所有数据都会丢失。

- 根据启动时的实例存储容量，M3 实例可能会在启动时忽略 AMI 实例存储块储存设备映射（除非在启动时指定它们）。您应在启动时指定实例存储块储存设备映射（即使启动的 AMI 在 AMI 中映射了实例存储卷），以确保实例存储卷在实例启动时可用。

块储存设备映射示例

此图显示了 EBS 支持的实例的块储存设备映射示例。它将 `/dev/sdb` 映射到 `ephemeral0`，并将两个 EBS 卷一个映射到 `/dev/sdh`，另一个映射到 `/dev/sdj`。图中还显示了作为根设备卷的 EBS 卷 `/dev/sda1`。

请注意，此块储存设备映射示例是在本主题中的示命令和 API 中例使用的。您可以在[为 AMI 指定块储存设备映射 \(p. 611\)](#)和[在启动实例时更新快设备映射 \(p. 613\)](#)中找到创建块储存设备映射的示例命令和 API。

如何使设备在操作系统可用

Amazon EC2 使用 `/dev/sdh` 和 `xvdh` 等设备名称来描述块储存设备。Amazon EC2 使用块储存设备映射来指定要连接到 EC2 实例的块储存设备。当块储存设备连接到实例后，您必须先将其安装到操作系统，然后才可以访问此储存设备。当块储存设备从实例断开后，就被操作系统卸载下来，而您也不能再访问该储存设备。

通过 Linux 实例，当实例第一次启动时，在块储存设备映射中指定的设备名称会被映射到相应的块储存设备。在默认情况下，实例类型决定要格式化并安装哪个实例存储卷。您可以在启动时安装额外的实例存储卷，前提是不得超过您的实例类型所允许的实例存储卷数量。有关更多信息，请参阅[Amazon EC2 实例存储 \(p. 591\)](#)。实例的块储存设备驱动程序决定在格式化和安装卷时要使用哪些设备。有关更多信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

AMI 块储存设备映射

各个 AMI 都拥有块储存设备映射，指定实例启动时要连接的块储存设备。Amazon 提供的 AMI 仅包含根设备。要向 AMI 添加更多块储存设备，必须创建自己的 AMI。

内容

- [为 AMI 指定块储存设备映射 \(p. 611\)](#)
- [查看 AMI 块储存设备映射中的 EBS 卷 \(p. 612\)](#)

为 AMI 指定块储存设备映射

创建 AMI 时，您可以使用两种方法来指定除根卷以外的卷。如果您在从该实例创建 AMI 前已将卷连接到运行中的实例，则 AMI 的块储存设备映射将包括这些相同的卷。对于 EBS 卷，这些现存的数据会保存在一个新的快照中，而且是块储存设备映射指定的新快照。而实例存储卷的数据无法保存。

对于 EBS 支持的 AMI，您可以使用块储存设备映射来添加 EBS 卷和实例存储卷。对于实例存储支持的 AMI，您只能添加实例存储卷，方法是在注册镜像时修改镜像清单文件中的块储存设备映射条目。

Note

对于 M3 实例，您必须在启动实例时，在块储存设备映射中指定适用于实例的实例存储卷。当您启动 M3 实例时，如果在块储存设备映射中为 AMI 指定的实例存储卷未指定为块储存设备映射的一部分，则该卷可能会被忽略。

使用控制台向 AMI 添加卷

- 打开 Amazon EC2 控制台。
- 在导航窗格中，选择 Instances。
- 选择一个实例，再依次选择 Actions、Image 和 Create Image。

4. 在 Create Image 对话框中，选择 Add New Volume。
5. 从 Type (类型) 列表中选择一种卷类型并从 Device (设备) 列表中选择一个设备名称。对于 卷，您可以选择指定快照、卷大小和 EBS 卷类型。
6. 选择 Create Image。

使用命令行向 AMI 添加卷

使用 [create-image](#) AWS CLI 命令可为由 EBS 支持的 AMI 指定块储存设备映射。使用 [register-image](#) AWS CLI 命令可为由实例存储支持的 AMI 指定块储存设备映射。

使用以下参数指定块储存设备映射：

```
--block-device-mappings [mapping, ...]
```

要添加实例存储卷，请使用以下映射：

```
{  
    "DeviceName": "/dev/sdf",  
    "VirtualName": "ephemeral0"  
}
```

要添加空的 100 GiB 磁介质卷，请使用以下映射：

```
{  
    "DeviceName": "/dev/sdg",  
    "Ebs": {  
        "VolumeSize": 100  
    }  
}
```

要添加基于快照的 EBS 卷，请使用以下映射：

```
{  
    "DeviceName": "/dev/sdh",  
    "Ebs": {  
        "SnapshotId": "snap-xxxxxxxx"  
    }  
}
```

要对设备省略映射，请使用以下映射：

```
{  
    "DeviceName": "/dev/sdj",  
    "NoDevice": ""  
}
```

或者，您可以使用 `-BlockDeviceMapping` 参数和以下命令 (适用于 Windows PowerShell 的 AWS 工具)：

- [New-EC2Image](#)
- [Register-EC2Image](#)

查看 AMI 块储存设备映射中的 EBS 卷

您可以轻松列举块储存设备映射中适用于 AMI 的 EBS 卷。

使用控制台查看 AMI 的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从 Filter 列表中选择 EBS images 以获取 EBS 支持的 AMI 的列表。
4. 选择所需的 AMI，然后查看 Details (详细信息) 选项卡。至少，以下信息适用于根设备：
 - Root Device Type (ebs)
 - Root Device Name (根设备名称) (如，/dev/sda1)
 - Block Devices (数据块储存设备) (例如，/dev/sda1=snap-1234567890abcdef0:8:true)

如果使用块储存设备映射创建的 AMI 带有额外卷，则 Block Devices (块储存设备) 字段会显示针对这些额外 EBS 卷的映射。(请注意，此屏幕不显示实例存储卷。)

使用命令行查看 AMI 的 EBS 卷

使用 [describe-images](#) (AWS CLI) 命令或 [Get-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具) 命令来枚举 AMI 块储存设备映射中的 EBS 卷。

实例块储存设备映射

在默认情况下，您启动的实例包含所有在 AMI 的块储存设备映射中指定的储存设备 (您是从该 AMI 启动实例的)。您可以在启动实例时，为实例指定要对块储存设备映射执行的更改，而这些更新会覆盖 AMI 的块储存设备映射或与其合并。但是，

限制

- 对于根卷，您只能修改下列内容：卷大小、卷类型和 Delete on Termination 标志。
- 修改 EBS 卷时，无法减小其大小。因此，您必须指定大小等于或大于 AMI 的块储存设备映射中指定的快照大小的快照。

内容

- [在启动实例时更新快设备映射 \(p. 613\)](#)
- [更新正在运行的实例的块储存设备映射 \(p. 615\)](#)
- [查看实例块储存设备映射中的 EBS 卷 \(p. 615\)](#)
- [查看实例存储卷的实例块储存设备映射 \(p. 616\)](#)

在启动实例时更新快设备映射

您可以在启动实例时向其添加 EBS 卷和实例存储卷。请注意，针对实例更新块储存设备映射不会对启动实例的 AMI 的块储存设备映射造成永久性更改。

使用控制台向实例添加卷

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面中，您可以按以下方法修改根卷、EBS 卷和实例存储卷：

- 若要更改根卷的大小，请查找 Type (类型) 列下的 Root (根) 卷，然后更改其 Size (大小) 字段。
- 要隐藏用于启动实例的 AMI 块储存设备映射所指定的 EBS 卷，请找到该卷并单击其对应的 Delete (删除) 图标。
- 要添加 EBS 卷，请选择 Add New Volume，从 Type 列表中选择 EBS，并填写 (Device、Snapshot 等) 字段。
- 要隐藏用于启动实例的 AMI 块储存设备映射所指定的实例存储卷，请找到该卷并选择其对应的 Delete 图标。
- 要添加实例存储卷，请选择 Add New Volume，从 Type 列表中选择 Instance Store，然后从 Device 中选择设备名称。

6. 完成其余向导页面，然后选择 Launch。

使用命令行向实例添加卷

使用 [run-instances](#) AWS CLI 命令可为实例指定块储存设备映射。

使用以下参数指定块储存设备映射：

```
--block-device-mappings [mapping, ...]
```

例如，假定 EBS 支持的 AMI 指定了以下块储存设备映射：

- /dev/sdb=ephemeral0
- /dev/sdh=snap-1234567890abcdef0
- /dev/sdj=:100

要防止 /dev/sdj 连接到从该 AMI 启动的实例，请使用以下映射：

```
{  
    "DeviceName": "/dev/sdj",  
    "NoDevice": ""  
}
```

要将 /dev/sdh 的大小增加到 300 GiB，请指定以下映射。请注意，您不必为 /dev/sdh 指定快照 ID，因为指定设备名称就足以识别卷。

```
{  
    "DeviceName": "/dev/sdh",  
    "Ebs": {  
        "VolumeSize": 300  
    }  
}
```

要额外附加一个实例存储卷 /dev/sdc，请指定以下映射。如果实例类型不支持多个实例存储卷，此映射将无效。

```
{  
    "DeviceName": "/dev/sdc",  
    "VirtualName": "ephemeral1"  
}
```

或者，您可以使用 `-BlockDeviceMapping` 参数和 [New-EC2Instance](#) 命令 (适用于 Windows PowerShell 的 AWS 工具)。

更新正在运行的实例的块储存设备映射

您可以使用 [modify-instance-attribute](#) AWS CLI 命令更新正在运行的实例的块储存设备映射。请注意，在更改此属性之前，您不需要停止该实例。

```
$ aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings file://mapping.json
```

例如，要在实例终止时保留根卷，请在 `mapping.json` 中指定以下内容：

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
}
```

或者，您可以使用 `-BlockDeviceMapping` 参数和 [Edit-EC2InstanceAttribute](#) 命令 (适用于 Windows PowerShell 的 AWS 工具)。

查看实例块储存设备映射中的 EBS 卷

您可以轻松枚举映射到实例的 EBS 卷。

Note

对于在 2009-10-31 API 发行之前启动的实例，AWS 不会显示块储存设备映射。您必须先断开并重新连接该卷，AWS 才能显示块相应的设备映射。

使用控制台查看实例的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances。
3. 在搜索栏中，键入 Root Device Type，然后选择 EBS。此操作会显示 EBS 支持的实例列表。
4. 选择所需的实例，然后查看 Description 选项卡中显示的详细信息。至少，以下信息适用于根设备：
 - 根设备类型 (ebs)
 - Root device (根设备) (例如，/dev/sda1)
 - Block devices (块储存设备) (例如 /dev/sda1、/dev/sdh 和 /dev/sdj)

如果使用块储存设备映射启动的实例有附加 EBS 卷，则 Block devices 字段会将这些附加卷也显示为根设备。(请记住，此对话框不显示实例存储卷。)

5. 要显示有关块储存设备的其他信息，请选择 Block devices 旁边的条目。此操作会显示块储存设备的以下信息：
 - EBS ID (vol-xxxxxxxx)
 - 根设备类型 (ebs)
 - 连接时间 (yyyy-mmThh:mm:ss.ssTZD)
 - 块储存设备状态 (attaching, attached, detaching, detached)
 - 终止时删除 (Yes, No)

使用命令行查看实例的 EBS 卷

使用 [describe-instances](#) (AWS CLI) 命令或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令来枚举实例的块储存设备映射中的 EBS 卷。

查看实例存储卷的实例块储存设备映射

当您查看实例的块储存设备映射时，可以只查看 EBS 卷，但是不能查看实例存储卷。您可以使用实例元数据来查询完整的块储存设备映射。所有针对实例元数据的请求的基本 URI 均为 `http://169.254.169.254/latest/`。

首先，连接到运行中的实例。

对正在运行的实例使用此查询以了解其块储存设备映射的相关信息。

```
$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

该响应包含实例的块储存设备名称。举例来说，由实例存储支持的 `m1.small` 实例的输出如下所示。

```
ami
ephemeral0
root
swap
```

`ami` 设备显然是实例的根设备。实例存储卷命名为 `ephemeral[0-23]`。交换设备用于存储页面文件。如果您还映射了多个 EBS 卷，它们会依次显示为 `ebs1`、`ebs2` 等。

要了解块储存设备映射中的单个块储存设备的详细信息，可将其名称添加到上述查询，如下所示。

```
$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

有关更多信息，请参阅 [实例元数据和用户数据 \(p. 295\)](#)。

使用公用数据集

Amazon Web Services 提供可无缝集成到基于 AWS 云的应用程序中的公用数据集存储库。Amazon 将数据集免费存储到社区中，与所有 AWS 服务一样，您只需要为自己的应用程序所用的计算和存储付费。

内容

- [公用数据集概念 \(p. 617\)](#)
- [查找公用数据集 \(p. 617\)](#)
- [从快照创建公用数据集卷 \(p. 618\)](#)
- [连接和装载公用数据集卷 \(p. 618\)](#)

公用数据集概念

以前，查找、下载、自定义以及分析大数据集，如人类基因组的映射和美国人口普查局的数据，需要几小时甚至几天才能完成。现在，任何人都可以通过 EC2 实例访问这些数据集并在数分钟内开始这些数据的计算工作。您还可以利用整个 AWS 生态系统，轻松与其他 AWS 用户协作工作。例如，您可以通过工具和应用程序生产或使用预先构建的系统镜像来分析数据集。通过利用经济实惠的服务，如 Amazon EC2，托管这些重要数据，AWS 希望为各个学科和行业的研究人员提供实用的工具，促进更多、更快的创新。

有关更多信息，请参阅 [AWS 上的公用数据集页面](#)。

可用的公用数据集

目前，以下类别中的公用数据集可用：

- 生物学 - 包括人类基因组计划、基因库和其他内容。
- 化学 - 包括多个版本的 PubChem 和其他内容。
- 经济学 - 包括人口普查数据、劳动统计数据、交通统计数据和其他内容。
- 百科知识 - 包括多种来源的维基百科数据和其他内容。

查找公用数据集

在能够使用公用数据集之前，必须查找该数据集，然后确定托管该数据集所采用的格式。这些数据集采用两种可能的格式：Amazon EBS 快照或 Amazon S3 存储桶。

查找公用数据集并确定其格式

1. 转到[公用数据集页面](#)以查看所有可用公用数据集的列表。您还可以在此页面上输入搜索短语以查询可用公用数据集列表。
2. 单击数据集的名称以查看其详细信息页面。
3. 在数据集详细信息页面上，查找快照 ID 列表以标识 Amazon EBS 格式化数据集或 Amazon S3 URL。

采用快照格式的数据集用于创建连接到 EC2 实例的新 EBS 卷。有关更多信息，请参阅 [从快照创建公用数据集卷 \(p. 618\)](#)。

对于采用 Amazon S3 格式的数据集，可以使用 AWS 开发工具包或 HTTP 查询 API 访问信息，也可以使用 AWS CLI 将数据复制或同步到实例或是从实例复制或同步数据。有关更多信息，请参阅 [Amazon S3 和 Amazon EC2 \(p. 605\)](#)。

还可以使用 Amazon EMR 分析和使用公用数据集。有关更多信息，请参阅 [Amazon EMR 是什么？](#)。

从快照创建公用数据集卷

要使用采用快照格式的公用数据集，请创建新卷，指定公用数据集的快照 ID。可以使用 AWS 管理控制台创建新卷，如下所示。如果您愿意，也可以使用 [create-volume](#) AWS CLI 命令。

从快照创建公用数据集卷

1. 打开 Amazon EC2 控制台。
2. 在导航栏中，选择您的数据集快照所处的区域。

Important

快照 ID 限制在单个区域，您无法从处于另一个区域的快照创建卷。此外，您只能将 EBS 卷连接到同一个可用区中的实例。有关更多信息，请参阅 [资源位置 \(p. 619\)](#)。

如果您需要在不同区域中创建此卷，则可以将快照复制到所需区域，然后将其恢复到该区域中的卷。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 561\)](#)。

3. 在导航窗格中，单击 Volumes (卷)。
4. 在上方窗格上，单击 Create Volume (创建卷)。
5. 在 Create Volume (创建卷) 对话框中的 Type (类型) 列表中，选择 通用型 SSD、预配置 IOPS SSD 或磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 519\)](#)。
6. 在 Snapshot (快照) 字段中，开始为数据集键入快照的 ID 或描述。从建议选项列表中选择快照。

Note

如果您预期看到的快照 ID 未出现，则您可能在 Amazon EC2 控制台中选择了不同区域。如果您在 [查找公用数据集 \(p. 617\)](#) 中标识的数据集未在其详细信息页面上指定区域，则它可能包含在 us-east-1 美国东部（弗吉尼亚北部）区域中。

7. 在 Size (大小) 字段中，输入卷的大小（以 GiB 或 TiB 为单位），或验证快照的默认大小是否足够。

Note

如果您指定卷大小和快照 ID，其大小必须等于或大于快照的大小。当您选择一种卷类型和一个快照 ID 时，最小和最大卷大小将显示在 Size (大小) 列表旁边。

8. 对于 预配置 IOPS SSD 卷，在 IOPS 字段中输入该卷可支持的每秒输入/输出操作 (IOPS) 的最大值。
9. 在 Availability Zone (可用区) 列表中，选择要在其中启动实例的可用区。

Important

EBS 卷只能连接到位于相同可用区中的实例。

10. 单击 Yes, Create (是，创建)。

Important

如果您创建的卷大于该快照的默认大小（通过在 [Step 7 \(p. 618\)](#) 中指定大小），您需要扩展卷上的文件系统以利用额外空间。有关更多信息，请参阅 [在 Linux 上修改 EBS 卷的大小、IOPS 或类型 \(p. 543\)](#)。

连接和装载公用数据集卷

创建新数据集卷之后，您需要将其连接到 EC2 实例才能访问数据（此实例还必须处于与新卷相同的可用区中）。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。

将卷连接到实例之后，您需要在实例上装载该卷。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 531\)](#)。

资源和标签

Amazon EC2 提供您可创建和使用的不同资源。这些资源中的一部分资源包括映像、实例、卷和快照。在您创建某个资源时，我们会为该资源分配一个唯一资源 ID。

可以用您定义的值标记某些资源，来帮助您组织和识别它们。

以下主题介绍了资源和标签，以及如何使用它们。

主题

- [资源位置 \(p. 619\)](#)
- [资源 ID \(p. 620\)](#)
- [列出并筛选您的资源 \(p. 623\)](#)
- [标记 Amazon EC2 资源 \(p. 626\)](#)
- [Amazon EC2 服务限制 \(p. 633\)](#)
- [Amazon EC2 使用率报告 \(p. 633\)](#)

资源位置

下表描述了何种 Amazon EC2 资源是全球性的、何种是区域性的，或何种是基于可用区域的。

| 资源 | 类型 | 说明 |
|------------------|---------|--|
| AWS 账户 | 服务全球 | 您可以在所有区域使用同一个 AWS 账户。 |
| 密钥对 | 全球性或区域性 | 您可以只在使用 Amazon EC2 创建密钥对的区域使用密钥对。您可以创建和上传所有区域均可使用的 RSA 密钥对。 有关更多信息，请参阅 Amazon EC2 密钥对 (p. 346)。 |
| Amazon EC2 资源标识符 | 区域性的 | 每个资源标识符（例如，AMI ID、实例 ID、EBS 卷 ID 或 EBS 快照 ID）都与其区域相关联，并且只能在创建资源的区域使用。 |

| 资源 | 类型 | 说明 |
|-----------|------|---|
| 用户提供的资源名称 | 区域性的 | 每个资源名称（例如，安全组名称或密钥对名称）都与其区域相关联，并且只能在创建资源的区域使用。尽管您可以在多个区域创建名称相同的资源，但是它们之间并无关联。 |
| AMI | 区域性的 | AMI 与文件位于 Amazon S3 的区域相关联。您可以将 AMI 从一个区域复制到另一个区域。有关更多信息，请参阅 复制 AMI (p. 117) 。 |
| 弹性 IP 地址 | 区域性的 | 弹性 IP 地址与区域相关联，并且只能与同一区域的实例相关联。 |
| 安全组 | 区域性的 | 安全组与区域相关联，并且只能分配给同一区域的实例。您不能使用安全组规则让一个实例与其所在区域外的实例通信。另一个区域实例的流量被视为 WAN 带宽。 |
| EBS 快照 | 区域性的 | EBS 快照与其区域相关联，并且只能用于在同一区域创建卷。您可以将快照从一个区域复制到另一个区域。有关更多信息，请参阅 复制 Amazon EBS 快照 (p. 561) 。 |
| EBS 卷 | 可用区域 | Amazon EBS 卷与其可用区相关联，只能与同一可用区内的实例相连接。 |
| 实例 | 可用区域 | 实例与您在其中启动实例的可用区相关联。但请注意，它的实例 ID 与区域相关联。 |

资源 ID

创建资源时，我们会为每个资源分配一个唯一资源 ID。您可以使用资源 ID 在 Amazon EC2 控制台中查找您的资源。如果您正在通过命令行工具或 Amazon EC2 API 使用 Amazon EC2，则某些命令需要资源 ID。例如，如果您正在使用 `stop-instances` AWS CLI 命令来停止实例，则必须在该命令中指定实例 ID。

资源 ID 长度

资源 ID 采用以下格式：资源标识符（例如，快照的 `snap`）后接连字符以及字母与数字的唯一组合。自 2016 年 1 月起，我们将逐步引入适合部分 Amazon EC2 和 Amazon EBS 资源类型的较长 ID。字母数字字符组合的长度采用 8 个字符的格式；新 ID 采用 17 个字符的格式，例如实例 ID 的 `i-1234567890abcdef0`。

支持的资源类型将有一个选择周期，在此周期内，您可以启用较长的 ID 格式。在为某个资源类型启用较长 ID 后，您创建的任何新资源在创建后将拥有较长的 ID，除非您明确禁用较长的 ID 格式。资源 ID 在创建后不可更改；因此，不会影响具有较短 ID 的现有资源。同样，如果您为某个资源类型禁用较长 ID，您创建的具有较长 ID 的任何资源不受影响。

所有支持的资源类型将拥有一个截止日期，在此日期后，此类型的所有新资源将默认为较长的 ID 格式，并且您不再能禁用较长的 ID 格式。您可以按 IAM 用户和 IAM 角色启用或禁用较长 ID。默认情况下，IAM 用户或角色的默认设置与根用户相同。

根据您创建账户的时间，支持的资源类型可能默认为使用较长的 ID。但是，在该资源类型的截止日期前，您可以选择不再使用较长 ID。有关更多信息，请参阅 [Amazon EC2 常见问题](#) 中的较长的 EC2 和 EBS 资源 ID。

无论个人设置如何，所有 IAM 用户和 IAM 角色均可查看创建的具有较长 ID 的资源，前提是他们拥有查看相关资源类型的权限。

主题

- [使用较长的 ID \(p. 621\)](#)

- [控制对较长 ID 设置的访问 \(p. 623\)](#)

使用较长的 ID

您可以为自己或账户中的其他 IAM 用户、IAM 角色和根用户查看和修改较长的 ID 设置。

主题

- [查看和修改较长的 ID 设置 \(p. 621\)](#)
- [查看和修改用户或角色的较长 ID 设置 \(p. 622\)](#)

查看和修改较长的 ID 设置

您可以使用 Amazon EC2 控制台或 AWS CLI 查看支持长 ID 的资源类型，并为自己启用或禁用较长的 ID 格式。本节中的程序适用于已登录控制台或提出请求的 IAM 用户或 IAM 角色，但不适用于整个 AWS 账户。

使用控制台查看和修改较长的 ID 设置

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在屏幕顶部的导航栏中，会显示当前区域。选择要查看或更改其较长 ID 设置的区域。设置不在区域之间共享。
3. 在控制面板中的 Account Attributes 下，选择 Resource ID length management。将列出支持较长 ID 的资源类型。您将自动切换为对每个资源类型使用较长 ID 的日期将在 Deadline 列中显示。
4. 要为支持的资源类型启用较长 ID 格式，请选中 Use Longer IDs 列的复选框。要禁用较长 ID 格式，请清除此复选框。

Important

如果您作为根用户登录，这些设置将适用于整个账户，除非 IAM 用户或角色登录并明确为其覆盖这些设置。无论个人设置如何，创建的具有较长 ID 的资源对所有 IAM 用户可见，只要他们有权查看相关资源类型。

使用 AWS CLI 查看和修改较长的 ID 设置

要查看所有受支持资源的较长 ID 设置，请使用 `describe-id-format` AWS CLI 命令：

```
aws ec2 describe-id-format

{
    "Statuses": [
        {
            "Deadline": "2016-11-01T13:00:00.000Z",
            "UseLongIds": false,
            "Resource": "instance"
        },
        {
            "Deadline": "2016-11-01T13:00:00.000Z",
            "UseLongIds": true,
            "Resource": "reservation"
        },
        {
            "Deadline": "2016-11-01T13:00:00.000Z",
            "UseLongIds": false,
            "Resource": "volume"
        },
        {
            "Deadline": "2016-11-01T13:00:00.000Z",
            "UseLongIds": false,
```

```
        "Resource": "snapshot"
    ]
}
```

结果适用于提出请求的 IAM 用户、IAM 角色或根用户，但不适用于整个 AWS 账户。上述结果表明，`instance`、`reservation`、`volume` 和 `snapshot` 资源类型可启用或禁用较长 ID；`reservation` 资源已启用。`Deadline` 字段指明您将自动切换为对该资源使用较长 ID 的日期（采用 UTC 表示）。如果截止日期尚不可用，则不会返回此值。

要为指定的资源启用较长 ID，请使用 [modify-id-format](#) AWS CLI 命令：

```
aws ec2 modify-id-format --resource resource-type --use-long-ids
```

要为指定的资源禁用较长 ID，请使用 [modify-id-format](#) AWS CLI 命令：

```
aws ec2 modify-id-format --resource resource-type --no-use-long-ids
```

如果您以根用户的身份使用这些操作，则这些设置将适用于整个账户，除非 IAM 用户或角色明确为其覆盖这些设置。这些命令仅应用于单个区域。要修改其他区域的设置，请在命令中使用 `--region` 参数。

Note

在 2015-10-01 版本的 Amazon EC2 API 中，如果您使用 IAM 角色凭证调用 `describe-id-format` 或 `modify-id-format`，结果将适用于整个 AWS 账户，而不是特定的 IAM 角色。在当前版本的 Amazon EC2 API 中，结果仅适用于 IAM 角色。

或者，您可以使用以下命令：

描述 ID 格式

- [DescribeldFormat](#) (Amazon EC2 API)
- [Get-EC2IdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

修改 ID 格式

- [ModifyIdFormat](#) (Amazon EC2 API)
- [Edit-EC2IdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

查看和修改用户或角色的较长 ID 设置

使用 `describe-identity-id-format` 和 `modify-identity-id-format` AWS CLI 命令，您可以查看受支持的资源类型，并为您账户中的特定 IAM 用户、IAM 角色或根用户启用较长 ID 设置。要使用这些命令，您必须在请求中指定 IAM 用户、IAM 角色或根账户用户的 ARN。例如，在账户 123456789012 中，角色“EC2Role”的 ARN 为 `arn:aws:iam::123456789012:role/EC2Role`。有关更多信息，请参阅 IAM 用户指南中的[委托人](#)。

要查看特定 IAM 用户或 IAM 角色的所有受支持资源的较长 ID 设置，请使用以下 AWS CLI 命令：

```
aws ec2 describe-identity-id-format --principal-arn arn-of-iam-principal
```

要为特定 IAM 用户或 IAM 角色的资源类型启用较长 ID 设置，请使用以下 AWS CLI 命令：

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --resource resource-type --use-long-ids
```

这些命令适用于请求中指定的 ARN，但不适用于提出请求的 IAM 用户、IAM 角色或根用户。

您可以使用下面的 AWS CLI 命令为所有 IAM 用户、IAM 角色和账户的根用户启用较长 ID 设置：

```
aws ec2 modify-identity-id-format --principal-arn all --resource resource-type --use-long-ids
```

或者，您可以使用以下命令：

描述 ID 格式

- [DescribeIdentityFormat](#) (Amazon EC2 API)
- [Get-EC2IdentityFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

修改 ID 格式

- [ModifyIdentityFormat](#) (Amazon EC2 API)
- [Edit-EC2IdentityFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

控制对较长 ID 设置的访问

默认情况下，IAM 用户和角色没有使用 `ec2:DescribeIdFormat`、`ec2:DescribeIdentityIdFormat`、`ec2:ModifyIdFormat` 和 `ec2:ModifyIdentityIdFormat` 操作的权限，除非他们通过关联的 IAM 策略明确获得了相应权限。例如，通过在策略语句中添加 `Action": "ec2:*` 元素可授予 IAM 角色使用所有 Amazon EC2 操作的权限。

为防止 IAM 用户和角色查看或修改其自身或您账户中的其他用户和角色的较长资源 ID 设置，请确保 IAM 策略包含以下语句：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "ec2:ModifyIdFormat",  
                "ec2:DescribeIdFormat",  
                "ec2:ModifyIdentityIdFormat",  
                "ec2:DescribeIdentityIdFormat"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

对于 `ec2:DescribeIdFormat`、`ec2:DescribeIdentityIdFormat`、`ec2:ModifyIdFormat` 和 `ec2:ModifyIdentityIdFormat` 操作，我们不支持资源级权限。

列出并筛选您的资源

您可以使用 Amazon EC2 控制台获取一些类型的资源的列表。您可以使用相应命令或 API 操作获取每种类型的资源的列表。如果您拥有许多资源，可以筛选结果以仅包含符合特定标准的资源。

主题

- [高级搜索 \(p. 624\)](#)
- [使用控制台列出资源 \(p. 624\)](#)

- [使用控制台筛选资源 \(p. 625\)](#)
- [使用 CLI 和 API 列出并筛选 \(p. 625\)](#)

高级搜索

高级搜索使您可以通过组合筛选条件执行搜索，从而获得精确的结果。您可以按关键字、用户定义的标签键和预定义资源属性进行筛选。

可用的特定搜索类型有：

- **按关键字搜索**

要按关键字进行搜索，请在搜索框中键入或粘贴要查找的内容，然后选择 Enter。例如，要搜索特定实例，可以键入实例 ID。

- **按字段搜索**

也可以按与资源关联的字段、标签和属性进行搜索。例如，若要查找处于停止状态的所有实例：

1. 在搜索框中，开始键入 **Instance State**。随着您的键入，将显示建议字段的列表。
2. 从列表中选择 **Instance State (实例状态)**。
3. 从建议值列表中选择 **Stopped (已停止)**。
4. 要进一步优化您的列表，请选择搜索框以获得更多搜索选项。

- **高级搜索**

可以通过添加多个筛选器创建高级查询。例如，可以按标签进行搜索，并查看生产堆栈中运行的 Flying Mountain 项目的实例，然后按属性搜索以查看所有 t2.micro 实例，或查看 us-west-2a 中的所有实例，或者查看同时符合这两个条件的实例。

- **逆向搜索**

您可以搜索与特定值不匹配的资源。例如，要列出未终止的所有实例，可按 **Instance State(实例状态)** 字段进行搜索，并为已终止值添加惊叹号前缀 (!)。

- **部分搜索**

按字段进行搜索时，还可以输入部分字符串以查找字段中包含该字符串的所有资源。例如，先按 **Instance Type (实例类型)** 搜索，然后键入 **t2** 以查找所有 t2.micro、t2.small 或 t2.medium 实例。

- **正则表达式**

当需要匹配字段中具有特定模式的值时，可以使用正则表达式。例如，先按名称标签搜索，然后键入 **^s.*** 以查看其名称标签以“s”开头的所有实例。正则表达式搜索不区分大小写。

获得搜索的精确结果之后，您可以为 URL 添加书签以便于参考。在具有数千实例的情况下，筛选条件和书签可以为您节省大量时间；您不必重复运行搜索。

结合搜索筛选条件

通常，具有相同键字段（例如，**tag:Name**、**search**、**Instance State**）的多个筛选条件会自动以 OR 运算符联接。这是特意设计的，因为绝大部分筛选条件如果以 AND 运算符联接将不合逻辑。例如，如果以“**Instance State=running AND Instance State=stopped**”为条件进行搜索，将返回零个结果。在许多情况下，您可以对不同键字段使用补充性搜索词来细化搜索结果，此时将自动改用 AND 规则。如果您搜索“**tag: Name:=All values AND tag:Instance State=running**”，您将获得包含这两个条件的搜索结果。要优化结果，您只需删除字符串中的一个筛选条件，直到结果符合您的要求。

使用控制台列出资源

您可以使用控制台查看最常用的 Amazon EC2 资源类型。要查看其他资源，请使用命令行界面或 API 操作。

要使用控制台列出 EC2 资源

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择与资源对应的选项，例如 AMI 或 Instances。
3. 页面会显示所有可用资源。

使用控制台筛选资源

您可以使用 Amazon EC2 控制台对最常用的资源类型执行筛选和分类。例如，可以使用实例页面上的搜索栏按标签、属性或关键字对实例进行分类。

您还可以使用每个页面上的搜索字段查找具有特定属性或值的资源。您可以使用正则表达式搜索部分或多个字符串。例如，要查找使用 MySG 安全组的所有实例，请在搜索字段中输入 MySG。结果将包括字符串中包含 MySG 的所有值，例如 MySG2 和 MySG3。要将结果限制为只显示 MySG，请在搜索字段中输入 \bMySG\b。要列出类型为 m1.small 或 m1.large 的所有实例，请在搜索字段输入 m1.small|m1.large。

列出 us-east-1b 可用区域中状态为 available 的卷

1. 在导航窗格中，选择 Volumes。
2. 单击搜索框，从菜单中选择 Attachment Status (连接状态)，然后选择 Detached (已断开)。(分离的卷可附加到同一个可用区域中的某个实例上。)
3. 再次单击搜索框，选择 State (状态)，然后选择 Available (可用)。
4. 再次单击搜索框中，选择 Availability Zone (可用区)，然后选择 us-east-1b。
5. 会显示所有符合此标准的卷。

列出由 Amazon EBS 支持的 64 位公有 Linux AMI

1. 在导航窗格中，选择 AMIs。
2. 在 Filter 窗格中，从 Filter 列表中依次选择 Public images、EBS images 和您的 Linux 分发版。
3. 在搜索字段中输入 x86_64。
4. 会显示所有符合此标准的卷。

使用 CLI 和 API 列出并筛选

每个资源类型都有相应的 CLI 命令或 API 请求，您可用来列出该类型的资源。例如，使用 `ec2-describe-images` 或 `DescribeImages` 可以列出 Amazon 系统映像 (AMI)。响应中包含您所有资源的信息。

资源的结果列表可能很长，建议您筛选结果以使结果中只留下符合一定标准的资源。您可以指定多个筛选值，也可以指定多个筛选条件。例如，您可以列出类型为 m1.small 或 m1.large 的所有实例，以及附加了一个被设置为在实例终止时删除的 EBS 卷的所有实例。该实例必须与结果中所包含的您的所有筛选条件相匹配。

您还可以将通配符与筛选值一同使用。星号 (*) 匹配的是零或更多字符，问号 (?) 恰好匹配一个字符。例如，您可以将 *database* 用作筛选值以获取描述中包含 database 的所有 EBS 快照。如果您要将 database 指定为筛选值，则只能返回描述为 database 的快照。筛选值区分大小写。我们只支持字符串精确匹配或子字符串匹配 (带通配符)。如果得到的资源列表很长，使用精确的字符串筛选条件可能会更快返回响应。

您的搜索中可包含通配符的字面值；您只需要在字符前用反斜线隔开字符。例如，用 *amazon\?\＼ 值搜索文字字符串 *amazon?\＼。

有关每个 Amazon EC2 资源支持的筛选器列表，请参阅相关文档：

- 对于 AWS CLI，请参阅 [AWS Command Line Interface Reference](#) 中的相关 命令。
- 对于 Windows PowerShell，请参阅 [适用于 Windows PowerShell 的 AWS 工具 Reference](#) 中的相关 Get 命令。
- 对于查询 API，请参阅 [DescribeAmazon EC2 API Reference](#) 中的相关 API 操作。

Note

描述操作的响应包含关于应用到您的资源的所有标签的信息。但是，在描述多个资源时，最终结果可能是一致的，而且可能不会返回您的所有标签。要确认资源的标签，请描述单个资源。

标记 Amazon EC2 资源

为了方便管理您的实例、映像以及其他 Amazon EC2 资源，您可以选择通过标签的形式为每个资源分配您自己的元数据。本主题介绍标签并说明如何创建标签。

内容

- [有关标签的基本知识 \(p. 626\)](#)
- [标记您的成员资源 \(p. 626\)](#)
- [标签限制 \(p. 628\)](#)
- [标记资源以便于计费 \(p. 628\)](#)
- [通过控制台使用标签 \(p. 629\)](#)
- [通过 CLI 或 API 使用标签 \(p. 631\)](#)

有关标签的基本知识

标签可让您按各种标准（例如用途、所有者或环境）对 AWS 资源进行分类。这在您具有相同类型的许多资源时会很有用 — 您可以根据分配给资源的标签快速识别特定资源。每个标签都包含您定义的一个键 和一个可选值。例如，您可以为账户中的 Amazon EC2 实例定义一组标签，以跟踪每个实例的所有者和堆栈级别。我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理资源时会更加轻松。您可以根据添加的标签搜索和筛选资源。

下图说明了标签的工作方式。在此示例中，您为每个实例分配了两个标签，一个是 `owner`，另一个是 `stack`。每个标签都有一个关联的值。

标签对 Amazon EC2 没有任何语义意义，应严格按字符串进行解析。同时，标签不会自动分配至您的资源。您可以修改标签的密钥和值，还可以随时删除资源的标签。您可以将标签的值设为空的字符串，但是不能将其设为空值。如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。如果删除资源，资源的所有标签也会被删除。

可以使用 AWS 管理控制台、AWS CLI 和 Amazon EC2 API 处理标签。

如果您使用的是 AWS Identity and Access Management (IAM)，则可以控制 AWS 账户中的哪个用户拥有创建、修改和删除标签的权限。有关更多信息，请参阅 [控制对 Amazon EC2 资源的访问 \(p. 366\)](#)。

标记您的成员资源

您可以标记您账户中已存在的大多数 Amazon EC2 资源。下表 (p. 627)列出了支持标记的资源。

如果使用的是 Amazon EC2 控制台，则您可以使用相关资源屏幕上的 Tags 选项卡或使用 Tags 屏幕向资源应用标签。某些资源屏幕允许您在创建资源时为其指定标签。在大多数情况下，控制台会在资源创建后（而不是在资源创建期间）立即应用标签。

如果使用的是 Amazon EC2 API、AWS CLI 或 AWS 软件开发工具包，则您可以使用 `CreateTags` EC2 API 操作向现有资源应用标签。此外，某些资源创建操作允许您在创建资源时为其指定标签。如果无法在资源创建期间应用标签，系统会回滚资源创建过程。这有助于确保要么创建带有标签的资源，要么根本不创建资源，即任何时候都不会创建出未标记的资源。通过在创建时标记资源，您不需要在资源创建后运行自定义标记脚本。

下表描述了可以标记的 Amazon EC2 资源以及可在创建时标记的资源。

Amazon EC2 资源标记支持

| 资源 | 支持标签 | 支持在创建时标记 (EC2 API、AWS CLI、AWS 软件开发工具包) |
|-------------------|------|--|
| AMI | 是 | 否 |
| 捆绑任务 | 否 | 否 |
| 客户网关 | 是 | 否 |
| 专用主机 | 否 | 否 |
| DHCP 选项 | 是 | 否 |
| EBS 快照 | 是 | 否 |
| EBS 卷 | 是 | 是 |
| 仅出口 Internet 网关 | 否 | 否 |
| 弹性 IP 地址 | 否 | 否 |
| 实例 | 是 | 是 |
| 实例存储卷 | 不适用 | 不适用 |
| Internet 网关 | 是 | 否 |
| 密钥对 | 否 | 否 |
| NAT 网关 | 否 | 否 |
| 网络 ACL | 是 | 否 |
| 网络接口 | 是 | 否 |
| 置放群组 | 否 | 否 |
| Reserved Instance | 是 | 否 |
| 预留实例出售清单 | 否 | 否 |
| 路由表 | 是 | 否 |
| 竞价型实例请求 | 是 | 否 |
| 安全组 – EC2-Classic | 是 | 否 |
| 安全组 – VPC | 是 | 否 |
| 子网 | 是 | 否 |
| 虚拟专用网关 | 是 | 否 |

| 资源 | 支持标签 | 支持在创建时标记 (EC2 API、AWS CLI、AWS 软件开发工具包) |
|----------|------|--|
| VPC | 是 | 否 |
| VPC 终端节点 | 否 | 否 |
| VPC 流日志 | 否 | 否 |
| VPC 对等连接 | 是 | 否 |
| VPN 连接 | 是 | 否 |

要在创建时标记资源或卷，您可以使用 Amazon EC2 控制台中的 Amazon EC2 启动实例向导、[RunInstances](#) Amazon EC2 API 或 [CreateVolume](#) Amazon EC2 API。Amazon EC2 控制台中的卷屏幕不支持在创建时标记。

您可以在 IAM 策略中向 [CreateVolume](#) 和 [RunInstances](#) Amazon EC2 API 操作应用基于标记的资源级权限，以对可在创建时标记资源的用户和组实施精细控制。您的资源从创建开始会受到适当的保护 – 标签会立即用于您的资源，因此控制资源使用的任何基于标签的资源级权限都会立即生效。可以更准确地对您的资源进行跟踪和报告。您可以强制对新资源使用标记，可以控制对资源设置哪些标签键和值。

此外，您还可以在 IAM 策略中对 [CreateTags](#) 和 [DeleteTags](#) Amazon EC2 API 操作应用资源级权限，从而控制对现有资源设置哪些标签键和值。有关更多信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 376\)](#) 和 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 398\)](#)。

有关标记资源以便于计费的更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的[使用成本分配标签](#)。

标签限制

下面是适用于标签的基本限制：

- 每个资源的标签数上限 - 50
- 最大密钥长度 - 127 个 Unicode 字符(采用 UTF-8 格式)
- 最大值长度 - 255 个 Unicode 字符 (采用 UTF-8 格式)
- 标签键和值要区分大小写。
- 请勿在标签名称或值中使用 aws: 前缀，因为它专为 AWS 使用预留。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。
- 如果您的标记方案将在多个服务和资源中使用，请记得其他服务可能对允许使用的字符有限制。通常允许使用的字符包括：可用 UTF-8 格式表示的字母、空格和数字以及特殊字符 + - = _ : / @。

您不能仅依据标签终止或删除资源，而必须指定资源的标识符。例如，要删除您使用名为 DeleteMe 的标签键标记的快照，您必须将 [DeleteSnapshots](#) 操作与快照的资源标识符 (如 snap-1234567890abcdef0) 结合使用。

您可以为公有或共享资源添加标签，但是您分配的标签仅对您的 AWS 账户可用，而对其他共享该资源的账户不可用。

您无法标记所有资源。有关更多信息，请参阅 [Amazon EC2 资源标记支持 \(p. 627\)](#)。

标记资源以便于计费

您可以使用标签来管理 AWS 账单，使其反映您的成本结构。要执行此操作，请注册以获取包含标签键值的 AWS 账户账单。有关设置包含标签的成本分配报告的更多信息，请参阅 AWS Account Billing 简介 中的[月度](#)

成本分配报告。如需查看组合资源的成本，请按具有相同标签键值的资源组织您的账单信息。例如，您可以将特定的应用程序名称用作几个资源的标签，然后组织账单信息，以查看在数个服务中的使用该应用程序的总成本。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的[使用成本分配标签](#)。

Note

如果您已启用报告，则可以在 24 小时后查看当月的数据。

通过控制台使用标签

通过 Amazon EC2 控制台，您可以查看同一区域中哪些标签是所有 Amazon EC2 资源都使用的。您可以按资源和资源类型来查看资源，也可以查看与指定标签相关的每种资源类型的项目数量。您还可以通过 Amazon EC2 控制台同时在一个或多个资源中应用或删除标签。

要了解有关使用筛选条件列出资源的更多信息，请参阅 [列出并筛选您的资源 \(p. 623\)](#)。

为便于使用并取得最佳结果，请使用 AWS 管理控制台中的标签编辑器，此编辑器提供了一种用于创建和管理标签的集中而统一的方法。有关更多信息，请参阅 Getting Started with the AWS Management Console 中的[使用标签编辑器](#)。

内容

- [显示标签 \(p. 629\)](#)
- [为单个资源添加和删除标签 \(p. 629\)](#)
- [为一组资源添加和删除标签 \(p. 630\)](#)
- [在启动实例时添加标签 \(p. 631\)](#)
- [按标签筛选资源列表 \(p. 631\)](#)

显示标签

您可以在 Amazon EC2 控制台中以两种不同的方式显示标签。您可以显示单个资源或所有资源的标签。

显示单个资源的标签

当您在 Amazon EC2 控制台中选择特定资源页面时，它会显示这些资源列表。例如，如果您在导航窗格中选择 Instances，则控制台会显示 Amazon EC2 实例列表。当您从其中一个列表中选择一种资源时（例如，实例），如果该资源支持标签，则您可以查看和管理标签。在大多数资源页面上，您可以在详细信息窗格的 Tags (标签) 选项卡中查看标签。

您可以在资源列表中添加列，以显示密钥相同的标签的所有值。通过该列，您可以按照标签对资源列表进行分类和筛选。资源列表中添加新列以显示标签的方法有两种。

- 在 Tags 选项卡上，选择 Show Column。新列将添加到控制台中。
- 选择 Show/Hide Columns 齿轮状图标，然后在 Show/Hide Columns 对话框中的 Your Tag Keys 下选择标签键。

显示所有资源的标签

您可以通过选择 Amazon EC2 控制台导航窗格中的 Tags (标签)，显示所有资源的标签。下图显示了 Tags (标签) 窗格，其中按资源类型列出了所有正在使用的标签。

为单个资源添加和删除标签

您可以直接在资源页面管理单个资源的标签。

向单个资源添加标签

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 在导航窗格中，选择资源类型（例如，Instances）。
4. 从资源列表中选择资源。
5. 在详细信息窗格中，选择 Tags（标签）选项卡。
6. 选择 Add/Edit Tags 按钮。
7. 在 Add/Edit Tags 对话框中，为每个标签指定密钥和值，然后选择 Save。

删除单个资源的标签

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 在导航窗格中，选择资源类型（例如，Instances）。
4. 从资源列表中选择资源。
5. 在详细信息窗格中，选择 Tags（标签）选项卡。
6. 依次选择 Add/Edit Tags、与标签对应的 Delete 图标和 Save。

为一组资源添加和删除标签

为一组资源添加标签

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 在导航窗格中，选择 Tags。
4. 在内容窗格的顶部，选择 Manage Tags。
5. 对于 Filter，选择要添加标签的资源的类型（如实例）。
6. 在资源列表中，选中要添加标签的资源旁边的复选框。
7. 在 Add Tag 下的 Key 和 Value 中，键入标签键和值，然后选择 Add Tag。

Note

如果您添加的新标签的标签键与现有标签的相同，则新标签将覆盖现有标签。

删除一组资源的标签

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 619\)](#)。
3. 在导航窗格中，依次选择 Tags、Manage Tags。
4. 要查看正在使用的标签，请选择 Show/Hide Columns 齿轮状图标，然后在 Show/Hide Columns 对话框中，选择要查看的标签键，然后选择 Close。
5. 对于 Filter，选择要删除标签的资源的类型（如实例）。
6. 在资源列表中，选中要删除标签的资源旁边的复选框。
7. 在 Remove Tag 下的 Key 中键入标签的名称，然后选择 Remove Tag。

在启动实例时添加标签

通过“启动向导”添加标签

1. 从导航栏中选择实例地区。该选择很重要，这是因为有些 Amazon EC2 资源可以在区域间共享，另一些却不能。请选择能满足您的需求的区域。有关更多信息，请参阅 [资源位置 \(p. 619\)](#)。
2. 选择 Launch Instance。
3. Choose an Amazon Machine Image (AMI) (选择Amazon 系统映像 (AMI)) 页面会显示称为“Amazon 系统映像 (AMI)”的基本配置的列表。选择要使用的 AMI，然后选择 Select。有关选择 AMI 的更多信息，请参阅 [查找 Linux AMI \(p. 62\)](#)。
4. 在 Configure Instance Details 页面上，根据需要配置实例设置，然后选择 Next: Add Storage。
5. 在 Add Storage (添加存储) 页面上，您可以为实例指定额外的存储卷。完成后，选择 Next: Add Tags。
6. 在 Add Tags 页面上，为实例、卷或两者指定标签。选择 Add another tag 以向您的实例添加多个标签。完成时选择 Next: Configure Security Group。
7. 在 Configure Security Group (配置安全组) 页面上，您可以从您所拥有的现有安全组中进行选择，或根据向导的指示创建新的安全组。完成操作后，选择 Review and Launch。
8. 检视您的设置。在您确认选择无误之后，选择 Launch。选择现有密钥对或创建新的密钥对，选中确认复选框，然后选择 Launch Instances。

按标签筛选资源列表

您可以基于一个或多个标签键和标签值来筛选资源列表。

按标签筛选资源列表

1. 标签列显示如下：
 - a. 选择资源。
 - b. 在详细信息窗格中，选择 Tags。
 - c. 在列表中查找标签，然后选择 Show Column。
2. 选择标签列右上角的筛选图标，以显示筛选列表。
3. 选择标签值，然后选择 Apply Filter 以筛选结果列表。

Note

有关筛选条件的更多信息，请参阅 [列出并筛选您的资源 \(p. 623\)](#)。

通过 CLI 或 API 使用标签

使用以下命令添加、更新、列出和删除资源标签。相应文档提供了示例。

| 任务 | AWS CLI | 适用于 Windows PowerShell 的 AWS 工具 | API 操作 |
|---------------|---------------|---------------------------------|--------------|
| 添加或覆盖一个或多个标签。 | create-tags | New-EC2Tag | CreateTags |
| 删除一个或多个标签。 | delete-tags | Remove-EC2Tag | DeleteTags |
| 描述一个或多个标签。 | describe-tags | Get-EC2Tag | DescribeTags |

您还可以根据标签筛选资源列表。以下示例演示了如何通过 [describe-instances](#) 命令使用标签来筛选实例。

Important

标签会立即应用于您的资源，因此在您的 IAM 策略中使用的任何基于标签的资源级权限都会立即生效。但是，在描述多个资源时，最终结果可能是一致的，而且可能不会返回您的所有标签。要确认资源的标签，请描述单个资源。

示例 1：描述具有指定标签键的实例

以下命令描述了具有 Stack 标签 (无论标签的值如何) 的实例。

```
aws ec2 describe-instances --filters Name=tag-key,Values=Stack
```

示例 2：描述具有指定标签的实例

以下命令描述了具有标签 Stack=production 的实例。

```
aws ec2 describe-instances --filters Name=tag:Stack,Values=production
```

示例 3：描述具有指定标签值的实例

以下命令描述了具有值为 production 的标签 (无论标签键如何) 的实例。

```
aws ec2 describe-instances --filters Name=tag-value,Values=production
```

某些资源创建操作允许您在创建资源时指定标签。以下操作支持在创建时进行标记。

| 任务 | AWS CLI | 适用于 Windows PowerShell 的 AWS 工具 | API 操作 |
|------------|-------------------------------|---------------------------------|------------------------------|
| 启动一个或多个实例。 | run-instances | New-EC2Instance | RunInstances |
| 创建 EBS 卷。 | create-volume | New-EC2Volume | CreateVolume |

以下示例说明如何在创建资源时应用标签。

示例 4：启动实例并向实例和卷应用标签

下面的命令启动一个实例并向此实例应用键为 webserver、值为 production 的标签。此命令还向创建的任何 EBS 卷 (此示例中为根卷) 应用键为 cost-center、值为 cc123 的标签。

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --subnet-id subnet-6e7f829e --tag-specifications 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]' 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

您可以在启动时向实例和卷应用相同的标签键和值。下面的命令启动一个实例并向此实例和创建的任何 EBS 卷应用键为 cost-center、值为 cc123 的标签。

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --subnet-id subnet-6e7f829e --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]' 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

示例 5：创建卷并应用标签

下面的命令创建一个卷并应用两个标签 : purpose = production 和 cost-center = cc123。

```
aws ec2 create-volume --availability-zone us-east-1a --volume-type gp2 --size 80 --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},{Key=cost-center,Value=cc123}]'
```

Amazon EC2 服务限制

Amazon EC2 提供您可使用的不同资源。这些资源包括映像、实例、卷和快照。在创建 AWS 账户时，我们根据区域设置对这些资源的默认限制。举例来说，对您可在某一区域中启动的实例数存在限制。因此，在美国西部（俄勒冈）区域启动实例时，请求一定不能导致您的用量超出您在该区域的当前实例限制。

Amazon EC2 控制台提供了对 Amazon EC2 和 Amazon VPC 控制台管理的资源的限制信息。您可以请求提高这些限制的值。使用我们提供的限制信息可管理您的 AWS 基础设施。需要时请提前计划请求提高限制。

有关其他服务的限制的更多信息，请参阅 Amazon Web Services 一般参考中的 [AWS 服务限制](#)。

查看当前限制

使用 Amazon EC2 控制台中的 EC2 Service Limits (EC2 服务限制) 页面可按区域查看 Amazon EC2 和 Amazon VPC 提供的资源的当前限制。

查看当前限制

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 Limits。
4. 在列表中找到资源。Current Limit (当前限制) 列显示您的账户对该资源的当前最大限制。

申请提高限制

使用 Amazon EC2 控制台中的 Limits (限制) 页面可按区域申请提高 Amazon EC2 或 Amazon VPC 提供的资源的限制。

申请提高限制

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 Limits。
4. 在列表中找到资源。选择 Request limit increase。
5. 填写提高限制表格中的必填字段。我们将通过您指定的联系方式进行响应。

Amazon EC2 使用率报告

通过 Amazon EC2 提供的使用率报告，您可以深入分析您实例的使用率。使用率报告中的数据每天会多次更新。您可以按 AWS 账户、区域、可用区、操作系统、实例类型、购买选项、租期和标签筛选报告。

要获取账户的使用率和成本数据，您必须具有其账户证书并为账户启用包含资源和标签的详细账单报告。如果您使用整合账单，则必须登录到付款人账户以查看付款人账户及其所有关联账户的数据。有关整合账单的信息，请参阅[使用整合账单为多个账户支付账单](#)。

主题

- [可用报告 \(p. 634\)](#)
- [开始设置使用率报告 \(p. 634\)](#)
- [向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限 \(p. 635\)](#)
- [实例使用率报告。 \(p. 636\)](#)
- [预留实例使用率报告 \(p. 638\)](#)

可用报告

您可以生成以下报告：

- [实例使用率报告 \(p. 636\)](#)。此报告包括按需实例、竞价型实例和预留实例的使用率。
- [预留实例使用率报告 \(p. 638\)](#)。此报告包括容量预留的使用率。

要查看报告，请打开 AWS 管理控制台。在导航窗格中，选择 Reports，然后选择您希望查看的报告。

开始设置使用率报告

在开始之前，请按以下过程所示，启用包含资源和标签的详细账单报告。完成此过程之后，我们将开始为实例收集使用率数据。如果您已启用了详细账单报告，则可以访问我们为您启用它们以来收集的使用率数据。

Important

要完成这些过程，必须使用 AWS 账户证书登录。如果使用 IAM 用户证书登录，则无法完成这些过程。

启用详细账单报告

1. 选择现有 Amazon S3 存储桶以接收使用率数据。请务必管理对此存储桶的访问，因为它包含账单数据。(我们不要求您保留这些文件；事实上，如果不使用它们，您可以立即将它们删除。)如果您没有存储桶，请按如下所示创建一个：
 - a. 打开 Amazon S3 控制台。
 - b. 选择 Create Bucket。
 - c. 在 Create a Bucket 对话框中，为您的存储桶输入一个名称(例如 用户名-ec2-usage-data)，选择一个区域，然后选择 Create。有关存储桶名称要求的更多信息，请参阅 Amazon Simple Storage Service 控制台用户指南 中的[创建存储桶](#)。
2. 打开账单和成本管理控制台 <https://console.aws.amazon.com/billing/home?#>。
3. 在导航窗格中选择 Preferences。
4. 选择 Receive Billing Reports。
5. 在 Save to S3 Bucket 中指定您的 Amazon S3 存储桶的名称。
6. 在 Receive Billing Reports 下，选择 sample policy。复制示例策略。请注意，示例策略使用您指定的存储桶名称。
7. 授予 AWS 权限以将使用率数据发布到 Amazon S3 存储桶。
 - a. 在另一个浏览器选项卡打开 Amazon S3 控制台。选择您的存储桶，选择 Properties，然后展开 Permissions。在 Permissions 部分，选择 Add bucket policy。将示例策略粘贴到文本区域中，然后选择 Save。在 Permissions 部分，选择 Save。
 - b. 返回包含示例策略的浏览器选项卡并选择 Verify。
8. 在 Report (报告) 下，选择 Detailed billing report with resources and tags (包含资源和标签的详细账单报告)。

9. 选择 Save preferences。

Note

最多需要一天，您就可以查看报告中的数据。

可以使用标签对实例分类。标记实例之后，您必须启用有关这些标签的报告。

启用按标签进行的使用率报告

1. 标记您的实例。为了获得最佳结果，请确保您将计划用于报告的每个标签添加到每个实例。有关如何标记实例的更多信息，请参阅[标记 Amazon EC2 资源 \(p. 626\)](#)。
2. 打开账单和成本管理控制台 <https://console.aws.amazon.com/billing/home?#>。
3. 在导航窗格中，选择 Preferences。
4. 在 Report 下，选择 Manage report tags。
5. 页面显示您已创建的标签列表。选择要用于对实例使用率数据进行筛选或分组的标签，然后单击 Save (保存)。我们自动从实例使用率报告中排除您未选择的所有标签。

Note

我们仅将这些更改应用于当前月的数据。这些更改最多一天就会生效。

向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限

默认情况下，IAM 用户无法访问 Amazon EC2 使用率报告。必须创建向 IAM 用户授予访问这些报告的权限的 IAM 策略。

以下策略允许用户查看两个 Amazon EC2 使用率报告。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2-reports:*",  
            "Resource": "*"  
        }  
    ]  
}
```

以下策略允许用户查看实例使用率报告。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2-reports:ViewInstanceUsageReport",  
            "Resource": "*"  
        }  
    ]  
}
```

以下策略允许用户查看预留实例使用率报告。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2-reports:ViewReservedInstanceUtilizationReport",
        "Resource": "*"
    }
]
```

有关更多信息，请参阅 IAM 用户指南 中的[权限与策略](#)。

实例使用率报告。

您可以使用实例使用率报告查看实例使用率和成本趋势。可以按实例小时数或成本查看使用率数据。可以选择查看使用率数据的每小时、每日和每月汇总。可以按区域、可用区、实例类型、AWS 账户、平台、租期、购买选项或标签对报告进行筛选或分组。配置报告之后，您可以对其进行添加标签，以方便以后返回。

下面是一些您可以通过创建实例使用率报告回答的问题的示例：

- 我在每种实例类型的实例上分别花费了多少？
- 特定部门使用的实例小时数是多少？
- 我的实例使用率在可用区间是如何分配的？
- 我的实例使用率在 AWS 账户间是如何分配的？

主题

- [报告格式 \(p. 636\)](#)
- [查看实例使用率 \(p. 636\)](#)
- [为自定义报告添加书签 \(p. 637\)](#)
- [导出使用率数据 \(p. 637\)](#)

报告格式

我们同时以图和表的形式显示您请求的使用率数据。

例如，下图按实例类型显示成本。图的色例指示哪种颜色表示哪个实例类型。要获取有关条形图的分段的详细信息，请将鼠标悬停在它上方。

对应表为每种实例类型显示一列。请注意，我们在列标题中包含一个色带，其颜色与图中的实例类型相同。

查看实例使用率

以下过程演示如何使用我们提供的一些功能生成使用率报告。

开始之前，您必须进行设置。有关更多信息，请参阅 [开始设置使用率报告 \(p. 634\)](#)。

按实例类型对实例使用率进行筛选和分组

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Reports，然后选择 EC2 Instance Usage Report。
3. 为 Unit (单位) 选择选项。要查看实例已运行的时间 (以小时为单位)，请选择 Instance Hours。要查看实例使用率的成本，请选择 Cost。

4. 为 Granularity (粒度) 和 Time range (时间范围) 选择选项。
 - 要查看针对时间范围内每小时汇总的数据，请选择 Hourly 粒度。查看每小时数据时，可以选择多达 2 天的时间范围。
 - 要查看针对时间范围内每天汇总的数据，请选择 Daily 粒度。查看每天数据时，可以选择多达 2 个月的时间范围。
 - 要查看针对时间范围内每个月汇总的数据，请选择 Monthly 粒度。
5. 在 Filter (筛选条件) 列表中，选择 Instance Type。在 Group by (分组依据) 列表中，选择 Instance Type。
6. 在筛选条件区域中，选择一个或多个实例类型，然后选择 Update Report。您指定的筛选条件会出现在 Applied Filters (应用的筛选条件) 下。

请注意，您可以通过选择页面顶部的 Reports 或 EC2 Management Console 返回 Amazon EC2 控制台。

基于标签对实例使用率分组

1. 打开实例使用率报告页面。
2. 为 Unit (单位) 选择选项。要查看实例已运行的时间 (以小时为单位)，请选择 Instance Hours。要查看实例使用率的成本，请选择 Cost。
3. 为 Granularity (粒度) 和 Time range (时间范围) 选择选项。
 - 要查看针对时间范围内每小时汇总的数据，请选择 Hourly 粒度。查看每小时数据时，可以选择多达 2 天的时间范围。
 - 要查看针对时间范围内每天汇总的数据，请选择 Daily 粒度。查看每天数据时，可以选择多达 2 个月的时间范围。
 - 要查看针对时间范围内每个月汇总的数据，请选择 Monthly 粒度。
4. 在 Group by (分组依据) 列表中，选择 Tag (标签)。
5. 选择 Key Name 框，从列表中选择一个名称，然后选择 Update Report。如果此列表中没有项目，则您必须启用按标签分组的使用率报告。有关更多信息，请参阅 [启用按标签进行的使用率报告 \(p. 635\)](#)。

为自定义报告添加书签

您可能希望再次生成自定义报告。通过为报告添加书签可实现此目的。

向自定义报告添加书签

1. 为报告选择选项和筛选条件。您进行的每个选择都会向控制台 URL 添加一个参数。例如，`granularity=Hourly` 和 `Filters=filter_list`。
2. 使用浏览器将控制台 URL 添加为书签。
3. 将来若要生成相同的报告，请使用您创建的书签。

导出使用率数据

您可能希望在其他报告中包含您的报告图或表。通过导出数据可实现此目的。

导出使用率数据

1. 为报告选择选项和筛选条件。
2. 要以 .csv 文件的形式从表中导出使用率数据，请选择 Download 并选择 CSV Only。

3. 要以 .png 文件的形式导出图表使用率数据，请选择 Download 并选择 Graph Only。

预留实例使用率报告

预留实例使用率报告描述您拥有的每组（或存储桶）Amazon EC2 预留实例在一段时间内的使用情况。每个存储桶都有区域、实例类型、账户、平台、租期和产品类型的唯一组合。您可以指定报告涵盖的时间范围，从自定义范围到数周、数月、一年或三年。可用数据取决于您为账户启用详细账单报告的时间（请参阅[开始设置使用率报告 \(p. 634\)](#)）。预留实例使用率报告会将您为存储桶中所使用实例支付的预留实例价格与按需价格进行对比，并显示您在报告涵盖的时间范围内节省的成本。

要获取账户的使用率和成本数据，您必须具有其账户证书并为账户启用包含资源和标签的详细账单报告。如果您使用整合账单并登录到付款人账户，可以查看付款人账户及其所有关联账户的数据。如果您使用整合账单并登录到关联账户之一，只能查看该关联账户的数据。有关整合账单的信息，请参阅[使用整合账单为多个账户支付账单](#)。

Note

预留实例存储桶使用与账单计算同样的方式跨 EC2-VPC 和 EC2-Classic 网络平台类型汇集预留实例。另外，存储桶中的预留实例可以会有不同的预付费用和小时价格。

下面是一些您可以使用预留实例使用率报告回答的问题的示例：

- 我使用预留实例的情况如何？
- 预留实例是否在帮助我节省开支？

有关预留实例的信息，请参阅[预留实例 \(p. 161\)](#)。

开始之前，您必须进行设置。有关更多信息，请参阅[开始设置使用率报告 \(p. 634\)](#)。

主题

- [了解报告 \(p. 638\)](#)
- [查看预留实例使用率 \(p. 639\)](#)
- [为自定义报告添加书签 \(p. 639\)](#)
- [导出使用率数据 \(p. 640\)](#)
- [选项参考 \(p. 640\)](#)

了解报告

预留实例使用率报告显示以图和表格式显示您请求的使用率数据。

要查看报告，请打开 AWS 管理控制台。在导航窗格中，选择 Reports，然后选择 EC2 Reserved Instance Usage Report。

报告按存储桶汇集了特定时间内的预留实例使用率数据。在报告中，表格中的每一行代表一个存储桶，提供以下指标：

- Count (数量) - 报告周期内同一时间拥有的最高预留实例数。
- Usage Cost (使用率成本) - 预留实例存储桶的实例使用率所产生的总预留实例使用费。
- Total Cost (总成本) – 与预留实例存储桶关联的使用成本加上使用期的摊销预付费用。

Note

如果存储桶中包含您在预留实例市场上售出的预留实例，而该实例在报告期间内的某一时间点处于活动状态，则存储桶总成本可能会被夸大，而您的成本节省量可能会被低估。

- **Savings (节省成本)** – 相应时间段内采用按需价格时的预留实例使用成本与实际成本 (总成本) 之间的差异。
- **Average Utilization (平均使用率)** – 相应时间段内预留实例存储桶的平均每小时使用率。
- **Maximum Utilization (最大使用率)** - 报告期内任一小时的最高使用率。

对于表中的每行 (即预留实例存储桶) , 在所选报告 Time range (时间范围) 内 , 图中基于所选 Show (显示) 指标表示数据。图中每个点代表一个时间点的指标。有关报告选项的信息 , 请参阅[选项参考 \(p. 640\)](#)。

表中每个所选行边缘处的色带对应于图中的报告行。您可以通过选中行开头的复选框 , 在图中显示行。

默认情况下 , 预留实例使用率报告为所有预留实例存储桶返回最近 14 天内的数据。图中显示表中前五个存储桶的平均使用率。您可以自定义报告图以显示某个时间段 (从 7 天到数周、数月或数年) 内的不同使用率 (平均使用率、最大使用率) 或成本 (总成本、使用率成本) 数据。

自定义报告

您可以使用 Time range (时间范围) 和 Filter (筛选条件) 选项自定义预留实例使用率报告。

Time range 提供常用相对时间范围的列表 , 从 Last 7 Days 到 Last 3 Years。选择最适合您需要的时间范围 , 然后选择 Update Report 以应用更改。要应用不在该列表中的时间范围 , 请选择 Custom (自定义) , 然后输入要运行报告的开始日期和结束日期。

通过 Filter 可以按以下一个或多个预留实例特性来筛选预留实例使用率报告的范围 : 区域、实例类型、账户、平台、租期和产品类型。例如 , 您可以按区域、区域中的特定可用区或两者来进行筛选。要按区域进行筛选 , 请选择 Regions , 然后选择您要在报告中包含的区域和可用区 , 并选择 Update Report。

如果不应用任何筛选条件 , 则报告将返回所有结果。

有关报告选项的信息 , 请参阅[选项参考 \(p. 640\)](#)。

查看预留实例使用率

在本部分中 , 我们将重点介绍图和表捕获的预留实例使用率的各个方面。为进行此讨论 , 我们将使用以下报告 (该报告基于测试数据)。

此预留实例使用率报告显示最近三年内的预留实例平均使用率。此报告显示有关账户的预留实例以及如何使用这些实例的以下信息。

- **Average Utilization (平均使用率)**

表中只有少量预留实例的使用情况不错。最突出的是四个 t2.micro 预留实例 (第 2、3 行) , 它们的使用率分别为 50% 和 100%。

- **Maximum Utilization (最大使用率)**

在三年报告期内 , 所有 t2.micro 预留实例都得到了充分利用。其余的预留实例利用率不高 , 导致成本节约未达到预期。

- **Savings (节省成本)**

报告显示 , 对于此测试账户 , 使用预留实例而不是按需实例只能在 美国东部 (弗吉尼亚北部) 中的四个 t2.micro 实例上产生节约。其余预留实例并没有足够的成本优势。

为自定义报告添加书签

您可能希望再次生成自定义报告。通过为报告添加书签可实现此目的。

向自定义报告添加书签

1. 为报告选择选项和筛选条件。您进行的每个选择都会向控制台 URL 添加一个参数。例如，`granularity=Hourly` 和 `Filters=filter_list`。
2. 使用浏览器将控制台 URL 添加为书签。
3. 将来若要生成相同的报告，请使用您创建的书签。

导出使用率数据

您可能希望在其他报告中包含您的报告图或表。通过导出数据可实现此目的。

导出使用率数据

1. 为报告选择选项和筛选条件。
2. 要以 `.csv` 文件的形式从表中导出使用率数据，请选择 `Download` 并选择 `CSV Only`。
3. 要以 `.png` 文件的形式导出图表使用率数据，请选择 `Download` 并选择 `Graph Only`。

选项参考

使用 `Show (显示)` 选项可指定报告图要显示的指标。

- **Average Utilization (平均使用率)**

显示所选时间范围内每小时的平均使用率，其中存储桶一小时的使用率是用于该小时的实例小时数除以该小时内拥有的预留实例总数。

- **Maximum Utilization (最大使用率)**

显示所选时间范围内任何小时的最高使用率，其中存储桶一小时的使用率是用于该小时的实例小时数除以该小时内拥有的预留实例总数。

- **总费用**

显示在生成报告的时间段内，存储桶中预留实例的使用率成本加上预付成本的摊销部分。

- **Usage Cost (使用率成本)**

基于每小时费用显示预留实例的所选存储桶的总成本。

使用 `Time range (时间范围)` 可指定报告所基于的时间段。

Note

所有时间都以 UTC 时间指定。

- **最近 7 天**

显示在当前和前六个日历日中的使用率数据。可以与每天或每月粒度一起使用。

- **最近 14 天**

显示在当前和前 13 个日历日中的使用率数据。可以与每天或每月粒度一起使用。

- **本月**

显示在当前日历月中的使用率数据。可以与每天或每月粒度一起使用。

- **最近 3 个月**

显示当前和前 2 个日历月中的使用率数据。可以与每天或每月粒度一起使用。

- 最近 6 个月

显示当前和前 5 个日历月中的使用率数据。可以与每月粒度一起使用。

- 最近 12 个月

显示当前和前 11 个日历月中的使用率数据。可以与每月粒度一起使用。

- 今年

显示在当前日历年中的使用率数据。可以与每月粒度一起使用。

- 最近 3 年

显示当前和前两个日历年中的使用率数据。可以与每月粒度一起使用。

- 自定义

显示输入的 Start (开始) 和 End (结束) 日期 (按 mm/dd/yyyy 格式指定) 之间的时间范围的数据。可以与每小时、每天或每月粒度一起使用，但是对于每小时数据只能指定最多两天的时间范围，对于每天数据只能指定最多两个月的时间范围，而对于每月数据只能指定最多三年的时间范围。

使用 Filter (筛选条件) 可限定报告中显示的数据的范围。

- 区域
- 实例类型
- 账户
- 平台
- 租期
- 产品类型

排查实例问题

以下文档可帮助您排查实例存在的问题。

内容

- [如果实例立即终止，怎么办？\(p. 642\)](#)
- [排查实例的连接问题 \(p. 643\)](#)
- [排查实例的停止问题 \(p. 649\)](#)
- [排查实例的终止\(关闭\)问题 \(p. 650\)](#)
- [对实例恢复故障进行排除故障 \(p. 650\)](#)
- [通过故障状态检查排查实例故障 \(p. 650\)](#)
- [排查实例的容量问题 \(p. 670\)](#)
- [获取控制台输出和重启实例 \(p. 671\)](#)
- [正在从错误的卷启动我的实例 \(p. 673\)](#)

有关 Windows 实例的更多帮助信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[排除 Windows 实例的故障](#)。

您还可以在 [Amazon EC2 forum](#) 搜索答案和发布问题。

如果实例立即终止，怎么办？

启动实例后，我们建议您检查其状态，确认其从 pending 状态变为 running 状态而不是 terminated 状态。

下面是实例可能立即终止的一些原因：

- 您已达到 EBS 卷限额。要了解有关容量限额的信息，并提交增加容量限额的申请，请参阅[请求提高 Amazon EBS 卷限制](#)。
- EBS 快照受损。

- 您用来启动实例的实例存储支持的 AMI 缺少必需部分 (一个 image.part.xx 文件)。

了解实例终止的原因

您可以使用 Amazon EC2 控制台、 CLI 或 API 获取有关实例终止原因的信息。

使用控制台了解实例终止的原因

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Instances，然后选择您的实例。
- 在 Description (描述) 选项卡上，找到标签 State transition reason (状态转换原因) 旁边的原因。如果实例仍在运行，则通常不会列出原因。如果您已明确停止或终止实例，则原因为 User initiated shutdown。

使用命令行了解实例终止的原因

- 使用 `describe-instances` 命令：

```
aws ec2 describe-instances --instance-id instance_id
```

- 在显示的 JSON 响应中，查找 StateReason 元素。其内容类似于以下示例。

```
"StateReason": {  
    "Message": "Client.UserInitiatedShutdown: User initiated shutdown",  
    "Code": "Client.UserInitiatedShutdown"  
},
```

此示例响应显示了在停止或终止运行中的实例后显示的原因代码。如果实例立即终止，则可以看到 code 和 message 元素，这些元素描述实例终止的原因 (例如，volumeLimitExceeded)。

排查实例的连接问题

下面是在您尝试连接到实例时可能遇到的问题与错误消息。

内容

- 连接到您的实例时出错：连接超时 (p. 644)
- 错误：服务器无法识别用户密钥 (p. 645)
- 错误：未找到主机密钥，权限被拒绝 (publickey)，或者 身份验证失败，权限被拒绝 (p. 646)
- 错误：未保护的私钥文件 (p. 647)
- 错误：服务器拒绝我们的密钥或 没有支持的身份验证方法 (p. 648)
- 在 Safari 浏览器上使用 MindTerm 时的错误 (p. 648)
- 使用 Mac OS X RDP 客户端时出错 (p. 648)
- 无法对实例执行 Ping 操作 (p. 648)

有关 Windows 实例的更多帮助信息，请参阅Amazon EC2 用户指南 (适用于 Windows 实例) 中的[排除 Windows 实例的故障](#)。

您还可以在 [Amazon EC2 forum](#) 搜索答案和发布问题。

连接到您的实例时出错：连接超时

如果在连接到您的实例时看到以下错误消息：Network error: Connection timed out 或 Error connecting to [instance], reason: -> Connection timed out: connect，请尝试以下选项：

- 检查您的安全组规则。您的某个安全组规则应该允许适当的端口传输来自公有 IPv4 地址的入站流量。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Instances，然后选择您的实例。

3. 在 Description 选项卡中的 Security groups 旁边，选择 view rules 以显示有效规则的列表。

4. 对于 Linux 实例：验证是否有允许流量从您的计算机到端口 22 (SSH) 的规则。

对于 Windows 实例：验证是否有允许流量从您的计算机到端口 3389 (RDP) 的规则。

如果您的安全组具有允许来自单个 IP 地址的入站流量的规则，则当您的计算机在企业网络上，或当您通过 Internet 服务提供商 (ISP) 进行连接时，此地址可能不是静态的。请改为指定客户端计算机使用的 IP 地址的范围。如果您的安全组没有上一步中所述的允许入站流量的规则，请向您的安全组添加一个规则。有关更多信息，请参阅[授权网络访问您的实例 \(p. 429\)](#)。

- [EC2-VPC] 查看子网的路由表。您的某个路由应该将流向 VPC 外的所有流量发送到 VPC 的 Internet 网关。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Instances，然后选择您的实例。

3. 在 Description 选项卡中，记下 VPC ID 和 Subnet ID 的值。

4. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

5. 在导航窗格中，选择 Internet Gateways。验证是否有 Internet 网关连接到您的 VPC。否则，选择 Create Internet Gateway 以创建 Internet 网关。选择 Internet 网关，然后选择 Attach to VPC 并按照说明将其附加到您的 VPC。

6. 在导航窗格中，选择 Subnets，然后选择您的子网。

7. 在 Route Table 选项卡上，验证带有 0.0.0.0/0 的路由是否为目的地，并验证您的 VPC 的 Internet 网关是否为目标。如果不是，请选择路由表的 ID (rtb-xxxxxxx) 以导航到路由表的 Routes 选项卡，依次选择 Edit、Add another route，在 Destination 中输入 0.0.0.0/0，从 Target 中选择您的 Internet 网关，然后选择 Save。

如果您使用实例的 IPv6 地址连接到实例，请检查是否有一个路由可以将所有 IPv6 流量 (::/0) 指向 Internet 网关。如果没有，请添加一个以 ::/0 为目的地并指向 Internet 网关的路由。

- [EC2-VPC] 检查子网的网络访问控制列表 (ACL)。该网络 ACL 必须允许适当的端口传输来自本地 IP 地址的入站和出站流量。默认网络 ACL 允许所有入站和出站流量。

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Your VPCs。

3. 在 Summary 选项卡上，找到 Network ACL，选择 ID (acl-xxxxxxx)，然后选择 ACL。

4. 在 Inbound Rules 选项卡上，验证规则是否允许来自您的计算机的流量。如果不允许，请删除或修改阻止来自您的计算机的流量的规则。

5. 在 Outbound Rules 选项卡上，验证规则是否允许到您的计算机的流量。如果不允许，请删除或修改阻止到您的计算机的流量的规则。

- 如果您的计算机在企业网络上，请询问网络管理员内部防火墙是否允许端口 22 (对于 Linux 实例) 或端口 3389 (对于 Windows 实例) 上来自您的计算机的入站和出站流量。

如果您的计算机有防火墙，请验证其是否允许端口 22 (对于 Linux 实例) 或端口 3389 (对于 Windows 实例) 上来自您的计算机的入站和出站流量。

- 检查您的实例是否具有公有 IPv4 地址。如果没有，您可以将弹性 IP 地址与您的实例关联。有关更多信息，请参阅[弹性 IP 地址 \(p. 467\)](#)。

- 检查实例上的 CPU 负载，服务器可能已超过负载。AWS 自动提供数据，例如 Amazon CloudWatch 指标和实例状态，您可以使用这些数据查看实例上 CPU 的负载情况；如有必要，还可以调整负载的处理方式。有关更多信息，请参阅 [使用 CloudWatch 监控您的实例 \(p. 320\)](#)。
- 如果您的负载是可变的，您可以使用 [Auto Scaling](#) 和 [Elastic Load Balancing](#) 自动增加或减少实例。
- 如果您的负载呈稳定增长的态势，您可以迁移到更大的实例类型。有关更多信息，请参阅 [调整您的实例大小 \(p. 156\)](#)。

要使用 IPv6 地址连接实例，请检查以下各项：

- 与您的子网关联的路由表必须含有一个将所有 IPv6 流量 (::/0) 指向 Internet 网关的路由。
- 您的安全组规则必须允许适当端口 (Linux 的端口 22 和 Windows 的端口 3389) 传输来自本地 IPv6 地址的入站流量。
- 您的网络 ACL 规则必须允许入站和出站 IPv6 流量。
- 如果您从旧版 AMI 启动实例，则其可能未针对 DHCPv6 进行配置 (IPv6 地址不会在网络接口上自动识别)。有关更多信息，请参阅 Amazon VPC 用户指南中的 [在实例中配置 IPv6](#)。
- 您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。

错误：服务器无法识别用户密钥

如果您使用 SSH 连接到实例

- 请在连接时使用 `ssh -vvv` 获得三倍的详细调试信息：

```
ssh -vvv -i [your key name].pem ec2-user@[public DNS address of your instance].compute-1.amazonaws.com
```

下列样本输出演示了如果您尝试使用服务器无法识别的密钥连接实例时您可能会看到的信息：

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
```

Permission denied (publickey).

如果您使用 SSH (MindTerm) 连接到实例

- 如果未启用 Java，则服务器不会识别该用户密钥。要启用 Java，请参阅 Java 文档中的[如何在 Web 浏览器中启用 Java？](#)。

如果您使用 PuTTY 连接到实例

- 验证您的私有密钥 (.pem) 文件已经转换为 PuTTY (.ppk) 可以识别的格式。有关转换您的私有密钥的更多信息，请参阅[使用 PuTTY 从 Windows 连接到 Linux 实例 \(p. 256\)](#)。

Note

在 PuTTYgen 中，加载您的私有密钥文件并选择 Save Private Key (保存私有密钥) 而不是 Generate (生成)。

- 验证您在连接时是否对为 AMI 使用了正确的用户名。在 PuTTY Configuration (PuTTY 配置) 窗口的 Host name (主机名) 框中输入用户名。
 - 对于 Amazon Linux AMI，用户名为 ec2-user。
 - 对于 RHEL AMI，用户名是 ec2-user 或 root。
 - 对于 Ubuntu AMI，用户名是 ubuntu 或 root。
 - 对于 Centos AMI，用户名是 centos。
 - 对于 Fedora AMI，用户名是 ec2-user。
 - 对于 SUSE，用户名是 ec2-user 或 root。
 - 另外，如果 ec2-user 和 root 无法使用，请与 AMI 供应商核实。
- 验证您的入站安全组规则允许入站流量进入合适的端口。有关更多信息，请参阅[授权网络访问您的实例 \(p. 429\)](#)。

错误：未找到主机密钥，权限被拒绝 (publickey)，或者 身份验证失败，权限被拒绝

如果您使用 SSH 连接到实例并得到以下任一错误：Host key not found in [directory]、Permission denied (publickey) 或 Authentication failed, permission denied，请验证您使用了 AMI 的相应用户名称进行连接且已为实例指定正确的私有密钥 (.pem) 文件。对于 MindTerm 客户端，在 Connect To Your Instance (连接到您的实例) 窗口中的 User name (用户名) 框中输入用户名。

正确的用户名如下所示：

- 对于 Amazon Linux AMI，用户名为 ec2-user。
- 对于 RHEL AMI，用户名是 ec2-user 或 root。
- 对于 Ubuntu AMI，用户名是 ubuntu 或 root。
- 对于 Centos AMI，用户名是 centos。
- 对于 Fedora AMI，用户名是 ec2-user。
- 对于 SUSE，用户名是 ec2-user 或 root。
- 另外，如果 ec2-user 和 root 无法使用，请与 AMI 供应商核实。

请确认您使用的私有密钥文件对应于您启动实例时选择的密钥对。

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 选择实例。在 Description 选项卡上，验证 Key pair name 的值。
3. 如果您启动实例时没有指定密钥对，则可以终止实例并启动新实例，从而确保指定密钥对。如果这是您一直使用的实例，但您不再具有密钥对的 .pem 文件，则可以使用新的密钥对取代该密钥对。有关更多信息，请参阅 [丢失私有密钥时连接到 Linux 实例 \(p. 351\)](#)。

如果您已经生成了您自己的密钥对，请确保您的密钥生成器被设置为创建 RSA 密钥。不接受 DSA 密钥。

如果您遇到 Permission denied (publickey) 错误但以上情况都不适用（例如，您之前能够连接），则可能是实例主目录的权限发生了更改。`/home/ec2-user/.ssh/authorized_keys` 的权限必须限制为仅限所有者。

在您的实例上验证权限

1. 停止您的实例并分离根卷。有关更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#) 和 [从实例断开 Amazon EBS 卷 \(p. 541\)](#)。
2. 在当前实例所在的可用区中启动一个临时实例（使用与您用于当前实例的 AMI 类似或相同的 AMI），并将根卷挂载到此临时实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 530\)](#)。
3. 连接临时实例，创建一个安装点并安装您挂载的卷。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 531\)](#)。
4. 在临时实例中，检查所挂载的卷的 `/home/ec2-user/` 目录的权限。如有必要，按如下方式调整权限：

```
chmod 600 mount_point/home/ec2-user/.ssh/authorized_keys
```

```
chmod 700 mount_point/home/ec2-user/.ssh
```

```
chmod 700 mount_point/home/ec2-user
```

5. 卸载此卷，将其与临时实例分离，然后将其重新挂载到原来的实例。确保为根卷指定正确的设备名称；例如，`/dev/xvda`。
6. 启动您的实例。如果不再需要临时实例，可以终止它。

错误：未保护的私钥文件

必须保护您的私钥文件，防止其他任何用户对其进行读写操作。如果除您外其他任何人都能够读取或写入您的私钥，则 SSH 会忽略您的密钥，并且您会看到以下警告消息。

```
@@@@@@@  
@      WARNING: UNPROTECTED PRIVATE KEY FILE!      @  
@  
Permissions 0777 for '.ssh/my_private_key.pem' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
bad permissions: ignore key: .ssh/my_private_key.pem  
Permission denied (publickey).
```

如果在尝试登录到您的实例时看到类似的消息，请检查此错误消息的第一行，验证您为实例使用的公钥是否正确。上面的示例对私有密钥 `.ssh/my_private_key.pem` 使用文件权限 0777，该权限允许任何人读取或写入该文件。此权限级别非常不安全，因此 SSH 会忽略此密钥。要修复此错误，请执行以下命令，替入您的私钥文件的路径。

```
chmod 0400 .ssh/my_private_key.pem
```

错误：服务器拒绝我们的密钥或 没有支持的身份验证方法

如果在使用 PuTTY 连接到您的实例时收到以下两种错误之一：`Error: Server refused our key` 或 `Error: No supported authentication methods available`，请验证在连接时是否为 AMI 使用了正确的用户名。在 PuTTY Configuration (PuTTY 配置) 窗口的 User name (用户名) 框中输入用户名。

正确的用户名如下所示：

- 对于 Amazon Linux AMI，用户名为 `ec2-user`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名是 `ubuntu` 或 `root`。
- 对于 CentOS AMI，用户名是 `centos`。
- 对于 Fedora AMI，用户名是 `ec2-user`。
- 对于 SUSE，用户名是 `ec2-user` 或 `root`。
- 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。

您还应验证您的私有密钥 (.pem) 文件已经正确转换为 PuTTY (.ppk) 可以识别的格式。有关转换您的私有密钥的更多信息，请参阅 [使用 PuTTY 从 Windows 连接到 Linux 实例 \(p. 256\)](#)。

在 Safari 浏览器上使用 MindTerm 时的错误

如果您使用 MindTerm 连接到实例并且使用 Safari Web 浏览器，则可能会收到以下错误：

```
Error connecting to your_instance_ip, reason:  
-> Key exchange failed: Host authentication failed
```

您需要更新浏览器的安全设置以允许 AWS 管理控制台在不安全模式下运行 JAVA 插件。

启用 JAVA 插件以便在不安全模式下运行

- 在 Safari 中，保持 Amazon EC2 控制台打开，依次选择 Safari、Preferences、Security。
- 选择 Plug-in Settings (在较旧版本的 Safari 上，选择 Manage Website Settings)。
- 选择左侧的 Java 插件，然后在 Currently Open Websites 列表中找到 AWS 管理控制台 URL。从其关联列表中选择 Run in Unsafe Mode (在不安全模式下运行)。
- 出现提示时，选择警告对话框中的 Trust。选择 Done 返回到浏览器。

使用 Mac OS X RDP 客户端时出错

如果您使用 Microsoft 网站的远程桌面连接客户端连接到 Windows Server 2012 R2 实例，则可能会收到以下错误：

```
Remote Desktop Connection cannot verify the identity of the computer that you want to  
connect to.
```

从 Apple iTunes 存储下载 Microsoft 远程桌面应用程序，然后使用该应用程序连接到实例。

无法对实例执行 Ping 操作

`ping` 命令是一种 ICMP 流量 — 如果您无法对实例执行 ping 操作，请确保您的入站安全组规则允许的 `Echo Request` 消息的 ICMP 流量来自所有资源，或来自从中发出命令的计算机或实例。如果您无法从实例发出

ping 命令，请确保您的出站安全组规则允许的 Echo Request 消息的 ICMP 流量发送到所有目标，或发送到您正在尝试对其执行 ping 操作的主机。

排查实例的停止问题

如果您已停止由 Amazon EBS 支持的实例，并且它“卡在”stopping 状态，这说明底层主计算机可能存在问题。

首先，尝试再次停止该实例。如果您正在使用 [stop-instances](#) (AWS CLI) 命令，请确保使用 --force 选项。

如果无法强制将实例停止，则可以从该实例创建 AMI，然后启动替代实例。

当实例不处于 running 状态时，不会向您收取任何实例小时数费用。

创建替代实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Image 和 Create Image。
4. 在 Create Image 对话框中，填写以下字段，然后选择 Create Image：
 - a. 为 AMI 指定名称和描述。
 - b. 选择 No reboot。
5. 从 AMI 启动实例，验证该实例是否正常运行。
6. 选择卡住的实例，然后依次选择 Actions、Instance State、Terminate。如果该实例也因卡住而终止，则 Amazon EC2 会自动强制其在几个小时内终止。

如果无法按上一步骤所述从该实例创建 AMI，则可以设置替代实例，如下所示：

创建替代实例 (如果上一步骤失败)

1. 选择实例，打开 Description (描述) 选项卡，查看 Block devices (块储存设备) 列表。选择每个卷并记下其卷 ID。请务必注意哪个卷是根卷。
2. 在导航窗格中，选择 Volumes。选择该实例的各个卷，然后依次选择 Actions、Create Snapshot。
3. 在导航窗格中，选择 Snapshots。选择您刚刚创建的快照，然后依次选择 Actions、Create Volume。
4. 启动与卡住的实例类型相同的实例 (Amazon Linux、Windows 等)。注意其根卷的卷 ID 和设备名称。
5. 在导航窗格中，选择 Instances，选择您刚刚启动的实例，然后依次选择 Actions、Instance State、Stop。
6. 在导航窗格中，选择 Volumes，选择已停止实例的根卷，然后依次选择 Actions、Detach Volume。
7. 选择您从卡住的实例创建的根卷，依次选择 Actions、Attach Volume，然后将其挂载到新实例以作为其根卷 (使用记下的设备名称)。将任何其他非根卷连接到该实例。
8. 在导航窗格中，选择 Instances，然后选择替代实例。依次选择 Actions、Instance State、Start。验证该实例是否正常运行。
9. 选择卡住的实例，然后依次选择 Actions、Instance State、Terminate。如果该实例也因卡住而终止，则 Amazon EC2 会自动强制其在几个小时内终止。

如果无法完成这些步骤，可以向 [Amazon EC2 forum](#) 发布帮助请求。为了帮助加快解决问题，请提供实例 ID 并描述已采取的步骤。

排查实例的终止(关闭)问题

当实例不处于 running 状态时，不会向您收取任何实例小时数费用。换言之，当您终止实例时，一旦实例的状态变为 shutting-down，就不再产生与该实例相关的费用。

延迟的实例终止

如果您的实例处于 shutting-down 状态超过数分钟，这可能是因为实例运行的关闭脚本造成了延迟。

另一个可能的原因是底层主机有问题。如果您的实例处于 shutting-down 状态已有数小时，Amazon EC2 会视之为卡住的实例，并会强制终止它。

如果您的实例看起来卡在正在终止状态已有数小时，请在 [Amazon EC2 forum](#) 发帖请求帮助。为了帮助加快解决问题，请提供实例 ID 并描述已采取的步骤。

已终止实例仍然显示

在您终止某个实例之后，它会在删除之前的短时间内保持可见。状态显示为 terminated。如果该条目在几小时之后未删除，请联系 Support。

自动启动或终止实例

如果您终止所有实例，则可以看到我们为您启动了一个新实例。如果您启动一个实例，则可以看到我们终止您的实例之一。如果您停止了某个实例，则可能会看到我们终止了该实例并启动了新实例。通常，这些行为意味着您已使用 Auto Scaling 或 Elastic Beanstalk 根据已定义的条件自动扩展计算资源。

有关更多信息，请参阅 [Auto Scaling 用户指南](#) 或 [AWS Elastic Beanstalk 开发人员指南](#)。

对实例恢复故障进行排除故障

以下问题可能会导致实例自动恢复失败：

- 替换硬件的临时容量不足。
- 该实例有一个附加实例存储，而自动实例恢复不支持该配置。
- 一项正在进行中的服务运行状况控制面板事件使恢复过程无法成功执行。有关服务可用性的最新信息，请参阅 <http://status.aws.amazon.com/>。
- 该实例已达到每天最多三次的恢复尝试操作限制。

自动恢复过程每天最多针对三个不同的故障尝试恢复您的实例。如果实例系统状态检查故障仍然存在，建议您手动启动和停止实例。有关更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

如果自动恢复失败，并且确定硬件性能下降是初始系统状态检查失败的根本原因，那么您的实例随后可能会被停用。

通过故障状态检查排查实例故障

主题

- [初始步骤 \(p. 651\)](#)
- [检索系统日志 \(p. 651\)](#)
- [诊断基于 Linux 的实例的系统日志错误 \(p. 652\)](#)

- 内存不足：终止进程 (p. 653)
- 错误：mmu_update 失败 (内存管理更新失败) (p. 653)
- I/O 错误 (块储存设备故障) (p. 654)
- IO 错误：既不是本地磁盘也不是远程磁盘 (破损的分布式块储存设备) (p. 655)
- request_module：runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) (p. 656)
- “严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配) (p. 656)
- “FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) (p. 657)
- ERROR：无效内核”(EC2 不兼容内核) (p. 658)
- request_module：runaway loop modprobe(在较旧的 Linux 版本上循环旧内核 modprobe) (p. 659)
- fsck：尝试打开时没有找到此文件或目录... (未找到文件系统) (p. 660)
- 安装文件系统时出现一般性错误 (安装失败) (p. 661)
- VFS：无法在未知块上安装根 fs (根文件系统不匹配) (p. 663)
- 错误：无法确定根设备的主/次编号...(根文件系统/设备不匹配) (p. 663)
- XENBUS：设备没有驱动程序... (p. 664)
- ... 没有检查时，已强制执行检查的工作日 (文件系统检查要求) (p. 665)
- fsck 卡在退出状态...(缺少设备) (p. 666)
- GRUB 提示 (grubdom>) (p. 666)
- 提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。(硬编码的 MAC 地址)。 (p. 668)
- 无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误) (p. 669)
- XENBUS：连接设备时超时 (Xenbus 超时) (p. 670)

初始步骤

如果您的实例没能通过状况检查，请首先确定您的应用程序是否存在任何问题。如果您验证的结果是实例没有按照预期运行应用程序，请执行以下步骤：

使用 Amazon EC2 控制台调查受损实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 在详细信息窗格中，选择 Status Checks，查看所有 System Status Checks 和 Instance Status Checks 的各项结果。

如果系统状态检查失败，您可以尝试以下一种选项：

- 创建实例恢复警报。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的[创建用于停止、终止或恢复实例的警报](#)。
- 对于使用由 Amazon EBS 支持的 AMI 的实例，停止并重启该实例。
- 对于使用实例存储支持的 AMI 的实例，可终止实例并启动替换实例。
- 等待 Amazon EC2 解决问题。
- 将您的问题发布到 [Amazon EC2 forum](#)。
- 检索系统日志并查找错误。

检索系统日志

如果实例状态检查失败，则您可以重启实例并检索系统日志。日志能够显示错误之处，从而帮助您诊断问题。重启可清除日志中不必要的信息。

重启实例并检索系统日志

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 依次选择 Actions、Instance State、Reboot。实例重启可能需要几分钟时间。
4. 验证问题是否依然存在；在一些情况下，重启可以解决此问题。
5. 待实例进入 running 状态后，依次选择 Actions、Instance Settings、Get System Log。
6. 查看屏幕上显示的日志，使用下面的已知系统日志错误语句列表来诊断问题。
7. 如果您的情况与我们的检查结果不同，或者，如果您的实例存在问题而我们的检查没有发现，请选择 Status Checks 选项卡上的 Submit feedback 帮助我们改进检测试验。
8. 如果您的问题没有得到解决，您可以将问题发布到 [Amazon EC2 forum](#)。

诊断基于 Linux 的实例的系统日志错误

对于未能通过实例状态检查的 Linux 实例，例如实例可到达性检查，请验证您是否按照上述步骤检索了系统日志。以下列表中包含一些常见的系统日志错误，还有一些建议您采取以解决此问题的针对性操作。

内存错误

- 内存不足：终止进程 (p. 653)
- 错误：mmu_update 失败 (内存管理更新失败) (p. 653)

设备错误

- I/O 错误 (块储存设备故障) (p. 654)
- IO 错误：既不是本地磁盘也不是远程磁盘 (破损的分布式块储存设备) (p. 655)

内核错误

- request_module : runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) (p. 656)
- “严重错误：内核太旧”和“fsck : 在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配) (p. 656)
- “FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) (p. 657)
- ERROR : 无效内核”(EC2 不兼容内核) (p. 658)

文件系统错误

- request_module : runaway loop modprobe(在较旧的 Linux 版本上循环旧内核 modprobe) (p. 659)
- fsck : 尝试打开时没有找到此文件或目录... (未找到文件系统) (p. 660)
- 安装文件系统时出现一般性错误 (安装失败) (p. 661)
- VFS : 无法在未知块上安装根 fs (根文件系统不匹配) (p. 663)
- 错误：无法确定根设备的主/次编号...(根文件系统/设备不匹配) (p. 663)
- XENBUS : 设备没有驱动程序... (p. 664)
- ... 没有检查时，已强制执行检查的工作日 (文件系统检查要求) (p. 665)
- fsck 卡在退出状态...(缺少设备) (p. 666)

操作系统错误

- GRUB 提示 (grubdom>) (p. 666)

- 提起接口 eth0 : 设备 eth0 的 MAC 地址与预期不同 , 驳回。(硬编码的 MAC 地址)。 (p. 668)
- 无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误) (p. 669)
- XENBUS : 连接设备时超时 (Xenbus 超时) (p. 670)

内存不足 : 终止进程

表明内存不足错误的系统日志条目如以下示例所示。

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

潜在原因

内存耗尽

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下任一操作 :</p> <ul style="list-style-type: none">停止并修改实例以使用不同的实例类型 , 然后再次启动实例。例如 , 一个更大或内存优化型实例类型。重启实例以使其恢复未受损状态。除非您更改实例类型 , 否则该问题可能还会出现。 |
| 实例存储支持的 | <p>请执行以下任一操作 :</p> <ul style="list-style-type: none">终止实例并启动新实例 , 指定一个不同的实例类型。例如 , 一个更大或内存优化型实例类型。重启实例以使其恢复未受损状态。除非您更改实例类型 , 否则该问题可能还会出现。 |

错误 : mmu_update 失败 (内存管理更新失败)

表示内存管理更新故障的系统日志条目与以下示例类似 :

```
...
Press `ESC' to enter the menu... 0  [H[J  Booting 'Amazon Linux 2011.09
(2.6.35.14-95.38.amzn1.i686)'

root (hd0)
Filesystem type is ext2fs, using whole disk
kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=
en_US.UTF-8 KEYTABLE=us
```

```
initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img
ERROR: mmu_update failed with rc=-22
```

潜在原因

Amazon Linux 的问题

建议采用的措施

将您的问题发布到[开发人员论坛](#)，或联系 [AWS Support](#)。

I/O 错误 (块储存设备故障)

表示输入/输出错误的系统日志条目类似于以下示例：

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

潜在原因

| 实例类型 | 潜在原因 |
|-----------------|--------------------|
| 由 Amazon EBS 支持 | 发生故障的 Amazon EBS 卷 |
| 实例存储支持的 | 发生故障的物理驱动器 |

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">停止实例。断开此卷。尝试恢复此卷。 |

| 对于此实例类型 | 请执行此操作 |
|---------|---|
| | <p>Note</p> <p>最好的做法是经常拍摄 Amazon EBS 卷的快照。这样能大幅降低因故障而导致数据丢失的风险。</p> <ol style="list-style-type: none"> 4. 重新将卷连接到实例。 5. 断开此卷。 |
| 实例存储支持的 | <p>终止实例并启动新的实例。</p> <p>Note</p> <p>无法恢复数据。从备份恢复。</p> <p>Note</p> <p>比较好的做法是使用 Amazon S3 或 Amazon EBS 进行备份。实例存储卷是直接与单个主机和磁盘故障相关的。</p> |

IO 错误：既不是本地磁盘也不是远程磁盘 (破损的分布式块储存设备)

表示设备的输入/输出错误的系统日志条目类似于以下示例：

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...
Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056
lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

潜在原因

| 实例类型 | 潜在原因 |
|-----------------|--------------------|
| 由 Amazon EBS 支持 | 发生故障的 Amazon EBS 卷 |
| 实例存储支持的 | 发生故障的物理驱动器 |

建议采用的措施

终止实例并启动新的实例。

对于由 Amazon EBS 支持的实例，您可以从最近拍摄的快照恢复数据，方法是从该快照创建映像。快照之后添加的任何数据都无法恢复。

request_module : runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe)

表示此条件的系统日志类似于下方显示的示例。使用不稳定或陈旧的 Linux 内核 (如 2.6.16-xenU) 可能会在启动时导致无法终止的循环环境。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1  
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007  
  
BIOS-provided physical RAM map:  
  
Xen: 0000000000000000 - 0000000026700000 (usable)  
  
0MB HIGHMEM available.  
...  
  
request_module: runaway loop modprobe binfmt-464c  
  
request_module: runaway loop modprobe binfmt-464c  
request_module: runaway loop modprobe binfmt-464c  
request_module: runaway loop modprobe binfmt-464c  
request_module: runaway loop modprobe binfmt-464c
```

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | 使用以下其中一个选项可使用较新的内核 (基于 GRUB 的内核或静态内核)。 选项 1：终止实例并启动新实例，指定 <code>-kernel</code> 和 <code>-ramdisk</code> 参数。 选项 2： <ol style="list-style-type: none">停止实例。修改内核和虚拟磁盘的属性以使用较新的内核。启动实例。 |
| 实例存储支持的 | 终止实例并启动新实例，指定 <code>-kernel</code> 和 <code>-ramdisk</code> 参数。 |

“严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)  
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007  
...  
FATAL: kernel too old
```

```
Kernel panic - not syncing: Attempted to kill init!
```

潜在原因

不可兼容的内核和用户空间

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none"> 停止实例。 修改配置以使用较新的内核。 启动实例。 |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none"> 创建使用较新内核的 AMI。 终止实例。 从您创建的 AMI 中启动新实例。 |

“FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失)

表示此条件的系统日志类似于下方显示的示例。

```
[ 0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No such
file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device. Common problems:
- Boot args (cat /proc/cmdline)
- Check rootdelay= (did the system wait long enough?)
- Check root= (did the system wait for the right device?)
- Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
ALERT! /dev/sdal does not exist. Dropping to a shell!

BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

(initramfs)

潜在原因

以下一个或多个条件可能会导致此问题：

- 虚拟磁盘缺失
- 缺少正确的虚拟磁盘模块
- Amazon EBS 根卷没有正确连接为 /dev/sda1

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 为 Amazon EBS 卷选择经过纠正的虚拟磁盘。2. 停止实例。3. 断开并修复该卷。4. 将卷连接到实例。5. 启动实例。6. 修改 AMI 以使用经过纠正的虚拟磁盘。 |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 终止此实例，然后启动包含正确虚拟磁盘的新实例。2. 创建包含正确虚拟磁盘的新 AMI。 |

ERROR : 无效内核"(EC2 不兼容内核)

表示此条件的系统日志类似于下方显示的示例。

```
...
root (hd0)

Filesystem type is ext2fs, using whole disk
kernel /vmlinuz root=/dev/sda1 ro
initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

Booting 'Fallback'
root (hd0)

Filesystem type is ext2fs, using whole disk
```

```
kernel /vmlinuz.old root=/dev/sda1 ro  
Error 15: File not found
```

潜在原因

以下一个或两个条件都可能会导致此问题：

- GRUB 不支持所提供的内核
- 后备内核不存在

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | 执行以下步骤： <ol style="list-style-type: none">1. 停止实例。2. 替换为正在工作的内核。3. 安装后备内核。4. 通过纠正内核修改 AMI。 |
| 实例存储支持的 | 执行以下步骤： <ol style="list-style-type: none">1. 终止此实例，然后启动包含正确内核的新实例。2. 创建包含正确内核的 AMI。3. (可选) 通过 AWS Support 寻求技术支持以便恢复数据。 |

request_module : runaway loop modprobe(在较旧的 Linux 版本上循环旧内核 modprobe)

表示此条件的系统日志类似于下方显示的示例。使用不稳定或陈旧的 Linux 内核 (如 2.6.16-xenU) 可能会在启动时导致无法终止的循环环境。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1  
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007  
  
BIOS-provided physical RAM map:  
  
Xen: 0000000000000000 - 0000000026700000 (usable)  
  
0MB HIGHMEM available.  
...  
  
request_module: runaway loop modprobe binfmt-464c  
request_module: runaway loop modprobe binfmt-464c
```

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | 使用以下其中一个选项可使用较新的内核 (基于 GRUB 的内核或静态内核)。 选项 1：终止实例并启动新实例，指定 <code>-kernel</code> 和 <code>-ramdisk</code> 参数。 选项 2： <ol style="list-style-type: none">1. 停止实例。2. 修改内核和虚拟磁盘的属性以使用较新的内核。3. 启动实例。 |
| 实例存储支持的 | 终止实例并启动新实例，指定 <code>-kernel</code> 和 <code>-ramdisk</code> 参数。 |

fsck : 尝试打开时没有找到此文件或目录... (未找到文件系统)

表示此条件的系统日志类似于下方显示的示例。

```
Welcome to Fedora
Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [ OK ]
Starting udev: [ OK ]
Setting hostname localhost: [ OK ]
No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[ OK ]
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem. If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
  e2fsck -b 8193 <device>

[FAILED]

*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
```

(or type Control-D to continue):

潜在原因

- 虚拟磁盘文件系统定义 /etc/fstab 中存在错误
- /etc/fstab 中存在配置错误的文件系统定义
- 硬盘丢失/故障

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 停止实例，断开根卷，修补/修改 /etc/fstab 该卷，将其连接到实例，然后启动该实例。2. 修改虚拟磁盘以使其包含经过修改的 /etc/fstab (如果适用)。3. 修改 AMI 以使用较新的虚拟磁盘。 <p>fstab 中的第 6 个字段定义此安装的可用性要求，非零值暗示将在该卷上执行文件系统检查并且必须成功完成。能否在 Amazon EC2 中使用此字段还不确定，因为故障一般会导致交互性控制台提示信息，但是目前此功能在 Amazon EC2 中尚不可用。请谨慎使用此功能，并阅读 Linux man 页面了解有关 fstab 的信息。</p> |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 终止实例并启动新的实例。2. 将所有不正确 Amazon EBS 卷与重启的实例断开。3. (可选) 通过 AWS Support 寻求技术支持以便恢复数据。 |

安装文件系统时出现一般性错误 (安装失败)

表示此条件的系统日志类似于下方显示的示例。

```
>Loading xenblk.ko module
xen-vbd: registered block device major 8

>Loading ehci-hcd.ko module
>Loading ohci-hcd.ko module
>Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

>Loading mbcache.ko module
>Loading jbd.ko module
>Loading ext3.ko module
Creating root device.
```

```
Mounting root filesystem.  
kjournald starting. Commit interval 5 seconds  
  
EXT3-fs: mounted filesystem with ordered data mode.  
  
Setting up other filesystems.  
Setting up new root fs  
no fstab.sys, mounting internal defaults  
Switching to new root and running init.  
unmounting old /dev  
unmounting old /proc  
unmounting old /sys  
mountall:/proc: unable to mount: Device or resource busy  
mountall:/proc/self/mountinfo: No such file or directory  
mountall: root filesystem isn't mounted  
init: mountall main process (221) terminated with status 1  
  
General error mounting filesystems.  
A maintenance shell will now be started.  
CONTROL-D will terminate this shell and re-try.  
Press enter for maintenance  
(or type Control-D to continue):
```

潜在原因

| 实例类型 | 潜在原因 |
|-----------------|--|
| 由 Amazon EBS 支持 | <ul style="list-style-type: none">断开或出故障的 Amazon EBS 卷。受损的文件系统。匹配错误的虚拟磁盘与 AMI 组合 (例如，Debian 虚拟磁盘和 SUSE AMI)。 |
| 实例存储支持的 | <ul style="list-style-type: none">发生故障的驱动器。损坏的文件系统。匹配错误的虚拟磁盘和组合 (例如，Debian 虚拟磁盘和 SUSE AMI)。 |

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">停止实例。断开根卷。将根卷连接到已知正在工作的实例。运行文件系统检查 (fsck -a /dev/...)。修正所有错误。从已知正在工作的实例断开卷。将卷连接到已停止的实例。启动实例。重新检查实例的状态。 |
| 实例存储支持的 | 请尝试以下任一操作： |

| 对于此实例类型 | 请执行此操作 |
|---------|--|
| | <ul style="list-style-type: none">启动新实例。(可选) 通过 AWS Support 寻求技术支持以便恢复数据。 |

VFS：无法在未知块上安装根 fs (根文件系统不匹配)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line: root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

潜在原因

| 实例类型 | 潜在原因 |
|-----------------|--|
| 由 Amazon EBS 支持 | <ul style="list-style-type: none">设备连接错误。根设备没有连接到正确的设备点。文件系统不是预期的格式。使用旧内核 (例如，2.6.16-XenU)。 |
| 实例存储支持的 | 硬件设备故障。 |

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下任一操作：</p> <ul style="list-style-type: none">停止实例，然后再重启。修改根卷以连接到正确的设备点，可能是 /dev/sda1，而不是 /dev/sda。停止并修改新内核。 |
| 实例存储支持的 | 终止实例并使用新内核启动新实例。 |

错误：无法确定根设备的主/次编号...(根文件系统/设备不匹配)

表示此条件的系统日志类似于下方显示的示例。

```
...
XENBUS: Device with no driver: device/vif/0
```

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

潜在原因

- 虚拟块储存设备驱动程序缺失或配置错误
- 设备枚举冲突 (sda 与 xvda , 或是 sda 而不是 sda1)
- DomU 内核选择错误

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 停止实例。2. 断开此卷。3. 修正设备映射问题。4. 启动实例。5. 修改 AMI 以解决设备映射问题。 |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 创建附有适当补丁程序的新 AMI (正确映射块储存设备)。2. 终止实例并从您创建的 AMI 中启动新实例。 |

XENBUS : 设备没有驱动程序...

表示此条件的系统日志类似于下方显示的示例。

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
```

```

Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#

```

潜在原因

- 虚拟块储存设备驱动程序缺失或配置错误
- 设备枚举冲突 (sda 与 xvda)
- DomU 内核选择错误

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none"> 1. 停止实例。 2. 断开此卷。 3. 修正设备映射问题。 4. 启动实例。 5. 修改 AMI 以解决设备映射问题。 |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none"> 1. 创建附有适当补丁程序的 AMI (正确映射块储存设备)。 2. 终止实例并使用您创建的 AMI 启动新实例。 |

... 没有检查时，已强制执行检查的工作日 (文件系统检 查要求)

表示此条件的系统日志类似于下方显示的示例。

```

...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced

```

潜在原因

文件系统检查时间已过；正在强制执行文件系统检查

建议采取的措施

- 耐心等候文件系统检查的完成。请注意，文件系统检查可能需要很长一段时间，具体取决于根文件系统的大小。
- 使用 tune2fs 或适合您的文件系统的工具修改文件系统，以去除强制执行文件系统检查 (fsck) 的功能。

fsck 卡在退出状态...(缺少设备)

表示此条件的系统日志类似于下方显示的示例。

```
Cleaning up ifupdown....  
Loading kernel modules...done.  
...  
Activating lvm and md swap...done.  
Checking file systems...fsck from util-linux-ng 2.16.2  
/sbin/fsck.xfs: /dev/sdh does not exist  
fsck died with exit status 8  
[31mfailed (code 8).[39;49m
```

潜在原因

- 为缺失的磁盘查找虚拟磁盘
- 强制执行文件系统一致性检查
- 磁盘故障或者已断开

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | 尝试以下一个或多个措施以解决此问题： <ul style="list-style-type: none">停止实例，将该卷连接到正在运行的实例。手动运行一致性检查。修正虚拟磁盘以使其包含相关实用程序。修改文件系统调整参数以删除一致性要求 (不推荐)。 |
| 实例存储支持的 | 尝试以下一个或多个措施以解决此问题： <ul style="list-style-type: none">通过正确的工具作业重新绑定虚拟磁盘。修改文件系统调整参数以删除一致性要求 (不推荐)。终止实例并启动新的实例。(可选) 通过 AWS Support 寻求技术支持以便恢复数据。 |

GRUB 提示 (grubdom>)

表示此条件的系统日志类似于下方显示的示例。

```
GNU GRUB version 0.97 (629760K lower / 0K upper memory)  
[ Minimal BASH-like line editing is supported. For  
the first word, TAB lists possible command  
completions. Anywhere else TAB lists the possible
```

```
completions of a device/filename. ]  
grubdom>
```

潜在原因

| 实例类型 | 潜在原因 |
|-----------------|---|
| 由 Amazon EBS 支持 | <ul style="list-style-type: none">缺少 GRUB 配置文件。使用了错误的 GRUB 映像，应使用不同位置的 GRUB 配置文件。使用了不受支持的文件系统存储您的 GRUB 配置文件 (例如，将您的根文件系统转换为 GRUB 早期版本不支持的类型)。 |
| 实例存储支持的 | <ul style="list-style-type: none">缺少 GRUB 配置文件。使用了错误的 GRUB 映像，应使用不同位置的 GRUB 配置文件。使用了不受支持的文件系统存储您的 GRUB 配置文件 (例如，将您的根文件系统转换为 GRUB 早期版本不支持的类型)。 |

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|--|
| 由 Amazon EBS 支持 | <p>选项 1：修改 AMI 并重启实例：</p> <ol style="list-style-type: none">修改源 AMI 以便在标准位置 (/boot/grub/menu.lst) 创建 GRUB 配置文件。验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。选择合适的 GRUB 映像 (hd0 – 第一个磁盘或 hd00 – 第一个磁盘，第一个分区)。终止实例并使用您创建的 AMI 启动新实例。 <p>选项 2：修正现有实例。：</p> <ol style="list-style-type: none">停止实例。断开根卷文件系统。将根卷文件系统连接到已知正在工作的实例。安装文件系统。创建 GRUB 配置文件。验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。断开文件系统。连接到原始实例。修改内核属性以便使用正确的 GRUB 映像 (第 1 个磁盘或其上的第 1 个分区)。启动实例。 |

| 对于此实例类型 | 请执行此操作 |
|---------|--|
| 实例存储支持的 | <p>选项 1：修改 AMI 并重启实例：</p> <ol style="list-style-type: none"> 使用位于标准位置 (<code>/boot/grub/menu.lst</code>) 的 GRUB 配置文件创建新 AMI。 选择合适的 GRUB 映像 (hd0 – 第一个磁盘或 hd00 – 第一个磁盘，第一个分区)。 验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。 终止实例并使用您创建的 AMI 启动新实例。 <p>选项 2：终止此实例并启动新实例，指定正确的内核。</p> <p>Note</p> <p>要从现有实例恢复数据，请联系 AWS Support。</p> |

提起接口 eth0：设备 eth0 的 MAC 地址与预期不同， 驳回。(硬编码的 MAC 地址)。

表示此条件的系统日志类似于下方显示的示例。

```
...
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring.
[FAILED]
Starting auditd: [ OK ]
```

潜在原因

AMI 配置中存在硬编码接口 MAC

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下任一操作：</p> <ul style="list-style-type: none"> 修改 AMI 以便删除硬编码和重启实例。 修改实例以删除硬编码 MAC 地址。 <p>或者</p> <p>执行以下步骤：</p> <ol style="list-style-type: none"> 停止实例。 断开根卷。 |

| 对于此实例类型 | 请执行此操作 |
|---------|---|
| | <ol style="list-style-type: none">3. 将卷附加到另一个实例并修改卷以删除硬编码的 MAC 地址。4. 将卷连接到原始实例。5. 启动实例。 |
| 实例存储支持的 | <p>执行以下任一操作：</p> <ul style="list-style-type: none">• 修改实例以删除硬编码 MAC 地址。• 终止实例并启动新的实例。 |

无法加载 SELinux 策略。计算机处于强制执行模式。正 在中断。(SELinux 配置错误)

表示此条件的系统日志类似于下方显示的示例。

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

潜在原因

SELinux 已在错误的情况下启动：

- GRUB 不支持所提供的内核
- 后备内核不存在

建议采取的措施

| 对于此实例类型 | 请执行此操作 |
|-----------------|---|
| 由 Amazon EBS 支持 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 停止失败的实例。2. 分离失败的实例的根卷。3. 将根卷连接到另一个 Linux 的运行实例 (之后称为“恢复实例”)。4. 连接到恢复实例并安装失败的实例的根卷。5. 在安装的根卷上禁用 SELinux。此过程因 Linux 分配而异；有关更多信息，请参阅特定于操作系统的文档。 <p>Note</p> <p>在某些系统上，可通过在 <code>/mount_point/etc/sysconfig/selinux</code> 文件中设置 <code>SELINUX=disabled</code> 来禁用 SELinux，其中 <code>mount_point</code> 是您在恢复实例上安装卷的位置。</p> <ol style="list-style-type: none">6. 从恢复实例卸载和分离根卷并将该根卷重新连接到原始实例。 |

| | |
|---------|---|
| 对于此实例类型 | 请执行此操作 |
| | 7. 启动实例。 |
| 实例存储支持的 | <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 终止实例并启动新的实例。2. (可选) 通过 AWS Support 寻求技术支持以便恢复数据。 |

XENBUS : 连接设备时超时 (Xenbus 超时)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1  
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007  
...  
XENBUS: Timeout connecting to devices!  
...  
Kernel panic - not syncing: No init found. Try passing init= option to kernel.
```

潜在原因

- 块储存设备未连接到实例
- 此实例使用非常陈旧的 DomU 内核

建议采取的措施

| | |
|-----------------|---|
| 对于此实例类型 | 请执行此操作 |
| 由 Amazon EBS 支持 | <p>执行以下任一操作：</p> <ul style="list-style-type: none">• 修改 AMI 和实例以便使用新内核并重启实例。• 重启实例。 |
| 实例存储支持的 | <p>执行以下任一操作：</p> <ul style="list-style-type: none">• 终止实例。• 修改 AMI 以使用新实例，使用此 AMI 启动新实例。 |

排查实例的容量问题

以下错误与实例容量有关。

错误 : InsufficientInstanceCapacity

如果您在尝试启动实例或启动已停止的实例时看到 `InsufficientInstanceCapacity` 错误，则表示 AWS 当前没有足够的可用容量来服务您的请求。尝试以下操作：

- 等待几分钟，然后再次提交您的请求；容量可能经常转移。

- 提交减少了实例数的新请求。例如，如果您要提交 1 个启动包含 15 个实例的请求，请改为尝试提交 3 个包含 5 个实例的请求或 15 个包含 1 个实例的请求。
- 如果您要启动实例，请提交新请求，无需指定可用区。
- 如果您要启动实例，请使用其他实例类型（可在后期调整大小）提交新请求。有关更多信息，请参阅 [调整您的实例大小 \(p. 156\)](#)。
- 尝试购买预留实例。预留实例是长期的容量预留。有关更多信息，请参阅：[Amazon EC2 预留实例](#)。

错误 : InstanceLimitExceeded

如果您在启动实例时看到 InstanceLimitExceeded 错误，这表示您已达到并行运行的实例数上限。对于新的 AWS 账户，默认限制为 20。如果需要更多运行实例，请填写[请求提高 Amazon EC2 实例限制](#)上的表单。

获取控制台输出和重启实例

控制台输出对于问题诊断是非常有价值的工具。它尤其适合用于排查内核问题和服务配置问题，它们可能会导致实例在 SSH 后台程序启动前终止或变得不可达到。

类似地，能够重启不可达到的实例对于故障排除和一般实例管理都很非常有用。

EC2 实例没有可供您查看控制台输出的物理显示器。它们还缺少允许您执行开启电源、重启或关闭等操作的物理控制系统。作为替代，您可以通过 Amazon EC2 API 和命令行界面 (CLI) 执行这些任务。

实例重启

就像可以通过按下重置按钮来重置计算机一样，您可以使用 Amazon EC2 控制台、CLI 或 API 来重置 EC2 实例。有关更多信息，请参阅 [重启您的实例 \(p. 265\)](#)。

Warning

对于 Windows 实例，此操作会强制执行重启，其结果可能会导致数据受损。

实例控制台输出

对于 Linux/Unix 实例，实例控制台输出显示了确切的控制台输出，在正常情况下，它们会显示在连接到计算机的物理显示器上。由于实例产生输出后将其发布到实例所有人可以检索到的位置，因此输出会被缓冲。

对于 Windows 实例，实例控制台输出显示了最近三个系统事件日志错误。

发布的输出不会持续更新；仅当它可能是最大值时。这包括实例启动、重启以及终止的不久后的值。

Note

仅保存最新发布的 64 KB 输出，可在最近一次发布后至少 1 小时都可以访问。

只有实例的所有人可以访问控制台输出。您可以使用控制台或命令行检索您的实例的控制台输出。

使用控制台获取控制台输出

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在左侧导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Instance Settings、Get System Log。

使用命令行获取控制台输出

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [get-console-output \(AWS CLI\)](#)
- [Get-EC2ConsoleOutput \(适用于 Windows PowerShell 的 AWS 工具\)](#)

有关常见的系统日志错误的更多信息，请参阅 [诊断基于 Linux 的实例的系统日志错误 \(p. 652\)](#)。

捕获无法访问的实例的屏幕截图

如果您无法通过 SSH 或 RDP 访问您的实例，您可以捕获实例的屏幕截图并将其作为图像查看。这可以让您了解实例的状态，更快地处理问题。

此屏幕截图不会产生数据传输费用。生成的图像为 JPG 格式，大小不超过 100kb。

访问实例控制台

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在左侧导航窗格中，选择 Instances。
3. 选择要捕获的实例。
4. 选择 Actions、Instance Settings。
5. 选择 Get Instance Screenshot。

右键单击图像，以下载并保存该图像。

使用命令行捕获屏幕截图

您可以使用以下任一命令。返回的内容采用 base64 编码。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [get-console-screenshot \(AWS CLI\)](#)
- [GetConsoleScreenshot \(Amazon EC2 查询 API\)](#)

主机发生故障时的实例恢复

如果底层主机上的硬件出现不可恢复性问题，AWS 可能会预定实例停止事件。我们会通过电子邮件提前通知您。

恢复发生故障的主机上运行的 Amazon EBS 支持的实例

1. 将您实例存储卷上的所有关键数据 Amazon EBS 或 Amazon S3。
2. 停止实例。
3. 启动实例。
4. 恢复所有重要数据。
5. [EC2-Classic] 如果实例有关联的弹性 IP 地址，您必须将其与实例重新关联。

有关更多信息，请参阅 [停止和启动您的实例 \(p. 263\)](#)。

恢复发生故障的主机上运行的实例存储支持的实例

1. 从该实例创建 AMI。

2. 将映像上传到 Amazon S3。
3. 将重要数据备份到 Amazon EBS 或 Amazon S3。
4. 终止实例。
5. 从 AMI 启动新实例。
6. 将所有重要数据恢复到新实例。
7. [EC2-Classic] 如果原始实例有关联的弹性 IP 地址，您必须将其与新实例相关联。

有关更多信息，请参阅 [创建由实例存储支持的 Linux AMI \(p. 78\)](#)。

正在从错误的卷启动我的实例

在某些情况下，您可能会发现某个并非挂载到 /dev/xvda 或 /dev/sda 的卷成为了您的实例的根卷。当您将另一个实例的根卷或从某个根卷的快照中创建的卷挂载到带有现有根卷的实例时，可能会发生这种情况。

这是由于 Linux 中的初始虚拟磁盘的工作方式导致的。它将选择在 /etc/fstab 中定义为 / 的卷，在某些分配（包括 Amazon Linux）中，这是由附加到卷分区的标签决定的。具体来说，您会发现您的 /etc/fstab 类似于以下内容：

```
LABEL=/ / ext4 defaults,noatime 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
```

并且，如果您检查两个卷的标签，您将看到它们都包含 / 标签：

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

在此示例中，您最终可以让 /dev/xvdf1（而不是您打算从中启动实例的 /dev/xvda1 卷）成为您的实例在初始虚拟磁盘运行后启动到的根设备。解决此问题相当简单；您可以使用相同的 e2label 命令更改您不想从中启动实例的挂载卷的标签。

Note

在某些情况下，在 /etc/fstab 中指定一个 UUID 可解决此问题，但是，如果两个卷都来自同一个快照，或者次要卷是从主要卷的快照中创建的，则它们将共享一个 UUID。

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

更改一个挂载卷的标签

1. 使用 e2label 命令将卷的标签更改为 / 之外的其他标签。

```
[ec2-user ~]$ sudo e2label /dev/xvdf1 old/
```

2. 验证卷是否有新标签。

```
[ec2-user ~]$ sudo e2label /dev/xvdf1  
old/
```

在进行此更改后，您应该能够重新启动实例并在实例启动时让初始虚拟磁盘选择适当的卷。

Important

如果您打算分离带有新标签的卷并将其返回给另一个实例以用作根卷，则必须再次执行上述步骤并将卷标签更改回其原来的值；否则，另一个实例将不能启动，因为虚拟磁盘将无法找到带有标签 / 的卷。

文档历史记录

下表介绍 Amazon EC2 文档的重要补充部分。我们还经常更新文档来处理您发送给我们的反馈意见。

当前 API 版本 : 2016-11-15。

| 功能 | API 版本 | 说明 | 发行日期 |
|--------------------------------|------------|---|------------------|
| 在创建过程中，为资源添加标签 | 2016-11-15 | 在创建过程中，您可以将标签应用于实例和卷。有关更多信息，请参阅 标记您的成员资源 (p. 626) 。此外，您可以使用基于标签的资源级权限来控制应用的标签。有关更多信息，请参阅 用于标记的资源级权限 (p. 396) 。 | 2017 年 3 月 28 日 |
| I3 实例 | 2016-11-15 | I3 实例是下一代存储优化型实例。有关更多信息，请参阅 存储优化型实例 (p. 146) 。 | 2017 年 2 月 23 日 |
| 对附加的 EBS 卷执行修改。 | 2016-11-15 | 对于附加到大多数 EC2 实例的大多数 EBS 卷，您可以在不分离卷或不停止实例的情况下修改卷大小、类型和 IOPS。有关更多信息，请参阅 在 Linux 上修改 EBS 卷的大小、IOPS 或类型 (p. 543) 。 | 2017 年 2 月 13 日 |
| 附加一个 IAM 角色 | 2016-11-15 | 您可以为现有实例连接、分离或替换 IAM 角色。有关更多信息，请参阅 适用于 Amazon EC2 的 IAM 角色 (p. 422) 。 | 2017 年 2 月 9 日 |
| 专用竞价型实例 | 2016-11-15 | 您可在 Virtual Private Cloud (VPC) 中的单租户硬件上运行竞价型实例。有关更多信息，请参阅 指定竞价型实例租赁 (p. 197) 。 | 2017 年 1 月 19 日 |
| IPv6 支持 | 2016-11-15 | 您可以将一个 IPv6 CIDR 与 VPC 和子网关联，并为 VPC 中的实例分配 IPv6 地址。有关更多信息，请参阅 Amazon EC2 实例 IP 寻址 (p. 453) 。 | 2016 年 12 月 1 日 |
| R4 实例 | 2016-09-15 | R4 实例是下一代内存优化型实例。R4 实例非常适合内存密集型、延迟敏感型工作负载，例如商业智能 (BI)、数据挖掘和分析、内存中数据库、分布式 Web 级内存缓存，以及非结构化大数据的应用程序性能实时处理。有关更多信息，请参阅 内存优化型实例 (p. 144) 。 | 2016 年 11 月 30 日 |
| 新的 t2.xlarge 和 t2.2xlarge 实例类型 | 2016-09-15 | T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本 | 2016 年 11 月 30 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|--|------------|---|-----------------|
| | | 要求的应用程序。有关更多信息，请参阅 T2 实例 (p. 139) 。 | |
| P2 实例 | 2016-09-15 | P2 实例使用 NVIDIA Tesla GPU K80 和适用于使用 CUDA 和 OpenCL 编程模型的通用 GPU 计算设计。有关更多信息，请参阅 Linux 加速计算实例 (p. 150) 。 | 2016 年 9 月 9 日 |
| m4.16xlarge 实例 | 2016-04-01 | 引入具有 64 个 vCPU 和 256GiB RAM 的 m4.16xlarge 实例，扩展了通用 M4 系列的范围。 | 2016 年 6 月 9 日 |
| 竞价型队列的自动扩展 | | 现在，您可以在竞价型队列设置扩展策略。有关更多信息，请参阅 竞价型队列的自动扩展 (p. 218) 。 | 2016 年 9 月 1 日 |
| Elastic Network Adapter (ENA) | 2016-04-01 | 您现在可以将 ENA 用于增强网络。有关更多信息，请参阅 增强联网类型 (p. 492) 。 | 2016 年 6 月 28 日 |
| 增强了对查看和修改较长 ID 的支持 | 2016-04-01 | 您现在可以查看和修改其他 IAM 用户、IAM 角色或根用户的较长 ID 设置。有关更多信息，请参阅 资源 ID (p. 620) 。 | 2016 年 6 月 23 日 |
| 在 AWS 账户之间复制加密的 Amazon EBS 快照 | 2016-04-01 | 您现在可以在 AWS 账户之间复制加密的 EBS 快照。有关更多信息，请参阅 复制 Amazon EBS 快照 (p. 561) 。 | 2016 年 6 月 21 日 |
| 捕获实例控制台的屏幕截图 | 2015-10-01 | 您现在可以在调试无法访问的实例时获取其他信息。有关更多信息，请参阅 捕获无法访问的实例的屏幕截图 (p. 672) 。 | 2016 年 24 月 5 日 |
| X1 实例 | 2015-10-01 | 专为正在运行的内存中数据库、大数据处理引擎和高性能计算 (HPC) 应用程序设计的内存优化的实例。有关更多信息，请参阅 内存优化型实例 (p. 144) 。 | 2016 年 18 月 5 日 |
| 两种新的 EBS 卷类型 | 2015-10-01 | 您现在可以创建经过吞吐量优化的 HDD (st1) 以及冷数据 HDD (sc1) 卷。有关更多信息，请参阅 Amazon EBS 卷类型 (p. 519) 。 | 2016 年 4 月 19 日 |
| 添加了针对 Amazon EC2 的新的 NetworkPacketsIn 和 NetworkPacketsOut 指标 | | 添加了针对 Amazon EC2 的新的 NetworkPacketsIn 和 NetworkPacketsOut 指标。有关更多信息，请参阅 实例指标 (p. 322) 。 | 2016 年 3 月 23 日 |
| 竞价型队列的 CloudWatch 指标 | | 您现在可以获取竞价型队列的 CloudWatch 指标。有关更多信息，请参阅 竞价型队列的 CloudWatch 指标 (p. 216) 。 | 2016 年 3 月 21 日 |
| 计划实例 | 2015-10-01 | 利用计划的预留实例 (计划实例)，您可以购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的容量预留。有关更多信息，请参阅 计划的预留实例 (p. 184) 。 | 2016 年 1 月 13 日 |
| 较长的资源 ID | 2015-10-01 | 我们将逐步引入某些 Amazon EC2 和 Amazon EBS 资源类型的更长 ID。在选择周期内，您可以为支持的资源类型启用较长 ID 格式。有关更多信息，请参阅 资源 ID (p. 620) 。 | 2016 年 1 月 13 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|--------------------------|------------|---|------------------|
| ClassicLink DNS 支持 | 2015-10-01 | 您可以对您的 VPC 启用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例和 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。有关更多信息，请参阅 启用 ClassicLink DNS 支持 (p. 441) 。 | 2016 年 1 月 11 日 |
| 新 t2.nano 实例类型 | 2015-10-01 | T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅 T2 实例 (p. 139) 。 | 2015 年 12 月 15 日 |
| 专用主机 | 2015-10-01 | Amazon EC2 专用主机是指实例容量供您专用的物理服务器。有关更多信息，请参阅 专用主机 (p. 227) 。 | 2015 年 11 月 23 日 |
| 竞价型实例持续时间 | 2015-10-01 | 现在，您可以为竞价型实例指定持续时间。有关更多信息，请参阅 指定竞价型实例的持续时间 (p. 197) 。 | 2015 年 10 月 6 日 |
| 竞价型队列修改请求 | 2015-10-01 | 您现在可以修改竞价型队列请求的目标容量。有关更多信息，请参阅 修改竞价型队列请求 (p. 208) 。 | 2015 年 9 月 29 日 |
| 竞价型队列多样化分配策略 | 2015-04-15 | 您现在可以使用单个竞价型队列请求在多个竞价池中分配竞价型实例。有关更多信息，请参阅 竞价型队列分配策略 (p. 192) 。 | 2015 年 9 月 15 日 |
| 竞价型队列实例权重 | 2015-04-15 | 您现在可以定义每个实例类型对应应用程序性能贡献的容量单位，并相应地为每个竞价池调整出价。有关更多信息，请参阅 竞价型队列实例权重 (p. 192) 。 | 2015 年 8 月 31 日 |
| 新的重启警报操作和用于警报操作的新 IAM 角色 | | 增加了重启警报操作和与警报操作一起使用的新 IAM 角色。有关更多信息，请参阅 创建停止、终止、重启或恢复实例的警报 (p. 332) 。 | 2015 年 7 月 23 日 |
| 新 t2.large 实例类型 | | T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅 T2 实例 (p. 139) 。 | 2015 年 6 月 16 日 |
| M4 实例 | | 实现了计算、内存和网络资源平衡的下一代通用型实例。M4 实例由带 AVX2 的自定义 Intel 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器支持。 | 2015 年 6 月 11 日 |
| 竞价型队列 | 2015-04-15 | 您可以管理竞价型实例的集合或队列，而不必管理单独的竞价型实例请求。有关更多信息，请参阅 竞价型队列的工作方式 (p. 191) 。 | 2015 年 5 月 18 日 |
| 将弹性 IP 地址迁移至 EC2-Classic | 2015-04-15 | 您可将分配为在 EC2-Classic 平台中使用的弹性 IP 地址迁移至 EC2-VPC 平台。有关更多信息，请参阅 将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 469) 。 | 2015 年 5 月 15 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|-----------------------|------------|--|-----------------|
| 将具有多个磁盘的 VM 作为 AMI 导入 | 2015-03-01 | VM Import 过程现在支持将具有多个磁盘的 VM 作为 AMI 导入。有关更多信息，请参阅 VM Import/Export 用户指南 中的 使用 VM Import/Export 将 VM 导入为映像 。 | 2015 年 4 月 23 日 |
| 新 g2.8xlarge 实例类型 | | 新 g2.8xlarge 实例受四种高性能 NVIDIA GPU 支持，非常适合 GPU 计算工作负载，包括大规模呈现、转码、机器学习以及其他需要大规模并行处理能力的服务器端工作负载。 | 2015 年 4 月 7 日 |
| D2 实例 | | <p>新一代 Amazon EC2 密集存储实例，经过优化，适用于需要顺序访问直接连接实例存储上大量数据的应用程序。D2 实例适合在密集存储系列中提供最佳性价比。由 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器提供支持，通过提供额外的计算能力、更多内存和增强联网功能，HS1 上的 D2 实例得到了极大改进。此外，D2 实例有四种实例大小可供选择，存储容量分别是 6TB、12TB、24TB 和 48TB。</p> <p>有关更多信息，请参阅 存储优化型实例 (p. 146)。</p> | 2015 年 3 月 24 日 |
| EC2 实例的自动恢复 | | <p>您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。恢复的实例与原始实例相同，包括实例 ID、IP 地址以及所有实例元数据。</p> <p>有关更多信息，请参阅 恢复您的实例 (p. 272)。</p> | 2015 年 1 月 12 日 |
| C4 实例 | | <p>新一代计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C4 实例基于自定义 2.9 GHz Intel® Xeon® E5-2666 v3 (Haswell) 处理器。C4 实例采用睿频加速技术，单核或双核经睿频加速后，处理器时钟频率可高达 3.5Ghz。C4 实例扩展自 C3 计算优化型实例的功能，可为客户在 EC2 实例中提供最高的处理器性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体力学。</p> <p>有关更多信息，请参阅 计算优化型实例 (p. 141)。</p> | 2015 年 1 月 11 日 |
| ClassicLink | 2014-10-01 | 您可使用 ClassicLink 将 EC2-Classic 实例链接到您账户中的 VPC。您可以将 VPC 安全组与 EC2-Classic 实例相关联，以便允许 EC2-Classic 实例与 VPC 中的实例使用私有 IP 地址进行通信。有关更多信息，请参阅 ClassicLink (p. 436) 。 | 2015 年 1 月 7 日 |
| 竞价型实例终止通知 | | <p>防范竞价型实例中断的最佳方法是为应用程序设计容错能力。此外，您还可以利用竞价型实例终止通知，该通知可在 Amazon EC2 必须终止您的竞价型实例时，提前两分钟发出警告。</p> <p>有关更多信息，请参阅 竞价型实例终止通知 (p. 224)。</p> | 2015 年 1 月 5 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|------------------------------------|------------|--|------------------|
| DescribeVolumes 分页支持 | 2014-09-01 | DescribeVolumes API 调用现在可使用 MaxResults 和 NextToken 参数支持结果分页。有关详细信息，请参阅 Amazon EC2 API Reference 中的 DescribeVolumes 。 | 2014 年 10 月 23 日 |
| T2 实例 | 2014-06-15 | T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅 T2 实例 (p. 139) 。 | 2014 年 6 月 30 日 |
| 新 EC2 Service Limits (EC2 服务限制) 页面 | | 使用 Amazon EC2 控制台中的 EC2 Service Limits (EC2 服务限制) 页面可按区域查看 Amazon EC2 和 Amazon VPC 提供的资源的当前限制。 | 2014 年 6 月 19 日 |
| Amazon EBS 通用型 SSD 卷 | 2014-05-01 | 通用型 SSD 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷的延迟通常不超过十毫秒，能突增至 3000 IOPS 很长时间，基本性能为 3 IOPS/GiB。通用型 SSD 卷的大小范围是 1 GiB 到 1 TiB。有关更多信息，请参阅 通用型 SSD (gp2) 卷 (p. 521) 。 | 2014 年 6 月 16 日 |
| Amazon EBS 加密 | 2014-05-01 | Amazon EBS 加密 提供 EBS 数据卷和快照的无缝加密，无需构建和维护安全密钥管理基础设施。通过使用 Amazon 托管密钥加密数据，EBS 加密可保护静态数据的安全。加密还发生在托管 EC2 实例的服务器上，当数据在 EC2 实例和 EBS 存储之间移动时提供数据加密。有关更多信息，请参阅 Amazon EBS Encryption (p. 568) 。 | 2014 年 5 月 21 日 |
| R3 实例 | 2014-02-01 | 新一代内存优化型实例具有最佳的每 GiB RAM 价格点和高性能。这些实例十分适合于关系数据库和 NoSQL 数据库、内存分析解决方案、科学计算以及其他可受益于 R3 实例的 vCPU 高内存、高计算性能和增强的联网功能的内存密集型应用程序。 有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2014 年 4 月 9 日 |
| 新 Amazon Linux AMI 版本 | | Amazon Linux AMI 2014.03 发布。 | 2014 年 3 月 27 日 |
| Amazon EC2 使用率报告 | | Amazon EC2 使用率报告是一组显示 EC2 的成本和使用率数据的报告。有关更多信息，请参阅 Amazon EC2 使用率报告 (p. 633) 。 | 2014 年 1 月 28 日 |
| 额外 M3 实例 | 2013-10-15 | 现在支持 M3 实例大小 m3.medium 和 m3.large。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2014 年 1 月 20 日 |
| I2 实例 | 2013-10-15 | 这些实例提供极高的 IOPS，并在 Linux 实例上支持 TRIM，可实现更好的 SSD 连续写入性能。I2 实例还支持增强型联网，从而减小实例间延迟、降低网络抖动，显著提高每秒数据包(PPS) 性能。有关更多信息，请参阅 存储优化型实例 (p. 146) 。 | 2013 年 12 月 19 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|-------------------------|------------|--|------------------|
| 更新了 M3 实例 | 2013-10-15 | M3 实例大小、 <code>m3.xlarge</code> 和 <code>m3.2xlarge</code> 现在支持具有 SSD 卷的实例存储。 | 2013 年 12 月 19 日 |
| 导入 Linux 虚拟机 | 2013-10-15 | VM Import 过程现在支持 Linux 实例的导入。有关更多信息，请参阅 VM Import/Export 用户指南 。 | 2013 年 12 月 16 日 |
| RunInstances 的资源级别权限 | 2013-10-15 | 您现在可以在 AWS Identity and Access Management 中创建策略以控制 Amazon EC2 RunInstances API 操作的资源级别权限。有关更多信息以及示例策略，请参阅 控制对 Amazon EC2 资源的访问 (p. 366) 。 | 2013 年 11 月 20 日 |
| C3 实例 | 2013-10-15 | 计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C3 实例还支持增强型联网，这种联网可减小实例间延迟、降低网络抖动并显著提高每秒数据包 (PPS) 性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体动力学。 有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2013 年 11 月 14 日 |
| 从 AWS Marketplace 启动实例 | | 您现在可以使用 Amazon EC2 启动向导从 AWS Marketplace 启动实例。有关更多信息，请参阅 启动 AWS Marketplace 实例 (p. 250) 。 | 2013 年 11 月 11 日 |
| G2 实例 | 2013-10-01 | 这些实例十分适用于视频创建服务、3D 可视化、流式处理图形密集型应用程序以及需要大规模并行处理能力的其他服务器端工作负载。有关更多信息，请参阅 Linux 加速计算实例 (p. 150) 。 | 2013 年 11 月 4 日 |
| 新启动向导 | | 提供一个重新设计的新的 EC2 启动向导。有关更多信息，请参阅 启动实例 (p. 244) 。 | 2013 年 10 月 10 日 |
| 修改 Amazon EC2 预留实例的实例类型 | 2013-10-01 | 您现在可以修改同一系列 (例如 M1、M2、M3、C1) 中 Linux 预留实例的实例类型。有关更多信息，请参阅 修改您的标准预留实例 (p. 178) 。 | 2013 年 10 月 09 日 |
| 新 Amazon Linux AMI 版本 | | Amazon Linux AMI 2013.09 发布。 | 2013 年 9 月 30 日 |
| 修改 Amazon EC2 预留实例 | 2013-08-15 | 您现在可以修改区域中的预留实例。有关详细信息，请参阅 修改您的标准预留实例 (p. 178) 。 | 2013 年 9 月 11 日 |
| 分配公有 IP 地址 | 2013-07-15 | 在 VPC 中启动实例时，现在可以分配公有 IP 地址。有关更多信息，请参阅 在实例启动期间分配公有 IPv4 地址 (p. 458) 。 | 2013 年 8 月 20 日 |
| 授予资源级别权限 | 2013-06-15 | Amazon EC2 支持新的 Amazon 资源名称 (ARN) 和条件键。有关更多信息，请参阅 Amazon EC2 的 IAM 策略 (p. 368) 。 | 2013 年 7 月 8 日 |
| 增量快照副本 | 2013-02-01 | 您现在可以执行增量快照副本。有关更多信息，请参阅 复制 Amazon EBS 快照 (p. 561) 。 | 2013 年 6 月 11 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|---------------------------------|-----------------|--|------------------|
| 新 Tags (标签) 页面 | | Amazon EC2 控制台中提供一个新的 Tags (标签) 页面。有关更多信息，请参阅 标记 Amazon EC2 资源 (p. 626) 。 | 2013 年 4 月 4 日 |
| 新 Amazon Linux AMI 版本 | | Amazon Linux AMI 2013.03 发布。 | 2013 年 3 月 27 日 |
| EBS 优化的额外实例类型 | 2013-02-01 | <p>以下实例类型现在可作为 EBS 优化的实例启动：<code>c1.xlarge</code>、<code>m2.2xlarge</code>、<code>m3.xlarge</code> 和 <code>m3.2xlarge</code>。</p> <p>有关更多信息，请参阅 Amazon EBS 优化实例 (p. 564)。</p> | 2013 年 3 月 19 日 |
| 将 AMI 从一个区域复制到另一个区域 | 2013-02-01 | <p>您可以将 AMI 从一个区域复制到另一个区域，以便快速轻松地在多个 AWS 区域启动一致的实例。</p> <p>有关更多信息，请参阅 复制 AMI (p. 117)。</p> | 2013 年 3 月 11 日 |
| 在默认 VPC 中启动实例 | 2013-02-01 | <p>您的 AWS 账户可以将实例启动为 EC2-Classic 或 EC2-VPC 平台，也可以根据各区域间的差异仅仅启动为 EC2-VPC 平台。如果您只能将实例启动为 EC2-VPC，我们会为您创建一个默认 VPC。当您启动实例时，我们会将其启动为默认 VPC，除非您创建了非默认 VPC 并在启动实例时对其进行指定。</p> <p>有关更多信息，请参阅 支持的平台 (p. 435)。</p> | 2013 年 3 月 11 日 |
| 内存增强型群集 (cr1.8xlarge) 实例类型 | 2012-12-01 | 拥有大量内存以及增强的 CPU 和网络性能。这些实例非常适合用于内存分析、图形分析和科学计算应用。 | 2013 年 1 月 21 日 |
| 高存储 (hs1.8xlarge) 实例类型 | 2012-12-01 | 高存储实例为每个实例提供非常高的存储密度以及读取和写入的高连续性。他们非常适合用于数据仓库、Hadoop/MapReduce 和并行文件系统。 | 2012 年 12 月 20 日 |
| EBS 快照副本 | 2012-12-01 | 您可以使用快照备份创建数据备份、创建新 Amazon EBS 卷，或创建 Amazon 系统映像 (AMI)。有关更多信息，请参阅 复制 Amazon EBS 快照 (p. 561) 。 | 2012 年 12 月 17 日 |
| 已更新 预配置 IOPS SSD 卷的 EBS 指标和状态检查 | 2012-10-01 | 已更新 EBS 指标，以便包含 预配置 IOPS SSD 卷的两项新指标。有关更多信息，请参阅 使用 CloudWatch 监控卷 (p. 534) 。还添加了 预配置 IOPS SSD 卷的新状态检查。有关更多信息，请参阅 使用状态检查来监控卷 (p. 536) 。 | 2012 年 11 月 20 日 |
| Linux 内核 | | 已更新了 AKI ID；已重组了分配内核；已更新了 PVOps 部分。 | 2012 年 11 月 13 日 |
| M3 实例 | 2012 年 10 月 1 日 | 提供新的 M3 超大型和 M3 双倍超大型实例类型。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2012 年 10 月 31 日 |
| 竞价型实例请求状态 | 2012-10-01 | 竞价型实例请求状态简化了确定您的竞价请求状态的过程。 | 2012 年 10 月 14 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|-------------------------------------|------------|--|------------------|
| 新 Amazon Linux AMI 版本 | | Amazon Linux AMI 2012.09 发布。 | 2012 年 10 月 11 日 |
| Amazon EC2 预留实例市场 | 2012-08-15 | 预留实例市场 将想要出售不再需要的 Amazon EC2 预留实例的卖方与正在寻找购买额外容量的买方匹配起来。通过 预留实例市场 购买和出售的预留实例与其他预留实例一样工作，不同的是他们受标准条款限制更少，并能以不同价格出售。 | 2012 年 9 月 11 日 |
| 适用于 Amazon EBS 的预配置 IOPS SSD | 2012-07-20 | 预配置 IOPS SSD 卷为 I/O 密集型工作负载，如依赖于稳定和快速响应时间的数据库应用程序，提供可预测、高性能的服务。有关更多信息，请参阅 Amazon EBS 卷类型 (p. 519) 。 | 2012 年 7 月 31 日 |
| 适用于 Amazon EC2 的高 I/O 实例 | 2012-06-15 | 高 I/O 实例通过使用基于 SSD 的本地实例存储提供低延时、高性能的磁盘 I/O。 | 2012 年 7 月 18 日 |
| IAM 对 Amazon EC2 实例的作用 | 2012-06-01 | 适用于 Amazon EC2 实例的 IAM 角色提供： <ul style="list-style-type: none"> 在 Amazon EC2 实例上运行的应用程序的 AWS 访问密钥。 Amazon EC2 实例上的 AWS 访问密钥的自动交替。 为 Amazon EC2 实例上请求 AWS 服务的运行应用程序细调权限。 | 2012 年 6 月 11 日 |
| 让启动和处理中断可能性变得更加容易的竞价型实例功能 | | 现在您可以按照以下方式管理您的竞价型实例： <ul style="list-style-type: none"> 使用 Auto Scaling 启动配置为竞价型实例竞价，并为竞价型实例的竞价设置日程表。有关更多信息，请参阅 Auto Scaling 用户指南 中的在 Auto Scaling 组中启动竞价型实例。 实例启动或终止时获得通知。 在 AWS 资源堆栈中使用 AWS CloudFormation 模板来启动竞价型实例。 | 2012 年 6 月 7 日 |
| 用于 Amazon EC2 状态检查的 EC2 实例导出和时间戳 | 2012-05-01 | 已添加将您原先导入到 EC2 的 Windows Server 实例导出的支持。 已添加对实例状态和系统状态时间戳的支持，该戳记显示状态检查失败的日期和时间。 | 2012 年 5 月 25 日 |
| Amazon VPC 实例和系统状态检查中的 EC2 实例导出和时间戳 | 2012-05-01 | 已添加将实例导出至 Citrix Xen、Microsoft Hyper-V 和 VMware vSphere 的支持。 已添加多实例和系统状态检查中的时间戳的支持。 | 2012 年 5 月 25 日 |
| 八倍超大型群集计算 | 2012-04-01 | 添加了对 VPC 中的 cc2.8xlarge 实例的支持。 | 2012 年 4 月 26 日 |
| AWS Marketplace AMIs | 2012-04-01 | 已添加对 AWS Marketplace AMIs 的支持。 | 2012 年 4 月 19 日 |
| 新 Linux AMI 版本 | | Amazon Linux AMI 2012.03 发布。 | 2012 年 3 月 28 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|--|------------|---|------------------|
| 新 AKI 版本 | | 我们发布了 AKI 版本 1.03 和适用于 AWS GovCloud (US) 区域的 AKI。 | 2012 年 3 月 28 日 |
| 中型实例、所有 AMI 上 64 位的支持和基于 Java 的 SSH 客户端 | 2011-12-15 | 已添加一种新的实例类型和 64 位信息的支持。添加了使用基于 Java 的 SSH 客户端连接到 Linux 实例的过程。 | 2012 年 3 月 7 日 |
| 预留实例定价套餐 | 2011-12-15 | 增加了新的一节来讨论如何充分利用预留实例定价套餐自带的折扣价格。 | 2012 年 3 月 5 日 |
| Amazon Virtual Private Cloud 中的适用于 EC2 实例的 Elastic Network Interfaces (ENIs) | 2011-12-01 | 已添加有关 VPC 中 适用于 EC2 实例的 Elastic Network Interfaces (ENIs) 的新章节。有关更多信息，请参阅 弹性网络接口 (p. 473) 。 | 2011 年 12 月 21 日 |
| 新 GRU 区域和 AKI | | 已添加适用于 SA-East-1 区域的新 AKI 版本的有关信息。此版本弃用了 AKI 版本 1.01。AKI 版本 1.02 将继续向后兼容。 | 2011 年 12 月 14 日 |
| Amazon EC2 预留实例的新产品类型 | 2011-11-01 | 您可以选择各种各样的预留实例产品，以满足您对实例的预期使用要求。 | 2011 年 12 月 1 日 |
| Amazon EC2 实例状态 | 2011-11-01 | 您可以查看您的实例状态的其他详细信息，包括 AWS 计划的可能会影响您的实例的事件。这些操作活动包括，执行软件更新和安全性补丁程序所要求的实例重启，和出现硬件问题时所需的实例停止。有关更多信息，请参阅 监控实例状态 (p. 313) 。 | 2011 年 11 月 16 日 |
| Amazon EC2 群集计算实例类型 | | Amazon EC2 八倍超大型群集计算 (cc2.8xlarge) 的补充支持。 | 2011 年 11 月 14 日 |
| 新 PDX 区域和 AKI | | 增加了适用于新 US-West 2 区域的新 AKI 版本的有关信息。 | 2011 年 11 月 8 日 |
| Amazon VPC 中的竞价型实例 | 2011-07-15 | 添加了 Amazon VPC 中的竞价型实例支持的有关信息。通过此更新，用户可以在 Virtual Private Cloud (VPC) 中启动竞价型实例。通过在 VPC 中启动竞价型实例，竞价型实例的用户可以享用 Amazon VPC 的优势。 | 2011 年 10 月 11 日 |
| 新 Linux AMI 版本 | | 已添加 Amazon Linux AMI 2011.09 版本的有关信息。此次更新消除了来自 Amazon Linux AMI 的 Beta 标记，支持将存储库锁定到一个特定版本的功能，并在已安装软件包可更新时（包括安全性更新），为您提供更新通知。 | 2011 年 9 月 26 日 |
| 适用于 CLI 工具用户的简化的 VM import 程序 | 2011-07-15 | <code>ImportInstance</code> 和 <code>ImportVolume</code> 的增强功能简化了 VM Import 过程；现在，创建导入任务后，系统会将映像上传到 Amazon EC2 上。此外，通过引入 <code>ResumeImport</code> ，用户可以从任务停止的时间点重新开始未完成的上传。 | 2011 年 9 月 15 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|--|------------|---|-----------------|
| 导入 VHD 文件格式的支持 | | VM Import 现在可导入 VHD 格式的虚拟机图像文件。VHD 文件格式与 Citrix Xen 和 Microsoft Hyper-V 虚拟化平台兼容。通过这种新产品，VM Import 现在支持 RAW、VHD 和 VMDK (与 VMware ESX 兼容的) 图像格式。有关更多信息，请参阅 VM Import/Export 用户指南 。 | 2011 年 8 月 24 日 |
| 更新至适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器 | | 适用于 VMware vCenter 虚拟设备 (连接器) 的 1.1 版本的 Amazon EC2 VM Import 连接器的有关补充信息。此次更新包括访问因特网的代理支持、更好的错误处理方法、任务进度栏准确性的提高以及一些 bug 修复。 | 2011 年 6 月 27 日 |
| 让 Linux AMI 运行用户提供的内核 | | 已添加 AKI 版本从 1.01 升级到 1.02 的相关信息。此版本更新了 PVGRUB，以解决与 t1.micro Linux 实例相关的启动失败问题。有关更多信息，请参阅 用户提供的内核 (p. 129) 。 | 2011 年 6 月 20 日 |
| 竞价型实例可用区定价更改 | 2011-05-15 | 添加了竞价型实例可用区定价功能的有关信息。在本版本中，我们添加了新的可用区定价选项，当您查询竞价型实例请求和现货价格历史记录时，返回的信息中包括这些新的定价选项。通过这些新增功能，可以更方便地确定将竞价型实例启动到特定可用区所需的价格。 | 2011 年 5 月 26 日 |
| AWS Identity and Access Management | | 已添加 AWS Identity and Access Management (IAM) 的有关信息，使用户可以指定借助 Amazon EC2 资源一般能使用哪些 Amazon EC2 功能。有关更多信息，请参阅 控制对 Amazon EC2 资源的访问 (p. 366) 。 | 2011 年 4 月 26 日 |
| 让 Linux AMI 运行用户提供的内核 | | 已添加让 Linux AMI 使用 PVGRUB Amazon Kernel Image (AKI) 来运行用户提供的内核的有关信息。有关更多信息，请参阅 用户提供的内核 (p. 129) 。 | 2011 年 4 月 26 日 |
| 专用实例 | | 专用实例是在 Amazon Virtual Private Cloud (Amazon VPC) 中启动的，是在主机硬件层次上物理隔离的实例。专用实例让您能享用 Amazon VPC 和 AWS 云的好处，包括按需弹性配置、仅为实际用量付费等，但同时也在硬件层次上隔离您的 Amazon EC2 计算实例。有关更多信息，请参阅 专用实例 (p. 237) 。 | 2011 年 3 月 27 日 |
| 预留实例更新至 AWS 管理控制台 | | 更新至 AWS 管理控制台让用户查看他们的预留实例以及购买额外预留实例，包括专用预留实例，变得更加简单。有关更多信息，请参阅 预留实例 (p. 161) 。 | 2011 年 3 月 27 日 |
| 新 Amazon Linux 参考 AMI | | 新的 Amazon Linux 参考 AMI 替代了 CentOS 参考 AMI。已删除 CentOS 参考 AMI 的有关信息，包含题为“Correcting Clock Drift for Cluster Instances on CentOS 5.4 AMI”的章节。有关更多信息，请参阅 加速计算实例的 AMI (p. 151) 。 | 2011 年 3 月 15 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|---|------------|---|------------------|
| 元数据信息 | 2011-01-01 | 已添加元数据的有关信息，将反映 2011-01-01 版本中的更改。有关更多信息，请参阅 实例元数据和用户数据 (p. 295) 和 实例元数据类别 (p. 302) 。 | 2011 年 3 月 11 日 |
| 适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器。 | | 已添加适用于 VMware vCenter 虚拟设备 (连接器) 的 Amazon EC2 VM Import Connector 的有关信息。这个连接器是一个用于 VMware vCenter 的插件，集成了 VMware vSphere 客户端，并提供了一个图形用户界面，您可以用它来将 VMware 虚拟机导入到 Amazon EC2 中。 | 2011 年 3 月 3 日 |
| 实施卷分离 | | 您现在可以使用 AWS 管理控制台来实施把一个 Amazon EBS 卷从一个实例中分离出来。有关更多信息，请参阅 从实例断开 Amazon EBS 卷 (p. 541) 。 | 2011 年 2 月 23 日 |
| 实例终止保护 | | 您现在可以使用 AWS 管理控制台来防止实例终止。有关更多信息，请参阅 为实例启用终止保护 (p. 268) 。 | 2011 年 2 月 23 日 |
| 校正 Amazon's CentOS 5.4 AMI 上的群集实例的 Clock Drift | | 已添加如何为 Amazon's CentOS 5.4 AMI 上的群集实例校正 Clock Drift 的有关信息。 | 2011 年 1 月 25 日 |
| VM Import | 2010-11-15 | 已添加有关 VM Import 的信息，允许您将虚拟机或卷导入到 Amazon EC2 中。有关更多信息，请参阅 VM Import/Export 用户指南 。 | 2010 年 12 月 15 日 |
| 实例的基本监控 | 2010-08-31 | 已添加有关 EC2 实例的基本监控的信息。 | 2010 年 12 月 12 日 |
| 群集 GPU 实例 | 2010-08-31 | Amazon EC2 为高性能计算 (HPC) 应用程序提供了 GPU 群集实例(cg1.4xlarge)。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2010 年 11 月 14 日 |
| 筛选条件和标记 | 2010-08-31 | 已添加列举、筛选和标记资源的有关信息。有关更多信息，请参阅 列出并筛选您的资源 (p. 623) 和 标记 Amazon EC2 资源 (p. 626) 。 | 2010 年 9 月 19 日 |
| 幂等实例启动 | 2010-08-31 | 已添加关于确保实例运行时的幂等性的信息。有关更多信息，请参阅 Amazon EC2 API Reference 中的 确保幂等性 。 | 2010 年 9 月 19 日 |
| 微型实例 | 2010-06-15 | Amazon EC2 为特定类型的应用程序提供 t1.micro 实例类型。有关更多信息，请参阅 T1 微型实例 (p. 154) 。 | 2010 年 9 月 8 日 |
| 适用于 Amazon EC2 的 AWS Identity and Access Management | | Amazon EC2 现在集成了 AWS Identity and Access Management (IAM)。有关更多信息，请参阅 控制对 Amazon EC2 资源的访问 (p. 366) 。 | 2010 年 9 月 2 日 |
| 群集实例 | 2010-06-15 | Amazon EC2 为您的高性能计算 (HPC) 应用程序提供了群集计算实例。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2010 年 7 月 12 日 |

| 功能 | API 版本 | 说明 | 发行日期 |
|--|------------|---|-----------------|
| Amazon VPC IP 地址指定 | 2010-06-15 | Amazon VPC 用户现在可以指定用于分配在 VPC 中启动的实例的 IP 地址。 | 2010 年 7 月 12 日 |
| 适用于 Amazon EBS 卷 Amazon CloudWatch 监控 | | Amazon CloudWatch 监控现在对 Amazon EBS 卷自动可用。有关更多信息，请参阅 使用 CloudWatch 监控卷 (p. 534) 。 | 2010 年 6 月 14 日 |
| 内存增强型超大型实例 | 2009-11-30 | Amazon EC2 现在支持内存增强型超大型 (m2.xlarge) 实例类型。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 Amazon EC2 实例 。 | 2010 年 2 月 22 日 |

AWS 词汇表

有关最新 AWS 术语，请参阅 AWS General Reference 中的 [AWS 词汇表](#)。