
Amazon Elastic Compute Cloud

用户指南（适用于 Linux 实例）



Amazon Elastic Compute Cloud: 用户指南 (适用于 Linux 实例)

Copyright © 2020 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
区域、可用区和本地区域	6
区域、可用区和本地区域概念	6
可用区	8
区域和终端节点	9
描述您的区域、可用区和本地区域	9
为资源指定区域	11
选择加入本地区域	12
在可用区或本地区域中启动实例	12
将实例迁移到其他可用区	12
根设备卷	13
根设备存储概念	13
根据根设备类型选择 AMI	14
确定实例的根设备类型	15
将根设备卷更改为持久保留	15
设置	18
注册 AWS	18
创建 IAM 用户	18
创建密钥对	19
创建 Virtual Private Cloud (VPC)	21
创建安全组	22
开始使用	24
概述	24
先决条件	25
步骤 1 : 启动实例	25
步骤 2 : 连接到您的实例	26
步骤 3 : 清除您的实例	26
后续步骤	26
最佳实践	27
教程	28
安装 LAMP 服务器 (Amazon Linux 2)	28
步骤 1 : 准备 LAMP 服务器	28
步骤 2 : 测试 LAMP 服务器	32
步骤 3 : 确保数据库服务器的安全	33
步骤 4 : (可选) 安装 phpMyAdmin	34
故障排除	37
相关主题	37
安装 LAMP 服务器 (Amazon Linux AMI)	37
步骤 1 : 准备 LAMP 服务器	38
步骤 2 : 测试 LAMP 服务器	41
步骤 3 : 确保数据库服务器的安全	43
步骤 4 : (可选) 安装 phpMyAdmin	44
故障排除	46
相关主题	47
教程 : 托管 WordPress 博客	47

先决条件	48
安装 WordPress	48
后续步骤	53
帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪	54
教程：在 Amazon Linux 2 上配置 SSL/TLS	54
先决条件	55
步骤 1：在服务器上启用 TLS	55
步骤 2：获取 CA 签名的证书	57
步骤 3：测试和强化安全配置	61
故障排除	63
证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用	64
教程：在 Amazon Linux 上配置 SSL/TLS	67
先决条件	68
步骤 1：在服务器上启用 TLS	68
步骤 2：获取 CA 签名的证书	70
步骤 3：测试和强化安全配置	74
故障排除	76
证书自动化：在 Amazon Linux 上将 Let's Encrypt 与 Certbot 结合使用	76
教程：提高应用程序的可用性	79
先决条件	80
对应用程序进行扩展和负载均衡	80
测试负载均衡器	81
Amazon 系统映像	83
使用 AMI	83
创建您自己的 AMI	83
购买、共享和出售 AMI	84
取消注册您的 AMI	84
Amazon Linux 2 和 Amazon Linux AMI	84
AMI 类型	84
启动许可	84
根设备存储	85
虚拟化类型	87
查找 Linux AMI	88
使用 Amazon EC2 控制台查找 Linux AMI	88
使用 AWS CLI 查找 AMI	89
查找快速启动 AMI	89
共享 AMI	90
查找共享 AMI	90
将 AMI 设为公用	92
将 AMI 与特定 AWS 账户共享	93
使用书签	95
共享 Linux AMI 指导原则	95
付费 AMI	99
出售 AMI	99
查找付费 AMI	99
购买付费 AMI	100
获取实例的产品代码	101
使用付费支持	101
付费和支持 AMI 的账单	101
管理 AWS Marketplace 订阅	101
创建 Amazon EBS 支持的 Linux AMI	102
创建 Amazon EBS 支持的 AMIs 的概述	102
从实例创建 Linux AMI	103
从快照创建 Linux AMI	104
创建由实例存储支持的 Linux AMI	105
由实例存储支持的 AMI 的创建过程概述	105
先决条件	105

设置 AMI 工具	106
通过实例存储支持的 实例创建 AMI	108
转换为 Amazon EBS 支持的 AMI	115
AMI 工具参考	118
将加密与 EBS 支持的 AMI 结合使用	134
启动实例场景	134
映像复制场景	137
复制 AMI	138
复制实例存储支持的 AMI 的权限	138
跨区域复制	139
跨账户复制	140
加密和复制	140
复制 AMI	141
停止待处理的 AMI 复制操作	142
取消注册您的 Linux AMI	142
清除由 Amazon EBS 支持的 AMI	143
清除由实例存储支持的 AMI	143
Amazon Linux	144
连接到 Amazon Linux 实例	145
识别 Amazon Linux 映像	145
AWS 命令行工具	146
程序包存储库	147
Extras 库 (Amazon Linux 2)	149
访问源软件包获取参考信息	149
cloud-init	149
订阅 Amazon Linux 通知	151
作为本地虚拟机运行 Amazon Linux 2	151
用户提供的内核	154
HVM AMIs (GRUB)	154
半虚拟化 AMIs (PV-GRUB)	155
实例	160
实例类型	160
可用实例类型	161
硬件规格	163
AMI 虚拟化类型	163
基于 Nitro 的实例	163
联网和存储功能	164
实例限制	166
通用实例	166
计算优化型实例	202
内存优化型实例	207
存储优化型实例	215
加速计算实例	222
查找实例类型	232
更改实例类型	233
获得推荐	237
实例购买选项	239
确定实例生命周期	240
按需实例	240
预留实例	243
计划实例	274
Spot 实例	277
专用主机	333
专用实例	356
按需容量预留	360
实例生命周期	370
实例启动	372

实例停止和启动 (仅限 Amazon EBS 支持的实例)	372
实例休眠 (仅限 Amazon EBS 支持的实例)	372
实例重启	372
实例停用	373
实例终止	373
重启、停止、休眠与终止之间的区别	373
启动	374
连接	423
停止和启动	445
休眠	447
重启	456
停用	456
终止	458
恢复	463
配置实例	464
常见配置方案	464
管理软件	465
管理用户	469
处理器状态控制	471
设置时间	476
优化 CPU 选项	480
更改主机名	490
设置动态 DNS	493
启动时运行命令	494
实例元数据和用户数据	499
Elastic Inference	522
识别实例	523
检查实例标识文档	523
检查系统 UUID	523
监控	525
自动和手动监控	525
自动监控工具	526
手动监控工具	526
监控的最佳实践	527
监控实例状态	527
实例状态检查	528
计划的事件	532
使用 CloudWatch 监控您的实例	538
启用详细监控	538
列出可用指标	539
获取指标的实例	547
绘制指标图形	554
创建警报	554
创建停止、终止、重启或恢复实例的警报	555
使用 CloudWatch Events 实现 Amazon EC2 的自动化	563
监控内存和磁盘指标	563
CloudWatch 代理	563
CloudWatch 监控脚本	563
使用 AWS CloudTrail 记录 API 调用	570
CloudTrail 中的 Amazon EC2 和 Amazon EBS 信息	570
了解 Amazon EC2 和 Amazon EBS 日志文件条目	571
审核通过 EC2 Instance Connect 连接的用户	572
网络功能	574
实例 IP 寻址	574
私有 IPv4 地址和内部 DNS 主机名	574
公有 IPv4 地址和外部 DNS 主机名	575
弹性 IP 地址 (IPv4)	576

Amazon DNS 服务器	576
IPv6 地址	576
使用实例的 IP 地址	576
多个 IP 地址	580
自带 IP 地址	587
要求	587
准备将您的地址范围引入您的 AWS 账户	587
预配置地址范围以用于 AWS	589
通过 AWS 公布地址范围	589
取消预配置地址范围	590
弹性 IP 地址	590
弹性 IP 地址基础信息	590
使用弹性 IP 地址	591
将反向 DNS 用于电子邮件应用程序	595
弹性 IP 地址限额	595
网络接口	595
网络接口基本知识	596
每个实例类型的每个网络接口的 IP 地址	596
网络接口的使用场景	605
网络接口最佳配置实践	606
使用网络接口	608
请求者托管的网络接口	615
增强联网	616
增强联网类型	616
在实例上启用增强联网	617
增强联网 : ENA	617
增强联网 : Intel 82599 VF	628
ENA 问题排查	633
Elastic Fabric Adapter	638
EFA 基础知识	639
支持的接口和库	640
支持的实例类型	640
支持 AMI	640
EFA 限制	640
EFA 和 MPI 入门	640
EFA 和 NCCL 入门	645
使用 EFA	658
监控 EFA	661
置放群组	662
集群置放群组	662
分区置放群组	663
分布置放群组	663
置放群组规则和限制	664
创建置放群组	665
在置放群组中启动实例	665
描述置放群组中的实例	666
更改实例的置放群组	667
删除置放群组	668
网络 MTU	669
巨型帧 (9001 MTU)	669
路径 MTU 发现	669
查看两个主机之间的路径 MTU	670
在您的 Linux 实例上检查并设置 MTU	670
故障排除	671
Virtual Private Cloud	671
Amazon VPC 文档	671
EC2-Classic	672

检测受支持的平台	672
EC2-Classic 中可用的实例类型	673
EC2-Classic 和 VPC 中的实例之间的区别	673
在 EC2-Classic 与 VPC 之间共享和访问资源	677
ClassicLink	678
从 EC2-Classic 迁移到 VPC	689
安全性	699
基础设施安全	699
网络隔离	699
物理主机上的隔离	700
控制网络流量	700
恢复功能	700
数据保护	701
静态加密	701
传输中加密	701
Identity and Access Management	701
网络访问您的实例	702
Amazon EC2 权限属性	702
IAM 和 Amazon EC2	702
IAM 策略	704
IAM 角色	749
网络访问	757
密钥对	759
使用 Amazon EC2 创建密钥对	760
将您自己的公有密钥导入 Amazon EC2	761
在 Linux 上检索密钥对的公有密钥	762
在 Windows 上检索密钥对的公有密钥	763
从实例检索密钥对的公有密钥	763
验证您的密钥对指纹	763
删除您的密钥对	764
添加或替换实例的密钥对	764
丢失私有密钥时连接到 Linux 实例	765
安全组	768
安全组规则	769
默认安全组	770
自定义安全组	771
使用安全组	771
安全组规则引用	775
更新管理	780
合规性验证	780
存储	781
Amazon EBS	782
Amazon EBS 的功能	782
EBS 卷	783
EBS 快照	812
EBS 数据服务	841
EBS 卷和 NVMe	860
EBS 优化	863
EBS 性能	875
EBS CloudWatch 指标	889
EBS CloudWatch Events	893
实例存储	903
实例存储生命周期	904
实例存储卷	904
添加实例存储卷	909
SSD 实例存储卷	912
实例存储交换卷	913

优化磁盘性能	915
文件存储	916
Amazon EFS	916
Amazon FSx	919
Amazon S3	919
Amazon S3 和 Amazon EC2	920
实例卷限制	921
特定于 Linux 的卷限制	921
特定于 Windows 的卷限制	921
实例类型限制	921
带宽与容量	922
设备命名	922
可用设备名称	922
设备名称注意事项	923
块储存设备映射	923
块储存设备映射的概念	924
AMI 块储存设备映射	926
实例块储存设备映射	928
资源和标签	932
资源位置	932
资源 ID	933
使用较长的 ID	934
控制对较长 ID 设置的访问	937
列出并筛选您的资源	937
高级搜索	938
使用控制台列出资源	939
使用控制台筛选资源	939
使用 CLI 和 API 列出并筛选	940
标记资源	940
有关标签的基本知识	941
标记资源	942
标签限制	944
标记资源以便于计费	944
通过控制台使用标签	945
通过 CLI 或 API 使用标签	948
服务限制	950
查看您的当前限制	950
申请提高限制	951
对使用端口 25 发送的电子邮件的限制	951
使用率报告	951
故障排除	953
排查启动问题	953
超出实例限制	953
实例容量不足	953
实例立即终止	954
连接到您的实例	955
连接到您的实例时出错：连接超时	955
错误：无法加载密钥...预期：任何私有密钥	957
错误：服务器无法识别用户密钥	957
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	958
错误：未保护的私钥文件	959
错误：私有密钥的格式必须以“----BEGIN RSA PRIVATE KEY----”开头，以“----END RSA PRIVATE KEY----”结尾	960
错误：服务器拒绝我们的密钥或 没有支持的身份验证方法	960
无法使用我的浏览器进行连接	961
无法对实例执行 Ping 操作	961
错误：服务器意外关闭了网络连接	961

停止实例	961
创建替代实例	961
终止实例	963
延迟的实例终止	963
已终止实例仍然显示	963
自动启动或终止实例	963
故障状态检查	963
查看状态检查信息	964
检索系统日志	964
诊断基于 Linux 的实例的系统日志错误	965
内存不足：终止进程	965
错误：mmu_update 失败（内存管理更新失败）	966
I/O 错误（块储存设备故障）	967
I/O 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）	968
request_module：runaway loop modprobe（在较旧的 Linux 版本上循环旧内核 modprobe）	968
“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）	969
“FATAL: Could not load /lib/modules”或者“BusyBox”（内核模块缺失）	970
ERROR：无效内核（EC2 不兼容内核）	971
fsck：尝试打开时没有找到此文件或目录...（未找到文件系统）	972
挂载文件系统时出现一般性错误（挂载失败）	973
VFS：无法在未知块上挂载根 fs（根文件系统不匹配）	975
错误：无法确定根设备的主/次编号...（根文件系统/设备不匹配）	976
XENBUS：设备没有驱动程序	976
... 没有检查时，已强制执行检查的工作日（文件系统检查要求）	977
fsck 卡在退出状态...（设备缺失）	978
GRUB 提示（grubdom>）	979
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）。	980
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）	981
XENBUS：连接设备时超时（Xenbus 超时）	982
对无法访问的实例进行故障排除	983
实例重启	983
实例控制台输出	983
捕获无法访问的实例的屏幕截图	984
主机发生故障时的实例恢复	985
正在从错误的卷启动	985
EC2Rescue for Linux	986
安装 EC2Rescue for Linux	987
(可选) 验证 EC2Rescue for Linux 的签名	987
使用 EC2Rescue for Linux	989
开发 EC2Rescue 模块	991
发送诊断中断	995
支持的实例类型	996
先决条件	996
发送诊断中断	998
文档历史记录	999

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 [Web 托管](#)。

如何开始使用 Amazon EC2

首先，您应进行设置以使用 Amazon EC2。设置完毕后，您便基本上完成了 Amazon EC2 入门教程。如果需要有关 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 \(p. 18\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 24\)](#)

基础知识

- [实例和 AMI \(p. 4\)](#)
- [区域和可用区 \(p. 6\)](#)

- [实例类型 \(p. 160\)](#)
- [标签 \(p. 940\)](#)

网络和安全性

- [Amazon EC2 密钥对 \(p. 759\)](#)
- [安全组 \(p. 768\)](#)
- [弹性 IP 地址 \(p. 590\)](#)
- [Amazon EC2 和 Amazon VPC \(p. 671\)](#)

存储

- [Amazon EBS \(p. 782\)](#)
- [实例存储 \(p. 903\)](#)

使用 Linux 实例

- AWS Systems Manager 用户指南 中的 [AWS Systems Manager Run Command](#)
- 教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 28)
- 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 54)
- 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：

- [Amazon EC2 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](#)。

要自动完成操作，例如在每次新的 Amazon EC2 实例启动时激活 Lambda 函数，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 命令的更多信息，请参阅 AWS CLI Command 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 PowerShell 的 AWS 工具 Cmdlet 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 [操作](#)。

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 和工具](#)。

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

您只需要按秒支付使用实例的费用，无需长期购买或预付款。

Savings Plans

可以通过承诺在 1 年或 3 年期限内保持一致的使用量（以美元/小时为单位）来降低您的 Amazon EC2 成本。

预留实例

可以通过承诺在 1 年或 3 年期限内提供特定的实例配置（包括实例类型和区域）来降低您的 Amazon EC2 成本。

Spot 实例

请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。

有关 Amazon EC2 的费用和价格的完整列表，请参阅 [Amazon EC2 定价](#)。

要计算示例预置环境的成本，请参阅 [云成本中心](#)。

若要查看您的账单，请转到 [AWS Billing and Cost Management 控制台](#) 中的 Billing and Cost Management Dashboard (账单和成本管理控制面板)。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](#)。

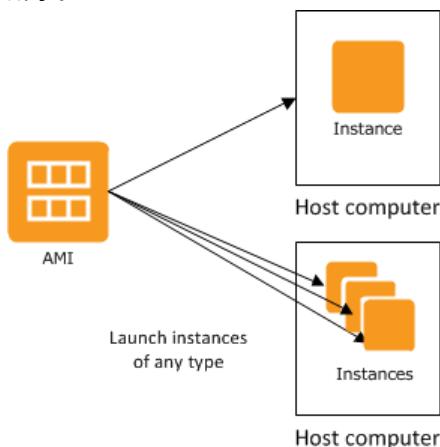
Trusted Advisor 可帮助您优化成本、安全性和您的 AWS 环境性能，有关其概述，请参阅 [AWS Trusted Advisor](#)。

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

实例是云中的虚拟服务器。启动时的实例配置是您在启动实例时指定的 AMI 的副本。

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 实例类型](#)。

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 运行需要根权限的命令。

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 \(p. 13\)](#)。

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 \(p. 923\)](#)。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。为保证重要数据的安全，应对多个实例使用复制策略，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 \(p. 781\)](#)。

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凭证并控制他们对 AWS 中资源和服务的访问权限。有关更多信息，请参阅[适用于 Amazon EC2 的 Identity and Access Management \(p. 701\)](#)。
- 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 \(p. 768\)](#)。
- 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 \(p. 96\)](#)。有关安全共享 AMI 的更多信息，请参阅[共享 AMI \(p. 90\)](#)。

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使用费用。而每次从停止状态过渡到运行状态时，都需要支付一个最低一分钟费用。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。根设备卷在默认情况下会被删除，但任何附加的 Amazon EBS 卷在默认情况下会被保留，这由每个卷的 `deleteOnTermination` 属性设置确定。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 \(p. 370\)](#)。

AMI

Amazon Web Services (AWS) 发布了许多包含常见软件配置的 [Amazon 系统映像 \(AMI\) \(p. 88\)](#) 供公众使用。此外，AWS 开发人员社区的会员也发布了他们的自定义 AMI。您也可以创建一个或多个自定义 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 \(p. 85\)](#)。

区域、可用区和本地区域

Amazon EC2 托管在全球多个位置。这些位置由区域、可用区和本地区域构成。每个区域都是一个单独的地理区域。每个区域均有多个相互隔离的位置，称为可用区。本地区域让您可以在多个离最终用户较近的位置放置资源（如计算和存储）。除非您特意选择这样做，否则资源不会跨区域复制。

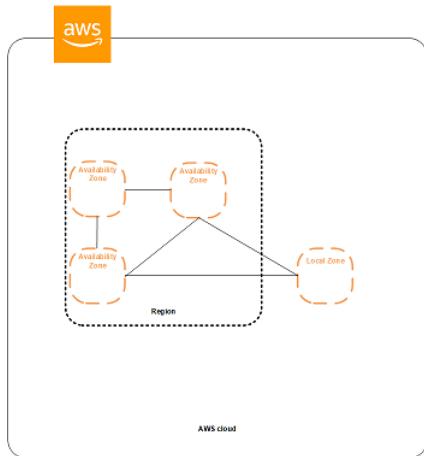
Amazon 运行着具有高可用性的先进数据中心。数据中心有时会发生影响托管于同一位置的所有实例的可用性的故障，虽然这种故障极少发生。如果您将所有实例都托管在受故障影响的同一个位置，则您的所有实例都将不可用。

目录

- 区域、可用区和本地区域概念 (p. 6)
- 可用区 (p. 8)
- 区域和终端节点 (p. 9)
- 描述您的区域、可用区和本地区域 (p. 9)
- 为资源指定区域 (p. 11)
- 选择加入本地区域 (p. 12)
- 在可用区或本地区域中启动实例 (p. 12)
- 将实例迁移到其他可用区 (p. 12)

区域、可用区和本地区域概念

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。本地区域是一种 AWS 基础设施部署，可将所选服务放在离最终用户较近的位置。本地区域是位于与您所在区域不同位置的区域的延伸。它为 AWS 基础设施提供了高带宽主干，非常适用于对延迟敏感的应用程序，例如机器学习。下图阐明了区域、可用区和本地区域之间的关系。



Amazon EC2 资源是以下类别之一：全局、与区域、可用区或本地区域相关联。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。

区域

从设计而言，每个 Amazon EC2 区域都与其他 Amazon EC2 区域隔离。这可实现最大程度的容错能力和稳定性。

当您查看资源时，只会看到与您指定的区域关联的资源。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。

当您启动某个实例时，必须选择位于同一区域的 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 \(p. 138\)](#)。

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 \(p. 590\)](#)。

可用区由区域代码后跟一个字母标识符表示；例如，us-east-1a。为确保资源分配到某个区域的各个可用区，我们将可用区独立映射到每个 AWS 账户的名称。例如，您的 AWS 账户的可用区 us-east-1a 可能与另一 AWS 账户的 us-east-1a 不在同一位置。

要跨账户协调可用区，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，use1-az1 是 us-east-1 区域的 AZ ID，它在每个 AWS 账户中的位置均相同。

通过查看 AZ ID，您可以确定一个账户中的资源相对于另一个账户中的资源所在的位置。例如，如果您在 AZ ID 为 use-az2 的可用区中与另一个账户共享一个子网，则在 AZ ID 也为 use-az2 的可用区中该账户便可使用这一子网。每个 VPC 和子网的 AZ ID 均显示在 Amazon VPC 控制台中。有关更多信息，请参阅Amazon VPC 用户指南中的[使用 VPC 共享](#)。

随着可用区域中内容的增加，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账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、可用区和本地区域 \(p. 9\)](#)。

本地区域

启动实例时，您可以选择本地区域，以便应用程序离最终用户较近。

本地区域允许您通过相同的 API 和工具集无缝连接到 AWS 区域中的所有服务（例如 Amazon Simple Storage Service 和 Amazon DynamoDB）。

本地区域并非在每个区域中均可用。有关支持本地区域的区域的信息，请参阅[the section called “可用区” \(p. 8\)](#)。

本地区域由区域代码后跟一个指示位置的标识符表示，例如 us-west-2-lax-1a。

要使用本地区域，您必须首先选择加入。有关更多信息，请参阅[the section called “选择加入本地区域” \(p. 12\)](#)。

选择加入本地区域后，您可以在本地区域中启动以下任何资源：

- Amazon Virtual Private Cloud 子网
- Amazon EC2 实例
- Amazon EBS 卷
- Amazon FSx 文件服务器
- 应用程序负载均衡器

您可以列出您的账户可用的本地区域。有关更多信息，请参阅 [描述您的区域、可用区和本地区域 \(p. 9\)](#)。

通过使用位于本地区域中的 Internet 网关来连接到公共 Internet。此配置为客户提供了本地传入和传出流量，这有助于减少延迟。

本地区域还支持连接到 AWS Direct Connect，允许客户通过专有网络连接路由其流量。

可用区

您的账户确定了适用于您的区域。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。
- AWS GovCloud (美国西部) 账户只能访问 AWS GovCloud (美国西部) 区域。有关更多信息，请参阅[AWS GovCloud \(美国西部 \) 区域](#)。
- 您只能通过 Amazon AWS (中国) 账户访问 北京和宁夏 区域。有关更多信息，请参阅[AWS 中国](#)。

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 (美国西部) 或中国区域。要使用 2019 年 3 月 20 日之后推出的区域，您必须启用区域。有关更多信息，请参阅 AWS General Reference 中的 [管理 AWS 区域](#)。

代码	名称	选择加入状态	本地区域
us-east-2	美国东部 (俄亥俄州)	可选	否
us-east-1	美国东部 (弗吉尼亚北部)	可选	否
us-west-1	美国西部 (加利福尼亚北部)	可选	否
us-west-2	美国西部 (俄勒冈)	可选	是 - us-west-2-lax-1a 您必须选择加入本地区域。
ap-east-1	亚太地区 (香港)	必需	否
ap-south-1	亚太地区 (孟买)	可选	否
ap-northeast-3	亚太区域 (大阪当地)	可选	否
ap-northeast-2	亚太区域 (首尔)	可选	否
ap-southeast-1	亚太区域 (新加坡)	可选	否

代码	名称	选择加入状态	本地区域
ap-southeast-2	亚太区域 (悉尼)	可选	否
ap-northeast-1	亚太区域 (东京)	可选	否
ca-central-1	加拿大 (中部)	可选	否
eu-central-1	欧洲 (法兰克福)	可选	否
eu-west-1	欧洲 (爱尔兰)	可选	否
eu-west-2	欧洲 (伦敦)	可选	否
eu-west-3	欧洲 (巴黎)	可选	否
eu-north-1	欧洲 (斯德哥尔摩)	可选	否
me-south-1	中东 (巴林)	必需	否
sa-east-1	南美洲 (圣保罗)	可选	否

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 账户的不同而异。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、可用区和本地区域 \(p. 9\)](#)。

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，必须指定其区域终端节点。有关 Amazon EC2 的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 (美国西部) 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 \(美国西部 \) 终端节点](#)。

描述您的区域、可用区和本地区域

您可以使用 Amazon EC2 控制台或命令行界面来确定适用于您账户的区域、可用区和本地区域。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、可用区和本地区域

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. 在导航窗格上，选择 EC2 Dashboard。
4. 可用区和本地区域在服务运行状况、可用区状态下列出。

使用 AWS CLI 查找您的区域、可用区和本地区域

1. 使用如下 [describe-regions](#) 命令描述为您的账户启用的区域。

```
aws ec2 describe-regions
```

要描述所有区域（包括为账户禁用的任何区域），请添加 `--all-regions` 选项，如下所示。

```
aws ec2 describe-regions --all-regions
```

2. 使用如下 [describe-availability-zones](#) 命令描述指定区域内的可用区和本地区域。

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

3. 使用如下 [describe-availability-zones](#) 命令描述可用区和本地区域，而不管选择加入状态。

```
aws ec2 describe-availability-zones --all-availability-zones
```

使用适用于 Windows PowerShell 的 AWS 工具 查找您的区域、可用区和本地区域

1. 使用如下 [Get-EC2Region](#) 命令描述适用于您的账户的区域。

```
PS C:\> Get-EC2Region
```

2. 使用如下 [Get-EC2AvailabilityZone](#) 命令描述指定区域内的可用区。

```
PS C:\> 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行为资源指定区域。

Note

部分 AWS 资源可能并非在所有区域、可用区和本地区域都可用。在特定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-east-2.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-east-2`。

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

选择加入本地区域

在为资源或服务指定本地区域之前，必须选择加入本地区域。

要选择加入本地区域，请转到 [AWS 本地区域](#) 站点，然后提出请求。

在可用区或本地区域中启动实例

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。

通过在本地区域中启动实例，您可以在最终用户附近运行延迟敏感型应用程序，同时享受 AWS 基础设施的优势。

当您启动实例时，可以选择指定您所用区域中的可用区或本地区域。如果您未指定可用区或本地区域，我们将为您选择一个可用区。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。

将实例迁移到其他可用区

如有必要，您可以将实例从一个可用区迁移到另一个可用区。例如，假设您正在尝试修改实例的实例类型，但我们无法在当前可用区中启动新实例类型的实例。在这种情况下，您可以将实例迁移到我们能够在其中启动该实例类型的可用区。

迁移过程包括：

- 从原始实例创建 AMI
- 在新可用区中启动实例
- 更新新实例的配置，如以下过程所示

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 \(p. 102\)](#)
 - [创建由实例存储支持的 Linux AMI \(p. 105\)](#)
 - [创建 Amazon EBS 支持的 Windows AMI](#)
2. 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中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 [在可用区或本地区域中启动实例 \(p. 12\)](#)。
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 \(p. 593\)](#)。
5. 如果原始实例是 Reserved Instance，请更改预留的可用区。（如果还更改了实例类型，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 \(p. 269\)](#)。
- 6.（可选）终止原始实例。有关更多信息，请参阅 [终止实例 \(p. 459\)](#)。

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 AMI，因为它们启动速度更快，而且采用了持久性存储。

有关 Amazon EC2 用于您的根卷的设备名称的更多信息，请参阅[Linux 实例上的设备命名 \(p. 922\)](#)。

主题

- [根设备存储概念 \(p. 13\)](#)
- [根据根设备类型选择 AMI \(p. 14\)](#)
- [确定实例的根设备类型 \(p. 15\)](#)
- [将根设备卷更改为持久保留 \(p. 15\)](#)

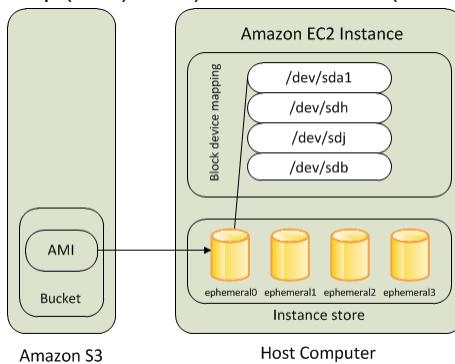
根设备存储概念

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 \(p. 85\)](#)。

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。

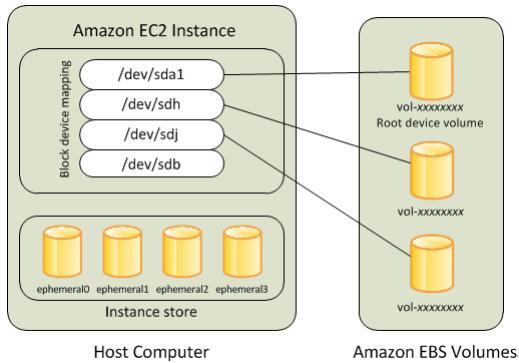


由实例存储支持的实例失败或终止后，该实例不能被恢复。如果您打算使用由 Amazon EC2 实例存储支持的实例，我们强烈建议您将数据跨多个可用区分配到实例存储中。您还应该定期将您的实例存储卷上的关键数据备份至持久性存储。

有关更多信息，请参阅[Amazon EC2 实例存储 \(p. 903\)](#)。

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，附加的卷中存储的数据不会受影响。当由 Amazon EBS 支持的实例处于停止状态时，您可以执行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、更改其大小或更新其使用的内核，或者您可以将您的根卷挂载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 \(p. 102\)](#)。
- 通过以下步骤将卷附加到一个新实例：
 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 卷重新附加到新实例。

有关更多信息，请参阅 [Amazon EBS 卷 \(p. 783\)](#)。

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 (公用映像)）。在“Search (搜索)”栏中选择 Platform (平台) 选择操作系统（例如 Amazon Linux），单击 Root Device Type (根设备类型) 选择 EBS images (EBS 映像)。
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（公用映像））。在“Search (搜索)”栏中选择 Platform (平台) 选择操作系统（例如 Amazon Linux），单击 Root Device Type (根设备类型) 选择 Instance store (实例存储)。
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. 检查描述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。您可以更改默认行为来确保卷在实例终止后保留。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。

主题

- [将根卷配置为在实例启动期间保留 \(p. 15\)](#)
- [配置根卷以便为正在运行的实例保留 \(p. 16\)](#)
- [确认已将根卷配置为保留 \(p. 17\)](#)

将根卷配置为在实例启动期间保留

可以将根卷配置为在使用 Amazon EC2 控制台或命令行工具启动实例时保留。

将根卷配置为在使用控制台启动实例时保留

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

2. 在导航窗格中，选择 Instances (实例)，然后选择 Launch Instance (启动实例)。
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. 完成其余向导页面上的操作，然后选择 Launch。

将根卷配置为在使用 AWS CLI 启动实例时保留

使用 [run-instances](#) 命令，并包含将 DeleteOnTermination 属性设置为 false 的块储存设备映射。

```
$ 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  
    }  
  }  
]
```

将根卷配置为在使用 Windows PowerShell 工具 启动实例时保留

使用 [New-EC2Instance](#) 命令，并包含将 DeleteOnTermination 属性设置为 false 的块储存设备映射。

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice  
C:\> $ebs.DeleteOnTermination = $false  
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping  
C:\> $bdm.DeviceName = "dev/xvda"  
C:\> $bdm.Ebs = $ebs  
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping $bdm ...other  
parameters...
```

配置根卷以便为正在运行的实例保留

配置根卷以便仅为使用命令行工具运行的实例保留。

配置根卷以便为使用 AWS CLI 运行的实例保留

使用 [modify-instance-attribute](#) 命令，并包含将 DeleteOnTermination 属性设置为 false 的块储存设备映射。

```
$ aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-  
mappings "[{\\"DeviceName\\": \"/dev/xvda\", \"Ebs\":{\\\"DeleteOnTermination\\\":true}}]"
```

配置根卷以便为使用适用于 Windows PowerShell 的 AWS 工具 运行的实例保留

使用 [Edit-EC2InstanceAttribute](#) 命令，并包含将 DeleteOnTermination 属性设置为 false 的块储存设备映射。

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification  
C:\> $ebs.DeleteOnTermination = $false
```

```
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping $bdm
```

确认已将根卷配置为保留

可以使用 Amazon EC2 控制台或命令行工具确认已将根卷配置为保留。

使用 Amazon EC2 控制台确认已将根卷配置为保留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)，然后选择实例。
3. 在 Description (描述) 选项卡中，选择 Root device (根设备) 的条目。如果将 Delete on termination (终止时删除) 设置为 false，则卷将配置为保留。

使用 AWS CLI 确认已将根卷配置为保留

使用 `describe-instances` 命令，并确认 `BlockDeviceMappings` 响应元素中的 `DeleteOnTermination` 属性设置为 `false`。

```
$ aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

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

使用适用于 Windows PowerShell 的 AWS 工具 确认已将根卷配置为保留

使用 `Get-EC2Instance` 命令，并确认 `BlockDeviceMappings` 响应元素中的 `DeleteOnTermination` 属性设置为 `false`。

```
C:\> (Get-EC2Instance -InstanceId i-i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

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 , 选择启动实例 , 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 \(p. 18\)](#)
2. [创建 IAM 用户 \(p. 18\)](#)
3. [创建密钥对 \(p. 19\)](#)
4. [创建 Virtual Private Cloud \(VPC\) \(p. 21\)](#)
5. [创建安全组 \(p. 22\)](#)

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://portal.aws.amazon.com/billing/signup>。
2. 按照屏幕上的说明进行操作。

在注册时 , 您将接到一通电话 , 要求您使用电话键盘输入一个验证码。

请记下您的 AWS 账号 , 因为在下一个任务中您会用到它。

创建 IAM 用户

AWS 中的服务 (例如 Amazon EC2) 要求您在访问时提供凭证 , 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。不过 , 我们不建议您使用 AWS 账户的证书访问 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 用户的凭证访问 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。

自行创建管理员用户并将该用户添加到管理员组 (控制台)

1. 使用 AWS 账户电子邮件地址和密码 , 以 [AWS 账户根用户](#) 身份登录到 IAM 控制台 (<https://console.aws.amazon.com/iam/>)。

Note

强烈建议您遵守以下使用 **Administrator** IAM 用户的最佳实践 , 妥善保存根用户凭证。只在执行少数[账户和服务管理任务](#) 时才作为根用户登录。

2. 在导航窗格中，选择用户，然后选择添加用户。
3. 对于 User name (用户名)，输入 **Administrator**。
4. 选中 AWS 管理控制台访问 旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. (可选) 默认情况下，AWS 要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in (用户必须在下次登录时创建新密码) 旁边的复选框以允许新用户在登录后重置其密码。
6. 选择下一步：权限。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group (创建组) 对话框中，对于 Group name (组名称)，输入 **Administrators**。
10. 选择 Filter policies (筛选策略)，然后选择 AWS managed-job function (AWS 托管的工作职能) 以筛选表内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group (创建组)。

Note

您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 AdministratorAccess 权限访问 AWS Billing and Cost Management 控制台。为此，请按照“[向账单控制台委派访问权限](#)”教程第 1 步中的说明进行操作。

12. 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 以便在列表中查看该组。
13. 选择下一步：标签。
14. (可选) 通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南 中的[标记 IAM 实体](#)。
15. 选择 Next: Review (下一步: 审核) 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限制用户对特定 AWS 资源的权限的信息，请参阅[访问管理和示例策略](#)。

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，在导航窗格中选择控制面板。从控制面板上，选择 Customize，然后输入别名，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 \(p. 702\)](#)。

创建密钥对

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

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[区域、可用区和本地区域 \(p. 6\)](#)。

创建密钥对

1. 使用您在上节中创建的 URL 登录到 AWS。
2. 从 AWS 仪表板中，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，如果您计划在美国东部（俄亥俄）区域中启动实例，则必须在美国东部（俄亥俄）区域中创建实例的密钥对。



4. 在导航窗格中的 NETWORK & SECURITY 下，选择 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；请选择箭头展开该窗格。您可能必须向下滚动才能看到 Key Pairs 链接。



5. 选择 Create Key Pair。

6. 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。使用一个容易记住的名称 (如您的 IAM 用户名) 后跟 -key-pair 加区域名称。例如，me-key-pair-useast2。
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
```

如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅 [错误：未保护的私钥文件 \(p. 959\)](#)。

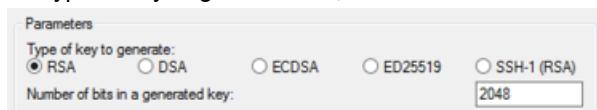
有关更多信息，请参阅 [Amazon EC2 密钥对 \(p. 759\)](#)。

使用密钥对连接到实例

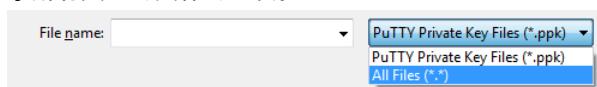
要从运行 Mac 或 Linux 的计算机连接到 Linux 实例，需要使用 -i 选项对 SSH 客户端指定 .pem 文件和私有密钥的路径。要从运行 Windows 的计算机连接到 Linux 实例，可以使用 PuTTY、Windows Subsystem for Linux 或 AWS Systems Manager 会话管理器。如果您计划使用 .ppk，则需要使用以下步骤将 PuTTY 文件转换为 .pem 文件。

(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。请务必安装整个套件。
2. 启动 PuTTYgen (例如，在开始菜单中，依次单击所有程序 > PuTTY > PuTTYgen)。
3. 在 Type of key to generate 下，选择 RSA。



4. 选择 Load。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. 选择您在上一个过程中创建的私有密钥文件，然后选择 Open。选择 OK 关闭确认对话框。
6. 选择 Save private key (保存私有密钥)。PuTTYgen 会显示一条警告，提示将在未提供口令的情况下保存密钥。选择是。
7. 为密钥指定密钥对所用的相同名称。PuTTY 会自动添加 .ppk 文件扩展名。

创建 Virtual Private Cloud (VPC)

通过 Amazon VPC，您可以在您定义的称为 Virtual Private Cloud (VPC) 的虚拟网络中启动 AWS 资源。在 VPC 中启动实例时需要较新的 EC2 实例类型。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 \(p. 22\)](#)。若要确定是否具有默认 VPC，请打开 Amazon EC2 控制台，在控制面板的账户属性下查找默认 VPC。如果您的控制面板上未列出默认 VPC，则可以使用以下步骤创建非默认 VPC。

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，选择 Launch VPC Wizard (启动 VPC 向导)。
4. 在 Step 1: Select a VPC Configuration 页面上，确保选中 VPC with a Single Public Subnet，然后选择 Select。
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，然后选择 Create VPC。在确认页面上，请选择 OK。

有关 VPC 的更多信息，请参阅 [Amazon VPC 用户指南](#)。

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[区域、可用区和本地区域 \(p. 6\)](#)。

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 浏览器中使用搜索短语“什么是我的 IP 地址”，或使用以下服务：[检查 IP](#)。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. 在导航窗格中，选择 Security Groups。
4. 选择 Create Security Group。
5. 输入新安全组的名称和描述。使用一个容易记住的名称 (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。
7. 在 Inbound 选项卡上，创建以下规则 (为每个新规则选择 Add Rule)，然后选择 Create：
 - 从 Type 列表中选择 HTTP，确保 Source 设置为 Anywhere (0.0.0.0/0)。
 - 从 Type 列表中选择 HTTPS，确保 Source 设置为 Anywhere (0.0.0.0/0)。
 - 从 Type 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，我们不建议您允许从所有 IPv4 地址 (0.0.0.0/0) 对您的实例进行 SSH 访问（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 \(p. 768\)](#)。

Amazon EC2 Linux 实例入门

让我们通过启动、连接以及使用 Linux 实例来开始使用 Amazon Elastic Compute Cloud (Amazon EC2)。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。

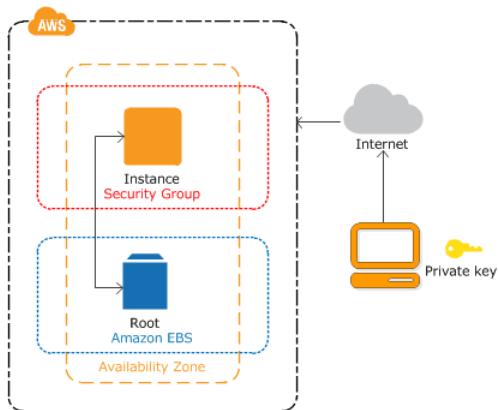
注册 AWS 后，可以通过 [AWS 免费套餐](#) 开始使用 Amazon EC2。如果您在过去 12 个月内创建过 AWS 账户，并且还没有超出 Amazon EC2 的免费套餐权益范围，则学完本教程不需要任何费用，因为我们会帮助您选择免费套餐权益范围内的选项。否则，您将从启动实例的那一刻开始承担标准的 Amazon EC2 使用费，直至终止实例（本教程最后一项任务），即使实例处于闲置状态也要计费。

目录

- [概述 \(p. 24\)](#)
- [先决条件 \(p. 25\)](#)
- [步骤 1：启动实例 \(p. 25\)](#)
- [步骤 2：连接到您的实例 \(p. 26\)](#)
- [步骤 3：清除您的实例 \(p. 26\)](#)
- [后续步骤 \(p. 26\)](#)

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 \(p. 25\)](#)
2. [连接到您的实例 \(p. 26\)](#)
3. [清除您的实例 \(p. 26\)](#)

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 \(p. 18\)](#)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 2 的 HVM 版本。请注意，这些 AMI 标记为“Free tier eligible”(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。
- 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。

- 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。
- 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 Show/Hide Columns (齿轮状图标)，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您的 Linux 实例。有关更多信息，请参阅[连接到 Linux 实例 \(p. 423\)](#)。

Important

除非您在启动实例时使用具有 .pem 文件的密钥对以及允许从您计算机进行 SSH 访问的安全组，否则您无法连接到实例。如果您无法连接到实例，请参阅[排查实例的连接问题 \(p. 955\)](#)以获得帮助。

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执行更多操作，请参阅[后续步骤 \(p. 26\)](#)。

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 (操作)、Instance State (实例状态) 和 Terminate (终止)。
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 AWS Systems Manager 用户指南 中的 [AWS Systems Manager Run Command](#)。
- 配置 CloudWatch 警报以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 \(p. 798\)](#) 和 [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。
- 安装 LAMP 堆栈。有关更多信息，请参阅 [教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 \(p. 28\)](#)。

针对 Amazon EC2 的最佳实践

此实践列表可帮助您从 Amazon EC2 获得最大的好处。

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 \(p. 769\)](#)。
- 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 2 或 Amazon Linux AMI 的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 [管理 Linux 实例上的软件](#)。

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 \(p. 85\)](#)。
- 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 \(p. 461\)](#)。
- 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集群，从而确保容错。
- 对 EBS 卷和快照进行加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 851\)](#)。

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 \(p. 499\)](#) 和 [标记您的 Amazon EC2 资源 \(p. 940\)](#)。
- 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 \(p. 950\)](#)。

备份和恢复

- 使用 [Amazon EBS 快照 \(p. 812\)](#)定期备份您的 EBS 卷，并从您的实例创建 [Amazon 系统映像 \(AMI\) \(p. 83\)](#)，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 \(p. 574\)](#)。
- 监控和响应事件。有关更多信息，请参阅 [监控 Amazon EC2 \(p. 525\)](#)。
- 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 \(p. 595\)](#)。对于自动解决方案，您可以使用 Amazon EC2 Auto Scaling。有关更多信息，请参阅 [Amazon EC2 Auto Scaling 用户指南](#)。
- 定期测试在您的实例和 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。有关视频，请参阅 [AWS 说明视频和实验室](#)。

教程

- 教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 28)
- 教程：使用 Amazon Linux AMI 安装 LAMP Web 服务器 (p. 37)
- 教程：使用 Amazon Linux 托管 WordPress 博客 (p. 47)
- 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 54)
- 教程：在 Amazon Linux 上配置 SSL/TLS (p. 67)
- 教程：提高应用程序在 Amazon EC2 上的可用性 (p. 79)

教程：在 Amazon Linux 2 上安装 LAMP Web 服务器

通过以下步骤，您可以将带 PHP 和 [MariaDB](#)（一个由社区开发的 MySQL 分支）支持的 Apache Web 服务器（有时称为 LAMP Web 服务器或 LAMP 堆栈）安装到您的 Amazon Linux 2 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。

Important

要在 Amazon Linux AMI 上设置 LAMP Web 服务器，请参阅[教程：使用 Amazon Linux AMI 安装 LAMP Web 服务器 \(p. 37\)](#)。

如果您正在尝试在 Ubuntu 或 Red Hat Enterprise Linux 实例上设置一个 LAMP web 服务器，则本教程不适合您。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。

选项：使用 Automation 完成本教程

要使用 AWS Systems Manager Automation 而不是以下任务完成本教程，请运行 [AWS Docs-InstallALAMPServer-AL2](#) Automation 文档。

任务

- 步骤 1：准备 LAMP 服务器 (p. 28)
- 步骤 2：测试 LAMP 服务器 (p. 32)
- 步骤 3：确保数据库服务器的安全 (p. 33)
- 步骤 4：(可选) 安装 phpMyAdmin (p. 34)
- 故障排除 (p. 37)
- 相关主题 (p. 37)

步骤 1：准备 LAMP 服务器

先决条件

本教程假定您已经使用 Amazon Linux 2 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 \(p. 25\)](#)。您还必须配置安全组，以便允许 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 [为您的 Linux 实例授权入站流量 \(p. 757\)](#)。

Note

以下过程将安装 Amazon Linux 2 上可用的最新 PHP 版本（当前为 PHP 7.2）。如果您计划使用本教程中所述的 PHP 应用程序之外的 PHP 应用程序，则应检查其与 PHP 7.2 的兼容性。

准备 LAMP 服务器

1. [连接到您的实例 \(p. 26\)](#)。
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。

`-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，则可以忽略该选项。

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

3. 安装 `lamp-mariadb10.2-php7.2` 和 `php7.2` Amazon Linux Extras 存储库，以获取适用于 Amazon Linux 2 的 LAMP MariaDB 和 PHP 程序包的最新版本。

```
[ec2-user ~]$ sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
```

Note

如果您收到指示 `sudo: amazon-linux-extras: command not found` 的错误，则表示您的实例未与 Amazon Linux 2 AMI 一起启动（也许您可以改用 Amazon Linux AMI）。您可以使用以下命令查看 Amazon Linux 的版本。

```
cat /etc/system-release
```

要在 Amazon Linux AMI 上设置 LAMP Web 服务器，请参阅[教程：使用 Amazon Linux AMI 安装 LAMP Web 服务器 \(p. 37\)](#)。

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

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 httpd mariadb-server
```

Note

您可以使用以下命令查看这些程序包的当前版本：

```
yum info package_name
```

5. 启动 Apache Web 服务器。

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

6. 使用 `systemctl` 命令配置 Apache Web 服务器，使其在每次系统启动时启动。

```
[ec2-user ~]$ sudo systemctl enable httpd
```

您可以通过运行以下命令验证 `httpd` 是否已启用：

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

7. 如果您尚未这样做，请添加安全规则以允许与您的实例的入站 HTTP (端口 80) 连接。默认情况下，初始化期间将为您的实例设置 launch-wizard-**N** 安全组。此组包含一条允许 SSH 连接的规则。
- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
 - 选择 Instances 并选择您的实例。
 - 在 Security groups 下，选择 view inbound rules。
 - 在您的默认安全组中应该看到以下规则列表：

```
Security Groups associated with i-1234567890abcdef0
Ports      Protocol      Source      launch-wizard-N
22        tcp            0.0.0.0/0    #
```

使用 [向安全组添加规则 \(p. 772\)](#) 中的过程，添加具有以下值的新入站安全规则：

- Type : HTTP
 - Protocol : TCP
 - Port Range : 80
 - Source : Custom
8. 测试您的 Web 服务器。在 Web 浏览器中，键入您的实例的公有 DNS 地址 (或公有 IP 地址)。如果 /var/www/html 中没有内容，您应该会看到 Apache 测试页面。您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选中 Public DNS (公有 DNS) 列；如果此列处于隐藏状态，请选择 Show/Hide Columns (显示/隐藏列) (齿轮状图标) 并选择 Public DNS (公有 DNS))。

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 \(p. 772\)](#)。

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。

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 Apache HTTP server installed at this site is working properly.

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".

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 served, follow the instructions in the file `/etc/httpd/conf/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:



Apache httpd 提供的文件保存在名为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录为 `/var/www/html`，默认情况下归根用户所有。

要允许 `ec2-user` 账户操作此目录中的文件，必须修改其所有权和权限。有多种方式可以完成此任务。在本教程中，可将 `ec2-user` 添加到 `apache` 组，将 `/var/www` 目录的所有权授予 `apache` 组，并为该组指定写入权限。

设置文件权限

1. 将您的用户 (这里指 `ec2-user`) 添加到 `apache`。

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

2. 先退出再重新登录以选取新组，然后验证您的成员资格。

- a. 退出 (使用 `exit` 命令或关闭终端窗口) :

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

- b. 要验证您是否为 `apache` 组的成员，请重新连接到实例，然后运行以下命令：

```
[ec2-user ~]$ groups
ec2-user adm wheel apache systemd-journal
```

3. 将 `/var/www` 及其内容的组所有权更改到 `apache` 组。

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

4. 要添加组写入权限以及设置未来子目录上的组 ID，请更改 `/var/www` 及其子目录的目录权限。

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

5. 要添加组写入权限，请递归地更改 /var/www 及其子目录的文件权限：

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

这样，ec2-user(和 apache 组的任何未来成员)可以添加、删除和编辑 Apache 文档根目录中的文件，允许您添加内容，如静态网站或 PHP 应用程序。

保护您的 Web 服务器 (可选)

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，对于您访问的 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。

有关在服务器上启用 HTTPS 的信息，请参阅 [教程：在 Amazon Linux 2 上配置 SSL/TLS \(p. 54\)](#)。

步骤 2：测试 LAMP 服务器

如果服务器已安装并运行，且文件权限设置正确，则 ec2-user 账户应该能够在 /var/www/html 目录(可从 Internet 访问)中创建 PHP 文件。

测试您的 LAMP 服务器

1. 在 Apache 文档根目录中创建一个 PHP 文件。

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

尝试运行该命令时，如果出现“Permission denied (权限被拒绝)”错误，请尝试先注销，再重新登录，以获取您在 [设置文件权限 \(p. 31\)](#) 中配置的适当组权限。

2. 在 Web 浏览器中，键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
```

您应该会看到 PHP 信息页面：

PHP Version 7.2.0

System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64
Build Date	Dec 13 2017 03:34:37
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.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-dba.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqlind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-session.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-mysqlind.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,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。您还可以使用以下命令验证已经安装了所有必需的程序包。

```
[ec2-user ~]$ sudo yum list installed httpd mariadb-server php-mysqlnd
```

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。另请验证在 `amazon-linux-extras` 命令的输出中启用了 `php7.2` 和 `lamp-mariadb10.2-php7.2` Extras。

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

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

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 Apache 文档根目录 (位于 `/var/www/html`)，您应该能够在您的实例的公有 DNS 地址中看到该内容。

步骤 3：确保数据库服务器的安全

MariaDB 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 MariaDB 服务器，我们也建议执行此步骤。

保护 MariaDB 服务器

1. 启动 MariaDB 服务器。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

- 运行 mysql_secure_installation。

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

- 在提示时，键入根账户的密码。

- 键入当前根密码。默认情况下，根账户没有设置密码。按 Enter。
- 键入 **y** 设置密码，然后键入两次安全密码。有关创建安全密码的更多信息，请访问 <https://identitysafe.norton.com/password-generator/>。确保将此密码存储在安全位置。

Note

设置 MariaDB 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。

- 键入 **y** 删除匿名用户账户。
- 键入 **y** 禁用远程根登录。
- 键入 **y** 删除测试数据库。
- 键入 **y** 重新加载权限表并保存您的更改。

- (可选) 如果您不打算立即使用 MariaDB 服务器，请停止它。您可以在需要时再次重新启动。

```
[ec2-user ~]$ sudo systemctl stop mariadb
```

- (可选) 如果您希望每次启动时 MariaDB 服务器都启动，请键入以下命令。

```
[ec2-user ~]$ sudo systemctl enable mariadb
```

步骤 4：(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。按照下述步骤操作，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。有关开发人员提供的安全建议，请参阅[保护 phpMyAdmin 安装](#)。有关在 EC2 实例上保护 Web 服务器的一般信息，请参阅[教程：在 Amazon Linux 2 上配置 SSL/TLS \(p. 54\)](#)。

安装 phpMyAdmin

- 安装所需的依赖项。

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

- 重启 Apache。

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

- 重启 php-fpm。

```
[ec2-user ~]$ sudo systemctl restart php-fpm
```

4. 导航到位于 /var/www/html 的 Apache 文档根。

```
[ec2-user ~]$ cd /var/www/html
```

5. 从 <https://www.phpmyadmin.net/downloads> 选择最新 phpMyAdmin 发行版的源软件包。要将文件直接下载到您的实例，请复制链接并将其粘贴到 wget 命令，如本示例中所述：

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. 使用以下命令创建 phpMyAdmin 文件夹并将程序包提取到其中。

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. 删除 *phpMyAdmin-latest-all-languages.tar.gz* tarball。

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (可选) 如果 MySQL 服务器未运行，请立即启动它。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

9. 在 Web 浏览器中，键入 phpMyAdmin 安装的 URL。此 URL 是实例的公有 DNS 地址 (或公有 IP 地址)，后接正斜杠和您安装目录的名称。例如：

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

您应该会看到 phpMyAdmin 登录页面：



10. 使用您先前创建的 `root` 用户名和 MySQL 根密码登录到 phpMyAdmin 安装。

您的安装仍需进行配置，然后才能投入使用。要配置 phpMyAdmin，您可以[手动创建配置文件](#)、[使用设置控制台](#)或者结合这两种方法。

有关使用 phpMyAdmin 的信息，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？

您可以通过运行以下命令验证 httpd 是否已启用：

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

如果 httpd 进程未运行，请重复[准备 LAMP 服务器 \(p. 29\)](#)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 \(p. 772\)](#)。

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，请参阅以下文档：

- [使用 WinSCP 将文件传输到您的 Linux 实例 \(p. 439\)](#)
- [使用 SCP 将文件从 Linux 传输到 Linux 实例 \(p. 427\)](#)
- [教程：使用 Amazon Linux 托管 WordPress 博客 \(p. 47\)](#)

有关本教程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/>
- MariaDB 数据库服务器：<https://mariadb.org/>
- 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>

有关注册 Web 服务器域名或将现有域名转移到此主机的更多信息，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 AMI 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）安装到您的 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。

Important

要在 Amazon Linux 2 上设置 LAMP Web 服务器，请参阅[教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 \(p. 28\)](#)。

如果您正在尝试在 Ubuntu 或 Red Hat Enterprise Linux 实例上设置一个 LAMP web 服务器，则本教程不适合您。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](#)。

选项：使用 Automation 完成本教程

要使用 AWS Systems Manager Automation 而不是以下任务完成本教程，请运行 [AWS Docs-InstallALAMPServer-AL Automation 文档](#)。

任务

- [步骤 1：准备 LAMP 服务器 \(p. 38\)](#)
- [步骤 2：测试 LAMP 服务器 \(p. 41\)](#)
- [步骤 3：确保数据库服务器的安全 \(p. 43\)](#)
- [步骤 4：\(可选\) 安装 phpMyAdmin \(p. 44\)](#)
- [故障排除 \(p. 46\)](#)
- [相关主题 \(p. 47\)](#)

步骤 1：准备 LAMP 服务器

先决条件

本教程假定您已经使用 Amazon Linux AMI 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 \(p. 25\)](#)。您还必须配置安全组，以便允许 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 [为您的 Linux 实例授权入站流量 \(p. 757\)](#)。

使用 Amazon Linux AMI 安装和启动 LAMP Web 服务器

1. [连接到您的实例 \(p. 26\)](#)。
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。

`-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，则可以忽略该选项。

```
[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 应用程序是否与其兼容。如果出现问题，您可能需要安装替代环境。有关更多信息，请参阅 [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 \(p. 46\)](#)。

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
```

Note

如果您收到错误 `No package package-name available`，则表示您的实例未与 Amazon Linux AMI 一起启动（也许您可以改用 Amazon Linux 2）。您可以使用以下命令查看 Amazon Linux 的版本。

```
cat /etc/system-release
```

4. 启动 Apache Web 服务器。

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

5. 使用 chkconfig 命令配置 Apache Web 服务器，使其在每次系统启动时启动。

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

当您成功地使用 chkconfig 命令启用服务时，该命令不提供任何确认消息。

您可以通过运行以下命令验证 httpd 是否已启用：

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

在运行级别 2、3、4 和 5 下，httpd 为 on (您希望看到的状态)。

6. 如果您尚未这样做，请添加安全规则以允许与您的实例的入站 HTTP (端口 80) 连接。默认情况下，初始化期间将为您的实例设置 launch-wizard-N 安全组。此组包含一条允许 SSH 连接的规则。
 - a. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
 - b. 选择 Instances 并选择您的实例。
 - c. 在 Security groups 下，选择 view inbound rules。
 - d. 在您的默认安全组中应该看到以下规则列表：

```
Security Groups associated with i-1234567890abcdef0
Ports      Protocol      Source          launch-wizard-N
22         tcp           0.0.0.0/0      #
```

使用 [向安全组添加规则 \(p. 772\)](#) 中的过程，添加具有以下值的新入站安全规则：

- Type : HTTP
- Protocol : TCP
- Port Range : 80
- Source : Custom

7. 测试您的 Web 服务器。在 Web 浏览器中，键入您的实例的公有 DNS 地址 (或公有 IP 地址)。如果 /var/www/html 中没有内容，您应该会看到 Apache 测试页面。您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选中 Public DNS (公有 DNS) 列；如果此列处于隐藏状态，请选择 Show/Hide Columns (显示/隐藏列) (齿轮状图标) 并选择 Public DNS (公有 DNS))。

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 \(p. 772\)](#)。

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

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

Apache httpd 提供的文件保存在名为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录为 `/var/www/html`，默认情况下归根用户所有。

```
[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
drwxr-xr-x 2 root root 4096 Aug 7 21:17 noindex
```

要允许 `ec2-user` 账户操作此目录中的文件，必须修改其所有权和权限。有多种方式可以完成此任务。在本教程中，可将 `ec2-user` 添加到 `apache` 组，将 `/var/www` 目录的所有权授予 `apache` 组，并为该组指定写入权限。

设置文件权限

- 将您的用户 (这里指 ec2-user) 添加到 apache。

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

- 先退出再重新登录以选取新组，然后验证您的成员资格。

- 退出 (使用 exit 命令或关闭终端窗口) :

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

- 要验证您是否为 apache 组的成员，请重新连接到实例，然后运行以下命令：

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

- 将 /var/www 及其内容的组所有权更改到 apache 组。

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

- 要添加组写入权限以及设置未来子目录上的组 ID，请更改 /var/www 及其子目录的目录权限。

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

- 要添加组写入权限，请递归地更改 /var/www 及其子目录的文件权限：

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

这样，ec2-user (和 apache 组的任何未来成员) 可以添加、删除和编辑 Apache 文档根目录中的文件，允许您添加内容，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，对于您访问的 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。

有关在服务器上启用 HTTPS 的信息，请参阅 [教程：在 Amazon Linux 上配置 SSL/TLS \(p. 67\)](#)。

步骤 2：测试 LAMP 服务器

如果服务器已安装并运行，且文件权限设置正确，则 ec2-user 账户应该能够在 /var/www/html 目录 (可以从 Internet 访问) 中创建 PHP 文件。

测试您的 LAMP Web 服务器

- 在 Apache 文档根目录中创建一个 PHP 文件。

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

尝试运行该命令时，如果出现“Permission denied (权限被拒绝)”错误，请尝试先注销，再重新登录，以获取您在 [步骤 1：准备 LAMP 服务器 \(p. 38\)](#) 中配置的适当组权限。

- 在 Web 浏览器中，键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
```

您应该会看到 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-mysqlind.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-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/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

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。您还可以使用以下命令验证已经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-mysqlind
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-mysqlind.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。

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

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

步骤 3：确保数据库服务器的安全

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，我们也建议执行此步骤。

确保数据库服务器的安全

- 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 ]
```

- 运行 mysql_secure_installation。

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

- 在提示时，键入根账户的密码。
 - 键入当前根密码。默认情况下，根账户没有设置密码。按 Enter。
 - 键入 Y 设置密码，然后键入两次安全密码。有关创建安全密码的更多信息，请访问 <https://identitysafe.norton.com/password-generator/>。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。

- 键入 Y 删除匿名用户账户。
- 键入 Y 禁用远程根登录。
- 键入 Y 删除测试数据库。
- 键入 Y 重新加载权限表并保存您的更改。

- (可选) 如果您不打算立即使用 MySQL 服务器，请停止它。您可以在需要时再次重新启动。

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

- (可选) 如果您希望每次启动时 MySQL 服务器都启动，请键入以下命令。

```
[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 Apache 文档根目录 (位于 /var/www/html)，您应该能够在您的实例的公有 DNS 地址中看到该内容。

步骤 4：(可选) 安装 phpMyAdmin

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。按照下述步骤操作，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。有关开发人员提供的安全建议，请参阅[保护 phpMyAdmin 安装](#)。

Note

Amazon Linux 包管理系统当前不支持 PHP 7 环境中的 phpMyAdmin 自动安装。本教程介绍如何手动安装 phpMyAdmin。

1. 使用 SSH 登录您的 EC2 实例。
2. 安装所需的依赖项。

```
[ec2-user ~]$ sudo yum install php70-mbstring.x86_64 php70-zip.x86_64 -y
```

3. 重启 Apache。

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

4. 导航到位于 /var/www/html 的 Apache 文档根。

```
[ec2-user ~]$ cd /var/www/html
[ec2-user html]$
```

5. 从 <https://www.phpmyadmin.net/downloads> 选择最新 phpMyAdmin 发行版的源软件包。要将文件直接下载到您的实例，请复制链接并将其粘贴到 wget 命令，如本示例中所述：

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. 使用以下命令创建 phpMyAdmin 文件夹并将程序包提取到其中。

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. 删除 `phpMyAdmin-latest-all-languages.tar.gz` tarball。

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (可选) 如果 MySQL 服务器未运行，请立即启动它。

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

9. 在 Web 浏览器中，键入 phpMyAdmin 安装的 URL。此 URL 是实例的公有 DNS 地址 (或公有 IP 地址)，后接正斜杠和您安装目录的名称。例如：

<http://my.public.dns.amazonaws.com/phpMyAdmin>

您应该会看到 phpMyAdmin 登录页面：



10. 使用您先前创建的 root 用户名和 MySQL 根密码登录到 phpMyAdmin 安装。

您的安装仍需进行配置，然后才能投入使用。要配置 phpMyAdmin，您可以[手动创建配置文件](#)、[使用设置控制台](#)或者结合这两种方法。

有关使用 phpMyAdmin 的信息，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？

您可以通过运行以下命令验证 httpd 是否已启用：

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

在运行级别 2、3、4 和 5 下，httpd 为 on (您希望看到的状态)。

如果 httpd 进程未运行，请重复[步骤 1：准备 LAMP 服务器 \(p. 38\)](#)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 \(p. 772\)](#)。

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 HTTP Server、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的建议安装了最新的软件包，您必须首先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到建议的环境，您必须先删除自定义软件包和依赖项：

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

现在，您可以如前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，请参阅以下文档：

- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 439)
- 使用 SCP 将文件从 Linux 传输到 Linux 实例 (p. 427)
- 教程：使用 Amazon Linux 托管 WordPress 博客 (p. 47)

有关本教程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>

有关注册 Web 服务器域名或将现有域名转移到此主机的更多信息，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](#)。

选项：使用 Automation 完成本教程

要使用 AWS Systems Manager Automation 而不是以下任务完成本教程，请运行以下其中一个 Automation 文档：[AWS Docs Hosting A WordPress Blog - AL](#) (Amazon Linux) 或 [AWS Docs Hosting A WordPress Blog - AL2](#) (Amazon Linux 2)。

先决条件

此教程假设您已遵照 [教程：使用 Amazon Linux AMI 安装 LAMP Web 服务器 \(p. 37\)](#) 中的所有步骤（适用于 Amazon Linux AMI），或 [教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 \(p. 28\)](#) 中的所有步骤（适用于 Amazon Linux 2）启动了一个 Amazon Linux 实例，其中包含支持 PHP 和数据库（MySQL 或 MariaDB）的功能正常的 Web 服务器。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。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 \(p. 772\)](#)。

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 \(p. 590\)](#)。

如果您的博客还没有域名，则可使用 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 命令下载最新的 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
```

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

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

为安装 WordPress 创建数据库用户和数据库

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。此过程帮助您创建自己的博客数据库，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. 启动数据库服务器。

- Amazon Linux 2

```
[ec2-user ~]$ sudo systemctl start mariadb
```

- Amazon Linux AMI

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

2. 以 root 用户身份登录数据库服务器。在系统提示时输入您的数据库 root 密码，它可能与您的 root 系统密码不同；如果您尚未给您的数据库服务器加密，它甚至可能是空的。

如果您尚未给您的数据库服务器加密，则必须执行这项操作。有关更多信息，请参阅 [保护 MariaDB 服务器 \(p. 33\)](#) (Amazon Linux 2) 或 [确保数据库服务器的安全 \(p. 43\)](#) (Amazon Linux AMI)。

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

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。

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

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。

```
CREATE DATABASE `wordpress-db`;
```

5. 对您之前创建的 WordPress 用户授予您数据库的完全访问权限。

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. 刷新数据库权限以接受您的所有更改。

```
FLUSH PRIVILEGES;
```

7. 退出 mysql 客户端。

```
exit
```

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 文件复制为一个名为 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 ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. 用您喜欢的文本编辑器 (例如 nano 或 vim) 编辑 wp-config.php 文件并输入适用于您的安装的值。如果没有常用的文本编辑器, nano 比较适合初学者使用。

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

- a. 查找定义 DB_NAME 的行并将 database_name_here 更改为您在 Step 4 (p. 49) 的 为安装 WordPress 创建数据库用户和数据库 (p. 48) 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 Step 3 (p. 48) 的 为安装 WordPress 创建数据库用户和数据库 (p. 48) 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 Step 3 (p. 48) 的 为安装 WordPress 创建数据库用户和数据库 (p. 48) 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.AV0pCKZZB,*-*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[Og%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?Zy4zUU4r99QQ_xGs2LTd%P; |
_e1tS)8_B/, .6[=UK<J_y9?JWG');
```

- e. 保存文件并退出您的文本编辑器。

将 WordPress 文件安装到 Apache 文档根目录下

- 现在，您已解压了安装文件夹、创建了 MySQL 数据库和用户并自定义了 WordPress 配置文件，那么也就准备好将您的安装文件复制到 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 服务器的实际根目录（例如，my.public.dns.amazonaws.com）还是位于根目录下的某个子目录或文件夹（例如，my.public.dns.amazonaws.com/blog）中。
- 如果希望 WordPress 在文档根目录下运行，请复制 wordpress 安装目录的内容（但不包括目录本身），如下所示：

```
[ec2-user ~]$ cp -r wordpress/* /var/www/html/
```

- 如果希望 WordPress 在文档根目录下的其他目录中运行，请先创建该目录，然后将文件复制到其中。在此示例中，WordPress 将从目录 blog 运行：

```
[ec2-user ~]$ mkdir /var/www/html/blog
[ec2-user ~]$ cp -r wordpress/* /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 文档根目录下后，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。要终止 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。

1. 使用您常用的文本编辑器（如 nano 或 vim）打开 httpd.conf 文件。如果没有常用的文本编辑器，nano 比较适合初学者使用。

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

2. 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>
```

3. 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
```

4. 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）。如果您尚未进行此操作，请应用以下组成员关系和权限（在 [LAMP Web 服务器教程（p. 37）](#) 中有更为详细的描述）。

1. 将 /var/www 及其内容的文件所有权授予 apache 用户。

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

2. 将 /var/www 及其内容的组所有权授予 apache 组。

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

3. 更改 /var/www 及其子目录的目录权限，以添加组写入权限及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 {} \;
```

4. 递归地更改 /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 {} \;
```

5. 重启 Apache Web 服务器，让新组和权限生效。

- Amazon Linux 2

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

- Amazon Linux AMI

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

使用 Amazon Linux 2 运行 WordPress 安装脚本

您已准备好安装 WordPress。您使用的命令取决于操作系统。此过程中的命令适用于 Amazon Linux 2。对 Amazon Linux AMI 使用此过程后面的过程。

1. 使用 systemctl 命令确保 httpd 和数据库服务在每次系统启动时启动。

```
[ec2-user ~]$ sudo systemctl enable httpd && sudo systemctl enable mariadb
```

2. 验证数据库服务器是否正在运行。

```
[ec2-user ~]$ sudo systemctl status mariadb
```

如果数据库服务未运行，请启动。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

3. 验证您的 Apache Web 服务器 (httpd) 正在运行。

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

如果 httpd 服务未运行，请启动。

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

4. 在 Web 浏览器中，键入您 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 安装脚本。提供 WordPress 安装所需的信息。选择安装 WordPress 完成安装。有关更多信息，请参阅 WordPress 网站上的[运行安装脚本](#)。

使用 Amazon Linux AMI 运行 WordPress 安装脚本

1. 使用 chkconfig 命令确保 httpd 和数据库服务在每次系统启动时启动。

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

2. 验证数据库服务器是否正在运行。

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

如果数据库服务未运行，请启动。

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

3. 验证您的 Apache Web 服务器 (httpd) 正在运行。

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

如果 httpd 服务未运行，请启动。

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

4. 在 Web 浏览器中，键入您 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 安装脚本。提供 WordPress 安装所需的信息。选择安装 WordPress 完成安装。有关更多信息，请参阅 WordPress 网站上的[运行安装脚本](#)。

后续步骤

在测试您的 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 \(p. 83\)](#)。

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[Amazon EBS 弹性卷 \(p. 841\)](#)。
- 将您的 MySQL 数据库移动到 [Amazon RDS](#) 以利用服务的轻松扩展功能。
- 迁移到更大的实例类型。有关更多信息，请参阅[更改实例类型 \(p. 233\)](#)。
- 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 \(p. 79\)](#)。

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。如果您不确定旧站点 URL 是什么，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：在 Amazon Linux 2 上配置 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。本教程介绍如何在具有 Amazon Linux 2 和 Apache Web 服务器的 EC2 实例上手动添加对 SSL/TLS 的支持。如果您计划提供商业级服务，[AWS Certificate Manager](#)（此处未作介绍）是一个不错的选择。

由于历史原因，Web 加密通常简称为 SSL。虽然 Web 浏览器仍支持 TLS，但下一代协议 TLS 不容易受到攻击。默认情况下，Amazon Linux 2 为所有版本的 SSL 禁用服务器端支持。[安全标准机构](#)认为 TLS 1.0 不

太安全，并且 IETF 即将正式弃用 TLS 1.0 和 TLS 1.1。本教程仅包含有关启用 TLS 1.2 的指导。（较新的 TLS 1.3 协议处于草案形式，但在 Amazon Linux 2 上尚不支持。）有关更新的加密标准的更多信息，请参阅 [RFC 7568](#) 和 [RFC 8446](#)。

在本教程中，将现代 Web 加密简称为 TLS。

Important

这些过程适用于 Amazon Linux 2。我们还假定您从新的 Amazon EC2 实例开始。如果您尝试在具有其他分配的实例上设置 LAMP Web 服务器，或者如果您重新使用旧的、现有实例，则本教程中的一些过程可能不适合您。有关 Ubuntu 上的 LAMP Web 服务器的信息，请参阅 Ubuntu 社区文档 [ApacheMySQLPHP](#)。有关 Red Hat Enterprise Linux 的信息，请参阅客户门户网站主题 [Web 服务器](#)。

目录

- [先决条件 \(p. 55\)](#)
- [步骤 1：在服务器上启用 TLS \(p. 55\)](#)
- [步骤 2：获取 CA 签名的证书 \(p. 57\)](#)
- [步骤 3：测试和强化安全配置 \(p. 61\)](#)
- [故障排除 \(p. 63\)](#)
- [证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 \(p. 64\)](#)

先决条件

在开始本教程之前，请完成以下步骤：

- 启动 EBS 支持的 Amazon Linux 2 实例。有关更多信息，请参阅[步骤 1：启动实例 \(p. 25\)](#)。
 - 配置安全组以允许您的实例接受以下 TCP 端口上的连接：
 - SSH (端口 22)
 - HTTP (端口 80)
 - HTTPS (端口 443)
- 有关更多信息，请参阅[为您的 Linux 实例授权入站流量 \(p. 757\)](#)。
- 安装 Apache Web 服务器。有关分步说明，请参阅[教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 \(p. 28\)](#)。仅需要 httpd 包及其依赖项，因此可以忽略涉及 PHP 和 MariaDB 的说明。
 - 要识别和验证网站，TLS 公有密钥基础设施 (PKI) 依赖于域名系统 (DNS)。要使用 EC2 实例托管公共网站，您需要为 Web 服务器注册一个域名，或者将现有域名转让给您的 Amazon EC2 主机。可通过很多第三方域注册和 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 TLS

该过程指导您完成在 Amazon Linux 2 上使用自签名数字证书设置 TLS 的过程。

Note

自签名证书对于测试是可接受的，但对于生产不是。如果您将自签名证书公开到 Internet，您的网站的访客将会看到安全警告。

在服务器上启用 TLS

1. [连接到您的实例 \(p. 26\)](#)并确认 Apache 正在运行。

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

如果返回的值不是“启用”，则启动 Apache 并将它设置为每次随系统一起启动。

```
[ec2-user ~]$ sudo systemctl start httpd && sudo systemctl enable httpd
```

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，则可以忽略该选项。

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

3. 现在，您的实例是最新的，请安装 Apache 模块 mod_ssl 以添加 TLS 支持。

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

您的实例现在具有以下文件，可使用这些文件配置安全服务器并创建证书以进行测试：

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

mod_ssl 的配置文件。它包含一些指令以指示 Apache 在何处查找以下信息：加密密钥和证书、要允许的 TLS 协议版本以及要接受的加密密码。

- /etc/pki/tls/certs/make-dummy-cert

用于为服务器主机生成自签名 X.509 证书和私有密钥的脚本。要测试是否正确设置 Apache 以使用 TLS，该证书是非常有用的。由于不提供身份证明，因此，不应在生产环境中使用该证书。如果在生产环境中使用该证书，则将在 Web 浏览器中触发警告。

4. 运行脚本以生成自签名虚拟证书和密钥以进行测试。

```
[ec2-user ~]$ cd /etc/pki/tls/certs  
sudo ./make-dummy-cert localhost.crt
```

这会在 /etc/pki/tls/certs/ 目录中生成一个新文件 localhost.crt。指定的文件名与 /etc/httpd/conf.d/ssl.conf 中的 SSLCertificateFile 指令指定的默认值匹配。

该文件包含自签名证书以及证书的私有密钥。Apache 要求证书和密钥采用 PEM 格式，其中包含 Base64 编码的 ASCII 字符，并用“BEGIN”和“END”行框起来，如以下简短示例所示。

```
-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwgSkAgEAAoIBAQD2KKx/8Zk94m1q  
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLjOOC18u1PTcGmAah5kEitCEc0wzmNeo  
BC10wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vr  
GvwnKoMh3DlK44D9dx7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMZoT  
...  
56tE7THvH7vOEF4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNMRHuyMcPODFs  
27hDzPDinrquSEvoZIggkDMlh2irTiiPj/GhkvtipoQlv0fK/VXw8vSgeaBuhwJvS  
LXU9HvYq0U604FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo  
4QQvAqOa8UheYeoXLdWcHaLP  
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----  
MIIEazCCA1OgAwIBAgICWxQwdQYJKoZIhvNAQELBQAwgbExCzAJBgNVBAYTAi0t  
MRIwEAYDVQQIDAlTb21lU3RhGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK  
DBBTb21lT3JnYW5pemFOaW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemFOaW9uYWxv
```

```
bml0MRkwFwYDVQQDDBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rUE/XzxRLBZOOwZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3DlK44D9d1U3
WanXWehT6FiSzvB4sTEXXJN2jdw8g+sHgnZ8zCosclknYhHrCVD2vnBlZJKSzvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHod0BQE8sBJxg==
-----END CERTIFICATE-----
```

文件名和扩展名只是为了提供便利，对功能没有影响。例如，只要 `ssl.conf` 文件中的相关指令使用相同的名称，您就可以将证书命名为 `cert.crt`、`cert.pem` 或任何其他文件名。

Note

在使用您自己的自定义文件替换默认 TLS 文件时，请确保它们采用 PEM 格式。

5. 打开 `/etc/httpd/conf.d/ssl.conf` 文件并注释掉以下行，因为自签名虚拟证书也包含密钥。如果在完成下一步之前没有注释掉该行，Apache 服务将无法启动。

```
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

6. 重启 Apache。

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

Note

确保 TCP 端口 443 在您的 EC2 实例上是可访问的，如前所述。

7. 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://` 一起输入浏览器 URL 栏中来对其进行测试。

由于您正在使用自签名的不可信主机证书连接到站点，因此您的浏览器可能会显示一系列安全警告。忽视这些警告并继续连接站点。

如果默认 Apache 测试页面打开，这意味着您已成功在服务器上配置 TLS。在浏览器和服务器之间传输的所有数据现在都已加密。

Note

为了防止站点访问者遇到警告屏幕，您必须获取一个可信 CA 签名证书，该证书不仅进行加密，而且还公开验证您是否为站点拥有者。

步骤 2：获取 CA 签名的证书

您可以使用以下过程获取 CA 签名证书：

- 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)
- 获取签名的主机证书
- 配置 Apache 以使用证书

从加密角度看，自签名 TLS X.509 主机证书与 CA 签名证书完全相同。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，或可通过由其他可信签署人组成的一系列信任访问，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 [dmoztools.net](#) 上可找到知名 CA 的列表。一些 CA 免费提供基础级别证书。其中最值得注意的 CA 是 [Let's Encrypt](#) 项目，该项目还支持证书创建和续订过程的自动化。有关将 Let's Encrypt 用作 CA 的更多信息，请参阅[证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 \(p. 64\)](#)。

主机证书的基础是密钥。从 2019 年开始，[政府](#)和[行业](#)群体建议 RSA 密钥使用 2048 位的最小密钥（模数）大小，旨在将文档一直保护到 2030 年。Amazon Linux 2 中的 OpenSSL 生成的默认模数大小为 2048 位，这适用于 CA 签名证书。在以下过程中，为需要自定义密钥的人员提供了一个可选步骤，例如，具有较大模数或使用不同加密算法的步骤。

除非您拥有注册并托管的 DNS 域，否则，有关获取 CA 签名主机证书的这些说明不适用。

获取 CA 签名的证书

1. [连接到您的实例 \(p. 26\)](#)并导航到 /etc/pki/tls/private/。这是存储 TLS 的服务器私有密钥的目录。如果您希望使用现有的主机密钥生成 CSR，请跳到步骤 3。
2. (可选) 生成新的私有密钥。下面是一些密钥配置示例。任何生成的密钥都可用于您的 Web 服务器，但它们实施安全的程度和类型有所不同。
 - 示例 1：创建默认 RSA 主机密钥。生成的文件 **custom.key** 是一个 2048 位 RSA 私有密钥。

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

- 示例 2：创建具有更大模数的更严格的 RSA 密钥。生成的文件 **custom.key** 是一个 4096 位 RSA 私有密钥。

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

- 示例 3：创建具有密码保护的 4096 位加密的 RSA 密钥。生成的文件 **custom.key** 是一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

Important

对密钥进行加密可增强安全性，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，都必须通过 SSH 连接提供密码（在上一示例中为“abcde12345”）。

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

- 示例 4：使用非 RSA 密码创建密钥。RSA 加密可能相对较慢，因为其公有密钥的大小基于两个大素数的乘积。不过，可以为 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，计算起来更快。

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

结果为一个使用 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所有权和权限（所有者=根、组=根、仅面向所有者的读取/写入权限）。命令将如以下示例所示。

```
[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。下面的示例使用了 **custom.key**。

```
[ec2-user ~]$ sudo openssl req -new -key custom.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主机证书来说，除 Common Name 以外的所有字段都是可选字段。

名称	描述	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 Corporation
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输入浏览器中的 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 www.example.com 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 *.example.com ）。	www.example.com
电子邮件地址	服务器管理员的电子邮件地址。	someone@example.com

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。您网站的访客如果输入这两个名称的任何一个，便可看到一个没有错误的连接。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。

Note

您的 CA 可能会针对各种用途发送多种格式的文件。在本教程中，您应只使用 PEM 格式的证书文件，此格式通常会（但不总是）标有 .pem 或 .crt 文件扩展名。如果您不确定要使用哪个文件，请使用文本编辑器打开这些文件，并查找一个包含一个或多个以下面的行开始的块的文件。

```
- - - - -BEGIN CERTIFICATE - - - - -
```

该文件还应以下面的行结束。

```
- - - - -END CERTIFICATE - - - - -
```

您还可以在命令行上测试文件，如下所示。

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

验证这些行是否显示在文件中。请勿使用结尾为 .p7b、.p7c 或类似文件扩展名的文件。

- 将新的 CA 签名证书和任何中间证书放在 /etc/pki/tls/certs 目录中。

Note

可通过多种方法将新证书上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。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 2 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。以下示例显示了要使用的命令。

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

这些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、组=根、所有者可以写入、组可以读取、任何人都可读取）。以下示例显示了要使用的命令。

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

这些命令应生成以下结果。

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

- 将用于创建 CSR 的私有密钥放在 /etc/pki/tls/private/ 目录中。

Note

可通过多种方法将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。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/private 目录内部，使用以下命令验证文件所有权、组和权限设置是否与高度限制的 Amazon Linux 2 默认权限（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。

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

这些命令应生成以下结果。

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

7. 编辑 /etc/httpd/conf.d/ssl.conf 以反映您的新证书和密钥文件。
 - a. 在 Apache 的 SSLCertificateFile 指令中提供 CA 签名主机证书的路径和文件名：

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

- b. 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
```

Note

一些 CA 将主机证书和中间证书合并到单个文件中，从而不再需要使用 SSLCACertificateFile 指令。请查询您的 CA 提供的说明。

- c. 在 Apache 的 SSLCertificateKeyFile 指令中提供私有密钥的路径和文件名（在该示例中为 custom.key）：

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

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

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

9. 通过在浏览器 URL 栏中输入带有 https:// 前缀的域名来测试您的服务器。您的浏览器应通过 HTTPS 加载测试页面而不会产生错误。

步骤 3：测试和强化安全配置

在 TLS 可操作且公开展示后，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，使用 www.example.com 格式输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。下表总结了具有与 Amazon Linux 2 上的默认 Apache 配置相同的设置以及默认 Certbot 证书的域的报告。

总评	B
证书	100%
协议支持	95%
密钥交换	70%
密码强度	90%

虽然概述信息显示配置基本正确，但详细报告标记了几个潜在的问题（在此处按严重性顺序列出）：

X 支持某些旧浏览器使用 RC4 密码。密码是加密算法的数学核心。RC4 是一种用于加密 TLS 数据流的快速密码，已知这种密码存在一些**严重缺点**。除非您有充分理由支持旧版浏览器，否则，应禁用该密码。

X 支持旧 TLS 版本。该配置支持 TLS 1.0（已弃用）和 TLS 1.1（即将弃用）。从 2018 年开始，仅建议使用 TLS 1.2。

X 不完全支持向前保密性。[向前保密性](#)是一种算法功能，它使用从私有密钥派生的临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。

纠正 TLS 配置并供将来使用

- 在文本编辑器中打开 /etc/httpd/conf.d/ssl.conf 配置文件，并在以下行的开头输入“#”以注释掉该行。

```
#SSLProtocol all -SSLv3
```

- 添加以下指令：

```
#SSLProtocol all -SSLv3
SSLPotocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

该指令显式禁用 SSL 版本 2 和 3 以及 TLS 版本 1.0 和 1.1。现在，服务器拒绝接受与使用 TLS 1.2 以外的任何协议的客户端之间的加密连接。指令中的冗长文字更清楚地向人类读者阐述为服务器配置的用途。

Note

以此方式禁用 TLS 1.0 和 1.1 版可阻止一小部分过时的 Web 浏览器访问您的网站。

修改允许的密码列表

- 在 /etc/httpd/conf.d/ssl.conf 配置文件中，找到包含 **SSLCipherSuite** 指令的部分，并通过在现有行的开头输入“#”来注释掉该行。

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

- 指定显式的密码套件，并指定密码顺序以优先使用向前保密性并避免不安全的密码。此处使用的 **SSLCipherSuite** 指令基于 [Mozilla SSL 配置生成器](#)的输出，该生成器根据服务器上运行的特定软件定制 TLS 配置。（有关更多信息，请参阅 Mozilla 的[有用资源安全性/服务器端 TLS](#)。）首先，通过使用以下命令的输出确定 Apache 和 OpenSSL 版本。

```
[ec2-user ~]$ yum list installed | grep httpd
[ec2-user ~]$ yum list installed | grep openssl
```

例如，如果返回的信息是 Apache 2.4.34 和 OpenSSL 1.0.2，我们将其输入到生成器中。如果您选择“现代”兼容性模型，这将创建一条 `SSLCipherSuite` 指令，虽然该指令积极实施安全性，但仍适用于大多数浏览器。如果您的软件不支持现代配置，则可以更新软件或改为选择“中间”配置。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-  
CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:  
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-  
AES128-SHA256
```

选定的密码名称中包含 `ECDHE`，它是 Elliptic Curve Diffie-Hellman Ephemeral 的缩写。术语 `ephemeral` 表示向前保密性。副作用是，这些密码不支持 RC4。

建议您使用密码的明确列表，而不是依赖于内容不可见的默认值或简短指令。

将生成的指令复制到 `/etc/httpd/conf.d/ssl.conf` 中。

Note

此处为方便阅读将指令显示为几行，但在复制到 `/etc/httpd/conf.d/ssl.conf` 时，该指令必须位于一行中，并且密码名称之间只有一个冒号（无空格）。

3. 最后，通过删除以下行开头的“#”来取消对该行的注释。

```
#SSLHonorCipherOrder on
```

该指令强制服务器优先使用排名较高的密码，包括（在该示例中）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。

在完成这两个过程后，将更改保存到 `/etc/httpd/conf.d/ssl.conf` 并重新启动 Apache。

如果在 [Qualys SSL Labs](#) 上再次测试域，将会看到已修复 RC4 漏洞和其他警告，并且摘要如下所示。

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

Important

在每次更新 OpenSSL 时，将引入新的密码并删除对旧密码的支持。使 EC2 Amazon Linux 2 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 Classic Load Balancer 用户指南 中的 [Elastic Load Balancing 的预定义 SSL 安全策略](#)。

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。

您可以从密钥中删除加密和密码要求。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`，则对 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 systemctl restart httpd
```

Apache 现在启动时应该不会提示您提供密码。

- 我运行时收到了错误 `sudo yum install -y mod_ssl`。

在为 SSL 安装所需的程序包时，您可能会看到与以下内容类似的错误。

```
Error: httpd24-tools conflicts with httpd-tools-2.2.34-1.16.amzn1.x86_64  
Error: httpd24 conflicts with httpd-2.2.34-1.16.amzn1.x86_64
```

这通常意味着您的 EC2 实例没有运行 Amazon Linux 2。本教程仅支持从官方 Amazon Linux 2 AMI 新创建的实例。

证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用

[Let's Encrypt](#) 证书颁发机构是电子前沿基金会 (EFF) 致力于对整个 Internet 进行加密的核心所在。按照该目标，Let's Encrypt 主机证书被设计为用最小的人工干预来进行创建、验证、安装和维护。证书管理的自动化方面由在 Web 服务器上运行的软件代理执行。在安装并配置代理后，它与 Let's Encrypt 安全地通信并在 Apache 和密钥管理系统上执行管理任务。本教程使用免费的 [Certbot](#) 代理，因为它允许您提供自定义的加密密钥作为您证书的基础，或允许代理自身根据其默认值创建密钥。您也可以将 Certbot 配置为定期续订您的证书，无需人工交互，如[自动化 Certbot \(p. 67\)](#) 中所述。有关更多信息，请参阅 Certbot [用户指南和手册页](#)。

虽然 Certbot 不受 Amazon Linux 2 官方支持，但可供下载并在安装时正常工作。建议您执行以下备份来保护数据并避免造成不便：

- 在开始之前，请为您的 Amazon EBS 根卷制作快照。这使您能够还原 EC2 实例的原始状态。有关创建 EBS 快照的信息，请参阅[创建 Amazon EBS 快照 \(p. 815\)](#)。
- 以下过程要求您编辑您的 `httpd.conf` 文件，该文件控制 Apache 的操作。Certbot 对此配置文件和其他配置文件进行其自动化更改。创建整个 `/etc/httpd` 目录的备份副本，以便您在需要时还原该目录。

准备安装

在安装 Certbot 之前，请完成以下过程。

- 下载 Extra Packages for Enterprise Linux (EPEL) 7 存储库程序包。需要这些程序包才能提供 Certbot 所需的依赖项。
 - 导航到您的主目录 (`/home/ec2-user`)。使用以下命令下载 EPEL。

```
[ec2-user ~]$ sudo wget -r --no-parent -A 'epel-release-*'.rpm' http://  
dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/
```

-
- b. 安装存储库程序包，如以下命令中所示。

```
[ec2-user ~]$ sudo rpm -Uvh dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release*.rpm
```

- c. 启用 EPEL，如以下命令中所示。

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

您可以使用以下命令确认已启用 EPEL。这应该返回类似于以下内容的信息。

```
[ec2-user ~]$ sudo yum repolist all

...
epel/x86_64                               Extra Packages for Enterprise Linux 7 - x86_64
                                         enabled: 12949+175
epel-debuginfo/x86_64                      Extra Packages for Enterprise Linux 7 - x86_64
                                         - Debug      enabled:     2890
                                         epel-source/x86_64          Extra Packages for Enterprise Linux 7 - x86_64
                                         - Source      enabled:         0
                                         epel-testing/x86_64        Extra Packages for Enterprise Linux 7 -
                                         Testing - x86_64           enabled:    778+12
                                         epel-testing-debuginfo/x86_64 Extra Packages for Enterprise Linux 7 -
                                         Testing - x86_64 - Debug   enabled:      107
                                         epel-testing-source/x86_64  Extra Packages for Enterprise Linux 7 -
                                         Testing - x86_64 - Source  enabled:         0
                                         ...
                                         
```

2. 编辑主要 Apache 配置文件 /etc/httpd/conf/httpd.conf。找到“Listen 80”指令并在后面添加以下行，将示例域名替换为实际公用名和主题替代名称 (SAN)。

```
<VirtualHost *:80>
  DocumentRoot "/var/www/html"
  ServerName "example.com"
  ServerAlias "www.example.com"
</VirtualHost>
```

保存文件，然后重新启动 Apache。

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

安装并运行 Certbot

此过程基于有关在 [Fedora](#) 和 [RHEL 7](#) 上安装 Certbot 的 EFF 文档。其中介绍 Certbot 的默认使用，即根据 2048 位 RSA 密钥生成证书。如果您要试验自定义密钥，可以从将 [ECDSA 证书与 Let's Encrypt 结合使用](#)开始。

1. 使用以下命令安装 Certbot 包和依赖项。

```
[ec2-user ~]$ sudo yum install -y certbot python2-certbot-apache
```

2. 运行 Certbot。

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

3. 在提示符“Enter email address (used for urgent renewal and security notices)”处，输入联系人地址并按 Enter。
4. 在提示符处，同意 Let's Encrypt 服务条款。输入“A”并按 Enter 以继续。

```
-----  
Please read the Terms of Service at  
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must  
agree in order to register with the ACME server at  
https://acme-v02.api.letsencrypt.org/directory  
-----  
(A)gree/(C)ancel: A
```

5. 完成授权以使 EFF 将您加入发送名单中，输入“Y”或“N”并按 Enter。
6. Certbot 显示您在 VirtualHost 数据块中提供的公用名和主题替代名称 (SAN)。

```
Which names would you like to activate HTTPS for?  
-----  
1: example.com  
2: www.example.com  
-----  
Select the appropriate numbers separated by commas and/or spaces, or leave input  
blank to select all options shown (Enter 'c' to cancel):
```

将输入保留空白并按 Enter。

7. Certbot 在创建证书和配置 Apache 时将显示以下输出。然后，它提示您有关将 HTTP 查询重定向到 HTTPS 的事项。

```
Obtaining a new certificate  
Performing the following challenges:  
http-01 challenge for example.com  
http-01 challenge for www.example.com  
Waiting for verification...  
Cleaning up challenges  
Created an SSL vhost at /etc/httpd/conf/httpd-le-ssl.conf  
Deploying Certificate for example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf  
Enabling site /etc/httpd/conf/httpd-le-ssl.conf by adding Include to root configuration  
Deploying Certificate for www.example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf  
  
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.  
-----  
1: No redirect - Make no further changes to the webserver configuration.  
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for  
new sites, or if you're confident your site works on HTTPS. You can undo this  
change by editing your web server's configuration.  
-----  
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```

要允许访客通过未加密的 HTTP 连接到服务器，请输入“1”。若要仅接受通过 HTTPS 的加密连接，请输入“2”。按 Enter 提交您的选择。

8. Certbot 完成 Apache 的配置并报告成功和其他信息。

```
Congratulations! You have successfully enabled https://example.com and  
https://www.example.com  
  
You should test your configuration at:  
https://www.ssllabs.com/ssltest/analyze.html?d=example.com  
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
```

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
`/etc/letsencrypt/live/certbot.oneeyedman.net/fullchain.pem`
Your key file has been saved at:
`/etc/letsencrypt/live/certbot.oneeyedman.net/privkey.pem`
Your cert will expire on 2019-08-01. To obtain a new or tweaked
version of this certificate in the future, simply run certbot again
with the "certonly" option. To non-interactively renew *all* of
your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot
configuration directory at `/etc/letsencrypt`. You should make a
secure backup of this folder now. This configuration directory will
also contain certificates and private keys obtained by Certbot so
making regular backups of this folder is ideal.

9. 在完成安装后，测试并优化您服务器的安全性，如[步骤 3：测试和强化安全配置 \(p. 61\)](#)中所述。

配置自动证书续订

Certbot 被设计成服务器系统的一个不可见的防错部分。默认情况下，它会生成具有短暂的 90 天到期时间的主机证书。如果您还未将系统配置为自动调用命令，则必须在到期之前手动重新运行 certbot 命令。此过程介绍如何通过设置 cron 作业来实现 Certbot 自动化。

自动化 Certbot

1. 在文本编辑器中打开 `/etc/crontab`，并添加类似于以下内容的行。

```
39      1,13    *      *      *      root     certbot renew --no-self-upgrade
```

完成后保存文件。这是命令的每个组成部分的说明。

`39 1,13 * * *`

排定一个在每天 01:39 和 13:39 运行的命令。所选的值是随机的，但 Certbot 开发人员建议每天运行该命令至少两次。这将确保立即撤销并替换任何发现已损坏的证书。

`root`

该命令使用根权限运行。

`certbot renew --no-self-upgrade`

将要运行的命令。`renew` 子命令会使 Certbot 检查任何先前获取的证书并续订即将到期的证书。`--no-self-upgrade` 标记可防止 Certbot 在没有您干预的情况下自行升级。

2. 重启 cron 守护程序。

```
[ec2-user ~]$ sudo systemctl restart crond
```

教程：在 Amazon Linux 上配置 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。本教程介绍如何在具有 Amazon Linux AMI 和 Apache Web 服务器的 EC2 实例上手动添加对 SSL/TLS 的支持。如果您计划提供商业级服务，[AWS Certificate Manager](#)（此处未作介绍）是一个不错的选择。

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，但使用其下一代协议 TLS 更不易受攻击。默认情况下，Amazon Linux AMI 将禁用所有版本的 SSL 的服务器端支持。[安全标准机构](#)认为

TLS 1.0 不太安全，并且 IETF 即将正式弃用 TLS 1.0 和 TLS 1.1。本教程仅包含有关启用 TLS 1.2 的指导。（较新的 TLS 1.3 协议处于草案形式，但在 Amazon Linux 2 上尚不支持。）有关更新的加密标准的更多信息，请参阅 [RFC 7568](#) 和 [RFC 8446](#)。

在本教程中，将现代 Web 加密简称为 TLS。

Important

这些过程适用于 Amazon Linux AMI。如果您尝试具有其他分配的实例上设置 LAMP Web 服务器，则本教程中的一些过程可能不适合您。有关 Ubuntu 上的 LAMP Web 服务器的信息，请参阅 Ubuntu 社区文档 [ApacheMySQLPHP](#)。有关 Red Hat Enterprise Linux 的信息，请参阅客户门户网站文档 [Web 服务器](#)。

目录

- [先决条件 \(p. 68\)](#)
- [步骤 1：在服务器上启用 TLS \(p. 68\)](#)
- [步骤 2：获取 CA 签名的证书 \(p. 70\)](#)
- [步骤 3：测试和强化安全配置 \(p. 74\)](#)
- [故障排除 \(p. 76\)](#)
- [证书自动化：在 Amazon Linux 上将 Let's Encrypt 与 Certbot 结合使用 \(p. 76\)](#)

先决条件

在开始本教程之前，请完成以下步骤：

- 使用 Amazon Linux AMI 启动 EBS 支持的实例。有关更多信息，请参阅 [步骤 1：启动实例 \(p. 25\)](#)。
 - 配置安全组以允许您的实例接受以下 TCP 端口上的连接：
 - SSH (端口 22)
 - HTTP (端口 80)
 - HTTPS (端口 443)
- 有关更多信息，请参阅 [为您的 Linux 实例授权入站流量 \(p. 757\)](#)。
- 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 \(p. 37\)](#)。仅需要 http24 包及其依赖项；可以忽略涉及 PHP 和 MySQL 的说明。
 - 为了识别和验证网站，TLS 公有密钥基础设施 (PKI) 依赖于域名系统 (DNS)。要使用 EC2 实例托管公共网站，您需要为 Web 服务器注册一个域名，或者将现有域名转让给您的 Amazon EC2 主机。可通过很多第三方域注册和 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 TLS

该过程指导您完成在 Amazon Linux 上使用自签名数字证书设置 TLS 的过程。

Note

自签名证书对于测试是可接受的，但对于生产不是。如果您将自签名证书公开到 Internet，则您网站的访客将收到安全警告。

在服务器上启用 TLS

1. [连接到您的实例 \(p. 26\)](#) 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
```

- 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，则可以忽略该选项。

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

- 现在，您的实例是最新的，请安装 Apache 模块 mod_ssl 以添加 TLS 支持：

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

您的实例现在具有以下文件，可使用这些文件配置安全服务器并创建证书以进行测试：

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

mod_ssl 的配置文件。它包含一些“指令”以指示 Apache 在何处查找以下信息：加密密钥和证书、要允许的 TLS 协议版本以及要接受的加密密码。

/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。在安装期间，OpenSSL 已使用此密钥生成自签名主机证书，您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。要测试是否正确设置 Apache 以使用 TLS，该证书是非常有用的。

.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-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvCNQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb21lU3RhGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bmlOMRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvCNQkBFhV
...
z5rRUE/XzxrLBZOOwZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
WanXWehT6FiSzvB4sTEXXJN2jdw8g+sHgnZ8zCoSclknYhHrCVD2vnBlZJKSzvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHod0BQE8sBJxg==
-----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 cert.crt 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.pem、ssl.conf 或任何其他文件名。

Note

在使用您自己的自定义文件替换默认 TLS 文件时，请确保它们采用 PEM 格式。

- 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主机证书连接到站点，因此您的浏览器可能会显示一系列安全警告。

忽视这些警告并继续连接站点。如果默认 Apache 测试页面打开，这意味着您已成功在服务器上配置 TLS。在浏览器和服务器之间传输的所有数据现在都被安全地加密了。

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

您可以使用以下过程获取 CA 签名证书：

- 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)
- 获取签名的主机证书
- 配置 Apache 以使用证书

从加密角度看，自签名 TLS X.509 主机证书与 CA 签名证书完全相同。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，或可通过由其他可信签署人组成的一系列信任访问，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 [dmoztools.net](#) 上可找到知名 CA 的列表。一些 CA 免费提供基础级别证书。其中最值得注意的是 [Let's Encrypt](#) 项目，该项目还支持证书创建和续订过程的自动化。有关将 Let's Encrypt 用作 CA 的更多信息，请参阅[证书自动化：在 Amazon Linux 上将 Let's Encrypt 与 Certbot 结合使用 \(p. 76\)](#)。

主机证书的基础是密钥。自 2017 年起，[政府](#)和[行业](#)群体建议对 RSA 密钥使用 2048 位的最小密钥 (模数) 大小，旨在保护文档直到 2030 年。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。

除非您拥有注册并托管的 DNS 域，否则，有关获取 CA 签名主机证书的说明将不适用。

获取 CA 签名的证书

1. [连接到您的实例 \(p. 26\)](#)并导航到 `/etc/pki/tls/private/`。这是存储适用于 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。下面是一些密钥配置示例。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。
 - 示例 1：创建默认 RSA 主机密钥。生成的文件 `custom.key` 是一个 2048 位 RSA 私有密钥。

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

- 示例 2：创建具有更大模数的更严格的 RSA 密钥。生成的文件 `custom.key` 是一个 4096 位 RSA 私有密钥。

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

- 示例 3：创建具有密码保护的 4096 位加密的 RSA 密钥。生成的文件 `custom.key` 是一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

Important

对密钥进行加密可增强安全性，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，都必须通过 SSH 连接提供密码（在上一示例中为“abcde12345”）。

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

- 示例 4：使用非 RSA 密码创建密钥。RSA 加密可能相对较慢，因为其公有密钥的大小基于两个大素数的乘积。不过，可以为 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，计算起来更快。

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

结果为一个使用 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所有权和权限（所有者=根、组=根、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。

- 使用您的首选密钥创建 CSR；下面的示例将使用 **custom.key**：

```
[ec2-user ~]$ sudo openssl req -new -key custom.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主机证书来说，除 Common Name 以外的所有字段都是可选字段。

名称	描述	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 Corporation
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	www.example.com

名称	描述	示例
	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> ）。	
电子邮件地址	服务器管理员的电子邮件地址。	someone@example.com

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。您网站的访客如果键入这两个名称的任何一个，便可看到一个没有错误的连接。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。

Note

您的 CA 可能会针对各种不同用途，发送多种格式的文件。对于本教程，您应该只使用 PEM 格式的证书文件，此格式通常会（但不总会）标有 `.pem` 或 `.crt` 扩展名。如果您不确定要使用哪个文件，请用文本编辑器打开这些文件，并查找包含一个或多个具有以下开头的块的文件：

```
- - - - -BEGIN CERTIFICATE - - - - -
```

该文件还应具有以下结尾：

```
- - - - -END CERTIFICATE - - - - -
```

您还可以如下所示在命令行上测试文件：

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

验证这些行是否显示在文件中。请勿使用结尾为 `.p7b`、`.p7c` 或类似文件扩展名的文件。

- 将新的 CA 签名证书和任何中间证书放在 `/etc/pki/tls/certs` 目录中。

Note

可通过多种方法将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在您的本地计算机和实例上打开一个文本编辑器（例如，`vi`、`nano` 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。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，使用以下命令验证文件所有权、组和权限设置是否与高度限制的 Amazon Linux 默认权限（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。

```
[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、组=根、所有者可以写入、组可以读取、任何人均可读取)。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
```

6. 如果您使用自定义密钥创建您的 CSR 和由此生成的主机证书，请从 /etc/pki/tls/private/ 目录中删除或重命名旧密钥，然后在该目录中安装新密钥。

Note

有多种方法可以将自定义密钥上传到 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并粘贴文件内容。当在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。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/private 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（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。命令如下：

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

上述命令应生成以下结果：

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

7. 编辑 /etc/httpd/conf.d/ssl.conf 以反映您的新证书和密钥文件。
 - a. 在 Apache 的 SSLCertificateFile 指令中提供 CA 签名主机证书的路径和文件名：

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

- b. 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
```

Note

一些 CA 将主机证书和中间证书组合到一个文件中，便不再需要此指令了。请查询您的 CA 提供的说明。

- c. 在 Apache 的 SSLCertificateKeyFile 指令中提供私有密钥的路径和文件名：

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

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

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

- 通过在浏览器 URL 栏中输入带有 `https://` 前缀的域名来测试您的服务器。您的浏览器应通过 HTTPS 加载测试页面而不会产生错误。

步骤 3：测试和强化安全配置

在 TLS 可操作且公开展示后，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。虽然概述信息显示配置基本正确，但详细报告标记了几个潜在的问题。例如：

- 支持某些旧浏览器使用 RC4 密码。密码是加密算法的数学核心。RC4 是一种用于加密 TLS 数据流的快速密码，已知这种密码存在一些[严重缺点](#)。除非您有充分理由支持旧版浏览器，否则，应禁用该密码。
- 支持旧 TLS 版本。该配置支持 TLS 1.0（已弃用）和 TLS 1.1（即将弃用）。从 2018 年开始，仅建议使用 TLS 1.2。

纠正 TLS 配置

- 在文本编辑器中打开 `/etc/httpd/conf.d/ssl.conf` 配置文件，并在以下每个行的开头键入“#”来注释掉这些行：

```
#SSLProtocol all -SSLv3  
#SSLProxyProtocol all -SSLv3
```

- 添加以下指令：

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

这些指令显式禁用 SSL 版本 2 和 3，以及 TLS 版本 1.0 和 1.1。现在，服务器拒绝接受与使用 TLS 1.2 以外的任何协议的客户端之间的加密连接。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。

Note

以此方式禁用 TLS 1.0 和 1.1 版可阻止一小部分过时的 Web 浏览器访问您的网站。

修改允许的密码列表

- 打开配置文件 `/etc/httpd/conf.d/ssl.conf`，找到包含用于配置 `SSLCipherSuite` 和 `SSLProxyCipherSuite` 的已注释掉的示例的部分。

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
#SSLProxyCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

保留它们不变，并在它们下面添加以下指令：

Note

此处为方便阅读将指令显示为几行，但这两个指令必须各在一行上且密码名称之间不能有空格。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES:!aNULL:!
eNULL:!EXPORT:!DES:
!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

SSLProxyCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-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：

- 对向前保密性的支持
- Strength
- Speed
- 具体密码位于密码系列之前
- 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很多可能的列表之一；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 Classic Load Balancer 用户指南中的 [Elastic Load Balancing 的预定义 SSL 安全策略](#)。

2. 通过删除“#”取消对以下行的注释：

```
#SSLHonorCipherOrder on
```

该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。

3. 重启 Apache。如果您在 [Qualys SSL Labs](#) 上再次测试域，应会发现 RC4 漏洞已修复。

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。

您可以从密钥中删除加密和密码要求。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`，则对 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。

证书自动化：在 Amazon Linux 上将 Let's Encrypt 与 Certbot 结合使用

[Let's Encrypt](#) 证书颁发机构是电子前沿基金会 (EFF) 致力于加密整个 Internet 的核心所在。按照该目标，Let's Encrypt 主机证书被设计为用最小的人工干预来进行创建、验证、安装和维护。证书管理的自动化方面由在 Web 服务器上运行的代理执行。在安装并配置代理后，它与 Let's Encrypt 安全地通信并在 Apache 和密钥管理系统上执行管理任务。本教程使用免费的 [Certbot](#) 代理，因为它允许您提供自定义的加密密钥作为您的证书的基础，或允许代理自身根据其默认值创建密钥。您也可以将 Certbot 配置为定期续订您的证书，无需人工交互，如[自动化 Certbot \(p. 67\)](#) 中所述。有关更多信息，请参阅 Certbot [用户指南](#)或[手册页](#)。

虽然 Certbot 不受 Amazon Linux AMI 官方支持，但可供下载并在安装后正常工作。建议您执行以下备份来保护数据并避免造成不便：

- 在开始之前，请为您的 Amazon EBS 根卷制作快照。这使您能够还原 EC2 实例的原始状态。有关创建 EBS 快照的信息，请参阅[创建 Amazon EBS 快照 \(p. 815\)](#)。
- 以下过程要求您编辑您的 `httpd.conf` 文件，该文件控制 Apache 的操作。Certbot 对此配置文件和其他配置文件进行其自动化更改。创建整个 `/etc/httpd` 目录的备份副本，以便您在需要时还原该目录。

安装并运行 Certbot

- 在您的实例上从 Fedora 项目启用 Extra Packages for Enterprise Linux (EPEL) 存储库。当您运行 Certbot 安装脚本时，EPEL 中的程序包作为依赖项是必需的。

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

- 使用以下命令，从 EFF 将最新版本的 Certbot 下载到您的 EC2 实例上。

```
[ec2-user ~]$ wget https://dl.eff.org/certbot-auto
```

- 使下载的文件成为可执行文件。

```
[ec2-user ~]$ chmod a+x certbot-auto
```

- 运行具有根权限和 `--debug` 标记的文件。

```
[ec2-user ~]$ sudo ./certbot-auto --debug
```

5. 在提示符“Is this ok [y/d/N]”处，键入“y”并按 Enter。
6. 在提示符“Enter email address (used for urgent renewal and security notices)”处，键入联系人地址并按 Enter。
7. 在提示符处，同意 Let's Encrypt 服务条款。键入“A”并按 Enter 以继续：

```
-----  
Please read the Terms of Service at  
https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.pdf. You must agree  
in order to register with the ACME server at  
https://acme-v01.api.letsencrypt.org/directory  
-----  
(A)gree/(C)ancel: A
```

8. 通过连续单击完成授权以使 EFF 将您放入发送名单上，具体做法是键入“Y”或“N”并按 Enter。
9. 在下面显示的提示符处，键入您的公用名（您的域的名称，如上所述）和您的主题替换名称（SAN），两个名称之间用空格或逗号分隔。然后按 Enter。在此示例中，已经提供了这些名称：

```
No names were found in your configuration files. Please enter in your domain  
name(s) (comma and/or space separated) (Enter 'c' to cancel): example.com  
www.example.com
```

10. 在具有默认 Apache 配置的 Amazon Linux 系统上，您将看到类似以下示例的输出，询问您提供的第一个名称。键入“1”并按 Enter。

```
Obtaining a new certificate  
Performing the following challenges:  
tls-sni-01 challenge for example.com  
tls-sni-01 challenge for www.example.com  
  
We were unable to find a vhost with a ServerName or Address of example.com.  
Which virtual host would you like to choose?  
(note: conf files with multiple vhosts are not yet supported)  
-----  
1: ssl.conf | HTTPS | Enabled  
-----  
Press 1 [enter] to confirm the selection (press 'c' to cancel): 1
```

11. 接下来，Certbot 询问第二个名称。键入“1”并按 Enter。

```
We were unable to find a vhost with a ServerName or Address of www.example.com.  
Which virtual host would you like to choose?  
(note: conf files with multiple vhosts are not yet supported)  
-----  
1: ssl.conf | HTTPS | Enabled  
-----  
Press 1 [enter] to confirm the selection (press 'c' to cancel): 1
```

此时，Certbot 创建密钥和 CSR：

```
Waiting for verification...  
Cleaning up challenges  
Generating key (2048 bits): /etc/letsencrypt/keys/0000_key-certbot.pem  
Creating CSR: /etc/letsencrypt/csr/0000_csr-certbot.pem
```

12. 授权 Certbot 以创建所有必需的主机证书。在提示输入每个名称时，键入“1”并按 Enter，如示例所示：

```
We were unable to find a vhost with a ServerName or Address of example.com.  
Which virtual host would you like to choose?  
(note: conf files with multiple vhosts are not yet supported)  
-----  
1: ssl.conf | | HTTPS | Enabled  
-----  
Press 1 [enter] to confirm the selection (press 'c' to cancel): 1  
Deploying Certificate for example.com to VirtualHost /etc/httpd/conf.d/ssl.conf  
  
We were unable to find a vhost with a ServerName or Address of www.example.com.  
Which virtual host would you like to choose?  
(note: conf files with multiple vhosts are not yet supported)  
-----  
1: ssl.conf | example.com | HTTPS | Enabled  
-----  
Press 1 [enter] to confirm the selection (press 'c' to cancel): 1  
Deploying Certificate for www.example.com to VirtualHost /etc/httpd/conf.d/ssl.conf
```

13. 选择是否允许与您的 Web 服务器建立不安全的连接。如果您选择选项 2 (如示例所示) , 则所有与您服务器的连接都将被加密或拒绝。

```
Please choose whether HTTPS access is required or optional.  
-----  
1: Easy - Allow both HTTP and HTTPS access to these sites  
2: Secure - Make all requests redirect to secure HTTPS access  
-----  
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
```

Certbot 完成 Apache 的配置并报告成功和其他信息 :

```
Congratulations! You have successfully enabled https://example.com and  
https://www.example.com
```

```
You should test your configuration at:  
https://www.ssllabs.com/ssltest/analyze.html?d=example.com  
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
```

IMPORTANT NOTES:

```
- Congratulations! Your certificate and chain have been saved at  
/etc/letsencrypt/live/example.com/fullchain.pem. Your cert will  
expire on 2017-07-19. To obtain a new or tweaked version of this  
certificate in the future, simply run certbot-auto again with the  
"certonly" option. To non-interactively renew *all* of your  
certificates, run "certbot-auto renew"  
....
```

14. 在完成安装后 , 测试并优化您服务器的安全性 , 如[步骤 3 : 测试和强化安全配置 \(p. 61\)](#)中所述。

Certbot 被设计成服务器系统的一个不可见的防错部分。默认情况下 , 它会生成具有短暂的 90 天到期时间的主机证书。如果您之前未将系统配置为自动调用命令 , 则必须手动重新运行 certbot 命令。此过程介绍如何通过设置 cron 作业来实现 Certbot 自动化。

配置自动证书续订

1. 首次成功运行 Certbot 后 , 用文本编辑器打开 /etc/crontab , 并添加类似如下的行 :

```
39      1,13    *      *      *      root    certbot renew --no-self-upgrade
```

完成后保存文件。这是每个组件的说明：

```
39 1,13 * * *
```

排定一个在每天 01:39 和 13:39 运行的命令。所选的值是随机的，但 Certbot 开发人员建议每天运行该命令至少两次。这将确保立即撤销并替换任何发现已损坏的证书。

root

该命令使用根权限运行。

```
certbot renew --no-self-upgrade
```

将要运行的命令。renew 子命令会使 Certbot 检查任何先前获取的证书并续订即将到期的证书。--no-self-upgrade 标记可防止 Certbot 在没有您干预的情况下自行升级。

2. 重启 cron 守护程序：

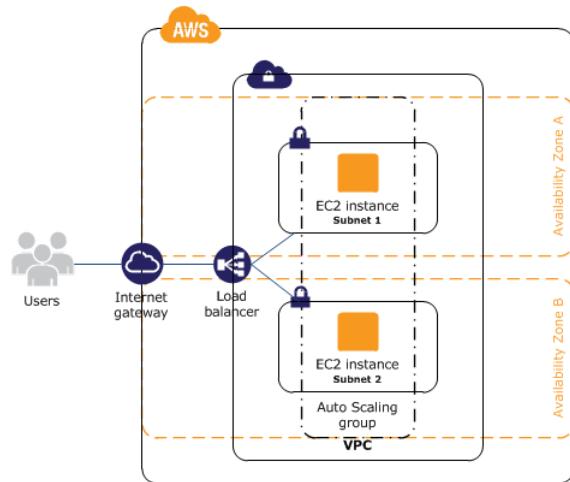
```
[ec2-user ~]$ sudo service crond restart
```

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 Amazon EC2 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。Amazon EC2 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 Amazon EC2 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 Amazon EC2 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 [Amazon EC2 Auto Scaling](#) 和 [Elastic Load Balancing](#)。



目录

- [先决条件 \(p. 80\)](#)
- [对应用程序进行扩展和负载均衡 \(p. 80\)](#)

- 测试负载均衡器 (p. 81)

先决条件

本教程假定您已执行以下操作：

1. 已创建了一个 Virtual Private Cloud (VPC)，它在两个或更多可用区中有一个公有子网。如果您尚未设置，请参阅[创建 Virtual Private Cloud \(VPC\) \(p. 21\)](#)。
2. 已在 VPC 中启动一个实例。
3. 已连接到该实例并对其进行自定义。例如，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：使用 Amazon Linux AMI 安装 LAMP Web 服务器 \(p. 37\)](#)。
4. 已测试实例上的应用程序以确保实例的配置是正确的。
5. 已从实例创建了自定义 Amazon 系统映像 (AMI)。有关更多信息，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 102\)](#)或[创建由实例存储支持的 Linux AMI \(p. 105\)](#)。
6. (可选) 如果不再需要该实例，已将其终止。
7. 已创建一个 IAM 角色，它为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 \(p. 752\)](#)。

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. 对于 Application Load Balancer，选择 Create。
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网。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”，Port 为“80”，Target type 为“instance”。
 - d. 对于 Health checks，保留默认协议和路径。
 - e. 选择 Next: Register Targets。
9. 在 Register Targets (注册目标) 页面上，选择 Next: Review (下一步: 审核) 继续到下一页，因为我们将使用 Amazon EC2 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 Amazon EC2 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 \(p. 80\)](#)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 \(p. 80\)](#)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 (高级详细信息) 并在 User data (用户数据) 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 Amazon EC2 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 (组大小)，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 (配置扩展策略) 页面上，选择 Review (审核)，因为我们打算让 Amazon EC2 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 (Auto Scaling 组) 页面选择 Auto Scaling 组，然后选择 Instances (实例) 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。

Amazon 系统映像 (AMI)

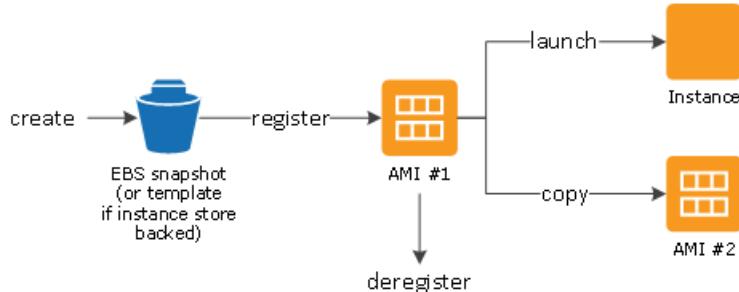
Amazon 系统映像 (AMI) 提供启动实例所需的信息。在启动实例时，您必须指定 AMI。在需要具有相同配置的多个实例时，您可以从单个 AMI 启动多个实例。在需要不同的配置的实例时，您可以使用其他 AMI 启动实例。

AMI 包括以下内容：

- 一个或多个 EBS 快照；对于由实例存储支持的 AMI，包括一个用于实例（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。
- 数据块设备映射，指定在实例启动时要附加到实例的卷。

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。）您可以在同一区域中或者向不同区域复制 AMI。不再需要某个 AMI 时，可以将其取消注册。



您可以搜索符合您的实例条件的 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 \(p. 84\)](#) 和 [查找 Linux AMI \(p. 88\)](#)。

从 AMI 启动实例后，您可以连接到该实例。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 \(p. 160\)](#)。

创建您自己的 AMI

您可从现有 AMI 启动实例，自定义实例，然后将此更新后的配置另存为自定义 AMI。从该新自定义 AMI 启动的实例包括您在创建 AMI 时设置的自定义项。

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 \(p. 13\)](#)。

要创建由 Amazon EBS 支持的 AMI，请参阅 [创建 Amazon EBS 支持的 Linux AMI \(p. 102\)](#)。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 \(p. 105\)](#)。

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[标记您的 Amazon EC2 资源 \(p. 940\)](#)。

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 \(p. 90\)](#)。

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 \(p. 99\)](#)。

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。从 AMI 启动的现有实例不受影响。有关更多信息，请参阅[取消注册您的 Linux AMI \(p. 142\)](#)。

Amazon Linux 2 和 Amazon Linux AMI

Amazon Linux 2 和 Amazon Linux AMI 是 AWS 提供、支持和维护的 Linux 映像。以下是一些 Amazon Linux 2 和 Amazon Linux AMI 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 \(p. 144\)](#)。

AMI 类型

可以基于以下特性选择要使用的 AMI：

- 区域 (请参阅[区域、可用区和本地区域 \(p. 6\)](#))
- 操作系统
- 架构 (32 位或 64 位)
- [启动许可 \(p. 84\)](#)
- [根设备存储 \(p. 85\)](#)

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	描述
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。
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 \(p. 90\)](#)。开发人员可以为其 AMI 收费。有关更多信息，请参阅[付费 AMI \(p. 99\)](#)。

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 \(p. 13\)](#)。

下表总结了使用两种类型的 AMI 时的重要区别。

特征	由 Amazon EBS 支持的 AMI	由 Amazon 实例存储支持的 AMI
实例的启动时间	通常不到 1 分钟	通常不到 5 分钟
根设备的大小限制	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，实例终止时将删除根卷。 [*] 默认情况下，在实例终止后，任何其他 Amazon EBS 卷上的数据仍然存在。	任意实例存储卷上的数据仅在实例的生命周期内保留。
修改	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 \(p. 15\)](#)。

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 (根设备类型) 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 实例存储支持的实例不能被停止，所以它们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 \(p. 445\)](#)。

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）。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。如果实例出故障或终止，实例存储卷上的所有数据均会删除。有关更多信息，请参阅 [实例存储生命周期 \(p. 904\)](#)。

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。对于大多数实例类型，Amazon EBS 支持的实例在默认情况下不具有实例存储卷。您可以使用块储存设备映射添加实例存储卷或连接 Amazon EBS 卷。有关更多信息，请参阅 [块储存设备映射 \(p. 923\)](#)。

启动时间

从 Amazon EBS 支持的 AMI 启动的实例比从实例存储支持的 AMI 启动的实例启动得快。当您从实例存储支持的 AMI 启动实例时，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 \(p. 102\)](#)。

如何向您收费

如果您使用由实例存储提供支持的 AMI，您需要为实例使用和在 Amazon S3 中存储 AMI 付费。如果您使用由 Amazon EBS 支持的 AMI，您需要为实例使用、Amazon EBS 卷的存储和使用、以 Amazon EBS 快照形式存储 AMI 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，每个自定义 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。一旦您启动实例时，我们便会收取最低一分钟的使用费用。一分钟之后，我们将按您使用的秒数收费。例如，如果您运行一个实例 20 秒后停止实例，我们将按一整分钟收取费用。如果您运行一个实例 3 分 40 秒，我们将收取 3 分 40 秒的使用费用。我们将对您的实例保持运行状态的每秒钟收取费用，最低一分钟，即使实例处于闲置状态并且您没有连接到它也是如此。

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。有关当前一代实例类型的更多信息，请参阅 [Amazon EC2 实例类型](#)。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](#)。

HVM AMI

硬件虚拟机 AMIs 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 [Linux 上的增强联网 \(p. 616\)](#) 和 [Linux 加速计算实例 \(p. 222\)](#)。

支持 HVM AMI 的所有实例类型。

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

半虚拟化 AMIs 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周期，然后对映像链式加载 `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 [启用您自己的 Linux 内核 \(p. 154\)](#)。

以下上一代实例类型支持 PV AMI：C1、C3、HS1、M1、M3、M2 和 T1。最新一代实例类型不支持 PV AMI。

以下 AWS 区域支持半虚拟化实例：亚太区域（东京）、亚太区域（新加坡）、亚太区域（悉尼）、欧洲（法兰克福）、欧洲（爱尔兰）、南美洲（圣保罗）、美国东部（弗吉尼亚北部）、美国西部（加利福尼亚北部）和美国西部（俄勒冈）。

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，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仍可以通过它们获得存储和网络 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)、64 位 (x86_64) 或 64 位 ARM (arm64)
- 根设备类型：Amazon EBS 或实例存储
- 提供商 (例如，Amazon Web Services)
- 其他软件 (例如，SQL Server)

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](#)。

目录

- [使用 Amazon EC2 控制台查找 Linux AMI \(p. 88\)](#)
- [使用 AWS CLI 查找 AMI \(p. 89\)](#)
- [查找快速启动 AMI \(p. 89\)](#)

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) 页面搜索所有可用的 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。AMI ID 在每个区域中都是唯一的。

使用“Choose AMI”(选择 AMI) 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，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 从控制台控制面板中，选择 Launch Instance。
4. 在快速启动选项卡上，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“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，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 在导航窗格中，选择 AMIs。
4. (可选) 使用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 \(p. 85\)](#)。
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 \(p. 376\)](#)。如果您没有准备好立即启动实例，请记下 AMI ID 以供将来使用。

使用 AWS CLI 查找 AMI

您可以使用适用于 Amazon EC2 的 AWS CLI 命令列出满足您需求的 Linux AMI。找到满足您需求的 AMI 之后，记录其 ID，以便用它来启动实例。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](#)。

`describe-images` 命令支持筛选参数。例如，使用 `--owners` 参数显示由 Amazon 拥有的公有 AMI。

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

您可以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"
```

Important

在 `describe-images` 命令中省略 `--owners` 标记将返回您拥有启动权限的所有映像，无论所有权如何。

查找快速启动 AMI

当您使用 Amazon EC2 控制台启动一个实例时，选择一个 Amazon 系统映像 (AMI) 页面将在快速启动选项卡中列出常用的 AMI。如果您想要使用其中一个快速启动 AMI 来自动启动实例，您需要以编程方式找到 AMI 当前版本的 ID。

要找到快速启动 AMI 的当前版本，您可以通过其 AMI 名称枚举所有 AMI，然后找到具有最新创建日期的 AMI。

Example 示例：查找当前 Amazon Linux 2 AMI

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=amzn2-ami-hvm-2.0.???????.?-x86_64-gp2' 'Name=state,Values=available' --query 'reverse(sort_by(Images, &CreationDate))[:1].ImageId' --output text
```

Example 示例：查找当前 Amazon Linux AMI

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=amzn-ami-hvm-????.?.?.???????.x86_64-gp2' 'Name=state,Values=available' --query 'reverse(sort_by(Images, &CreationDate))[:1].ImageId' --output text
```

Example 示例：查找当前 Ubuntu Server 16.04 LTS AMI

```
aws ec2 describe-images --owners 099720109477 --filters 'Name=name,Values=ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-???????' 'Name=state,Values=available' --query 'reverse(sort_by(Images, &CreationDate))[:1].ImageId' --output text
```

Example 示例：查找当前 Red Hat Enterprise Linux 7.5 AMI

```
aws ec2 describe-images --owners 309956199498 --filters 'Name=name,Values=RHEL-7.5_HVM_GA*' 'Name=state,Values=available' --query 'reverse(sort_by(Images, &CreationDate))[:1].ImageId' --output text
```

Example 示例：查找当前 SUSE Linux Enterprise Server 15 AMI

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=suse-sles-15-v????????-hvm-ssd-x86_64' 'Name=state,Values=available' --query 'reverse(sort_by(Images, &CreationDate))[:1].ImageId' --output text
```

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](#)。

目录

- [查找共享 AMI \(p. 90\)](#)
- [将 AMI 设为公用 \(p. 92\)](#)
- [将 AMI 与特定 AWS 账户共享 \(p. 93\)](#)
- [使用书签 \(p. 95\)](#)
- [共享 Linux AMI 指导原则 \(p. 95\)](#)

查找共享 AMI

可以使用 Amazon EC2 控制台或命令行查找共享 AMI。

Note

AMI 是一种区域性资源。因此，在搜索共享 AMI（公有或私有）时，必须在共享此 AMI 的区域中进行搜索。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](#)。

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。

- 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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 AMIs。
- 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。
- 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 (AWS CLI)

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。

示例：列出所有公用 AMI

以下命令将列出所有公用 AMI，包括您拥有的所有公用 AMI。

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

示例：使用显式启动许可列出 AMI

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 AMI。

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

示例：列出 Amazon 拥有的 AMI

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
```

示例：列出账户拥有的 AMI

以下命令列出指定 AWS 账户拥有的 AMI。

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

示例：使用筛选条件确定 AMI 的范围

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"
```

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凭证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的实例的访问，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凭证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：

```
[ec2-user ~]$ 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 `sshd_config` 文件并编辑行，如下所示：

```
PermitRootLogin without-password
```

或者，您可以禁用以根用户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：

```
[ec2-user ~]$ sudo rm /etc/rsyslog.config  
[ec2-user ~]$ 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 \(p. 93\)](#)）。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。

无法公开带有加密卷的 AMI。

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 \(p. 138\)](#)。

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 \(p. 95\)](#)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，或包含加密卷的快照，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 (AWS CLI)

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。

可以在具有 AMI 启动许可的账户的列表中添加或删除账户 ID。要将 AMI 设为公有，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

1. 使用 `modify-image-attribute` 命令可将 `all` 组添加到指定 AMI 的 `launchPermission` 列表，如下所示。

```
aws ec2 modify-image-attribute --image-id ami-0abcdef1234567890 --launch-permission "Add=[{Group=all}]"
```

2. 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-0abcdef1234567890 --attribute launchPermission
```

- 3.（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，因此不受该命令影响。

```
aws ec2 modify-image-attribute --image-id ami-0abcdef1234567890 --launch-permission "Remove=[{Group=all}]"
```

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。如果共享带有加密卷的 AMI，那么还必须共享用于对这些卷加密的所有 CMK。有关更多信息，请参阅[共享 Amazon EBS 快照 \(p. 822\)](#)。

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 \(p. 138\)](#)。

可以共享 AMI 的 AWS 账户数量没有限制。

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 账号字段中指定您想与之共享 AMI 的用户的 AWS 账号，然后选择添加权限。
要与多个用户共享此 AMI，请重复此步骤，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。不过，您确实需要共享用于对 AMI 引用的快照加密的所有 CMK。有关更多信息，请参阅[共享 Amazon EBS 快照 \(p. 822\)](#)。

6. 完成后选择保存。
7. (可选) 要查看您已共享 AMI 的 AWS 账户 ID，请在列表中选择此 AMI，然后选择权限选项卡。要查找与您共享的 AMI，请参阅[查找共享 AMI \(p. 90\)](#)。

共享 AMI (AWS CLI)

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

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-0abcdef1234567890 --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
```

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。不过，您确实需要共享用于对 AMI 引用的快照加密的所有 CMK。有关更多信息，请参阅[共享 Amazon EBS 快照 \(p. 822\)](#)。

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-0abcdef1234567890 --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，因此不受该命令影响。

```
aws ec2 reset-image-attribute --image-id ami-0abcdef1234567890 --attribute launchPermission
```

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. 键入一个带有下列信息的 URL，其中 region 表示您的 AMI 驻留的区域：

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

例如，此 URL 从 us-east-1 区域的 ami-0abcdef1234567890 AMI 启动实例：

```
https://console.aws.amazon.com/ec2/v2/home?region=us-  
east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
```

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

- 在使用 AMI 工具之前对其进行更新 (p. 96)
- 对根禁用基于密码的远程登录 (p. 96)
- 禁用本地根访问 (p. 96)
- 删除 SSH 主机密钥对 (p. 96)
- 安装公有密钥凭证 (p. 97)
- 禁用 sshd DNS 检查 (可选) (p. 98)
- 标识您的身份 (p. 98)
- 保护自己 (p. 98)

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](#)

在使用 AMI 工具之前对其进行更新

对于实例存储支持的 AMI，建议您的 AMI 先下载和更新 Amazon EC2 AMI 创建工具，然后再使用这些工具。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 2，安装 aws-amitools-ec2 软件包，并使用以下命令将 AMI 工具添加到 PATH。对于 Amazon Linux AMI，默认情况下已安装 aws-amitools-ec2 程序包。

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

使用以下命令升级 AMI 工具：

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

对于其他发行版，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
```

若您的发行版不同或您未运行 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

该命令不影响 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。

安装公有密钥凭证

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。

很多发行版（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凭证。如果您的发行版不支持 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根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

若您的发行版不同或您未运行 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。

保护自己

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 `--exclude directory` 使用 `ec2-bundle-vol` 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`（对于根账户）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 \(p. 121\)](#)。
- 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。将上述密钥和凭证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。

目录

- [出售 AMI \(p. 99\)](#)
- [查找付费 AMI \(p. 99\)](#)
- [购买付费 AMI \(p. 100\)](#)
- [获取实例的产品代码 \(p. 101\)](#)
- [使用付费支持 \(p. 101\)](#)
- [付费和支持 AMI 的账单 \(p. 101\)](#)
- [管理 AWS Marketplace 订阅 \(p. 101\)](#)

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，如由 Amazon EBS 支持的 AMI、预留实例和 Spot 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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 AMIs。
- 对于第一个筛选条件，选择公有映像。

4. 在搜索栏中选择拥有者，然后选择 AWS Marketplace。
5. 如果您知道产品代码，请选择产品代码，然后键入产品代码。

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 AWS CLI 查找付费 AMI

您可以使用以下 [describe-images \(AWS CLI\)](#) 查找付费 AMI。

```
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"  
    }  
,
```

如果您知道产品代码，可以按产品代码筛选结果。此示例返回具有指定产品代码的最新 AMI。

```
aws ec2 describe-images --owners aws-marketplace \  
--filters "Name=product-code,Values=product_code" \  
--query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

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 \(p. 389\)](#)。

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 \(p. 389\)](#)。

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 \(p. 499\)](#)。

要检索产品代码，请使用以下命令：

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

如果您的实例支持它，您可以使用 GET 命令：

```
[ec2-user ~]$ 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。

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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS 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. 选择 Your Marketplace Account。
3. 选择 Manage your software subscriptions。
4. 会列出当前所有订阅。选择 Usage Instructions 以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 <https://console.aws.amazon.com/ec2/>。
 - b. 在导航窗格中，选择 Instances。
 - c. 选择所需实例，然后依次选择 Actions、Instance State、Terminate。
 - d. 当系统提示您确认时，选择 Yes, Terminate。
2. 登录到 [AWS Marketplace](#)，选择 Your Marketplace Account，然后选择 Manage your software subscriptions。
3. 选择 Cancel subscription。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。这可以是您从 AWS Marketplace 获得的 AMI、您使用 [AWS Server Migration Service](#) 或 [VM Import/Export](#) 创建的 AMI 或您可以访问的任何其他 AMI。根据您的需要自定义实例后，创建并注册新的 AMI，用它来启动具有这些自定义项的新实例。

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 AMIs 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 \(p. 85\)](#)。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 \(p. 105\)](#)。

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](#)。

创建 Amazon EBS 支持的 AMIs 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。在注销 AMI 并删除快照之前，您需要支付快照的费用。有关更多信息，请参阅[取消注册您的 Linux AMI \(p. 142\)](#)。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 \(p. 851\)](#)。

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）。您可能会发现先创建卷的快照，然后再创建 AMI 后会更高效。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 \(p. 815\)](#)。

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。

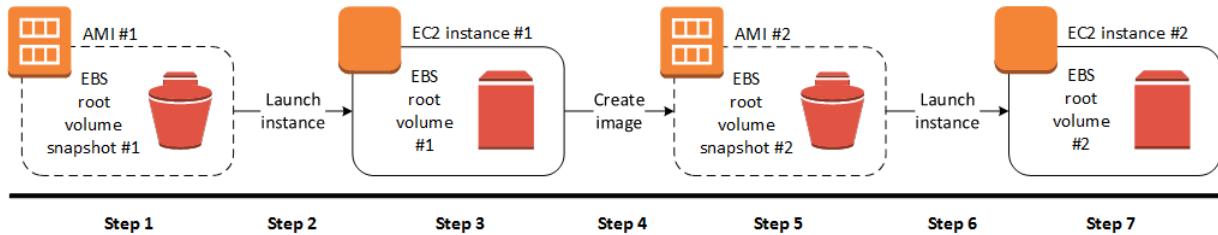
如果除了根设备卷之外，您还向实例添加了实例存储卷或 EBS 卷，则新 AMI 的块储存设备映射包含这些卷的信息，并且您从新 AMI 启动的实例的块储存设备映射自动包含这些卷的信息。新实例的块储存设备映射中指定的实例存储卷是新的，不包含用于创建 AMI 的实例的实例存储卷中的任何数据。EBS 卷上的数据会持久保留。有关更多信息，请参阅 [块储存设备映射 \(p. 923\)](#)。

Note

当您从由 EBS 支持的 AMI 创建新实例时，应该先初始化其根卷及任何额外的 EBS 存储，然后再将其投入生产。有关更多信息，请参阅 [初始化 Amazon EBS 卷](#)。

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

- 选择一个适当的 EBS 支持的 AMI 作为新 AMI 的起点，并在启动前根据需要对其进行配置。有关更多信息，请参阅 [使用启动实例向导启动实例 \(p. 375\)](#)。
- 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 [使用启动实例向导启动实例 \(p. 375\)](#)。
- 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
 - 附加其他 Amazon EBS 卷
- (可选) 创建所有附加到您的实例的卷的快照。有关创建快照的更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 815\)](#)。
- 在导航窗格中，选择 Instances，选择您的实例，然后选择 Actions、Image、Create Image。

Tip

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

- 在 Create Image 对话框中，指定以下信息，然后选择 Create Image。
 - 映像名称 – 映像的唯一名称。
 - 映像描述 – 映像的可选描述，最多 255 个字符。
 - 不重启 – 默认情况下未选中此选项。Amazon EC2 将关闭实例，为附加的任意卷制作快照，创建和注册 AMI，然后重新启动实例。选择 No reboot 可避免将实例关闭。

Warning

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

- 实例卷 – 使用此部分中的字段可以修改根卷，添加其他的 Amazon EBS 和实例存储卷。要了解每个字段的信息，可将光标暂停在每个字段旁的 i 图标上，以显示字段工具提示。下面列出了一些要点。
 - 要更改根卷的大小，请在 Volume Type 中找到 Root，对于 Size (GiB)，键入所需的值。
 - 如果选择 Delete on Termination，则当您终止从此 AMI 创建的实例时，将删除 EBS 卷。如果取消选择 Delete on Termination，则当您终止实例时，不会删除 EBS 卷。有关更多信息，请参阅[在实例终止时保留 Amazon EBS 卷 \(p. 461\)](#)。
 - 要添加 Amazon EBS 卷，请选择添加新卷（这将添加一个新行）。对于 Volume Type，选择 EBS，并填写行中的字段。当您从新的 AMI 启动实例时，额外的卷会自动附加到该实例。您必须格式化并挂载空卷。您必须挂载基于快照的卷。
 - 要添加实例存储卷，请参阅[将实例存储卷添加到 AMI \(p. 910\)](#)。当您从新的 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。
- 7. 要在创建 AMI 时查看其状态，请在导航窗格中，选择 AMIs。最初，状态是 pending，但过几分钟就会变成 available。

(可选) 要查看为新的 AMI 创建的快照，请选择快照。您从此 AMI 启动实例时，我们使用此快照创建其根设备卷。
- 8. 从新 AMI 启动实例。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。
- 9. 新的正在运行的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。

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 \(p. 922\)](#)。
 - 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 \(p. 87\)](#)。
 - (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，则您每次启动使用此 AMI 实例时，都必须指定 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 \(p. 848\)](#)。

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)

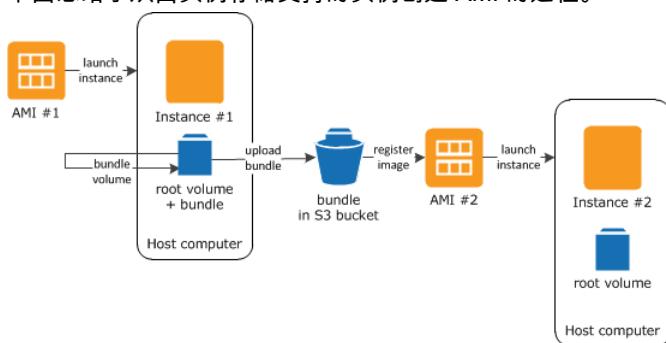
创建由实例存储支持的 Linux AMI

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。

用于 Amazon EBS 支持的 AMI 的 AMI 创建过程有所不同。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 \(p. 85\)](#)。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 \(p. 102\)](#)。

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。该过程完成之后，您会得到一个捆绑，该捆绑由映像清单 (`image.manifest.xml`) 以及包含根卷模板的文件 (`image.part.xx`) 组成。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 Linux AMI \(p. 142\)](#)。

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 \(p. 923\)](#)。

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 \(p. 106\)](#)。

- 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 和秘密访问密钥。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 \(p. 108\)](#)。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 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem` 证书。
 - [AWS GovCloud (US-West)] 使用 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` 证书。
- 连接到您的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、删除临时文件及修改 Linux 配置。

任务

- [设置 AMI 工具 \(p. 106\)](#)
- [通过实例存储支持的 Amazon Linux 实例创建 AMI \(p. 109\)](#)
- [通过实例存储支持的 Ubuntu 实例创建 AMI \(p. 111\)](#)
- [将实例存储支持的 AMI 转换为 Amazon EBS 支持的 AMI \(p. 115\)](#)

设置 AMI 工具

您可使用 AMI 工具创建和管理实例存储支持的 Linux AMIs。要使用这些工具，必须在 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。

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：

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

2. 使用 wget 或 curl 等工具下载 RPM 文件。例如：

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. 使用以下命令验证 RPM 文件的签名：

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

上述命令应指示该文件的 SHA1 和 MD5 哈希值是 OK。如果该命令指示这些哈希值是 NOT OK，请使用以下命令查看该文件的标头 SHA1 和 MD5 哈希值：

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

然后，将您的文件的标头 SHA1 和 MD5 哈希值与以下经验证的 AMI 工具哈希值进行比较，以确认文件的真实性：

- 标头 SHA1 : a1f662d6f25f69871104e6a62187fa4df508f880

- MD5 : 9faff05258064e2f7909b66142de6782

如果您的文件的标头 SHA1 和 MD5 哈希值与经验证的 AMI 工具哈希值相匹配，请继续下一步。

4. 使用以下命令安装 RPM :

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. 使用 [ec2-ami-tools-version \(p. 118\)](#) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ ec2-ami-tools-version
```

Note

如果您收到一个加载错误，例如“cannot load such file -- ec2/amitools/version (LoadError)”(无法加载此类文件 -- ec2/amitools/version (LoadError))，请完成下一步骤以将 AMI 工具安装的位置添加到 RUBYLIB 路径。

6. (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。

```
[ec2-user ~]$ 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，以前加载错误中的丢失文件位于 /usr/lib/ruby/site_ruby 和 /usr/lib64/ruby/site_ruby。

b. 将上一步的位置添加到您的 RUBYLIB 路径中。

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
site_ruby
```

c. 使用 [ec2-ami-tools-version \(p. 118\)](#) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ 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：

```
[ec2-user ~]$ 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：

```
[ec2-user ~]$ 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。

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

请注意，.zip 文件包含文件夹 ec2-ami-tools-**x.x.x**，其中 **x.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：

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

- 将工具添加到您的 PATH 环境变量。例如：

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

- 您可以使用 [ec2-ami-tools-version \(p. 118\)](#) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ ec2-ami-tools-version
```

管理签名证书

AMI 工具中的某些命令需要签名证书 (也称为 X.509 证书)。您必须创建证书，然后将其上传到 AWS。例如，您可以使用第三方工具 (例如 OpenSSL) 创建证书。

创建签名证书

- 安装和配置 OpenSSL。
- 使用 `openssl genrsa` 命令创建私有密钥，并将输出保存到 .pem 文件。我们建议您创建 2048 或 4096 位 RSA 密钥。

```
openssl genrsa 2048 > private-key.pem
```

- 使用 `openssl req` 命令生成证书。

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -out certificate.pem
```

要将证书上传到 AWS，请使用 [upload-signing-certificate](#) 命令。

```
aws iam upload-signing-certificate --user-name user-name --certificate-body file://path/to/certificate.pem
```

要列出用户的证书，请使用 [list-signing-certificates](#) 命令：

```
aws iam list-signing-certificates --user-name user-name
```

要对用户禁用或重新启用签名证书，请使用 [update-signing-certificate](#) 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](#) 命令：

```
aws iam delete-signing-certificate --user-name user-name --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

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 \(p. 105\)](#)。

主题

- [通过实例存储支持的 Amazon Linux 实例创建 AMI \(p. 109\)](#)
- [通过实例存储支持的 Ubuntu 实例创建 AMI \(p. 111\)](#)

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 发行版的实例。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 \(p. 111\)](#)。

准备使用 AMI 工具 (仅限 HVM 实例)

1. AMI 工具需要有 GRUB Legacy，才能正确启动。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 Amazon Linux 实例创建 AMI

此过程假设您满足 [先决条件 \(p. 105\)](#) 中的先决条件。

1. 将您的凭证上传到您的实例。我们使用这些凭证确保只有您和 Amazon EC2 才能访问您的 AMI。

- a. 在您的实例上为凭证创建临时目录，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凭证。

- b. 使用安全复制工具 (如 [scp \(p. 427\)](#)) 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。以下 scp 命令中的 `-i my-private-key.pem` 选项是您用于通过 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 \(p. 121\)](#) 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凭证的目录。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。如果您在 /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 选项指定不同的位置来存储捆绑。某些实例会在 /mnt 或 /media/ephemeral0 上装载您可以使用的临时存储，您还可以[创建 \(p. 798\)](#)、[连接 \(p. 800\)](#)和[装载 \(p. 801\)](#)新 Amazon EBS 卷以存储捆绑。

- a. 您必须以根用户身份运行 ec2-bundle-vol 命令。对于大部分命令，您可以使用 sudo 获得提升的权限，但是在这种情况下，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，请如下所示运行 [ec2-bundle-vol \(p. 121\)](#) 命令：

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXY1BH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXY1BH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --partition gpt
```

Note

对于中国（北京）和 AWS GovCloud (US-West) 区域，请使用 --ec2cert 参数并根据[先决条件 \(p. 105\)](#)指定证书。

创建映像可能需要几分钟时间。该命令完成后，您的 /tmp (非默认) 目录会包含捆绑 (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) 要添加更多实例存储卷，请在 image.manifest.xml 文件中为您的 AMI 编辑块储存设备映射。有关更多信息，请参阅[块储存设备映射 \(p. 923\)](#)。

- 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。

Note

有关排除的文件的列表，请参阅[ec2-bundle-vol \(p. 121\)](#)。

```
<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。

- 要将捆绑上传到 Amazon S3，请如下所示运行 [ec2-upload-bundle \(p. 131\)](#) 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
```

Important

要在美国东部（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。

- (可选) 将捆绑上传到 Amazon S3 之后，您可以使用以下 `rm` 命令将捆绑从实例上的 `/tmp` 目录中删除：

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

Important

如果您在 [Step 2 \(p. 109\)](#) 中使用 `-d /path/to/bundle/storage` 选项指定了路径，请使用该路径，而不是 `/tmp`。

- 要注册您的 AMI，请按以下所示运行 `register-image` 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
```

Important

如果您先前为 [ec2-upload-bundle \(p. 131\)](#) 命令指定了某个区域，请为该命令再次指定该区域。

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 发行版的实例。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 \(p. 109\)](#)。

准备使用 AMI 工具 (仅限 HVM 实例)

AMI 工具需要有 GRUB Legacy，才能正确启动。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。

- 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 \(p. 112\)](#)。如果传统 GRUB 已存在，您可以跳到[Step 2 \(p. 112\)](#)。

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. 使用您的发行版的软件包管理器安装以下分区管理软件包。

- gdisk (此软件包在某些发行版中可能名为 gptfdisk)
- kpartx
- parted

使用以下命令。

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. 检查您的实例的内核参数。

```
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. 使用您常用的文本编辑器（如 vim 或 nano）编辑 /boot/grub/menu.lst 文件，以更改控制台并将先前确定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 分区表和装载在 /boot/efi 中的单独 EFI 分区。ec2-bundle-vol 命令不会捆绑此引导分区，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 Ubuntu 实例创建 AMI

此过程假设您满足[先决条件 \(p. 105\)](#)中的先决条件。

1. 将您的凭证上传到您的实例。我们使用这些凭证确保只有您和 Amazon EC2 才能访问您的 AMI。
 - a. 在您的实例上为凭证创建临时目录，如下所示：

```
ubuntu:~$ mkdir /tmp/cert
```

这使您可以从创建的映像中排除您的凭证。

- b. 使用安全复制工具（如[scp \(p. 427\)](#)）将您的 X.509 证书和私有密钥从您的计算机复制到您实例上的 /tmp/cert 目录。以下 scp 命令中的 -i *my-private-key.pem* 选项是您用于通过 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. 通过从您的实例内运行[ec2-bundle-vol \(p. 121\)](#)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凭证的目录。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。如果您在 /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* 选项指定不同的位置来存储捆绑。某些实例会在 /mnt 或 /media/ephemeral0 上装载您可以使用的临时存储，您还可以[创建 \(p. 798\)](#)、[连接 \(p. 800\)](#)和[装载 \(p. 801\)](#)新 Amazon EBS 卷以存储捆绑。

- a. 您必须以根用户身份运行 ec2-bundle-vol 命令。对于大部分命令，您可以使用 sudo 获得提升的权限，但是在这种情况下，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，请如下所示运行 [ec2-bundle-vol \(p. 121\)](#) 命令。

```
root@ubuntu:# 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
```

Important

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。

创建映像可能需要几分钟时间。该命令完成后，您的 tmp 目录会包含捆绑 (image.manifest.xml 以及多个 image.part.**xx** 文件)。

- c. 从 root shell 退出。

```
root@ubuntu:# exit
```

3. (可选) 要添加更多实例存储卷，请在 image.manifest.xml 文件中为您的 AMI 编辑块储存设备映射。有关更多信息，请参阅[块储存设备映射 \(p. 923\)](#)。

- 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。

```
<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 , 请如下所示运行 [ec2-upload-bundle \(p. 131\)](#) 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
```

Important

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。

5. (可选) 将捆绑上传到 Amazon S3 之后 , 您可以使用以下 `rm` 命令将捆绑从实例上的 `/tmp` 目录中删除 :

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

Important

如果您在 [Step 2 \(p. 113\)](#) 中指定了带有 `-d /path/to/bundle/storage` 选项的路径 , 请在下面使用该路径 , 而不是 `/tmp`。

6. 要注册您的 AMI , 请按以下所示运行 `register-image` AWS CLI 命令。

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-
type hvm
```

Important

如果您先前为 [ec2-upload-bundle \(p. 131\)](#) 命令指定了某个区域 , 请为该命令再次指定该区域。

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

- 从 Amazon EBS 支持的 AMI 启动 Amazon Linux 实例。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。Amazon Linux 实例会预安装 AWS CLI 和 AMI 工具。
- 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。
 - 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
```

- 使用安全复制工具（如 /tmp/certscp）将您的 X.509 私有密钥从您的计算机复制到您实例上的[\(p. 427\)](#) 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
```

- 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
```

- 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](#) 命令将该卷附加到 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
```

- 创建用于捆绑的文件夹。

```
[ec2-user ~]$ mkdir /tmp/bundle
```

- 使用 /tmp/bundle 命令将由实例存储支持的 AMI 的捆绑下载到 [ec2-download-bundle \(p. 126\)](#)。

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m  
image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /path/  
to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

- 使用 [ec2-unbundle \(p. 130\)](#) 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 \(p. 130\)](#) 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装载的设备名称。

```
[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，要装载的分区是 /dev/sdb1，但您的设备名称可能有所不同。如果您的卷未分区，则要装载的设备类似于 /dev/sdb (没有设备分区尾部数字)。

11. 为新 Amazon EBS 卷创建装载点并装载该卷。

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. 使用您常用的文本编辑器 (如 vim 或 nano) 在 EBS 卷上打开 /etc/fstab 文件，然后删除实例存储 (临时) 卷的所有条目。因为 Amazon EBS 卷装载在 /mnt/ebs 上，所以 fstab 文件位于 /mnt/ebs/etc/fstab 处。

```
[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 DeviceName=device-name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

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
```

AMI 工具参考

您可以使用 AMI 工具命令创建和管理实例存储支持的 Linux AMI。要设置这些工具，请参阅[设置 AMI 工具 \(p. 106\)](#)。

有关您的访问密钥的信息，请参阅[有关管理 AWS 访问密钥的最佳实践](#)。

命令

- [ec2-ami-tools-version \(p. 118\)](#)
- [ec2-bundle-image \(p. 119\)](#)
- [ec2-bundle-vol \(p. 121\)](#)
- [ec2-delete-bundle \(p. 124\)](#)
- [ec2-download-bundle \(p. 126\)](#)
- [ec2-migrate-manifest \(p. 128\)](#)
- [ec2-unbundle \(p. 130\)](#)
- [ec2-upload-bundle \(p. 131\)](#)
- [AMI 工具的常用选项 \(p. 134\)](#)

ec2-ami-tools-version

描述

描述 AMI 工具的版本。

语法

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

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-user ~]$ ec2-ami-tools-version  
1.5.2 20071010
```

ec2-bundle-image

描述

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

-c, --cert 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

-k, --privatekey 路径

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。请注意，不需要在您的 AWS 账户中注册该密钥。

必需：是

-u, --user 账户

用户的 AWS 账户 ID (不包含破折号)。

必需：是

-i, --image 路径

指向待捆绑映像的路径。

必需：是

-d, --destination 路径

要在其中创建捆绑的目录。

默认值：/tmp

必需：否

--ec2cert 路径

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

us-gov-west-1 和 cn-north-1 区域使用非默认公有密钥凭证，必须随该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/`。如果您将来自 RPM 或 ZIP 文件的 AMI 工具安装在了 [设置 AMI 工具 \(p. 106\)](#) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 `us-gov-west-1` 和 `cn-north-1` 区域。

`-r, --arch` 指导视频

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

`--productcodes` `code1,code2,...`

在注册时附加到映像的产品代码，用逗号隔开。

必需：否

`-B, --block-device-mapping` 映射

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：

- `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

`-p, --prefix` 前缀

捆绑的 AMI 文件的文件名前缀。

默认：映像文件的名称。例如，如果映像路径为 `/var/spool/my-image/version-2/debian.img`，则默认前缀为 `debian.img`。

必需：否

`--kernel` `kernel_id`

已淘汰。使用 [register-image](#) 设置内核。

必需：否

`--ramdisk` `ramdisk_id`

已淘汰。使用 [register-image](#) 设置 RAM 磁盘 (若需要)。

必需：否

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-user ~]$ 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

描述

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 [创建由实例存储支持的 Linux AMI \(p. 105\)](#)。

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

`-c, --cert` 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

`-k, --privatekey` 路径

用户的 PEM 编码 RSA 密钥文件的路径。

必需：是

`-u, --user` 账户

用户的 AWS 账户 ID (不包含破折号)。

必需：是

`-d, --destination destination`

要在其中创建捆绑的目录。

默认值：`/tmp`

必需：否

`--ec2cert 路径`

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

`us-gov-west-1` 和 `cn-north-1` 区域使用非默认公有密钥凭证，必须随该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/`。如果您将来自 RPM 或 ZIP 文件的 AMI 工具安装在了 [设置 AMI 工具 \(p. 106\)](#) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 `us-gov-west-1` 和 `cn-north-1` 区域。

`-r, --arch 指导视频`

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。

有效值：`i386 | x86_64`

必需：否

`--productcodes code1,code2,...`

在注册时附加到映像的产品代码，用逗号隔开。

必需：否

`-B, --block-device-mapping 映射`

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：

- `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

`-a, --all`

捆绑所有目录，包括远程装载的文件系统上的目录。

必需：否

`-e, --exclude directory1,directory2,...`

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 `--all` 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。

必需：否

`-i, --include file1,file2,...`

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。

必需：否

--no-filter

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。

必需：否

-p, --prefix 前缀

捆绑的 AMI 文件的文件名前缀。

默认值：`image`

必需：否

-s, --size size

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。

默认值：10240

必需：否

--[no-]inherit

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 `--inherit` 但实例元数据不可访问，则捆绑将失败。

必需：否

-v, --volume 体积

要从中创建捆绑的装载卷的绝对路径。

默认值：根目录 (/)

必需：否

-P, --partition type

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 gpt。

有效值：`mbr | gpt | none`

必需：否

-S, --script script

将在捆绑前运行的自定义脚本。该脚本必须获得一个参数，即卷的装载点。

必需：否

--fstab 路径

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

--generate-fstab

使用 Amazon EC2 提供的 `fstab` 捆绑卷。

必需：否

--grub-config

将捆绑到映像中的备用 GRUB 配置文件的路径。默认情况下，`ec2-bundle-vol` 预计克隆的映像上存在 `/boot/grub/menu.lst` 或 `/boot/grub/grub.conf`。该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

--kernel kernel_id

已淘汰。使用 [register-image](#) 设置内核。

必需：否

--ramdiskramdisk_id

已淘汰。使用 [register-image](#) 设置 RAM 磁盘 (若需要)。

必需：否

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-user ~]$ 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

描述

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

-b, --bucket 存储桶

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

-a, --access-key access_key_id

AWS 访问密钥 ID。

必需：是

-s, --secret-key secret_access_key

AWS 秘密访问密钥。

必需：是

-t, --delegation-token token

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：AWS_DELEGATION_TOKEN 环境变量的值 (若已设置)。

--region region

要在请求签名中使用的区域。

默认值：us-east-1

必需：若使用签名版本 4 则必需

--sigv version

对请求进行签名时要使用的签名版本。

有效值：2 | 4

默认值：4

必需：否

-m, --manifest 路径

清单文件的路径。

必需：您必须指定 --prefix 或 --manifest。

-p, --prefix 前缀

捆绑的 AMI 文件名前缀。请提供完整前缀。例如，如果前缀是 image.img，请使用 -p image.img 而不是 -p image。

必需：您必须指定 --prefix 或 --manifest。

--clear

删除指定的捆绑之后删除 Amazon S3 存储桶 (若为空)。

必需 : 否

--retry

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需 : 否

-y, --yes

自动假定所有提示的回答为 yes。

必需 : 否

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-user ~]$ ec2-delete-bundle -b aws-s3-bucket1 -a your_access_key_id -s your_secret_access_key
Deleting files:
aws-s3-bucket1/
image.manifest.xml
aws-s3-bucket1/
image.part.00
aws-s3-bucket1/
image.part.01
aws-s3-bucket1/
image.part.02
aws-s3-bucket1/
image.part.03
aws-s3-bucket1/
image.part.04
aws-s3-bucket1/
image.part.05
aws-s3-bucket1/image.part.06
Continue? [y/n]
y
Deleted aws-s3-bucket1/image.manifest.xml
Deleted aws-s3-bucket1/image.part.00
Deleted aws-s3-bucket1/image.part.01
Deleted aws-s3-bucket1/image.part.02
Deleted aws-s3-bucket1/image.part.03
Deleted aws-s3-bucket1/image.part.04
Deleted aws-s3-bucket1/image.part.05
Deleted aws-s3-bucket1/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

描述

从 Amazon S3 存储下载指定的实例存储支持的 Linux AMIs。

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

-b, --bucket 存储桶

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

-a, --access-key *access_key_id*

AWS 访问密钥 ID。

必需：是

-s, --secret-key *secret_access_key*

AWS 秘密访问密钥。

必需：是

-k, --privatekey 路径

用于解密清单的私有密钥。

必需：是

--url *url*

Amazon S3 服务 URL。

默认值：<https://s3.amazonaws.com/>

必需：否

--region 区域

要在请求签名中使用的区域。

默认值：`us-east-1`

必需：若使用签名版本 4 则必需

--sigv *version*

对请求进行签名时要使用的签名版本。

有效值：`2 | 4`

默认值：`4`

必需：否

-m, --manifest *file*

清单文件的名称 (无路径)。我们建议您指定清单 (-m) 或前缀 (-p)。

必需：否

-p, --prefix 前缀

捆绑的 AMI 文件的文件名前缀。

默认值 : image

必需 : 否

-d, --directory directory

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

--retry

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需 : 否

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 `aws-s3-bucket1` Amazon S3 存储桶下载捆绑。

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b aws-s3-bucket1/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 aws-s3-bucket1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.00 ...
Downloaded image.part.00 from aws-s3-bucket1
Downloading part image.part.01 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.01 ...
Downloaded image.part.01 from aws-s3-bucket1
Downloading part image.part.02 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.02 ...
Downloaded image.part.02 from aws-s3-bucket1
Downloading part image.part.03 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.03 ...
Downloaded image.part.03 from aws-s3-bucket1
Downloading part image.part.04 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.04 ...
Downloaded image.part.04 from aws-s3-bucket1
Downloading part image.part.05 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.05 ...
Downloaded image.part.05 from aws-s3-bucket1
Downloading part image.part.06 from aws-s3-bucket1/bundles/bundle_name to mybundle/
image.part.06 ...
Downloaded image.part.06 from aws-s3-bucket1
```

ec2-migrate-manifest

描述

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

-c, --cert 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

-k, --privatekey 路径

用户的 PEM 编码 RSA 密钥文件的路径。

必需：是

--manifest 路径

清单文件的路径。

必需：是

-a, --access-key *access_key_id*

AWS 访问密钥 ID。

必需：若使用自动映射则必需。

-s, --secret-key *secret_access_key*

AWS 秘密访问密钥。

必需：若使用自动映射则必需。

--region 区域

要在映射文件中查找的区域。

必需：若使用自动映射则必需。

--no-mapping

禁用内核和 RAM 磁盘的自动映射。

迁移期间，Amazon EC2 会将清单文件中的内核和 RAM 磁盘替换为目标区域指定的内核和 RAM 磁盘。除非提供了 **--no-mapping** 参数，否则 **ec2-migrate-bundle** 便可能使用 **DescribeRegions** 和 **DescribeImages** 操作执行自动映射。

必需：若您不提供用于自动映射的 **-a**、**-s** 和 **--region** 选项，则必需。

--ec2cert 路径

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

us-gov-west-1 和 **cn-north-1** 区域使用非默认公有密钥凭证，必须随该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/`。如果您将来自 ZIP 文件的 AMI 工具安装在 [设置 AMI 工具 \(p. 106\)](#) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 **us-gov-west-1** 和 **cn-north-1** 区域。

--kernel kernel_id

要选择的内核的 ID。

Important

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 [启用您自己的 Linux 内核 \(p. 154\)](#)。

必需：否

--ramdisk ramdisk_id

供选择的 RAM 磁盘的 ID。

Important

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 [启用您自己的 Linux 内核 \(p. 154\)](#)。

必需：否

输出

描述捆绑过程的阶段和状态的状态消息。

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-user ~]$ 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

描述

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

-k, --privatekey 路径

您的 PEM 编码 RSA 密钥文件的路径。

必需：是

-m, --manifest 路径

清单文件的路径。

必需：是

-s, --source source_directory

包含捆绑的目录。

默认：当前目录。

必需：否

-d, --destination destination_directory

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

此 Linux 和 UNIX 示例解绑 `image.manifest.xml` 文件中指定的 AMI。

```
[ec2-user ~]$ 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

描述

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[创建由实例存储支持的 Linux AMI \(p. 105\)](#)。

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

-b, --bucket 存储桶

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

-a, --access-key `access_key_id`

您的 AWS 访问密钥 ID。

必需：是

-s, --secret-key secret_access_key

您的 AWS 秘密访问密钥。

必需：是

-t, --delegation-token token

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：AWS_DELEGATION_TOKEN 环境变量的值（若已设置）。

-m, --manifest 路径

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

--url url

已淘汰。请使用 **--region** 选项，除非您的存储桶被限制到 EU 位置（且不是 eu-west-1）。**--location** 标记是确定该特定位置限制的唯一途径。

Amazon S3 终端节点服务 URL。

默认值：<https://s3.amazonaws.com/>

必需：否

--region 区域

要在请求签名中为目标 S3 存储桶使用的区域。

- 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限制的存储桶（在 us-east-1 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 us-east-1 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 us-east-1），则该工具将报错退出。

如果您的存储桶被限制到 EU 位置（不是 eu-west-1），请改用 **--location** 标记。**--location** 标记是确定该特定位置限制的唯一途径。

默认值：us-east-1

必需：若使用签名版本 4 则必需

--sigv version

对请求进行签名时要使用的签名版本。

有效值：2 | 4

默认值：4

必需：否

--acl acl

捆绑的映像的访问控制列表策略。

有效值：public-read | aws-exec-read

默认值 : aws-exec-read

必需 : 否

-d, --directory directory

包含捆绑的 AMI 段的目录。

默认 : 包含清单文件的目录 (参阅 -m 选项)。

必需 : 否

--part part

开始上传指定的段及所有后续段。例如 : --part 04。

必需 : 否

--retry

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需 : 否

--skipmanifest

不上传清单。

必需 : 否

--location 位置

已淘汰。请使用 --region 选项，除非您的存储桶被限制到 EU 位置 (且不是 eu-west-1)。--location 标记是确定该特定位置限制的唯一途径。

目标 Amazon S3 存储桶的位置限制。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限制的存储桶 (在 us-east-1 中)。

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。

必需 : 否

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-user ~]$ ec2-upload-bundle -b aws-s3-bucket1/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 aws-s3-bucket1 ...
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

大多数 AMI 工具接受以下可选参数。

--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信息。

将加密与 EBS 支持的 AMI 结合使用

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。在启动实例和复制映像时，您可以包含 EBS 完全加密支持。在提供了 AWS KMS 的所有区域中，支持在这些操作中使用加密参数。

从 AMIs 中启动带加密 EBS 卷的 EC2 实例的方式与其他实例相同。另外，从未加密 EBS 快照支持的 AMI 中启动实例时，您可以在启动过程中将部分或全部卷加密。

与 EBS 卷相似，可使用默认 AWS Key Management Service 客户主密钥 (CMK) 或您指定的客户托管密钥加密 AMI 中的快照。在所有情况下，您都必须拥有使用所选密钥的权限。

带加密快照的 AMI 可以跨 AWS 账户共享。有关更多信息，请参阅[共享 AMI](#)。

启动实例场景

Amazon EC2 实例是通过 AWS 管理控制台 或者直接使用 Amazon EC2 API 或 CLI，使用 RunInstances 操作以及通过数据块设备映射提供的参数在 AMI 中启动的。有关数据块设备映射的更多信息，请参阅[数据块设备映射](#)。有关通过 AWS CLI 控制数据块设备映射的示例，请参阅[启动、列出和终止 EC2 实例](#)。

如果不使用显式加密参数，在默认情况下，RunInstances 操作会在从 AMI 的源快照中还原 EBS 卷时保持这些快照的现有加密状态。如果启用[默认加密](#)，从 AMI 中（无论使用加密还是未加密的快照）创建的所有卷都会被加密。如果在默认情况下并未启用加密，则实例保持 AMI 的加密状态。

您也可以启动实例，同时通过提供加密参数来对结果卷应用新的加密状态。因此，会观察到以下行为：

启动时不指定加密参数

- 未加密快照会还原为未加密卷，除非已在默认情况下启用加密，那么所有新创建的所有卷都将加密。
- 您拥有的加密快照会还原为使用相同 CMK 加密的卷。
- 您未拥有的加密快照（例如，与您共享了 AMI）会还原到由您的 AWS 账户的默认 CMK 加密的卷。

可以通过提供加密参数覆盖默认行为。可用参数包括 `Encrypted` 和 `KmsKeyId`。仅设置 `Encrypted` 参数会得到以下结果：

已设置 `Encrypted`，但未指定 `KmsKeyId` 时的实例启动行为

- 未加密快照会还原到由您的 AWS 账户的默认 CMK 加密的 EBS 卷。
- 您拥有的加密快照会还原到由相同 CMK 加密的 EBS 卷。（也就是说，`Encrypted` 参数没有影响。）
- 您未拥有的加密快照（例如，与您共享了 AMI）会还原到由您的 AWS 账户的默认 CMK 加密的卷。（也就是说，`Encrypted` 参数没有影响。）

如果同时设置 `Encrypted` 和 `KmsKeyId` 参数，可以为加密操作指定非默认 CMK。会实现以下行为：

同时设置 `Encrypted` 和 `KmsKeyId` 的实例

- 未加密快照会还原到由指定 CMK 加密的 EBS 卷。
- 加密快照还原为未使用原始 CMK 加密，而是使用指定 CMK 加密的 EBS 卷。

提交 `KmsKeyId` 但没有同时设置 `Encrypted` 参数会导致错误。

以下部分提供使用非默认加密参数从 AMI 中启动实例的示例。在以下每个场景中，提供给 `RunInstances` 操作的参数会导致在使用快照还原卷的过程中加密状态发生变化。

Note

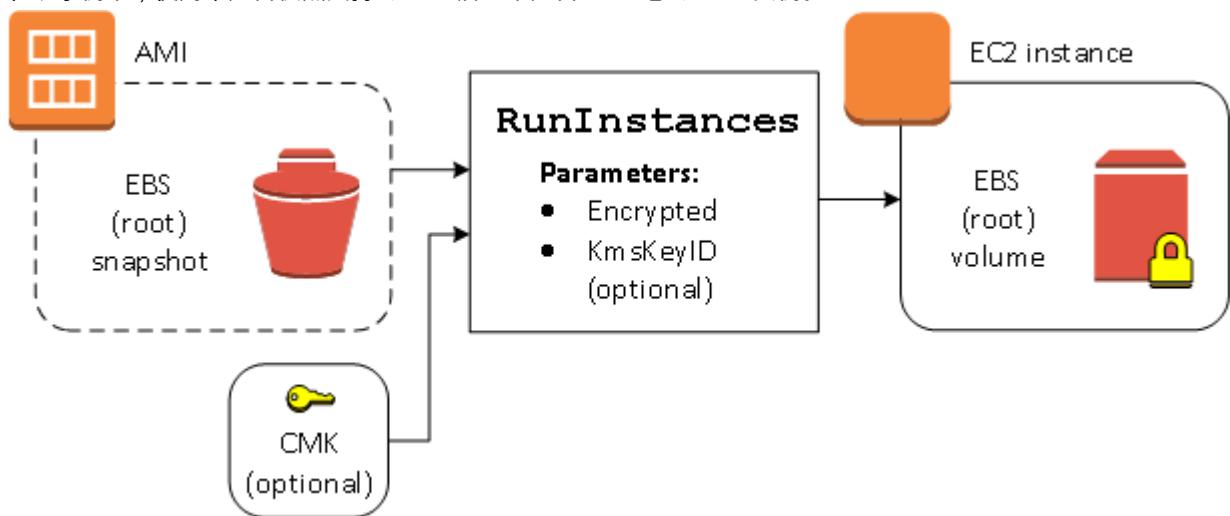
有关从 AMI 中启动实例的详细控制台过程，请参阅[启动实例](#)。

有关 `RunInstances` API 的文档，请参阅[RunInstances](#)。

有关 AWS Command Line Interface 中的 `run-instances` 命令的文档，请参阅[run-instances](#)。

在启动过程中加密卷

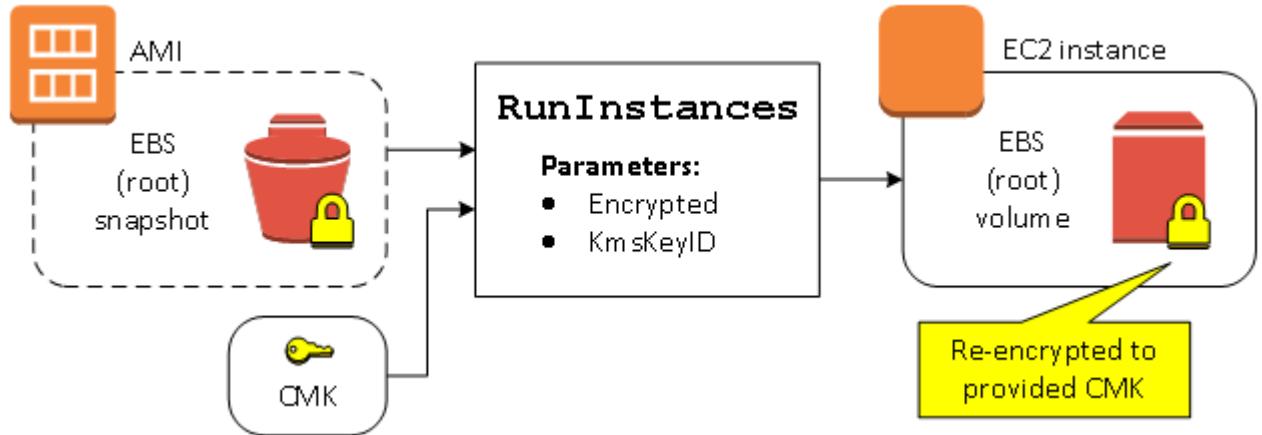
在该示例中，使用未加密快照支持的 AMI 启动带加密 EBS 卷的 EC2 实例。



仅使用 `Encrypted` 参数的结果是对该实例中的卷行加密。提供 `KmsKeyId` 参数是可选的。如果未指定密钥 ID，会使用 AWS 账户的默认 CMK 加密卷。要使用您拥有的不同 CMK 加密卷，请提供 `KmsKeyId` 参数。

在启动过程中重新加密卷

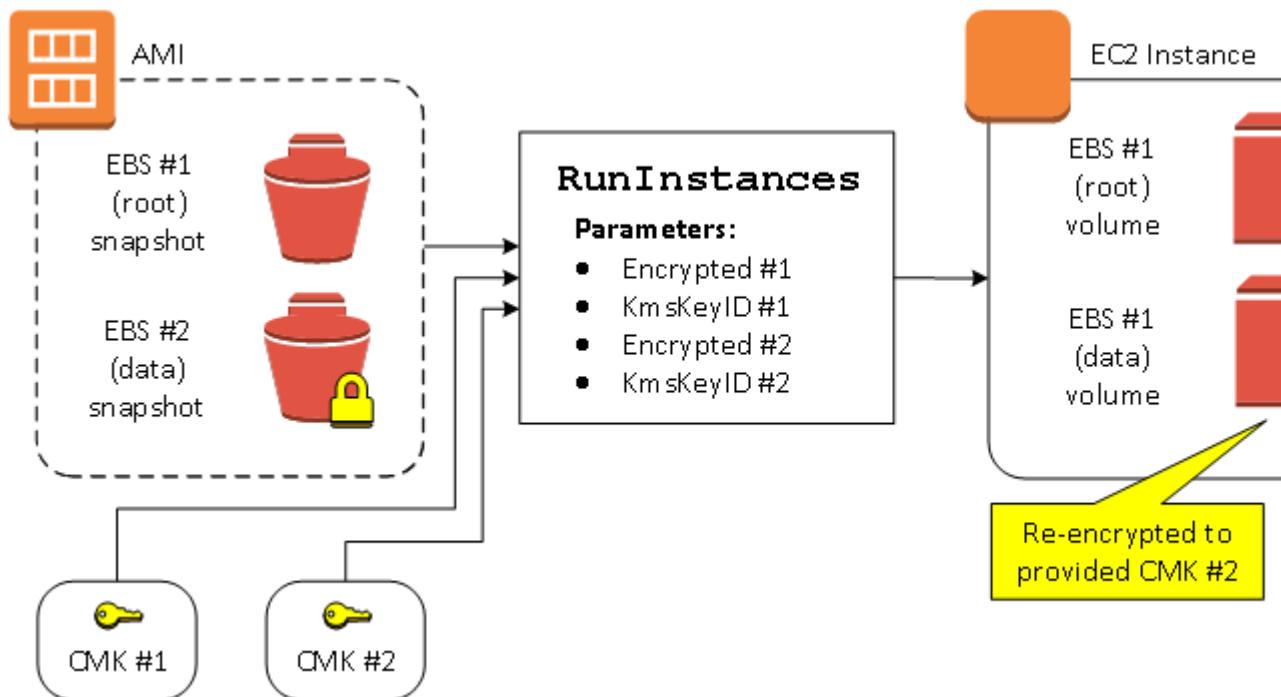
在该示例中，使用加密快照支持的 AMI 启动带有由新 CMK 加密的 EBS 卷的 EC2 实例。



如果您拥有 AMI 且未提供加密参数，则生成的实例具有由与快照相同的密钥加密的卷。如果 AMI 是与他人共享而不是由您拥有，且您未提供加密参数，则由您的默认 CMK 对卷进行加密。如果按所示提供加密参数，则会由指定 CMK 对卷进行加密。

在启动过程中更改多个卷的加密状态

在这一更为复杂的示例中，会使用多个快照（分别具有自己的加密状态）支持的 AMI 启动带有新加密卷和重新加密卷的 EC2 实例。



在这种情况下，会为 `RunInstances` 操作提供用于各个源快照的加密参数。在指定所有可用的加密参数后，无论您是否拥有 AMI，结果实例都相同。

映像复制场景

可通过 AWS 管理控制台 或者直接使用 Amazon EC2 API 或 CLI , 使用 `CopyImage` 操作复制 Amazon EC2 AMI。

如果不使用显式加密参数，在默认情况下，`CopyImage` 操作会在复制 AMI 的源快照时保持这些快照的现有加密状态。您也可以复制 AMI，同时通过提供加密参数来对其关联的 EBS 快照应用新的加密状态。因此，会观察到以下行为：

复制时不指定加密参数

- 未加密快照会复制为另一个未加密快照，除非已在默认情况下启用加密，那么所有新创建的快照都将加密。
- 您拥有的加密快照会复制为使用相同密钥加密的快照。
- 您未拥有的加密快照（例如，与您共享了 AMI）会复制到由您的 AWS 账户的默认 CMK 加密的快照。

可以通过提供加密参数覆盖以上所有默认行为。可用参数包括 `Encrypted` 和 `KmsKeyId`。仅设置 `Encrypted` 参数会得到以下结果：

已设置 `Encrypted`，但未指定 `KmsKeyId` 时的复制映像行为

- 未加密快照会复制到由 AWS 账户的默认 CMK 加密的快照。
- 加密快照会复制到由相同 CMK 加密的快照。（也就是说，`Encrypted` 参数没有影响。）
- 您未拥有的加密快照（例如，与您共享了 AMI）会复制到由您的 AWS 账户的默认 CMK 加密的卷。（也就是说，`Encrypted` 参数没有影响。）

通过同时设置 `Encrypted` 和 `KmsKeyId` 参数，可以为加密操作指定客户托管的 CMK。会实现以下行为：

同时设置 `Encrypted` 和 `KmsKeyId` 时的复制映像行为

- 未加密快照会复制到由指定 CMK 加密的快照。
- 加密快照会复制到未使用原始 CMK 加密，而是使用指定 CMK 加密的快照。

提交 `KmsKeyId` 但没有同时设置 `Encrypted` 参数会导致错误。

以下部分提供使用非默认加密参数复制 AMI，导致更改加密状态的示例。

Note

有关复制 AMI 的详细控制台程序，请参阅[复制 AMI](#)。

有关 `CopyImage` API 的文档，请参阅[复制映像](#)。

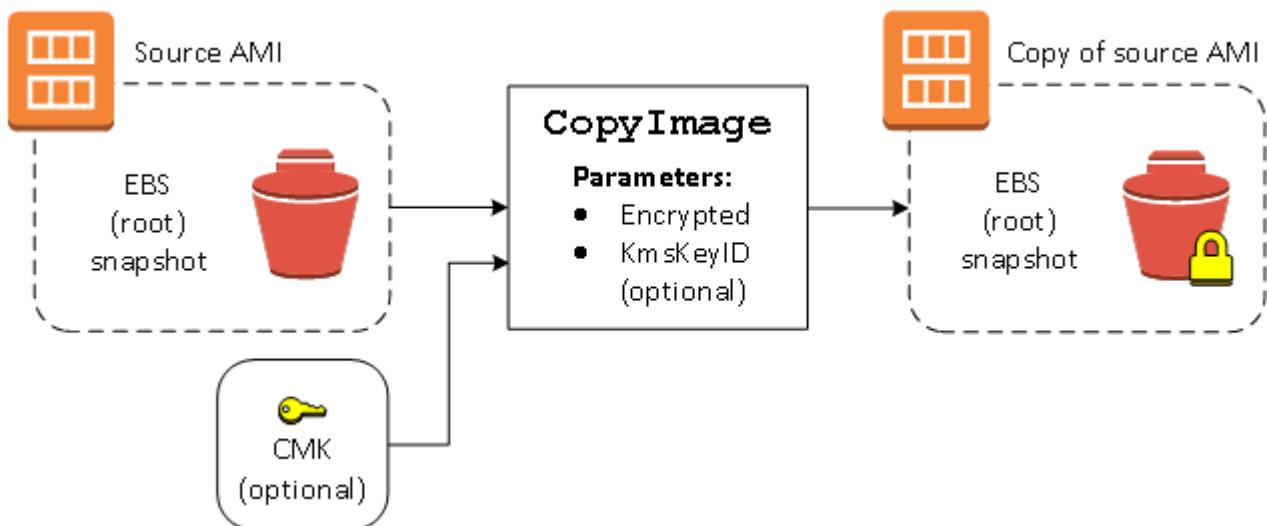
有关 AWS Command Line Interface 中 `copy-image` 命令的文档，请参阅[复制映像](#)。

在复制过程中将未加密映像加密

在这种情况下，将使用未加密根快照提供支持的 AMI 复制到使用加密根快照的 AMI。`CopyImage` 操作将通过两个加密参数（包括 CMK）进行调用。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 AMIs 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。

Note

启用[默认加密](#) (p. 853) 与针对 AMI 中的所有快照将 `Encrypted` 参数设置为 `true` 的效果相同。



设置 `Encrypted` 参数会对此实例的单一快照进行加密。如果您未指定 `KmsKeyId` 参数，则使用默认 CMK 来对快照副本加密。

Note

您也可以复制带多个快照的映像，并单独配置每个快照的加密状态。

复制 AMI

您可以使用 AWS 管理控制台、AWS Command Line Interface 或开发工具包、或者 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)。可以复制由 Amazon EBS 支持的 AMIs 和由实例存储支持的 AMIs。您可以复制带加密快照的 AMI，并在复制过程中更改加密状态。

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。(唯一的例外是在选择加密或重新加密快照时。) 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。

您无法复制从 AWS Marketplace 获取的 AMI，无论您是直接获取还是将它与您共享。而应使用 AWS Marketplace AMI 启动一个 EC2 实例，然后从该实例中创建一个 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 102\)](#)。

复制实例存储支持的 AMI 的权限

如果您使用 IAM 用户复制实例存储支持的 AMI，则用户必须具有以下 Amazon S3 权限：`s3:CreateBucket`、`s3:GetBucketAcl`、`s3>ListAllMyBuckets`、`s3:GetObject`、`s3:PutObject` 和 `s3:PutObjectAcl`。

以下示例策略允许用户将指定的存储桶中的 AMI 源复制到指定的区域。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
"Effect": "Allow",
"Action": "s3>ListAllMyBuckets",
"Resource": [
    "arn:aws:s3:::/*"
]
},
{
    "Effect": "Allow",
    "Action": "s3GetObject",
    "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*"
    ]
}
]
```

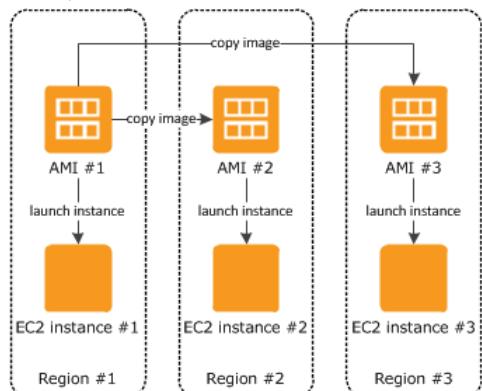
要查找 AMI 源存储桶的 Amazon 资源名称 (ARN) , 请通过 <https://console.aws.amazon.com/ec2/> 打开 Amazon EC2 控制台 , 在导航窗格中选择 AMI , 然后在源列中找到该存储桶名称。

跨区域复制

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 , 您可以根据相同的 AMI 在不同的区域中启动一致的实例。
- **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、在不同的区域中复制的两个 AMIs 以及从它们中启动的 EC2 实例之间的关系。从 AMI 中启动实例时 , 该实例位于 AMI 所在的区域中。如果您更改源 AMI , 并希望在目标区域中的 AMIs 上反映这些更改 , 您必须将源 AMI 重新复制到目标区域中。



在首次将实例存储支持的 AMI 复制到一个区域时，我们为复制到该区域的 AMIs 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 AMIs 存储在该存储桶中。存储桶名称具有以下格式：amis-for-**account-in-region-hash**。例如：amis-for-123456789012-in-us-east-2-yhjmxvp6。

先决条件

在复制 AMI 之前，您必须确保更新源 AMI 的内容以支持在不同的区域中运行。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，从目标区域上的新 AMI 中启动的实例可能仍会使用源区域中的资源，这可能会影响性能和成本。

限制

- 目标区域限制为 50 个并发 AMI 副本。
- 您无法将半虚拟化 (PV) AMI 复制到不支持 PV AMI 的区域。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 87\)](#)。

跨账户复制

您可以与其他 AWS 账户共享 AMI。共享 AMI 不影响 AMI 的所有权。拥有它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 \(p. 93\)](#)。

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 传输费用，您需要支付目标区域中的目标 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。如果共享 AMI 带有加密快照，拥有者必须同时与您共享一个或多个密钥。

加密和复制

下表显示了各种 AMI 复制场景的加密支持。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	描述	支持
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

Note

在 CopyImage 操作期间加密仅适用于 Amazon EBS 支持的 AMIs。因为实例存储支持的 AMI 不依赖于快照，所以不能使用复制来更改其加密状态。

默认情况下（即未指定加密参数的情况下）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由相同客户主密钥 (CMK) 加密的相同目标快照。在默认情况下，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。

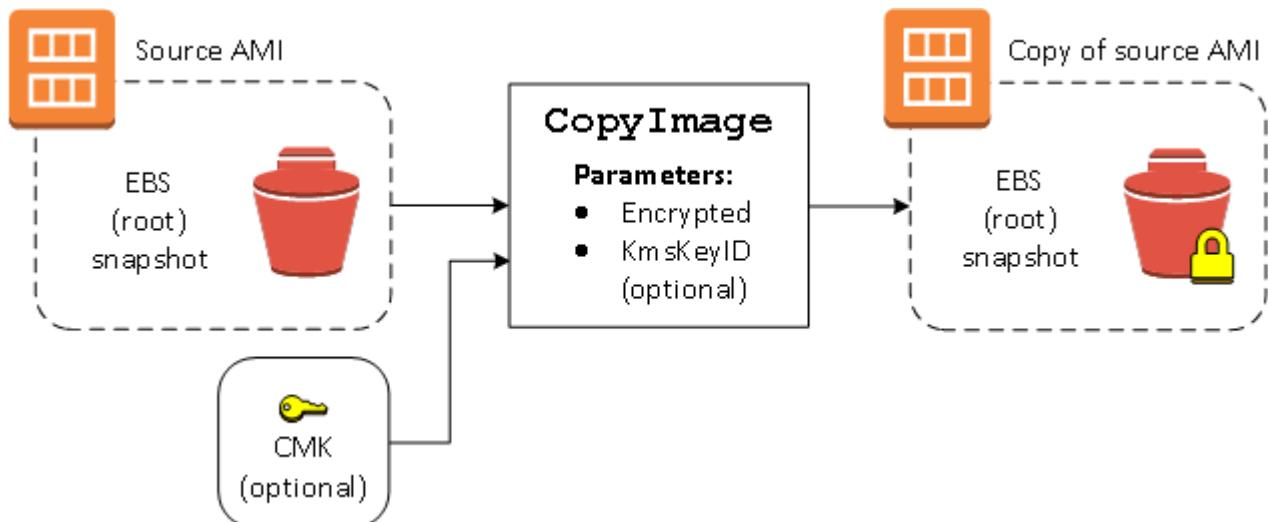
如果您在复制 AMI 的过程中指定对应加密参数，可以将其备份快照加密或重新加密。以下示例显示为 CopyImage 操作提供加密参数以更改目标 AMI 的加密状态的一个非默认案例。

将未加密的源 AMI 复制到加密目标 AMI

在这种情况下，将使用未加密根快照提供支持的 AMI 复制到使用加密根快照的 AMI。CopyImage 操作将通过两个加密参数（包括 CMK）进行调用。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 AMIs 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。

Note

启用[默认加密 \(p. 853\)](#)与针对 AMI 中的所有快照将 Encrypted 参数设置为 true 的效果相同。



设置 Encrypted 参数会对此实例的单一快照进行加密。如果您未指定 KmsKeyId 参数，则使用默认 CMK 来对快照副本加密。

有关复制带加密快照的 AMIs 的更多信息，请参阅[将加密与 EBS 支持的 AMI 结合使用 \(p. 134\)](#)。

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 \(p. 102\)](#)和[查找 Linux AMI \(p. 88\)](#)。

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，选择映像和 AMI 以显示区域中可供使用的 AMIs 列表。
3. 选择要复制的 AMI，然后选择操作和复制 AMI。
4. 在复制 AMI 对话框中，指定以下信息，然后选择复制 AMI：
 - 目标区域：在其中复制 AMI 的区域。
 - 名称：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。如果您启用[默认加密](#)，会同步设置加密选项，且不能通过 AMI 控制台取消设置该选项。
 - 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 AWS CLI 来复制 AMI

您可使用 [copy-image](#) 命令复制 AMI。您必须指定源和目标区域。您可以使用 --source-region 参数指定源区域。您可以使用 --region 参数或环境变量指定目标区域。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：--encrypted 和 --kms-key-id。

使用 Windows PowerShell 工具来复制 AMI

您可使用 [Copy-EC2Image](#) 命令复制 AMI。您必须指定源和目标区域。您可以使用 -SourceRegion 参数指定源区域。您可以使用 -Region 参数或 Set-AWSDefaultRegion 命令指定目标区域。有关更多信息，请参阅[指定 AWS 区域](#)。

在复制期间加密目标快照时，您必须指定这些额外参数：-Encrypted 和 -KmsKeyId。

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，从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，然后选择操作和取消注册。
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 Linux 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。有关更多信息，请参阅确定 AMI 的根设备类型 (p. 85)。

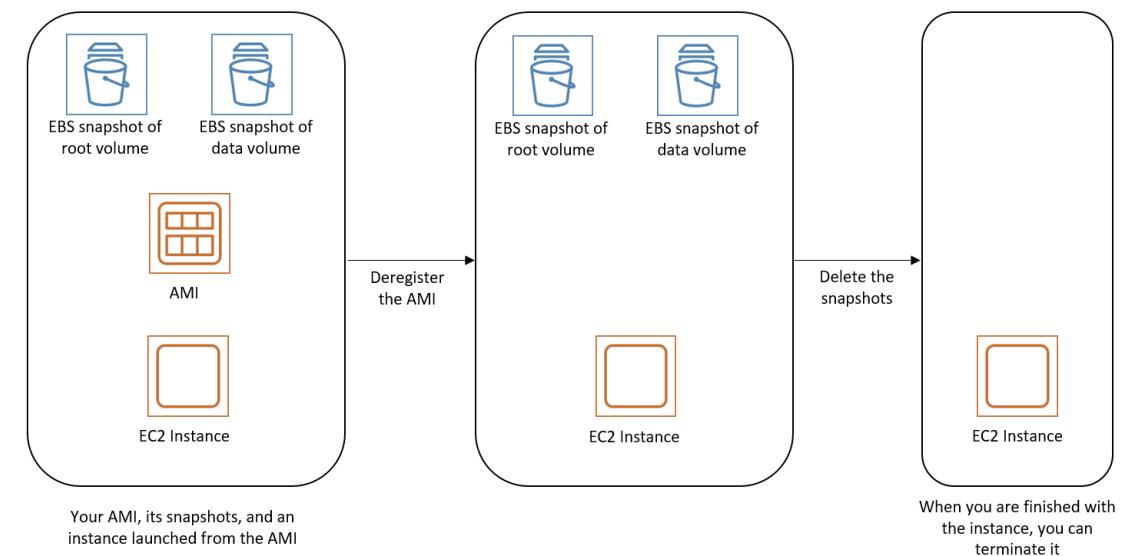
目录

- 清除由 Amazon EBS 支持的 AMI (p. 143)
- 清除由实例存储支持的 AMI (p. 143)

清除由 Amazon EBS 支持的 AMI

在取消注册由 Amazon EBS 支持的 AMI 时，不会影响在 AMI 创建过程中为实例的卷创建的快照。这些快照将继续产生存储费用。因此，如果使用完这些快照，应将其删除。

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。

Note

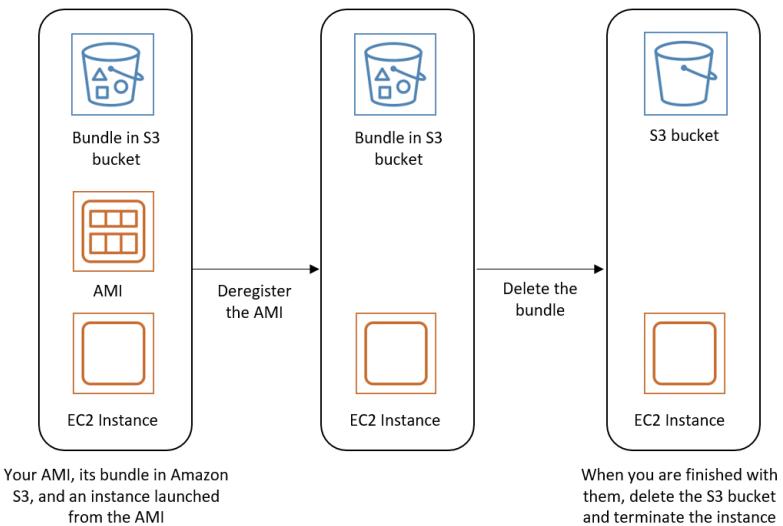
控制台可能需要几分钟时间才能从列表中删除该 AMI。选择 Refresh 以刷新状态。

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
```

2. 使用 [ec2-delete-bundle \(p. 124\)](#) (AMI 工具) 命令删除 Amazon S3 中的捆绑包，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 轻松集成的程序包，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。许多在 CentOS (及类似发行版) 上开发的应用程序在 Amazon Linux 上运行。

AWS 提供了两个版本的 Amazon Linux : Amazon Linux 2 和 Amazon Linux AMI。有关更多信息 (包括 AMI 的完整列表)，请参阅 [Amazon Linux 2](#) 和 [Amazon Linux AMI](#)。有关 Amazon Linux Docker 容器映像，请参阅 Docker Hub 上的 [amazonlinux](#)。

如果您要从其他 Linux 发行版迁移至 Amazon Linux，我们建议您迁移至 Amazon Linux 2。如果您目前使用的是 Amazon Linux AMI，则建议您迁移至 Amazon Linux 2。要迁移至 Amazon Linux 2，请启动实例或使用当前映像创建虚拟机。在 Amazon Linux 2 上安装您的应用程序以及应用程序所需的任何程序包。测试您的

应用程序，并进行使其在 Amazon Linux 2 上运行所需的任何更改。有关在 AWS 外部运行 Amazon Linux 的更多信息，请参阅[作为本地虚拟机运行 Amazon Linux 2 \(p. 151\)](#)。

目录

- [连接到 Amazon Linux 实例 \(p. 145\)](#)
- [识别 Amazon Linux 映像 \(p. 145\)](#)
- [AWS 命令行工具 \(p. 146\)](#)
- [程序包存储库 \(p. 147\)](#)
- [Extras 库 \(Amazon Linux 2\) \(p. 149\)](#)
- [访问源软件包获取参考信息 \(p. 149\)](#)
- [cloud-init \(p. 149\)](#)
- [订阅 Amazon Linux 通知 \(p. 151\)](#)
- [作为本地虚拟机运行 Amazon Linux 2 \(p. 151\)](#)

连接到 Amazon Linux 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。

识别 Amazon Linux 映像

每个映像都包含用于识别它的唯一的 /etc/image-id 文件。此文件包含有关映像的以下信息：

- `image_name`、`image_version`、`image_arch` — 来自 Amazon 用于构建映像的构建配方的值。
- `image_stamp` — 映像创建期间随机生成的一个唯一的十六进制值。
- `image_date` — 映像创建的 UTC 时间，采用 YYYYMMDDhhmmss 格式
- `recipe_name`、`recipe_id` — Amazon 用于构建映像的构建配方的名称和 ID。

Amazon Linux 包含 /etc/system-release 文件，用于指定当前已安装的版本。此文件使用 yum 进行更新，是 system-release RPM 的一部分。

Amazon Linux 还包含遵循 CPE 规范的 /etc/system-release 的机器可读版本；请参阅 /etc/system-release-cpe。

Amazon Linux 2

以下是当前 Amazon Linux 2 版本的 /etc/image-id 示例：

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn2-ami-hvm"
image_version="2"
image_arch="x86_64"
image_file="amzn2-ami-hvm-2.0.20180810-x86_64.xfs.gpt"
image_stamp="8008-2abd"
image_date="20180811020321"
recipe_name="amzn2 ami"
recipe_id="c652686a-2415-9819-65fb-4dee-9792-289d-1e2846bd"
```

以下是当前 Amazon Linux 2 版本的 /etc/system-release 示例：

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux 2
```

以下是 Amazon Linux 2 的 /etc/os-release 示例：

```
[ec2-user ~]$ cat /etc/os-release
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
HOME_URL="https://amazonlinux.com/"
```

Amazon Linux AMI

以下是当前 Amazon Linux AMI 版本的 /etc/image-id 示例：

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn-ami-hvm"
image_version="2018.03"
image_arch="x86_64"
image_file="amzn-ami-hvm-2018.03.0.20180811-x86_64.ext4.gpt"
image_stamp="cc81-f2f3"
image_date="20180811012746"
recipe_name="amzn ami"
recipe_id="5b283820-dc60-a7ea-d436-39fa-439f-02ea-5c802dbd"
```

以下是当前 Amazon Linux AMI 版本的 /etc/system-release 示例：

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux AMI release 2018.03
```

AWS 命令行工具

以下 AWS 集成命令行工具及使用方法包含在 Amazon Linux AMI 中或 Amazon Linux 2 的默认存储库中。有关 Amazon Linux AMI 中的程序包的完整列表，请参阅 [Amazon Linux AMI 2017.09 程序包](#)。

- aws-amitools-ec2
- aws-apitools-as
- aws-apitools-cfn
- aws-apitools-ec2
- aws-apitools-elb
- aws-apitools-mon
- aws-cfn-bootstrap
- aws-cli

Amazon Linux 2 和最低版本的 Amazon Linux (amzn-ami-minimal-* 和 amzn2-ami-minimal-*) 并不总是包含所有这些程序包；但您可以使用以下命令来从默认存储库中安装它们：

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

对于使用 IAM 角色启动的实例，提供了一个简单脚本，用于在安装凭证文件后准备 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，为了支持您安装多个版本的 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

由 /etc/profile.d/aws-apitools-common.sh 用于设置产品特定的环境变量，如 EC2_HOME。

程序包存储库

Amazon Linux 2 和 Amazon Linux AMI 旨在与每个 Amazon EC2 AWS 区域中托管的在线程序包存储库结合使用。这些存储库为 Amazon Linux 2 和 Amazon Linux AMI 中的程序包提供持续更新，还可访问数百个常见的开源服务器应用程序。这些存储库在所有区域中提供，可使用 yum 更新工具进行访问。通过在每个区域托管存储库，我们可以快速部署更新，不会产生任何数据传输费。

Amazon Linux 2 和 Amazon Linux AMI 会定期进行更新，增强安全性及功能。如果您不需要保留实例的数据或自定义项，则只需使用当前 AMI 启动新实例。如果您需要保留实例的数据或自定义项，则可以通过 Amazon Linux 程序包存储库维护这些实例。这些存储库包含所有更新后的程序包。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 和更新程序包仍继续可用。

Important

您的实例必须具有 Internet 访问权限才能访问该存储库。

要安装程序包，请使用以下命令：

```
[ec2-user ~]$ sudo yum install package
```

对于 Amazon Linux AMI，系统配置了对 Extra Packages for Enterprise Linux (EPEL) 存储库的访问权限，但默认情况下未启用。Amazon Linux 2 未配置为使用 EPEL 存储库。除了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。您可以使用以下命令来启用 EPEL 存储库：

- 对于 Amazon Linux 2：

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- 对于 Amazon Linux AMI：

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

如果您发现 Amazon Linux 不包含您需要的应用程序，您只需直接在 Amazon Linux 实例上安装该应用程序即可。Amazon Linux 使用 RPM 和 yum 来管理程序包，而这可能是安装新应用程序的最简单的方式。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 `cloud-init` 程序包中的 `PACKAGE_SETUP` 操作，在实例启动时，上传应用程序。有关更多信息，请参阅[cloud-init \(p. 149\)](#)。

安全更新

安全更新通过程序包存储库提供，而更新后的 AMI 安全警报在 [Amazon Linux 安全中心](#) 中发布。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 配置为在启动时下载和安装关键或重要安全更新。我们建议您在启动后针对您的用例进行必要的更新。例如，您可能希望在启动时应用所有更新（而不仅仅是安全更新），或者评估各个更新并仅应用适用于您系统的更新。这是使用以下 `cloud-init` 设置进行控制的：`repo_upgrade`。下方 `cloud-init` 配置片段显示了如何修改传递到实例初始化用户数据文本中的设置：

```
#cloud-config
repo_upgrade: security
```

`repo_upgrade` 的可能值如下所示：

`security`

应用 Amazon 标记为安全更新的明显关键或重要更新。

`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 会在启动时执行适用于所有已安装程序包的安全升级。在您使用 `/etc/mota` 文件登录时，Amazon Linux 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`。

存储库配置

利用 Amazon Linux，AMI 将被视为实时快照，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程序包。

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 2017.09 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` 功能禁用滚动更新。`lock-on-launch` 功能会锁定您的实例，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 2017.09 AMI，使其仅接收早于 2018.03 AMI 发布的更新，直至您准备好迁移到 2018.03 AMI 为止。

Important

如果锁定到并非最新的存储库版本，则您不会收到后续更新。要接收连续更新流，您必须使用最新的 AMI，或持续更新您的 AMI，使存储库指向最新版本。

要在新实例中启用 `lock-on-launch` 功能，请使用已传递到 `cloud-init` 的以下用户数据启动它：

```
#cloud-config
repo_releasever: 2017.09
```

将现有实例锁定到当前 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。

Extras 库 (Amazon Linux 2)

利用 Amazon Linux 2，您可以使用 Extras 库来在您的实例上安装应用程序和软件更新。这些软件更新称为主题。您可以安装主题的某特定版本或忽略要使用最新版本的版本信息。

要列出可用的主题，请使用以下命令：

```
[ec2-user ~]$ amazon-linux-extras list
```

要启用主题并安装其程序包的最新版本以确保最新，请使用以下命令：

```
[ec2-user ~]$ sudo amazon-linux-extras install topic
```

要启用主题并安装其程序包的特定版本以确保稳定性，请使用以下命令：

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

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 `yumdownloader --source` 命令在您正在运行的实例中查看源。例如：

```
[ec2-user ~]$ yumdownloader --source bash
```

您可以对源 RPM 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。

cloud-init

cloud-init 程序包是由 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 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，您可以将通用 AMI 用于许多使用案例，并在启动时进行动态配置。Amazon Linux 还使用 cloud-init 执行 `ec2-user` 账户的初始配置。

有关更多信息，请参阅 [cloud-init 文档](#)。

Amazon Linux 使用在 `/etc/cloud/cloud.cfg.d` 和 `/etc/cloud/cloud.cfg` 中发现的 cloud-init 操作。您可以在 `/etc/cloud/cloud.cfg.d` 中创建自己的 cloud-init 操作文件。此目录中的所有文件均由 cloud-init 读取。它们是按词典顺序进行读取的，并且文件随后将覆盖之前文件中的值。

cloud-init 程序包将在启动时对实例执行这些（以及其他）常见配置任务：

- 设置默认区域设置。

- 设置主机名。
- 解析并处理用户数据。
- 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。
- 准备存储库以进行程序包管理。
- 处理用户数据中定义的软件包操作。
- 执行在用户数据中找到的用户脚本。
- 装载实例存储卷 (如果适用)。
 - 默认情况下，`ephemeral0` 实例存储卷装载在 `/media/ephemeral0` (如果它存在且包含有效的文件系统；否则将不会安装)。
 - 默认情况下，将装载与实例关联的所有交换卷 (仅适用于 `m1.small` 和 `c1.medium` 实例类型)。
- 您可以使用以下 `cloud-init` 指令覆盖默认实例存储卷安装：

```
#cloud-config
mounts:
- [ ephemeral0 ]
```

有关对安装的更多控制，请参阅 `cloud-init` 文档中的[安装](#)。

- 在实例启动时，不会格式化支持 TRIM 的实例存储卷，因此，您必须先对这些卷进行分区和格式化，然后才能装载它们。有关更多信息，请参阅[实例存储卷 TRIM 支持 \(p. 913\)](#)。您可以在启动时使用 `disk_setup` 模块对您的实例存储卷进行分区和格式化。有关更多信息，请参阅 `cloud-init` 文档中的[磁盘设置](#)。

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。如果多部分内容型文件的格式是受支持的格式，则 `cloud-init` 可以处理它的各部分内容。
- Base64 解码
 - 如果用户数据是使用 base64 编码的，`cloud-init` 将决定它能否将解码后的数据当作其中一种受支持的数据类型进行理解。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。要了解支持的配置格式的带注释示例，请查看示例。
- Upstart 作业

- 开头为 `#upstart-job` 或 `Content-Type: text/upstart-job`。
- 此内容存储在 `/etc/init` 中的一个文件里，`upstart` 使用内容的方式与其他 `upstart` 作业相同。
- 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` 下的一个文件中并会立即执行。
 - 这是最早可用的 "hook"。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。

订阅 Amazon Linux 通知

要收到新 AMI 发布通知，可使用 Amazon SNS 订阅。

订阅 Amazon Linux 通知

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 在导航栏中，将区域更改为 美国东部（弗吉尼亚北部）（如果需要）。必须选择所订阅的 SNS 通知在创建时所在的区域。
3. 在导航窗格中，依次选择 Subscriptions 和 Create subscription。
4. 对于 Create subscription 对话框，执行以下操作：
 - a. [Amazon Linux 2] 对于主题 ARN，复制并粘贴以下 Amazon 资源名称 (ARN)：`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`。
 - b. [Amazon Linux] 对于主题 ARN，复制并粘贴以下 Amazon 资源名称 (ARN)：`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`。
 - c. 对于协议，选择电子邮件。
 - d. 对于终端节点，输入可以用于接收通知的电子邮件地址。
 - e. 选择 Create subscription。
5. 您将收到一封主题行为“AWS Notification - Subscription Confirmation”(AWS 通知 - 订阅确认) 的确认电子邮件。打开电子邮件，然后选择 Confirm subscription 以完成订阅。

每当发布新的 AMI 时，我们都会向相应主题的订阅者发送通知。若不想再接收这些通知，请使用以下过程取消订阅。

取消订阅 Amazon Linux 通知

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 在导航栏中，将区域更改为 美国东部（弗吉尼亚北部）（如果需要）。必须使用创建 SNS 通知的区域。
3. 在导航窗格中，选择订阅，选择订阅，然后选择操作和删除订阅。
4. 当系统提示进行确认时，选择 Delete。

作为本地虚拟机运行 Amazon Linux 2

使用 Amazon Linux 2 虚拟机 (VM) 映像进行本地开发和测试。这些映像适用于以下虚拟化平台：

- VMWare
- KVM
- VirtualBox (Oracle VM)
- Microsoft Hyper-V

要将 Amazon Linux 2 虚拟机映像用于受支持的虚拟化平台之一，请执行以下操作：

- 步骤 1：准备 `seed.iso` 启动映像 (p. 152)
- 步骤 2：下载 Amazon Linux 2 VM 映像 (p. 153)
- 步骤 3：启动并连接到新 VM (p. 153)

步骤 1：准备 `seed.iso` 启动映像

`seed.iso` 启动映像包含启动新虚拟机所需的初始配置信息，如网络配置、主机名和用户数据。

Note

`seed.iso` 启动映像仅包括启动 VM 所需的配置信息。不包括 Amazon Linux 2 操作系统文件。

要生成 `seed.iso` 启动映像，需要两个配置文件：

- `meta-data` — 此文件包括 VM 主机名和静态网络设置。
- `user-data` — 此文件配置用户账户，并指定其密码、密钥对以及访问机制。默认情况下，Amazon Linux 2 VM 映像会创建 `ec2-user` 用户账户。使用 `user-data` 配置文件设置默认用户账户的密码。

创建 `seed.iso` 启动盘

1. 创建一个名为 `seedconfig` 的新文件夹并导航到该文件夹。
2. 创建 `meta-data` 配置文件。
 - a. 创建名为 `meta-data` 的新文件。
 - b. 使用首选编辑器打开 `meta-data` 文件，并添加以下内容。

```
local-hostname: vm_hostname
# eth0 is the default network interface enabled in the image. You can configure
static network settings with an entry like the following.
network-interfaces: |
    auto eth0
    iface eth0 inet static
        address 192.168.1.10
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.254
```

将 `vm_hostname` 替换为您选择的 VM 主机名，并根据需要配置网络设置。

- c. 保存并关闭 `meta-data` 配置文件。

有关示例 `meta-data` 配置文件（用于指定 VM 主机名 (`amazonlinux.onprem`)、配置默认网络接口 (`eth0`) 并为必要的网络设备指定静态 IP 地址），请参阅[示例 Seed.iso 文件](#)。

3. 创建 `user-data` 配置文件。
 - a. 创建名为 `user-data` 的新文件。
 - b. 使用首选编辑器打开 `user-data` 文件，并添加以下内容。

```
#cloud-config
#vim:syntax=yaml
users:
# A user by the name `ec2-user` is created in the image by default.
- default
```

```
chpasswd:  
list: |  
ec2-user:plain_text_password  
# In the above line, do not add any spaces after 'ec2-user:'.
```

将 *plain_text_password* 替换为您为默认 ec2-user 用户帐户选择的密码。

- c. (可选) 默认情况下，VM 每次启动时，cloud-init 都会应用网络设置。添加以下内容，以防止 cloud-init 在每次启动时都应用网络设置，并保留首次启动期间应用的网络设置。

```
# NOTE: Cloud-init applies network settings on every boot by default. To retain  
network settings from first  
boot, add following 'write_files' section:  
write_files:  
- path: /etc/cloud/cloud.cfg.d/80_disable_network_after_firstboot.cfg  
content: |  
# Disable network configuration after first boot  
network:  
config: disabled
```

- d. 保存并关闭 user-data 配置文件。

还可以创建其他用户账户并指定其访问机制、密码和密钥对。有关支持的指令的更多信息，请参阅[模块](#)。有关创建三个其他用户并为默认 ec2-user 用户帐户指定自定义密码的示例 user-data 文件，请参阅[示例 Seed.iso 文件](#)。

4. 使用 seed.iso 和 meta-data 配置文件创建 user-data 启动映像。

对于 Linux，请使用类似 genisoimage 的工具。导航到 seedconfig 文件夹，并执行以下命令。

```
$ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

对于 macOS，请使用类似 hdiutil 的工具。从 seedconfig 文件夹往上导航一级，执行以下命令。

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata  
seedconfig/
```

步骤 2：下载 Amazon Linux 2 VM 映像

我们为受支持的每个虚拟化平台提供不同的 Amazon Linux 2 VM 映像。下载所选平台对应的 VM 映像：

- VMWare
- KVM
- Oracle VirtualBox
- Microsoft Hyper-V

步骤 3：启动并连接到新 VM

要启动和连接到新 VM，必须要有 seed.iso 启动映像（在步骤 1 中创建）和 Amazon Linux 2 VM 映像（在步骤 2 中下载）。具体步骤因您选择的 VM 平台而异。

首次启动时，您必须将 seed.iso 启动映像连接到 VM。seed.iso 仅在初始启动期间评估。

在 VM 启动后，使用在 user-data 配置文件中定义的用户账户之一登录。对于 VMWare 之外的虚拟化平台，在首次登录后，可以将 seed.iso 启动映像与 VM 断开连接。

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 \(p. 87\)](#)。

目录

- [HVM AMIs \(GRUB\) \(p. 154\)](#)
- [半虚拟化 AMIs \(PV-GRUB\) \(p. 155\)](#)

HVM AMIs (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 发行版配合使用。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 AMIs 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，可在两个内核条目中进行选择：Amazon Linux 2018.03（此 AMI 的原始内核），以及 Vanilla Linux 4.16.4（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。

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 \(p. 983\)](#)。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` 以启用 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 4.16.4
root (hd0)
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initrd.img-4.16.4

title Amazon Linux 2018.03 (4.14.26-46.32.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-4.14.26-46.32.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initramfs-4.14.26-46.32.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 AMIs (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 是半虚拟化引导加载器，运行经过修补的 GNU GRUB 0.97 版本。当您启动实例时，PV-GRUB 会启动引导过程，然后链式加载由映像的 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 发行版配合使用。较旧发行版（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，而较新发行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），无需执行额外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行版兼容。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[配置 GRUB \(p. 155\)](#) 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 \(p. 155\)](#)
- [为半虚拟化 AMIs 配置 GRUB \(p. 155\)](#)
- [Amazon PV-GRUB Kernel Image ID \(p. 156\)](#)
- [更新 PV-GRUB \(p. 158\)](#)

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。
- 集群 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 外有一个独立的引导分区。然后，您可以通过 LVM 创建逻辑卷。

为半虚拟化 AMIs 配置 GRUB

要引导 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。

以下是在启动带 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 2018.03（此 AMI 的原始内核），以及 Vanilla Linux 4.16.4（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 4.16.4
root (hd0)
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.16.4

title Amazon Linux 2018.03 (4.14.26-46.32.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.14.26-46.32.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.14.26-46.32.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-West)

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. 查找您的实例的内核 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"  
}  
]  
}
```

此内核映像是 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 \(p. 156\)](#) 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 \(p. 156\)](#) 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. 修改用于您的实例的内核映像。

```
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 \(p. 18\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 24\)](#)
- [实例生命周期 \(p. 370\)](#)

您需先回答以下问题，然后才能启动生产环境。

问：哪种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 \(p. 160\)](#)。

问：哪个购买选项最能满足我的需求？

Amazon EC2 支持按需实例（默认值）、Spot 实例和预留实例。有关更多信息，请参阅[实例购买选项 \(p. 239\)](#)。

问：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 \(p. 85\)](#)。

问：我能否在混合环境中远程管理 EC2 实例以及设备的队列？

AWS Systems Manager 可让您在混合环境中安全地远程管理 Amazon EC2 实例、本地实例和虚拟机（VM）（包括来自其他云提供商的虚拟机）的配置。有关更多信息，请参阅[AWS Systems Manager 用户指南](#)。

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，无论实际的基础硬件是什么。

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。如果一个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。但是，当某个资源利用不充分时，会有实例会在该资源可用时消耗其更多的份额。

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。

目录

- 可用实例类型 (p. 161)
- 硬件规格 (p. 163)
- AMI 虚拟化类型 (p. 163)
- 基于 Nitro 的实例 (p. 163)
- 联网和存储功能 (p. 164)
- 实例限制 (p. 166)
- 通用实例 (p. 166)
- 计算优化型实例 (p. 202)
- 内存优化型实例 (p. 207)
- 存储优化型实例 (p. 215)
- Linux 加速计算实例 (p. 222)
- 查找实例类型 (p. 232)
- 更改实例类型 (p. 233)
- 获取实例类型建议 (p. 237)

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。

有关最新一代实例类型的更多信息，请参阅 [Amazon EC2 实例类型](#)。

实例系列	当前一代实例类型
通用型	a1.medium a1.large a1.xlarge a1.2xlarge a1.4xlarge m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge m5.large m5.xlarge m5.2xlarge m5.4xlarge m5.8xlarge m5.12xlarge m5.16xlarge m5.24xlarge m5.metal m5a.large m5a.xlarge m5a.2xlarge m5a.4xlarge m5a.8xlarge m5a.12xlarge m5a.16xlarge m5a.24xlarge m5ad.large m5ad.xlarge m5ad.2xlarge m5ad.4xlarge m5ad.8xlarge m5ad.12xlarge m5ad.16xlarge m5ad.24xlarge m5d.large m5d.xlarge m5d.2xlarge m5d.4xlarge m5d.8xlarge m5d.12xlarge m5d.16xlarge m5d.24xlarge m5d.metal m5dn.large m5dn.xlarge m5dn.2xlarge m5dn.4xlarge m5dn.8xlarge m5dn.12xlarge m5dn.16xlarge m5dn.24xlarge m5n.large m5n.xlarge m5n.2xlarge m5n.4xlarge m5n.8xlarge m5n.12xlarge m5n.16xlarge m5n.24xlarge t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge t3.nano t3.micro t3.small t3.medium t3.large t3.xlarge t3.2xlarge t3a.nano t3a.micro t3a.small t3a.medium t3a.large t3a.xlarge t3a.2xlarge
计算优化	c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c5.large c5.xlarge c5.2xlarge c5.4xlarge c5.9xlarge c5.12xlarge c5.18xlarge c5.24xlarge c5.metal c5d.large c5d.xlarge

实例系列	当前一代实例类型
	c5d.2xlarge c5d.4xlarge c5d.9xlarge c5d.12xlarge c5d.18xlarge c5d.24xlarge c5d.metal c5n.large c5n.xlarge c5n.2xlarge c5n.4xlarge c5n.9xlarge c5n.18xlarge c5n.metal
内存优化	r4.large r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge r5.large r5.xlarge r5.2xlarge r5.4xlarge r5.8xlarge r5.12xlarge r5.16xlarge r5.24xlarge r5.metal r5a.large r5a.xlarge r5a.2xlarge r5a.4xlarge r5a.8xlarge r5a.12xlarge r5a.16xlarge r5a.24xlarge r5ad.large r5ad.xlarge r5ad.2xlarge r5ad.4xlarge r5ad.12xlarge r5ad.24xlarge r5d.large r5d.xlarge r5d.2xlarge r5d.4xlarge r5d.8xlarge r5d.12xlarge r5d.16xlarge r5d.24xlarge r5d.metal r5dn.large r5dn.xlarge r5dn.2xlarge r5dn.4xlarge r5dn.8xlarge r5dn.12xlarge r5dn.16xlarge r5dn.24xlarge r5n.large r5n.xlarge r5n.2xlarge r5n.4xlarge r5n.8xlarge r5n.12xlarge r5n.16xlarge r5n.24xlarge u-6tb1.metal u-9tb1.metal u-12tb1.metal u-18tb1.metal u-24tb1.metal x1.16xlarge x1.32xlarge x1e.xlarge x1e.2xlarge x1e.4xlarge x1e.8xlarge x1e.16xlarge x1e.32xlarge z1d.large z1d.xlarge z1d.2xlarge z1d.3xlarge z1d.6xlarge z1d.12xlarge z1d.metal
存储优化	d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge h1.2xlarge h1.4xlarge h1.8xlarge h1.16xlarge i3.large i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge i3.metal i3en.large i3en.xlarge i3en.2xlarge i3en.3xlarge i3en.6xlarge i3en.12xlarge i3en.24xlarge i3en.metal
加速计算	f1.2xlarge f1.4xlarge f1.16xlarge g3s.xlarge g3.4xlarge g3.8xlarge g3.16xlarge g4dn.xlarge g4dn.2xlarge g4dn.4xlarge g4dn.8xlarge g4dn.12xlarge g4dn.16xlarge p2.xlarge p2.8xlarge p2.16xlarge p3.2xlarge p3.8xlarge p3.16xlarge p3dn.24xlarge inf1.xlarge inf1.2xlarge inf1.6xlarge inf1.24xlarge

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，但我们将继续支持上一代的这些数据库实例。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 m3.medium m3.large m3.xlarge m3.2xlarge t1.micro
计算优化	c1.medium c1.xlarge cc2.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge

实例系列	上一代实例类型
内存优化	m2.xlarge m2.2xlarge m2.4xlarge cr1.8xlarge r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge
存储优化	hs1.8xlarge i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge
加速计算	g2.2xlarge g2.8xlarge

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 实例类型](#)。

要确定最适合您的需求的实例类型，我们建议启动一个实例，并使用自己的基准测试应用程序。由于您是按实例秒付费的，因此在做出决策前测试多个实例类型将会既方便又经济。

如果您的需求有变化，甚至是在做出决策后，您可以在以后调整您的实例的大小。有关更多信息，请参阅 [更改实例类型 \(p. 233\)](#)。

Note

Amazon EC2 实例通常在 64 位虚拟 Intel 处理器上运行，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 实例类型](#)。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。

AMI 虚拟化类型

实例的虚拟化类型由用于启动该实例的 AMI 决定。当前一代实例类型仅支持硬件虚拟机 (HVM)。某些上一代实例类型支持半虚拟化 (PV)，某些 AWS 区域支持半虚拟化实例。有关更多信息，请参阅 [Linux AMI 虚拟化类型 \(p. 87\)](#)。

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。

基于 Nitro 的实例

Nitro 系统是 AWS 构建的硬件和软件组件的集合，可实现高性能、高可用性和高安全性。此外，Nitro 系统还提供了裸机功能，从而消除了所有虚拟化开销并支持需要完全访问主机硬件的工作负载。

Nitro 组件

以下组件属于 Nitro 系统的一部分：

- Nitro 管理程序 - 一种轻量级管理程序，可管理内存和 CPU 分配并为多数工作负载提供了与裸机不相上下的性能。
- Nitro 卡
 - 本地 NVMe 存储卷
 - 联网硬件支持

- 管理
- 监控
- 安全性
- Nitro 安全芯片，集成到主板中

实例类型

以下实例基于 Nitro 系统：

- A1、C5、C5d、C5n、G4、I3en、Inf1、M5、M5a、M5ad、M5d、M5dn、M5np3dn.24xlarge、R5、R5a、R5ad、和 z1d
- 裸机：c5.metal, c5d.metal, c5n.metal, i3.metal, i3en.metal, m5.metal, m5d.metal, r5.metal, r5d.metal, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, and z1d.metal

资源

有关更多信息，请观看以下视频：

- [AWS re:Invent 2017 : Amazon EC2 Nitro 系统架构](#)
- [AWS re:Invent 2017 : Amazon EC2 裸机实例](#)
- [Nitro 项目 : 下一代 EC2 基础设施](#)

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

- 所有当前生成实例类型以及 C3、R3 和 I2 以前生成实例类型都支持 IPv6。
- 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：
 - 将支持的实例类型启动到集群置放群组中，以针对高性能计算 (HPC) 应用程序优化您的实例。通用集群置放群组中的实例可以受益于高带宽、低延迟的联网。有关更多信息，请参阅 [置放群组 \(p. 662\)](#)。
 - 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 \(p. 616\)](#)。
- 为增强网络启用的当前生成实例类型具有以下网络性能属性：
 - 通过私有 IPv4 或 IPv6 位于相同区域内的流量可以支持 5 Gbps 用于单流流量，以及最多 25 Gbps 用于多流流量（取决于实例类型）。
 - 在同一个区域中，通过公有 IP 地址空间或者通过 VPC 终端节点往返于 Amazon S3 存储桶之间的流量可以使用所有可用的实例聚合带宽。
- 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（巨型帧），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 \(MTU\) \(p. 669\)](#)。

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。一些支持实例存储卷的实例类型使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。一些实例类型支持 NVMe 实例存储卷。一些实例类型支持 NVMe EBS 卷。有关更多信息，请参阅 [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#) 和 [NVMe SSD 卷 \(p. 912\)](#)。

- 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 优化的实例 \(p. 863\)](#)。

联网和存储功能总结

下表总结了当前一代实例类型支持的联网和存储功能。

	仅限于 EBS	NVMe EBS	实例存储	置放群组	增强联网
A1	是	是	否	是	ENA
C4	是	否	否	是	Intel 82599 VF
C5	是	是	否	是	ENA
C5d	否	是	NVMe *	是	ENA
C5n	是	是	否	是	ENA
D2	否	否	HDD	是	Intel 82599 VF
F1	否	否	NVMe *	是	ENA
G3	是	否	否	是	ENA
G4	否	是	NVMe *	是	ENA
HS1	否	否	HDD *	是	ENA
I3	否	否	NVMe *	是	ENA
I3en	否	是	NVMe *	是	ENA
M4	是	否	否	是	m4.16xlarge: ENA 所有其他尺寸： Intel 82599 VF
M5	是	是	否	是	ENA
M5a	是	是	否	是	ENA
M5ad	否	是	NVMe *	是	ENA
M5d	否	是	NVMe *	是	ENA
M5dn	否	是	NVMe *	是	ENA
M5n	是	是	否	是	ENA
P2	是	否	否	是	ENA
P3	是	否	否	是	ENA
P3dn	否	是	NVMe *	是	ENA
R4	是	否	否	是	ENA
R5	是	是	否	是	ENA

	仅限于 EBS	NVMe EBS	实例存储	置放群组	增强联网
R5a	是	是	否	是	ENA
R5ad	否	是	NVMe *	是	ENA
R5d	否	是	NVMe *	是	ENA
R5dn	否	是	NVMe *	是	ENA
R5n	是	是	否	是	ENA
T2	是	否	否	否	否
T3	是	是	否	否	ENA
T3a	是	是	否	否	ENA
u-xtb1.metal	是	是	否	否	ENA
X1	否	否	SSD	是	ENA
X1e	否	否	SSD *	是	ENA
z1d	否	是	NVMe *	是	ENA

* 根设备卷必须是 Amazon EBS 卷。

下表总结了前一代实例类型支持的联网和存储功能。

	实例存储	置放群组	增强联网
C3	SSD	是	Intel 82599 VF
G2	SSD	是	否
I2	SSD	是	Intel 82599 VF
M3	SSD	否	否
R3	SSD	是	Intel 82599 VF

实例限制

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[我可以在 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 \(p. 950\)](#)。

通用实例

通用型实例提供了平衡的计算、内存和网络资源，可用于多种工作负载。

A1 实例

A1 实例非常适合 Arm 生态系统支持的横向扩展工作负载。这些实例非常适合以下应用：

- Web 服务器
- 容器化微服务
- 缓存机群
- 分布式数据存储
- 需要 Arm 基础设施集的应用程序

有关更多信息，请参阅 [Amazon EC2 A1 实例](#)。

M5、M5a、M5ad、M5d、M5dn 和 M5n 实例

这些实例提供了理想的云基础设施，面向部署在云中的广泛应用程序，提供平衡的计算、内存和网络资源。M5 实例非常适合以下应用程序：

- Web 和应用程序服务器
- 中小型数据库
- 游戏服务器
- 缓存机群
- 为 SAP、Microsoft SharePoint、集群计算和其他企业应用程序运行后端服务器

m5.metal 和 m5d.metal 实例为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。这些实例非常适合：

- 需要访问虚拟环境中不可用或不完整支持的低级硬件功能（如 Intel VT）的工作负载
- 需要非虚拟化环境进行许可或支持的应用程序

有关更多信息，请参阅 [Amazon EC2 M5 实例](#)。

T2、T3 和 T3a 实例

这些实例提供基准水平的 CPU 性能，并且能够在您的工作负载需要时突增到更高的性能。无限制实例可以将较高的 CPU 性能保持所需的任意时间。有关更多信息，请参阅 [可突增性能实例 \(p. 175\)](#)。这些实例非常适合以下应用：

- 网站和 Web 应用程序
- 代码存储库
- 开发、构建、测试和存放环境
- 微服务

有关更多信息，请参阅 [Amazon EC2 T2 实例](#) 和 [Amazon EC2 T3 实例](#)。

目录

- [硬件规格 \(p. 168\)](#)
- [实例性能 \(p. 170\)](#)
- [网络性能 \(p. 171\)](#)
- [SSD I/O 性能 \(p. 172\)](#)
- [实例功能 \(p. 173\)](#)
- [发行说明 \(p. 174\)](#)
- [可突增性能实例 \(p. 175\)](#)

硬件规格

以下是通用型实例的硬件规格摘要。

实例类型	默认 vCPU	内存 (GiB)
a1.medium	1	2
a1.large	2	4
a1.xlarge	4	8
a1.2xlarge	8	16
a1.4xlarge	16	32
m4.large	2	8
m4.xlarge	4	16
m4.2xlarge	8	32
m4.4xlarge	16	64
m4.10xlarge	40	160
m4.16xlarge	64	256
m5.large	2	8
m5.xlarge	4	16
m5.2xlarge	8	32
m5.4xlarge	16	64
m5.8xlarge	32	128
m5.12xlarge	48	192
m5.16xlarge	64	256
m5.24xlarge	96	384
m5.metal	96	384
m5a.large	2	8
m5a.xlarge	4	16
m5a.2xlarge	8	32
m5a.4xlarge	16	64
m5a.8xlarge	32	128
m5a.12xlarge	48	192
m5a.16xlarge	64	256
m5a.24xlarge	96	384

实例类型	默认 vCPU	内存 (GiB)
m5ad.large	2	8
m5ad.xlarge	4	16
m5ad.2xlarge	8	32
m5ad.4xlarge	16	64
m5ad.8xlarge	32	128
m5ad.12xlarge	48	192
m5ad.16xlarge	64	256
m5ad.24xlarge	96	384
m5d.large	2	8
m5d.xlarge	4	16
m5d.2xlarge	8	32
m5d.4xlarge	16	64
m5d.8xlarge	32	128
m5d.12xlarge	48	192
m5d.16xlarge	64	256
m5d.24xlarge	96	384
m5d.metal	96	384
m5dn.large	2	8
m5dn.xlarge	4	16
m5dn.2xlarge	8	32
m5dn.4xlarge	16	64
m5dn.8xlarge	32	128
m5dn.12xlarge	48	192
m5dn.16xlarge	64	256
m5dn.24xlarge	96	384
m5n.large	2	8
m5n.xlarge	4	16
m5n.2xlarge	8	32
m5n.4xlarge	16	64
m5n.8xlarge	32	128
m5n.12xlarge	48	192

实例类型	默认 vCPU	内存 (GiB)
m5n.16xlarge	64	256
m5n.24xlarge	96	384
t2.nano	1	0.5
t2.micro	1	1
t2.small	1	2
t2.medium	2	4
t2.large	2	8
t2.xlarge	4	16
t2.2xlarge	8	32
t3.nano	2	0.5
t3.micro	2	1
t3.small	2	2
t3.medium	2	4
t3.large	2	8
t3.xlarge	4	16
t3.2xlarge	8	32
t3a.nano	2	0.5
t3a.micro	2	1
t3a.small	2	2
t3a.medium	2	4
t3a.large	2	8
t3a.xlarge	4	16
t3a.2xlarge	8	32

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 实例类型](#)。

有关指定 CPU 选项的更多信息，请参阅 [优化 CPU 选项 \(p. 480\)](#)。

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。有些通用型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅 [Amazon EBS 优化的实例 \(p. 863\)](#)。

一些通用型实例类型提供了在 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 \(p. 471\)](#)。

网络性能

您可以对受支持的实例类型启用增强联网功能。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 \(p. 616\)](#)。

使用 Elastic Network Adapter (ENA) 来增强网络的实例类型提供较高的每秒数据包数性能，并始终保持较低的延迟。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。使用 ENA 并且使用“最高 10 Gbps”或“最高 25 Gbps”的网络性能记录的实例大小使用一种网络 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。实例在网络带宽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。

以下是支持增强联网的通用型实例的网络性能摘要。

实例类型	网络性能	增强联网
t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge	最高 1 Gbps	
t3.nano t3.micro t3.small t3.medium t3.large t3.xlarge t3.2xlarge t3a.nano t3a.micro t3a.small t3a.medium t3a.large t3a.xlarge t3a.2xlarge	最高 5 Gbps	ENa (p. 617)
m4.large	中	Intel 82599 VF (p. 628)
m4.xlarge m4.2xlarge m4.4xlarge	高	Intel 82599 VF (p. 628)
a1.medium a1.large a1.xlarge a1.2xlarge a1.4xlarge m5.large m5.xlarge m5.2xlarge m5.4xlarge m5a.large m5a.xlarge m5a.2xlarge m5a.4xlarge m5a.8xlarge m5ad.large m5ad.xlarge m5ad.2xlarge m5ad.4xlarge m5ad.8xlarge m5d.large m5d.xlarge m5d.2xlarge m5d.4xlarge	最高 10 Gbps	ENa (p. 617)
m4.10xlarge	10Gbps	Intel 82599 VF (p. 628)
m5.8xlarge m5.12xlarge m5a.12xlarge m5ad.12xlarge m5d.8xlarge m5d.12xlarge	10 Gbps	ENa (p. 617)
m5a.16xlarge m5ad.16xlarge	12 Gbps	ENa (p. 617)

实例类型	网络性能	增强联网
m5.16xlarge m5a.24xlarge m5ad.24xlarge m5d.16xlarge	20 Gbps	ENI (p. 617)
m5dn.4xlarge 及更小 m5n.4xlarge 及更小	最高 25 Gbps	ENI (p. 617)
m4.16xlarge m5.24xlarge m5.metal m5d.24xlarge m5d.metal m5dn.8xlarge m5n.8xlarge	25 Gbps	ENI (p. 617)
m5dn.12xlarge m5n.12xlarge	50 Gbps	ENI (p. 617)
m5dn.16xlarge m5n.16xlarge	75 Gbps	ENI (p. 617)
m5dn.24xlarge m5n.24xlarge	100 Gbps	ENI (p. 617)

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，则您可以获得下表所列的 IOPS (4096 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	写入 IOPS
m5ad.large *	30000	15000
m5ad.xlarge *	59,000	29,000
m5ad.2xlarge *	117,000	57,000
m5ad.4xlarge *	234,000	114,000
m5ad.8xlarge	466666	233333
m5ad.12xlarge	700,000	340,000
m5ad.16xlarge	933333	466666
m5ad.24xlarge	1400000	680,000
m5d.large *	30000	15000
m5d.xlarge *	59,000	29,000
m5d.2xlarge *	117,000	57,000
m5d.4xlarge *	234,000	114,000
m5d.8xlarge	466666	233333
m5d.12xlarge	700,000	340,000

实例大小	100% 随机读取 IOPS	写入 IOPS
m5d.16xlarge	933333	466666
m5d.24xlarge	1400000	680,000
m5d.metal	1400000	680,000
m5dn.large *	30000	15000
m5dn.xlarge *	59,000	29,000
m5dn.2xlarge *	117,000	57,000
m5dn.4xlarge *	234,000	114,000
m5dn.8xlarge	466666	233333
m5dn.12xlarge	700,000	340,000
m5dn.16xlarge	933333	466666
m5dn.24xlarge	1400000	680,000

* 对于这些实例，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保留空白间。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。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 \(p. 913\)](#)。

实例功能

通用型实例的功能汇总如下：

	仅限于 EBS	NVMe EBS	实例存储	置放群组
A1	是	是	否	是
M4	是	否	否	是
M5	是	是	否	是
M5a	是	是	否	是
M5ad	否	是	NVMe *	是
M5d	否	是	NVMe *	是

	仅限于 EBS	NVMe EBS	实例存储	置放群组
M5dn	否	是	NVMe *	是
M5n	是	是	否	是
T2	是	否	否	否
T3	是	是	否	否
T3a	是	是	否	否

* 根设备卷必须是 Amazon EBS 卷。

有关更多信息，请参阅下列内容：

- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [置放群组 \(p. 662\)](#)

发行说明

- M5、M5d 和 T3 实例配备 3.1 GHz Intel Xeon Platinum 8000 系列处理器。
- M5a、M5ad 和 T3a 实例配备了 2.5 GHz AMD EPYC 7000 系列处理器。
- A1 实例配备基于 64 位 Arm 架构的 2.3 GHz AWS Graviton 处理器。
- M4、M5、M5a、M5ad、M5d、t2.large 和更大、t3.large 和更大以及 t3a.large 和更大实例类型需要使用 64 位 HVM AMIs。它们具有高内存，需要 64 位操作系统才能利用这一容量。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。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- A1 实例具有以下要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。
 - 必须使用适用于 64 位 Arm 架构的 AMI。
 - 必须支持通过带有 ACPI 表的 UEFI 进行引导，以及支持 ACPI 热插拔 PCI 设备。

以下 AMI 满足这些要求：

- Amazon Linux 2 (64 位 ARM)
- Ubuntu 16.04 或更高版本 (64 位 Arm)
- Red Hat Enterprise Linux 7.6 或更高版本 (64 位 Arm)
- SUSE Linux Enterprise Server 15 或更高版本 (64 位 Arm)
- M5、M5a、M5ad、M5d、M5dn、M5n、T3 和 T3a 实例具有以下要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。

以下 AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 linux-aws 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本

- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本
- A1、M5、M5a、M5ad、M5d、M5dn、M5n、T3 和 T3a 实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。每个实例至少附加 1 个网络接口。例如，如果在仅限 EBS 的实例上没有附加其他网络接口，您可以附加 27 个 EBS 卷到该实例。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- A1、M5、M5a、M5ad、M5d、M5dn、M5n、T3 和 T3a 实例应登录到系统或安装了 acpid，以支持通过 API 请求执行完全关闭。
- 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 实例请求表](#)。

可突增性能实例

可突增性能实例（包括 T3、T3a 和 T2 实例）旨在提供基准水平的 CPU 性能，并且能够在您的工作负载需要时突增到更高的水平。可突增性能实例非常适合用于各种通用应用程序。示例包括微服务、低延迟交互式应用程序、中小型数据库、虚拟桌面、开发、构建和暂存环境、代码存储库以及产品原型。

可突增性能实例是唯一将积分用于 CPU 使用的实例类型。有关实例定价的更多信息以及其他硬件详细信息，请参阅[Amazon EC2 定价](#)和[Amazon EC2 实例类型](#)。

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](#)。

目录

- [可突增性能实例要求 \(p. 175\)](#)
- [最佳实践 \(p. 176\)](#)
- [可突增性能实例的 CPU 积分和基准性能 \(p. 176\)](#)
- [可突增性能实例的无限模式 \(p. 178\)](#)
- [可突增性能实例的标准模式 \(p. 185\)](#)
- [使用可突增性能实例 \(p. 195\)](#)
- [监控 CPU 积分 \(p. 199\)](#)

可突增性能实例要求

以下是这些实例的要求：

- 这些实例可以作为按需实例、预留实例和 Spot 实例，但不能用作计划实例或专用实例。它们在专用主机上也不受支持。有关更多信息，请参阅[实例购买选项 \(p. 239\)](#)。
- 确保您选择的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。随着您的工作负载对内存和 CPU 的需求随时间增加，您可以扩展到相同实例类型或其他实例类型的更大实例大小。

- 有关其他要求，请参阅[通用型实例发行说明 \(p. 174\)](#)。

最佳实践

按照这些最佳实践可以从可突增性能实例获得最大的好处。

- 使用推荐的 AMI – 使用提供所需驱动程序的 AMI。有关更多信息，请参阅[发行说明 \(p. 174\)](#)。
- 启用实例恢复 – 创建一个 CloudWatch 警报，监控 EC2 实例并在实例由于任何原因而受损时自动恢复实例。有关更多信息，请参阅[向 Amazon CloudWatch 警报添加恢复操作 \(p. 558\)](#)。

可突增性能实例的 CPU 积分和基准性能

传统 Amazon EC2 实例类型提供固定的性能，而可突增性能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。一个 CPU 积分提供一个完整 CPU 核心在一分钟内的性能。

目录

- [CPU 积分 \(p. 176\)](#)
- [基准性能 \(p. 178\)](#)

CPU 积分

一个 CPU 积分等于一个 vCPU 按 100% 使用率运行一分钟。vCPU 数、使用率和时间的其他组合也可以等于一个 CPU 积分。例如，一个 CPU 积分等于一个 vCPU 按 50% 使用率运行两分钟，或者两个 vCPU 按 25% 使用率运行两分钟。

获得 CPU 积分

每个可突增性能实例以设定的每小时速率（以毫秒级精度）持续获得 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量 CPU 积分。

如果可突增性能实例使用的 CPU 资源少于基准性能所需的数量（例如，处于空闲状态时），则未使用的 CPU 积分将累积到 CPU 积分余额中。如果可突增性能实例需要突增至基准性能水平以上，它将花费累积积分。可突增性能实例累积的积分越多，在需要更高性能时，它突增到基准以上的时间就越长。

下表列出了可突增性能实例类型、每小时获得 CPU 积分的速率、实例可以累积获得的最大 CPU 积分数、每个实例的 vCPU 数以及以完整核心性能百分比形式表示的基准性能水平（使用单个 vCPU）。

实例类型	每小时获得的 CPU 积分	可累积获得的最大积分数*	vCPU	每个 vCPU 的基准性能
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22.5%**
t2.2xlarge	81.6	1958.4	8	17%**
t3.nano	6	144	2	5%**

实例类型	每小时获得的 CPU 积分	可累积获得的最大积分数*	vCPU	每个 vCPU 的基准性能
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**

* 可累积的积分数等于可在 24 小时周期内获得的积分数。

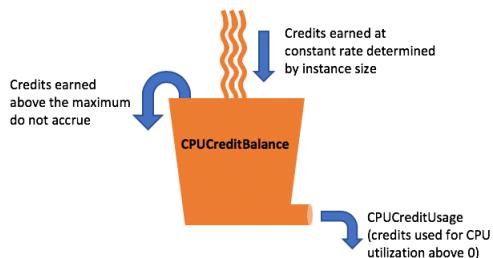
** 下表列出了每个 vCPU 的基准性能。对于具有多个 vCPU 的实例大小，要计算实例的基准 CPU 使用率，请将 vCPU 百分比乘以 vCPU 数。例如，t3.large 实例有两个 vCPU，它们为实例提供 60% 的基准 CPU 利用率 (2 个 vCPU x 每 vCPU 30% 的基准性能)。在 CloudWatch 中，CPU 使用率按各个 vCPU 显示。因此，以基准性能运行的 t3.large 实例的 CPU 使用率在 CloudWatch CPU 指标中显示为 30%。

CPU 积分获得率

每小时获得的 CPU 积分数是由实例大小决定的。例如，t3.nano 每小时获得 6 个积分，而 t3.small 每小时获得 24 个积分。上表列出了所有实例的积分获得率。

CPU 积分累积限制

虽然获得的积分在运行的实例上从不过期，但实例可累积获得的积分数存在限制。该限制由 CPU 积分余额限制决定。在到达限制后，获得的任何新积分都会被丢弃，如下图所示。存储桶已满表示达到 CPU 积分余额限制，而溢出指示超出限制的新获得积分。



对于每种 实例大小，CPU 积分余额限制是不同的。例如，`t3.micro` 实例可在 CPU 积分余额中累积最多 288 个获得的 CPU 积分。上表列出了每个 实例可以累积获得的最大积分数。

Note

`T2` 标准实例也获得启动积分。启动积分不计入 CPU 积分余额限制。如果 `T2` 实例尚未使用其启动积分，并保持闲置状态 24 小时，同时累积获得的积分，则其 CPU 积分余额将超过限制。有关更多信息，请参阅 [启动积分 \(p. 185\)](#)。

`T3` 和 `T3a` 实例不会获得启动积分。默认情况下，这些实例以 `unlimited` 模式启动，因此可以在启动时立即突增，无需任何启动积分。

累积的 CPU 积分生命期

运行的实例上的 CPU 积分不会过期。

对于 `T3` 和 `T3a`，CPU 积分余额在实例停止后保留七天，然后，积分将会丢失。如果在七天内启动实例，则不会丢失积分。

对于 `T2`，CPU 积分余额在实例停止与启动之间不保留。如果您停止 `T2` 实例，实例将失去其所有累积积分。

有关更多信息，请参阅 [CloudWatch 指标表 \(p. 200\)](#) 中的 `CPUCreditBalance`。

基准性能

一个实例每小时获得的积分数可以使用 CPU 使用率的百分比形式表示。这称为基准性能，有时干脆称为基准。例如，具有两个 vCPU 的 `t3.nano` 实例每小时获得 6 个积分，因而每个 vCPU 的基准性能为 5% (3/60 分钟)。具有四个 vCPU 的 `t3.xlarge` 实例每小时获得 96 个积分，因而每个 vCPU 的基准性能为 40% (24/60 分钟)。

可突增性能实例的无限模式

配置为 `unlimited` 的可突增性能实例可以承受所需的任何时段的高 CPU 性能。如果在滚动 24 小时或实例生命周期（以较短者为准）内实例的平均 CPU 使用率等于或低于基准，实例的每小时价格自动涵盖所有 CPU 使用峰值。

对于绝大多数通用型工作负载，配置为 `unlimited` 的实例可提供足够高的性能，而不会收取任何额外的费用。如果实例长时间以较高的 CPU 使用率运行，可能会按每 vCPU 小时的 [固定费率](#) 收取额外的费用。有关实例定价的信息，请参阅 [Amazon EC2 定价](#) 以及 [Amazon EC2 按需定价](#) 中的“无限定价”部分。

Important

如果您使用的 `t2.micro` 实例享受 [AWS 免费套餐](#) 优惠并将其配置为 `unlimited`，在滚动 24 小时内的平均使用率超过实例基准时，可能会收取相应的费用。

目录

- [无限模式概念 \(p. 178\)](#)
- [示例：无限模式 \(p. 182\)](#)

无限模式概念

`unlimited` 是用于可突增性能实例的积分数配置选项。可以随时对正在运行或已停止的实例启用或禁用它。您可以在每个 AWS 区域的账户级别将 `unlimited` 设置为每个可突增性能实例系列的默认积分选项，以便账户中所有新的可突增性能实例都使用默认积分选项启动。

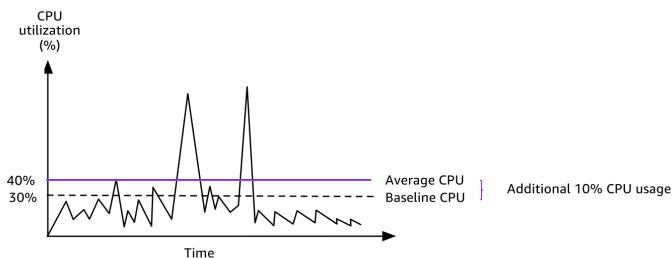
Note

默认情况下，`T3` 和 `T3a` 实例以 `unlimited` 模式启动。默认情况下，`T2` 实例作为 `standard` 启动。您可以在每个 AWS 区域的账户级别更改默认值。有关更多信息，请参阅 [设置账户的默认积分规范 \(p. 199\)](#)。

无限可突增性能实例的工作原理

如果配置为 `unlimited` 的可突增性能实例用完其 CPU 积分余额，它可能会花费超额积分以突增到基准以上。在该实例的 CPU 使用率低于基准时，实例会使用它获得的 CPU 积分支付以前花费的超额积分。凭借获得 CPU 积分来支付超额积分的能力，Amazon EC2 可以在 24 小时周期内将实例的 CPU 使用率保持在平均水平。如果 24 小时的平均 CPU 使用率超过基准，则会按每 vCPU 小时的 **固定费率** 对实例收取额外的使用费用。

下图显示 `t3.large` 的 CPU 使用率。`t3.large` 的基准 CPU 使用率为 30%。如果实例在 24 小时内以平均 30% CPU 使用率或更低运行，则没有额外费用，因为费用已由实例每小时价格所涵盖。但是，如果实例在 24 小时内以平均 40% CPU 使用率运行，如图中所示，则会按每 vCPU 小时的 **固定费率** 对实例收取额外的 10% CPU 使用率费用。



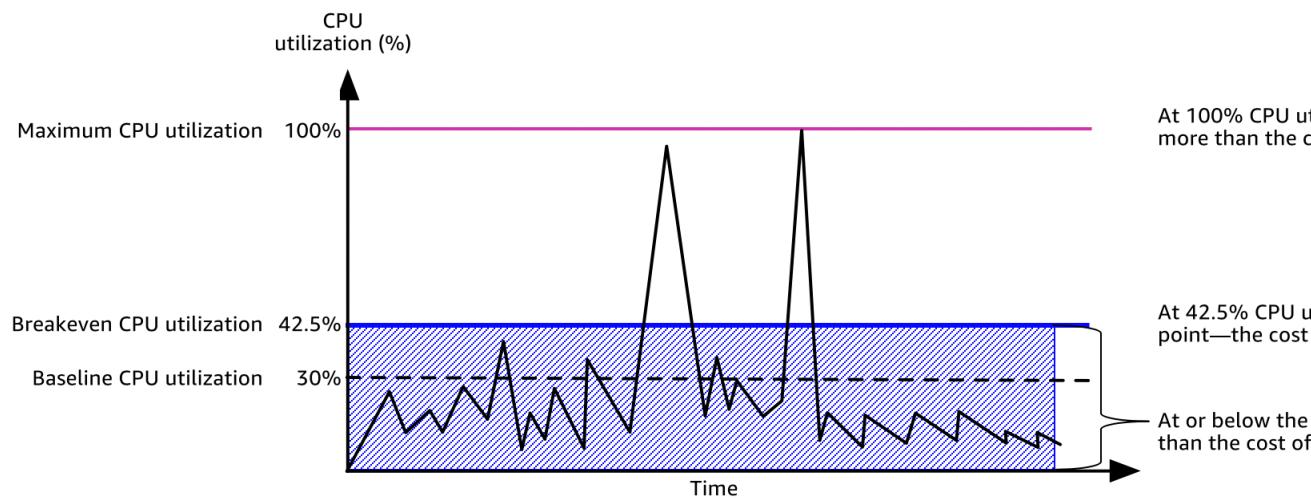
有关每个实例类型的每个 vCPU 的基准性能以及每个实例类型可获得的积分数的更多信息，请参阅 [积分表 \(p. 176\)](#)。

何时使用无限模式与固定 CPU

当确定您在 `unlimited` 模式下是否应使用可突增性能实例（如 T3）或固定性能实例（如 M5）时，您需要确定收支平衡 CPU 使用率。可突增性能实例的收支平衡 CPU 使用率是可突增性能实例与固定性能实例的费用相同的点。收支平衡 CPU 使用率可帮助您确定以下内容：

- 如果 24 小时内的平均 CPU 使用率等于或低于收支平衡 CPU 使用率，请在 `unlimited` 模式下使用可突增性能实例，以便您可以受益于可突增性能实例的较低价格，同时获得与固定性能实例相同的性能。
- 如果 24 小时内的平均 CPU 使用率高于收支平衡 CPU 使用率，可突增性能实例将花费比同等大小的固定性能实例更多的费用。如果 T3 实例以 100% CPU 持续突增，则您最终要支付的价格约为同等大小 M5 实例的价格的 1.5 倍。

下图显示了其中 `t3.large` 花费与 `m5.large` 花费相同的收支平衡 CPU 使用率点。`t3.large` 的收支平衡 CPU 使用率点为 42.5%。如果平均 CPU 使用率为 42.5%，则运行 `t3.large` 的费用与 `m5.large` 的运行费用相同，如果平均 CPU 使用率高于 42.5%，则前者费用更高。如果工作负载需要低于 42.5% 的平均 CPU 使用率，您可以受益于 `t3.large` 的较低价格，同时获得与 `m5.large` 相同的性能。



下表显示了如何计算收支平衡的 CPU 使用率阈值，以便您可以确定何时使用 `unlimited` 模式的可突增性能实例或固定性能实例将更为便宜。表中的列标记为 A 到 K。

实例类型	vCPU	T3 价格*/小时	M5 价格*/小时	价格差异	每个 vCPU 的 T3 基准性能 (%)	向超额积分每 vCPU 小时收取费用	每 vCPU 分钟收费	每 vCPU 可用的额外突增分钟数	可用的额外 CPU %	收支平衡 CPU %
A	B ,	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0.0835 美元	0.096 美元	0.0125 USD	30%	\$0.05	0.000833 美元	15	12.5%	42.5%

* 价格基于 us-east-1 和 Linux OS。

该表提供以下信息：

- 列 A 显示实例类型 `t3.large`。
- 列 B 显示 `t3.large` 的 vCPU 数。
- 列 C 显示每小时 `t3.large` 的价格。
- 列 D 显示每小时 `m5.large` 的价格。
- 列 E 显示 `t3.large` 和 `m5.large` 之间的价格差异。
- 列 F 显示 `t3.large` 的每个 vCPU 的基准性能（即为 30%）。在基准时，实例的每小时成本涵盖 CPU 使用率的成本。
- 列 G 显示向实例收取的额外每 vCPU 小时的固定费率（如果实例在耗尽其获得的积分后以 100% CPU 突增）。
- 列 H 显示向实例收取的额外每 vCPU 分钟的固定费率（如果实例在耗尽其获得的积分后以 100% CPU 突增）。

- 列 I 显示 t3.large 可每小时以 100% CPU 突增的同时支付与 m5.large 相同的每小时价格的额外分钟数。
- 列 J 显示该实例可突增的同时支付与 m5.large 相同的每小时价格的超过基准的额外 CPU 使用率 (单位为 %)。
- 列 K 显示 t3.large 在支付不超过 m5.large 的费用的情况下可突增的收支平衡 CPU 使用率 (单位为 %)。除此之外 , t3.large 的费用超过 m5.large。

下表显示了与类似大小的 M5 实例类型相比 T3 实例类型的收支平衡 CPU 使用率 (单位为 %)。

T3 实例类型	T3 的收支平衡 CPU 使用率 (单位为 %) (与 M5 相比)
t3.large	42.5%
t3.xlarge	52.5%
t3.2xlarge	52.5%

超额积分会产生费用

如果实例的平均 CPU 使用率等于或低于基准，则实例不会产生额外的费用。由于实例在 24 小时周期内可获得 [最大数量的积分 \(p. 176\)](#) (例如 , t3.micro 实例可在 24 小时周期内获得最多 288 个积分) 的原因，因此在花费的超额积分不超过最大积分数时，不会立即向您收费。

但是，如果 CPU 利用率保持在基准以上，则实例无法获得足够的积分来支付已花费的超额积分。对于未支付的超额积分，按每 vCPU 小时的固定费率收取额外的费用。

在出现以下任一情况时，将对之前花费的超额积分收费：

- 花费的超额积分超出实例可在 24 小时周期内获得的 [最大积分数 \(p. 176\)](#)。对于超出最大积分数的所花费超额积分，将在该小时结束时向您收费。
- 实例已停止或终止。
- 实例从 `unlimited` 切换为 `standard`。

花费的超额积分是通过 CloudWatch 指标 `CPUSurplusCreditBalance` 跟踪的。通过 CloudWatch 指标 `CPUSurplusCreditsCharged` 来跟踪收费的超额积分。有关更多信息，请参阅[可突增性能实例的其他 CloudWatch 指标 \(p. 199\)](#)。

T2 无限没有启动积分

T2 标准实例可收到[启动积分 \(p. 185\)](#)，但 T2 无限实例不会收到启动积分。T2 无限实例可以随时突增到基准以上，而不会收取额外的费用，但前提是在滚动 24 小时时间段或其生命周期 (以较短者为准) 内实例的平均 CPU 使用率等于或低于基准。因此，T2 无限实例不需要启动积分，即可在启动后立即达到较高的性能。

如果 T2 实例从 `standard` 切换到 `unlimited`，则将从 `CPUCreditBalance` 中扣除所有累积的启动积分，然后再结转剩余的 `CPUCreditBalance`。

Note

T3 和 T3a 实例从来不会收到启动积分。

启用无限模式

默认情况下，T3 和 T3a 实例以 `unlimited` 模式启动。T2 实例默认情况下以 `standard` 模式启动，但您可在启动时启用 `unlimited`。

您可以随时在正在运行或停止的实例上从 `unlimited` 切换到 `standard` 以及从 `standard` 切换到 `unlimited`。有关更多信息，请参阅 [以“无限”或“标准”模式启动可突增性能实例 \(p. 196\)](#) 和 [修改可突增性能实例的积分规范 \(p. 198\)](#)。

您可以在每个 AWS 区域的账户级别将 `unlimited` 设置为每个可突增性能实例系列的默认积分选项，以便账户中所有新的可突增性能实例都使用默认积分选项启动。有关更多信息，请参阅[设置账户的默认积分规范 \(p. 199\)](#)。

您可以使用 Amazon EC2 控制台或 AWS CLI，检查可突增性能实例已配置为 `unlimited` 还是 `standard`。有关更多信息，请参阅 [查看可突增性能实例的积分规范 \(p. 197\)](#) 和 [查看默认积分规范 \(p. 199\)](#)。

在无限模式和标准模式之间切换时，积分会出现什么情况

`CPUCreditBalance` 是跟踪实例产生的积分数的 CloudWatch 指标。`CPUSurplusCreditBalance` 是跟踪实例所用超额积分数的 CloudWatch 指标。

当您将配置为 `unlimited` 的实例更改为 `standard` 时，会出现以下情况：

- `CPUCreditBalance` 值保持不变并进行结转。
- 立即针对 `CPUSurplusCreditBalance` 值进行收费。

在 `standard` 实例切换到 `unlimited` 时，会出现以下情况：

- 将结转包含已累积获得的积分的 `CPUCreditBalance` 值。
- 对于 T2 标准实例，将从 `CPUCreditBalance` 值中扣除所有启动积分，并且将结转包含已累积获得的积分的剩余 `CPUCreditBalance` 值。

监控积分使用情况

要了解您实例花费的积分是否超过基准提供的积分，您可以使用 CloudWatch 指标来跟踪使用情况，并且可以设置小时警报，以便获得积分使用情况通知。有关更多信息，请参阅[监控 CPU 积分 \(p. 199\)](#)。

示例：无限模式

以下示例介绍当实例配置为 `unlimited` 时的积分使用情况。

示例

- [示例 1：介绍 T3 无限的积分使用情况 \(p. 182\)](#)
- [示例 2：介绍 T2 无限的积分使用情况 \(p. 183\)](#)

示例 1：介绍 T3 无限的积分使用情况

在此示例中，您可以查看作为 `unlimited` 启动的 `t3.nano` 实例的 CPU 利用率，以及它如何花费获得的积分和超额积分来保持 CPU 性能。

`t3.nano` 实例在 24 小时滚动周期内获得 144 个 CPU 积分，这些积分可兑换 144 分钟 vCPU 使用时间。在实例用完 CPU 积分余额（由 CloudWatch 指标 `CPUCreditBalance` 表示）时，它会花费超额 CPU 积分—（尚未获得的积分）—以突增所需的时间。由于 `t3.nano` 实例在 24 小时周期内最多可获得 144 个积分，因此，在花费的超额积分不超过该最大积分数时，不会立即向您收费。如果花费 144 个以上的 CPU 积分，则会在该小时结束时对超出的部分进行收费。

下图所示的示例旨在说明实例如何使用超额积分突增到基准以上，甚至在用完 `CPUCreditBalance` 后。以下工作流程引用图中的编号数据点：

P1 – 在图表中的 0 小时处，实例以 `unlimited` 模式启动并立即开始获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%），不使用任何积分。所有未使用的积分都累积到积分余额中。对于前 24 小时，`CPUCreditUsage` 为 0，而 `CPUCreditBalance` 值达到其最大值 144。

P2 – 对于接下来的 12 小时，CPU 利用率为 2.5%，这低于 5% 基准。实例获得的积分多于花费的积分，但 `CPUCreditBalance` 值不能超过其最大值 144 个积分。

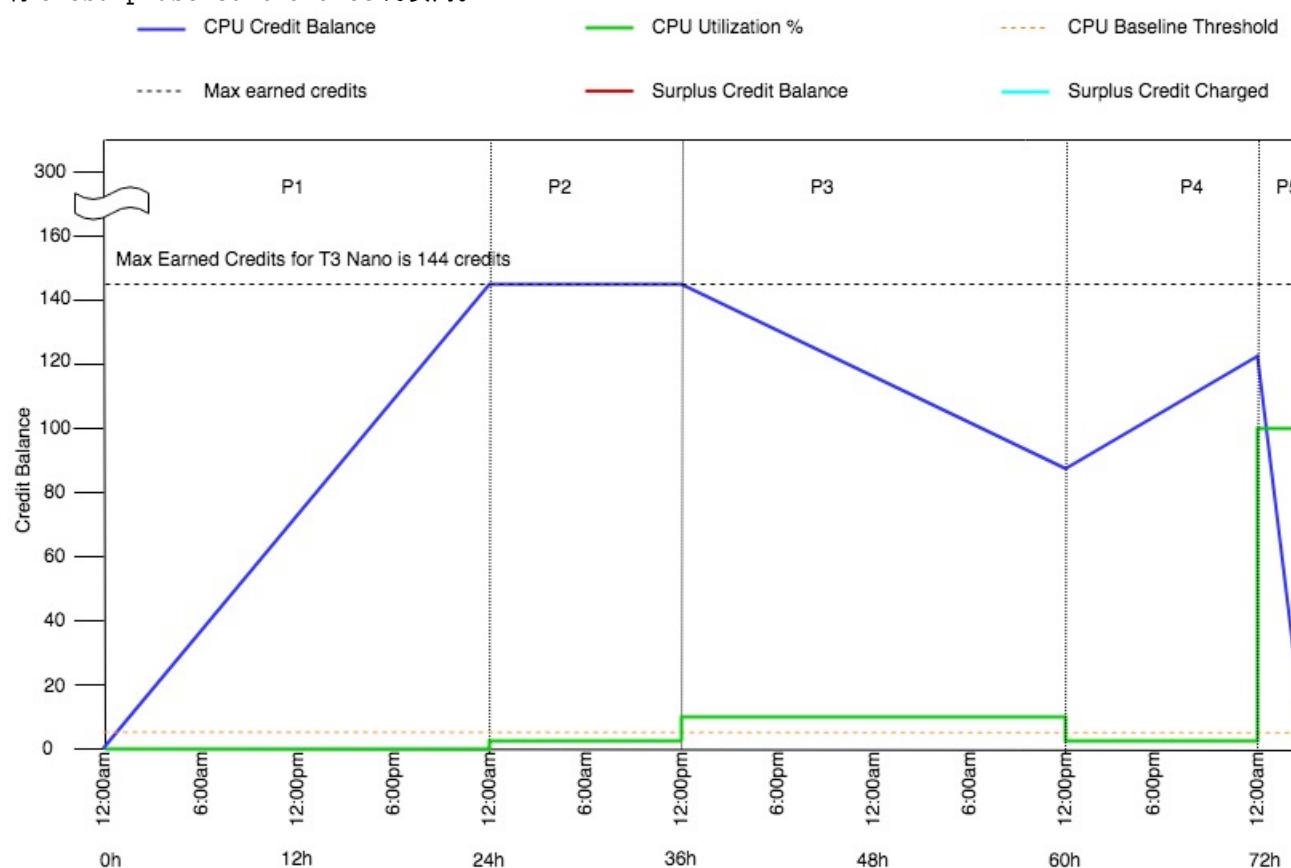
P3 – 对于接下来的 24 小时，CPU 利用率为 7%（高于基准），这要求花费 57.6 个积分。实例花费的积分多于获得的积分，`CPUCreditBalance` 值降至 86.4 个积分。

P4 – 对于接下来的 12 小时，CPU 利用率降至 2.5%（低于基准），这要求花费 36 个积分。同时，实例获得 72 个积分。实例获得的积分多于花费的积分，`CPUCreditBalance` 值增至 122 个积分。

P5 – 对于接下来的 5 小时，实例突增至 100% CPU 利用率，并花费总计 570 个积分来持续突增。在进入此期间的大约一小时内，此实例用完其整个 `CPUCreditBalance` 122 个积分，并开始花费超额积分来维持高的 CPU 性能，在此期间总共花费 448 个超额积分 ($570-122=448$)。当 `CPUSurplusCreditBalance` 值达到 144 个 CPU 积分 (`t3.nano` 实例在 24 小时内可获得的最大值) 时，之后任何花费的超额积分都无法由获得的积分抵消。之后花费的超额积分总计为 304 个积分 ($448-144=304$)，这会导致这一小时结束后对于这 304 个积分收取很小的一笔附加费。

P6 – 对于接下来的 13 小时，CPU 利用率为 5%（基准）。实例获得的积分与花费的积分一样多，而无需额外支付 `CPUSurplusCreditBalance` 的费用。`CPUSurplusCreditBalance` 值保持为 144 个积分。

P7 – 对于本例中的最后 24 小时，实例空闲，CPU 利用率为 0%。在此期间，实例获得 144 个积分，用于支付 `CPUSurplusCreditBalance` 的费用。



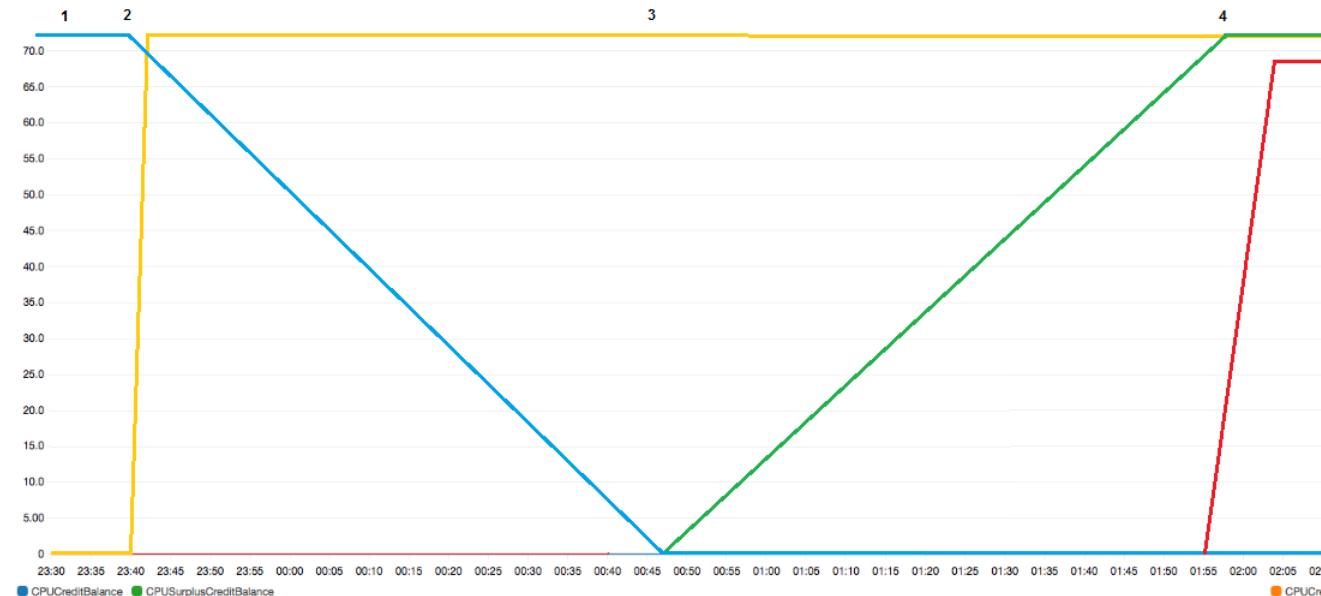
示例 2：介绍 T2 无限的积分使用情况

在此示例中，您可以查看作为 `unlimited` 启动的 `t2.nano` 实例的 CPU 利用率，以及它如何花费获得的积分和超额积分来保持 CPU 性能。

`t2.nano` 实例在 24 小时滚动周期内获得 72 个 CPU 积分，这些积分可兑换 72 分钟 vCPU 使用时间。在实例用完 CPU 积分余额（由 CloudWatch 指标 `CPUCreditBalance` 表示）时，它会花费超额 CPU 积分—（尚未获得的积分）—以突增所需的时间。由于 `t2.nano` 实例在 24 小时周期内最多可获得 72 个积分，因此，在花费的超额积分不超过该最大积分数时，不会立即向您收费。如果花费 72 个以上的 CPU 积分，则会在该小时结束时对超出的部分进行收费。

下图所示的示例旨在说明实例如何使用超额积分突增到基准以上，甚至在用完 `CPUCreditBalance` 后。您可以假定，在图表的时间线开始时，实例累积的积分余额等于它可在 24 小时内获得的最大积分数。以下工作流程引用图中的编号数据点：

- 1 – 在前 10 分钟内，`CPUCreditUsage` 设置为 0 并且 `CPUCreditBalance` 值始终为最大值 72。
- 2 – 在 23:40，随着 CPU 使用率增加，实例花费 CPU 积分并且 `CPUCreditBalance` 值减少。
- 3 – 在大约 00:47，实例用完全部 `CPUCreditBalance`，并开始花费超额积分以保持较高的 CPU 性能。
- 4 – 一直花费超额积分，直到 1:55，此时 `CPUSurplusCreditBalance` 值达到 72 个 CPU 积分。这等于 `t2.nano` 实例在 24 小时周期内可获得的最大积分数。以后花费的任何超额积分无法由 24 小时周期内获得的积分抵消，这会导致在该小时结束时收取少量的额外费用。
- 5 – 在大约 2:20，实例继续花费超额积分。此时，CPU 使用率低于基准并且实例开始获得积分，每小时 3 个积分（或每 5 分钟 0.25 个积分），它使用这些积分来支付 `CPUSurplusCreditBalance`。在 `CPUSurplusCreditBalance` 值减少到 0 后，实例开始在其 `CPUCreditBalance` 中累积获得积分（每 5 分钟 0.25 个积分）。



All metrics Graphed metrics (4) Graph options

Label	Details	Statistic	Period
CPUCreditBalance	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUCreditBalance	Maximum	5 Minutes
CPUCreditUsage	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUCreditUsage	Maximum	5 Minutes
CPUSurplusCreditBalance	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUSurplusCreditBalance	Maximum	5 Minutes
CPUSurplusCreditsCharged	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUSurplusCreditsCharged	Maximum	5 Minutes

计算账单

超额积分每 vCPU 小时收取 0.05 美元。在 1:55 和 2:20 之间，实例大约花费 25 个超额积分，这相当于 0.42 个 vCPU 小时。

该实例产生的额外费用为 $0.42 \text{ vCPU 小时} \times 0.05 \text{ 美元/vCPU 小时} = 0.021 \text{ 美元}$ ，舍入到 0.02 美元。

下面是该 T2 无限实例的月末账单：

Amazon Elastic Compute Cloud running Linux/UNIX	\$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	\$4.18
Amazon Elastic Compute Cloud T2 CPU Credits			
\$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	\$0.02	

您可以设置账单提醒以每小时通知一次产生的任何费用，并在必要时采取相应的措施。

可突增性能实例的标准模式

配置为 `standard` 的可突增性能实例适用于具有平均 CPU 利用率的工作负载，它始终低于实例的基准性能。为了突增到基准以上，实例会花费在其 CPU 积分余额中累积的积分。如果实例累积的积分较少，性能将逐渐下降到基准性能水平，因此，在累积的 CPU 积分余额用完时，实例的性能不会急剧下降。有关更多信息，请参阅 [可突增性能实例的 CPU 积分和基准性能 \(p. 176\)](#)。

目录

- [标准模式概念 \(p. 185\)](#)
- [示例：标准模式 \(p. 187\)](#)

标准模式概念

`standard` 是用于可突增性能实例的配置选项。可以随时对正在运行或已停止的实例启用或禁用它。您可以在每个 AWS 区域的账户级别将 `standard` 设置为每个可突增性能实例系列的默认积分选项，以便账户中所有新的可突增性能实例都使用默认积分选项启动。

Note

默认情况下，T3 和 T3a 实例以 `unlimited` 模式启动。默认情况下，T2 实例作为 `standard` 启动。您可以在每个 AWS 区域的账户级别更改默认值。有关更多信息，请参阅 [设置账户的默认积分规范 \(p. 199\)](#)。

标准可突增性能实例的工作原理

当配置为 `standard` 的可突增性能实例处于运行状态时，它会以设定的每小时速率（以毫秒级精度）持续获得积分。对于 T2 标准模式，在实例停止后，会丢失累积的全部积分，积分余额会重置为零。在它重新启动后，会接受一组新的启动积分，并开始累积获得积分。对于 T3 和 T3a 标准模式，CPU 积分余额在实例停止后保留七天，然后，积分将会丢失。如果在七天内启动实例，则不会丢失积分。

T2 标准实例接收两种类型的 CPU 积分：获得的积分以及启动积分。在 T2 标准实例处于运行状态时，它会以固定的每小时速率（以毫秒级精度）持续获得积分。在一开始，该实例尚未获得积分来提供良好的初始体验；因此为了提供良好的初始体验，一开始会收到启动积分，可以先花费，同时累积获得积分。

T3 和 T3a 标准实例不会收到启动积分。

启动积分

在启动时，T2 标准实例的每个 vCPU 获得 30 个启动积分。例如，`t2.micro` 实例具有一个 vCPU 并获得 30 个启动积分，而 `t2.xlarge` 实例具有 4 个 vCPU 并获得 120 个启动积分。启动积分旨在提供良好的初始体验，以使实例能够在启动后（没有累积获得积分之前）立即突增到更高的性能。

首先花费启动积分，再使用获得的积分。未花费的启动积分将累积到 CPU 积分余额中，但不会计入 CPU 积分余额限制。例如，`t2.micro` 实例的 CPU 积分余额限制为 144 个获得的积分。如果实例启动并保持空闲状态 24 小时，其 CPU 积分余额将达到 174（30 个启动积分 + 144 个获得的积分），这已超过限制。不过，在实例花费 30 个启动积分后，积分余额就不能超过 144 个。有关每种实例大小的 CPU 积分余额限制的更多信息，请参阅 [积分表 \(p. 176\)](#)。

下表列出了在启动时分配的初始 CPU 积分以及 vCPU 数。

实例类型	启动积分	vCPU
t1.micro	15	1
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

启动积分限制

T2 标准实例接收启动积分的次数存在限制。在每个区域，每 24 个小时的滚动周期内，每个账户中所有 T2 标准实例组合的默认限制是 100 次启动。例如，当一个实例在 24 小时周期内停止并启动 100 次时，或当 100 个实例在 24 小时周期内启动时，或者其他组合等同于 100 次启动时，将达到此限制。新账户可能具有较低的限制，该限制随着时间根据您的使用情况而增加。

Tip

要确保您的工作负载始终获得所需的性能，请切换到[可突增性能实例的无限模式 \(p. 178\)](#)或考虑使用更大的实例。

启动积分和获得的积分之间的区别

下表列出了启动积分和获得的积分之间的区别。

	启动积分	获得的积分
积分获得率	在启动时，T2 标准实例的每个 vCPU 获得 30 个启动积分。 如果 T2 实例从 <code>unlimited</code> 切换到 <code>standard</code> ，则在切换时不会获得启动积分。	每个 T2 实例以固定的每小时速率（以毫秒级精度）持续获得 CPU 积分，具体取决于实例大小。有关每种实例大小获得的 CPU 积分数量的更多信息，请参阅 积分表 (p. 176) 。
积分获得限制	对于每个区域，在每 24 个小时的滚动周期内，每个账户中所有 T2 标准实例组合的启动积分接收限制是 100 次启动。新账户可能具有较低的限制，该限制随着时间根据您的使用情况而增加。	T2 实例累积的积分数不能超过 CPU 积分余额限制。如果 CPU 积分余额已达到其限制，则将丢弃在达到限制后获得的任何积分。启动积分不计入限制。有关每种 T2 实例大小的 CPU 积分余额限制的更多信息，请参阅 积分表 (p. 176) 。
积分使用	首先花费启动积分，再使用获得的积分。	只有花完所有启动积分后才能花费获得的积分。
过期积分	在 T2 标准实例运行过程中，启动积分不会过期。当 T2 标准实例停止或切换至“T2 无限”时，所有启动积分都将丢失。	在 T2 实例运行过程中，已累积获得的积分不会过期。T2 实例停止后，将丢失所有已累积获得的积分。

CloudWatch 指标 `CPUCreditBalance` 可跟踪已累积的启动积分和已累积获得的积分数。有关更多信息，请参阅 [CloudWatch 指标表 \(p. 200\)](#) 中的 `CPUCreditBalance`。

示例：标准模式

以下示例介绍当实例配置为 `standard` 时的积分使用情况。

示例

- [示例 1：介绍 T3 标准的积分使用情况 \(p. 187\)](#)
- [示例 2：介绍 T2 标准的积分使用情况 \(p. 188\)](#)

示例 1：介绍 T3 标准的积分使用情况

在本示例中，您将了解作为 `standard` 启动的 `t3.nano` 实例如何获得、累积和使用获得的积分。您可以看到积分余额如何反映累积的获得的积分。

Note

配置为 `standard` 的 T3 和 T3a 实例不会收到启动积分。

运行的 `t3.nano` 实例每 24 小时获得 144 个积分。其积分余额限制为 144 个获得的积分。达到该限制后，将丢弃获得的任何新积分。有关可获得和可累积的积分数的更多信息，请参阅 [积分表 \(p. 176\)](#)。

您可启动 T3 标准实例并立即使用它。或者，您可能在启动 T3 标准实例后让其闲置几天，再在该实例上运行应用程序。实例是正在被使用还是闲置决定积分是消耗还是累积。如果实例从启动时开始保持闲置状态 24 小时，则积分余额将达到其限制，这是可以累积的获得积分的最大数目。

本示例介绍启动后闲置 24 小时的实例，并向您分析 96 小时内共 7 个时段的积分情况，演示获得、累积、使用和丢弃积分的速率以及每个时段结束时的积分余额值。

以下工作流程引用图中的编号数据点：

P1 – 在图表中的 0 小时处，实例以 `standard` 模式启动并立即开始获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%），不使用任何积分。所有未使用的积分都累积到积分余额中。对于前 24 小时，`CPUCreditUsage` 为 0，而 `CPUCreditBalance` 值达到其最大值 144。

P2 – 对于接下来的 12 小时，CPU 利用率为 2.5%，这低于 5% 基准。实例获得的积分多于花费的积分，但 `CPUCreditBalance` 值不能超过其最大值 144 个积分。所获得的超过限制的所有积分都会被丢弃。

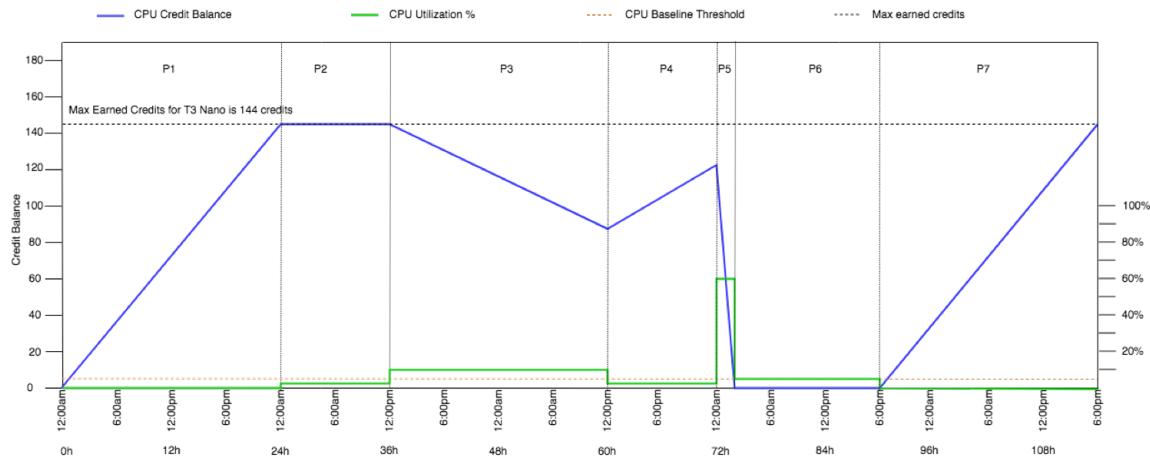
P3 – 对于接下来的 24 小时，CPU 利用率为 7%（高于基准），这要求花费 57.6 个积分。实例花费的积分多于获得的积分，`CPUCreditBalance` 值降至 86.4 个积分。

P4 – 对于接下来的 12 小时，CPU 利用率降至 2.5%（低于基准），这要求花费 36 个积分。同时，实例获得 72 个积分。实例获得的积分多于花费的积分，`CPUCreditBalance` 值增至 122 个积分。

P5 – 对于接下来的两个小时，实例突增至 100% CPU 利用率，并耗尽其整个 `CPUCreditBalance` 值的 122 个积分。在此期间结束时，`CPUCreditBalance` 为零，CPU 利用率会被强制降低到基准性能级别 5%。在基准时，实例获得的积分与花费的积分一样多。

P6 – 对于接下来的 14 小时，CPU 利用率为 5%（基准）。实例获得的积分与花费的积分一样多。`CPUCreditBalance` 值保持为 0。

P7 – 对于本例中的最后 24 小时，实例空闲，CPU 利用率为 0%。在此期间，实例获得 144 个积分，这些积分将累积到其 `CPUCreditBalance` 中。



示例 2：介绍 T2 标准的积分使用情况

在本示例中，您将了解作为 standard 启动的 `t2.nano` 实例如何获得、累积和使用启动积分和获得的积分。您还可以了解积分余额如何反映累积获得的积分和累积启动积分。

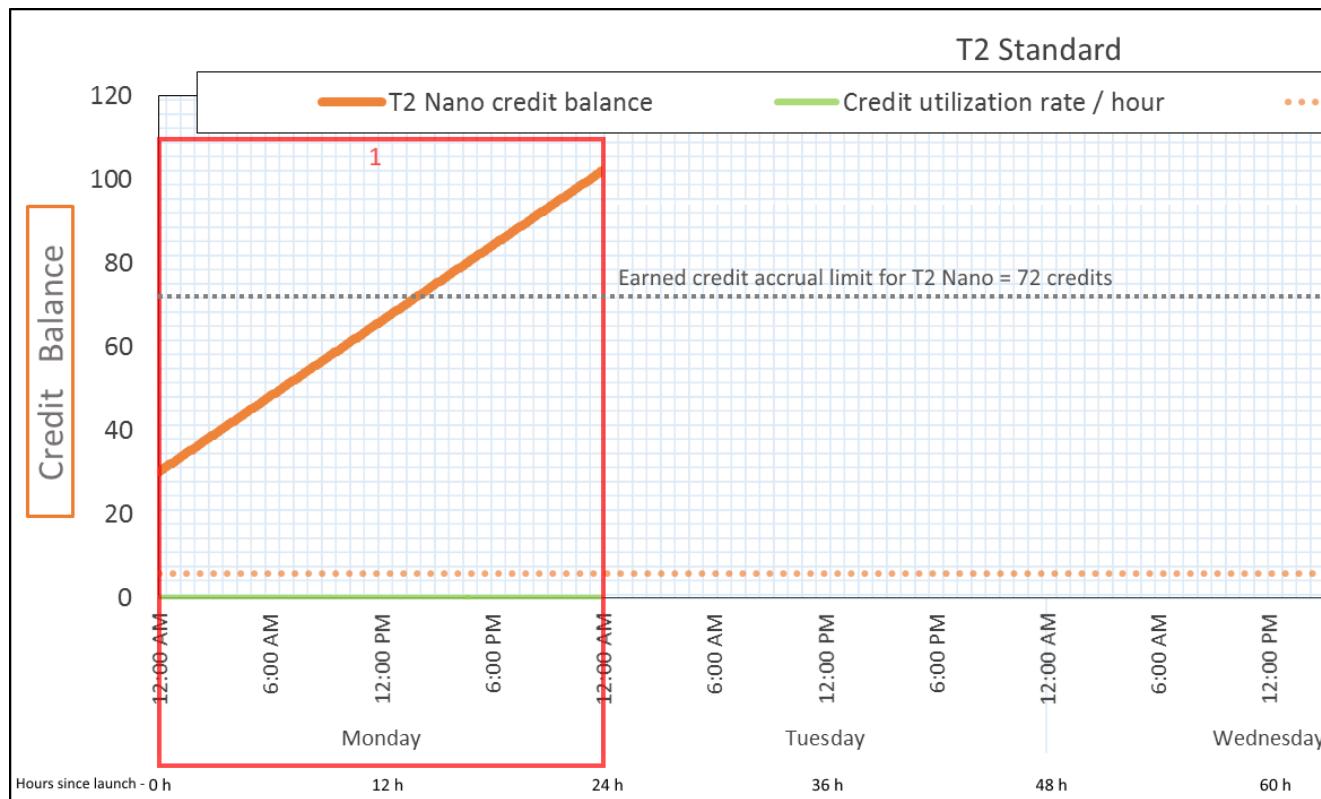
启动时，`t2.nano` 实例获得 30 启动积分，之后每 24 小时获得 72 积分。其积分余额限制是获得的 72 积分；启动积分不计入该限制。达到该限制后，将丢弃获得的任何新积分。有关可获得和可累积的积分数的更多信息，请参阅[积分表 \(p. 176\)](#)。有关限制的更多信息，请参阅[启动积分限制 \(p. 186\)](#)。

您可启动 T2 标准实例并立即使用它。或者，您可能在启动 T2 标准实例后让其闲置几天，再在该实例上运行应用程序。实例是正在被使用还是闲置决定积分是消耗还是累积。如果实例自启动后闲置 24 小时，积分余额将超过其限制，因为积分余额同时反映累积获得的积分和累积启动积分。不过，使用 CPU 后，会先使用启动积分。此后，积分余额限制始终反映可累积获得的最大积分。

本示例介绍启动后闲置 24 小时的实例，并向您分析 96 小时内共 7 个时段的积分情况，演示获得、累积、使用和丢弃积分的速率以及每个时段结束时的积分余额值。

第 1 个时段：1 – 24 小时

在图上的第 0 小时，T2 实例作为 standard 启动并立即获得 30 启动积分。当它处于运行状态时，会获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%）——不使用任何积分。所有未使用的积分都累积到积分余额中。在启动后大约 14 小时，积分余额为 72（30 启动积分 + 获得的 42 积分），这与实例在 24 小时内获得的积分相同。在启动后 24 小时，积分余额超过 72，因为未使用的启动积分累积到了积分余额中（积分余额为 -102 积分：30 启动积分 + 72 获得积分）。



积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 0 积分
积分余额	102 积分 (30 启动积分 + 获得的 72 积分)

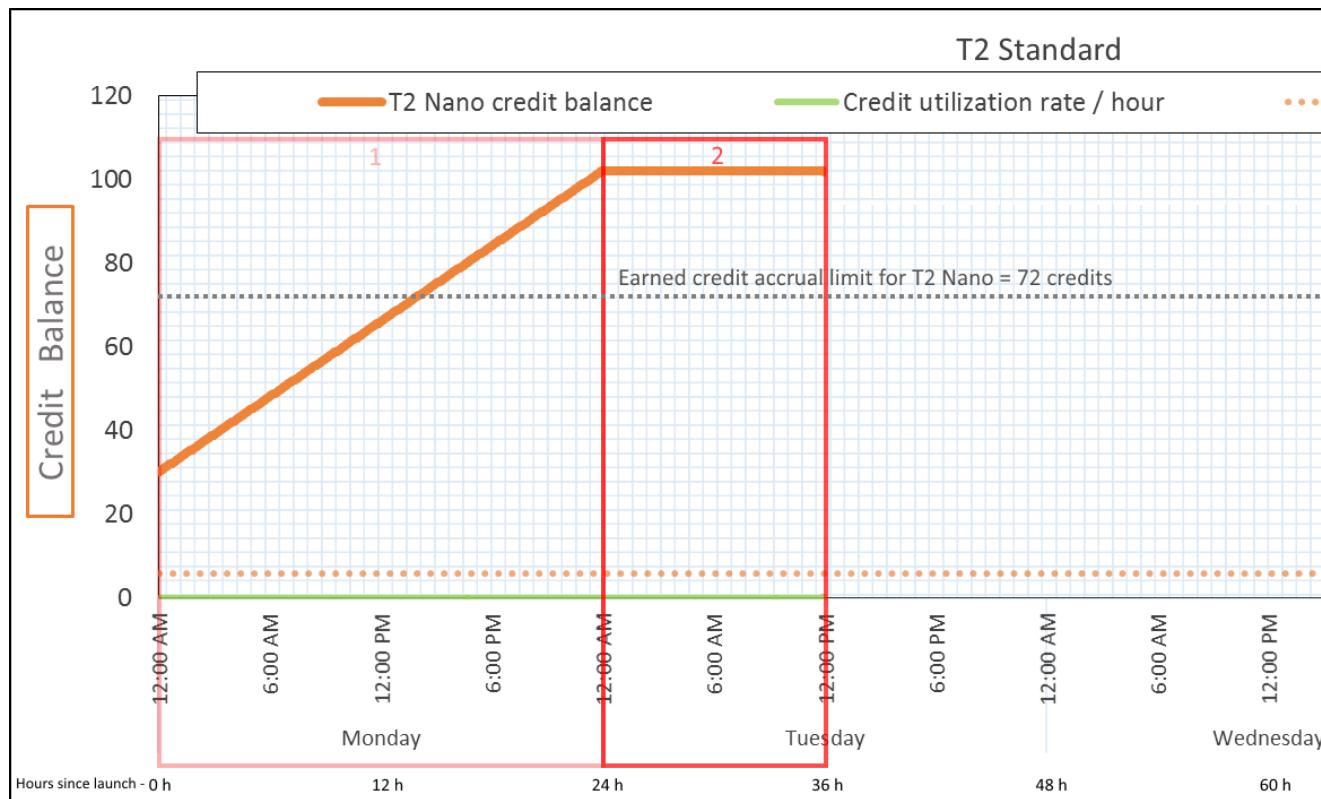
结论

如果启动后没有 CPU 利用率，实例累积的积分将超过其在 24 小时内获得的积分 (30 启动积分 + 获得的 72 积分 = 102 积分)。

在真实场景中，EC2 实例在启动和运行时会使用少量积分，以防止积分余额达到本实例中的最大理论值。

第 2 个时段：25 – 36 小时

在接下来 12 小时，实例继续保持闲置状态并获得积分，但积分余额不会增加。积分余额保持在 102 (30 启动积分 + 获得的 72 积分)。积分余额已达到 72 累积获得的积分限制，因此会丢弃新获得的积分。



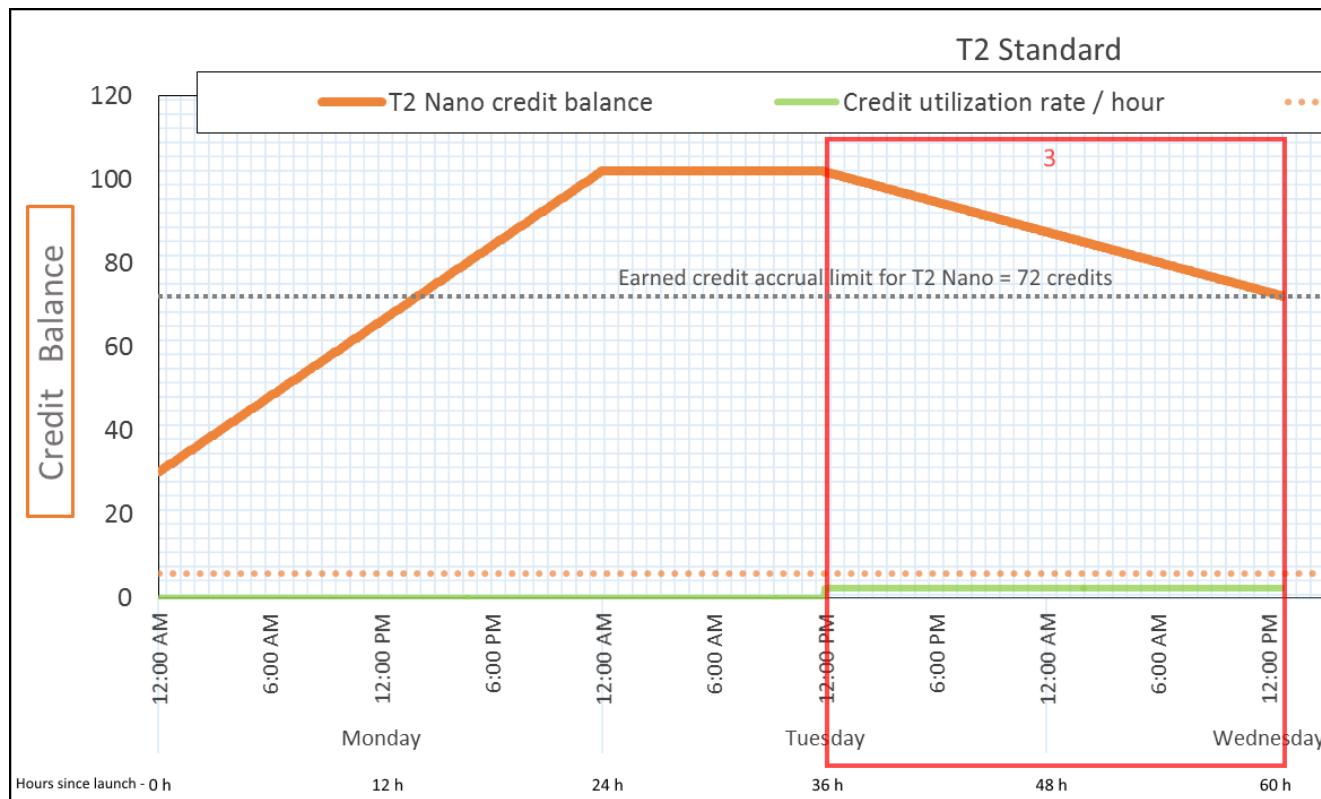
积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分 (每小时 3 积分)
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	102 积分 (30 启动积分 + 72 获得积分) — 余额保持不变

结论

如果积分余额已达到其限制，实例会继续获得积分，但不会累积更多获得的积分。达到该限制后，会丢弃新获得的积分。启动积分不计入积分余额限制。如果余额包含累积的启动积分，余额将超过该限制。

第 3 个时段：37 – 61 小时

在接下来 25 小时，实例使用 2% CPU，需要 30 积分。在同一周期，它获得 75 积分，但积分余额减少。余额减少的原因是先使用累积的启动积分，并且由于积分余额已达到其获得的 72 积分限制，因此丢弃了新获得的积分。



积分使用率	24 小时 28.8 积分 (每小时 1.2 积分 , 2% CPU 利用率 , 40% 积分获得率) — 25 小时 30 积分
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	72 积分 (使用了 30 启动积分 ; 剩余获得的 72 积分未使用)

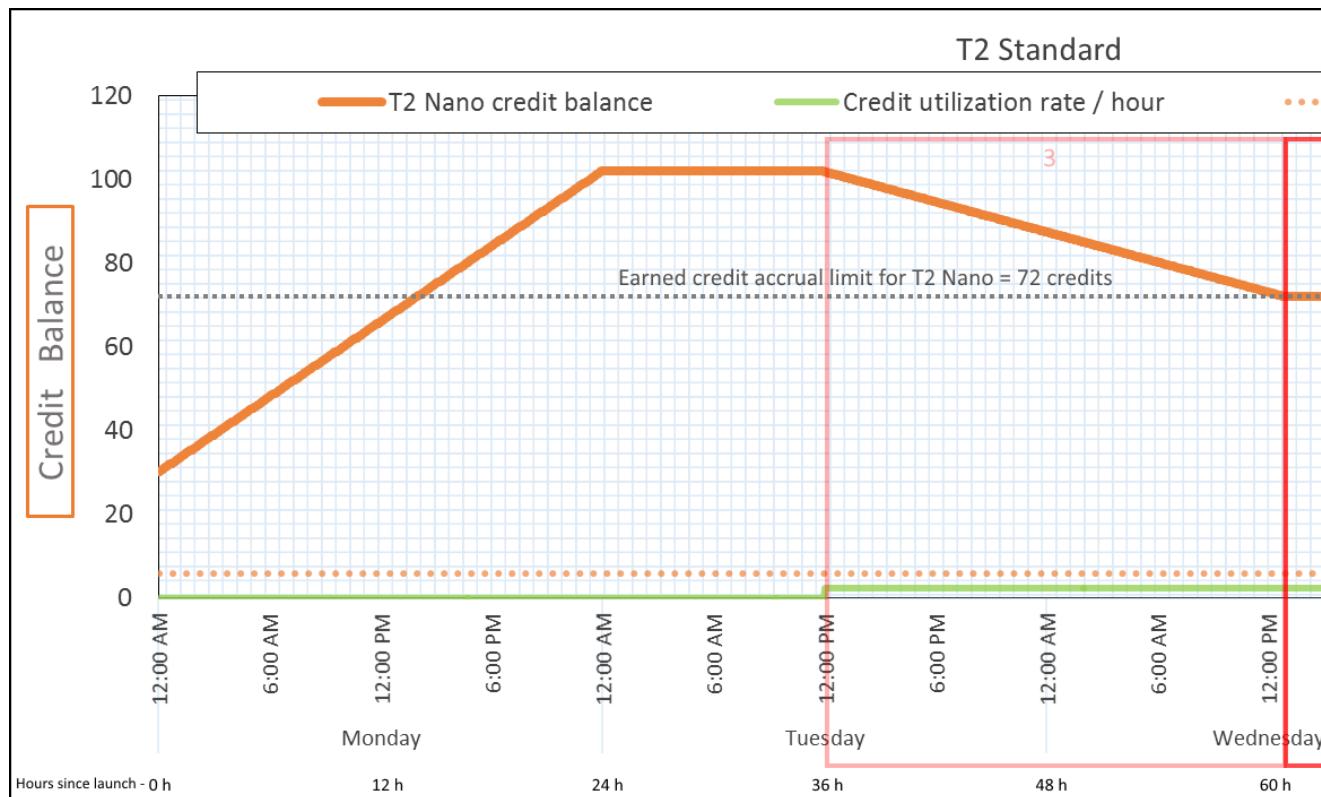
结论

实例先使用启动积分，再使用获得的积分。启动积分不计入积分限制。使用启动积分后，积分余额永远不会超过在 24 小时内可获得的积分。此外，实例运行时，不会获得更多启动积分。

第 4 个时段 : 62 – 72 小时

在接下来 11 小时，实例使用 2% CPU，需要 13.2 积分。这与上一周期的 CPU 利用率相同，但积分余额不会减少。它保持在 72 积分。

积分余额不减少的原因是积分获得率高于积分使用率。实例使用 13.2 积分的同时，获得 33 积分。不过，由于余额限制是 72 积分，因此会丢弃获得的超过该限制的任何积分。积分余额保持在 72 积分，这与第 2 个时段保持在 102 积分不同，因为没有累积的启动积分。



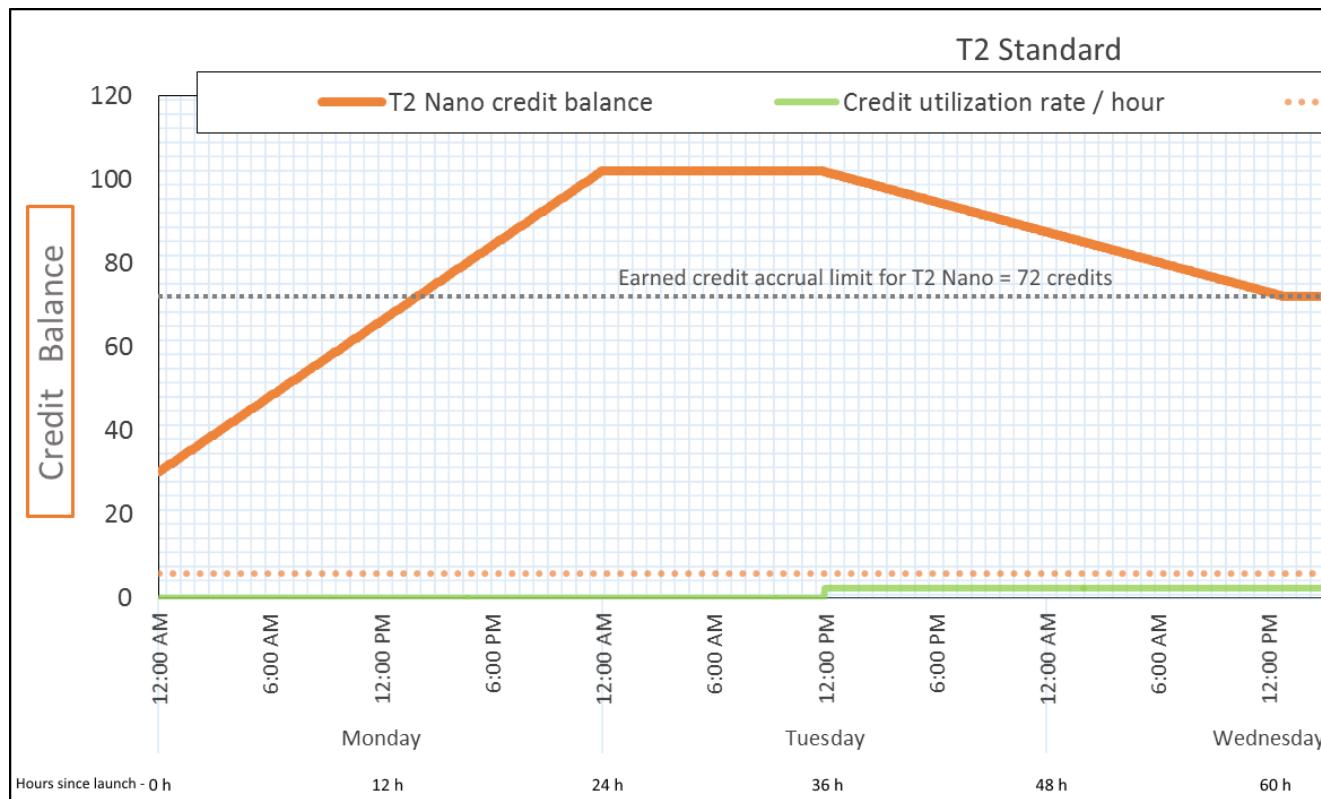
积分使用率	24 小时 28.8 积分 (每小时 1.2 积分 , 2% CPU 利用率 , 40% 积分获得率) — 11 小时 13.2 积分
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 43.2 积分 (60% 积分获得率)
积分余额	72 积分 (0 启动积分 , 获得的 72 积分) — 余额达到其限制

结论

使用启动积分后，积分余额限制由实例在 24 小时内可获得的积分数决定。如果实例获得的积分多于使用的积分，则会丢弃新获得的超过限制的积分。

第 5 个时段 : 73 – 75 小时

在接下来 3 小时，实例的 CPU 利用率激增至 20%，需要 36 积分。在相同的 3 小时内，实例获得 9 积分，导致净余额减少 27 积分。在这 3 小时结束时，积分余额为累积获得的 45 积分。



积分使用率	24 小时 288 积分 (每小时 12 积分 , 20% CPU 利用率 , 400% 积分获得率) — 3 小时 36 积分
积分获得率	每 24 小时 72 积分 (3 小时 9 积分)
积分丢弃率	每 24 小时 0 积分
积分余额	45 积分 (以前的余额 (72) - 使用的积分 (36) + 获得的积分 (9)) — 余额按每 24 小时 216 积分的速率减少 (使用率 288/24 + 获得率 72/24 = 余额减少率 216/24)

结论

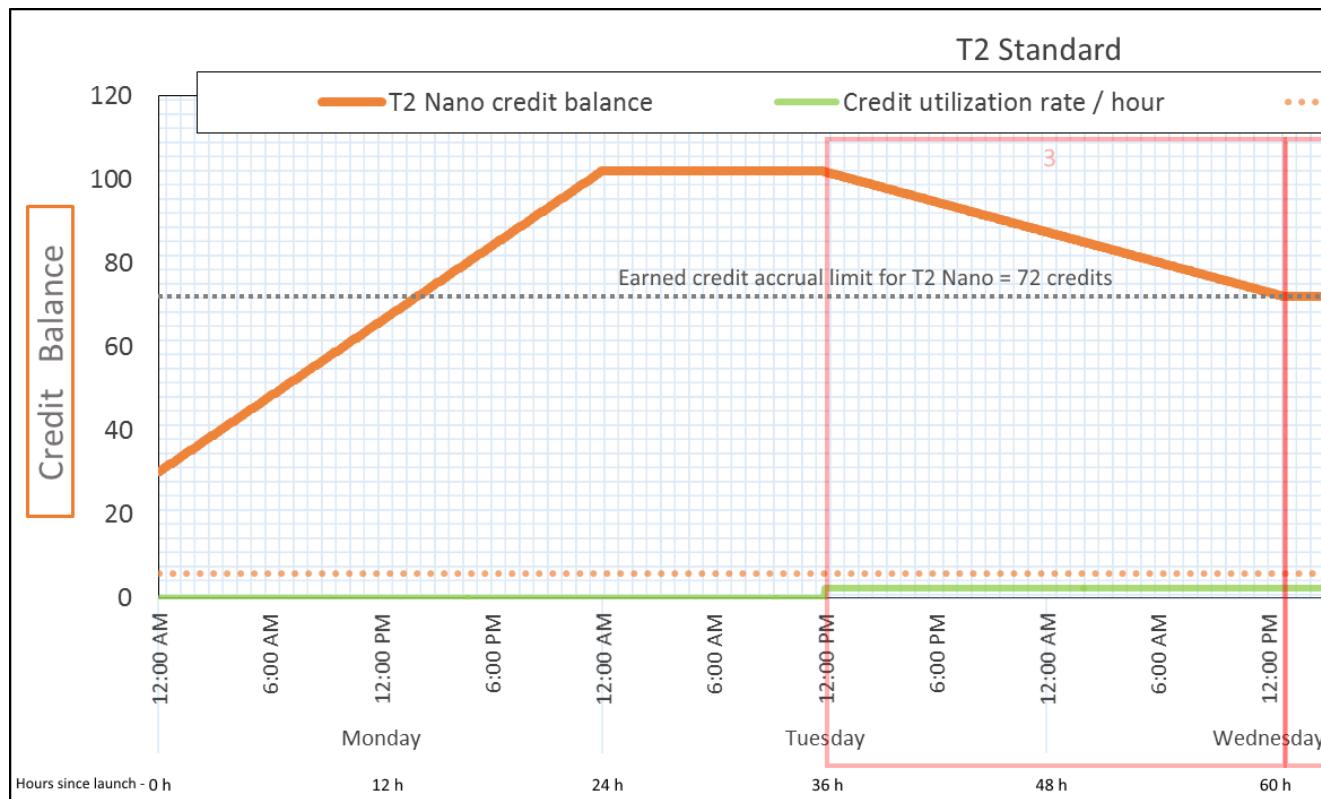
如果实例使用的积分多于获得的积分，则其积分余额将减少。

第 6 个时段 : 76 – 90 小时

在接下来 15 小时，实例使用 2% CPU，需要 18 积分。这与第 3 个和第 4 个时段的 CPU 利用率相同。不过，此周期的积分余额增加，而第 3 个时段的积分余额减少，第 4 个时段的保持不变。

在第 3 个时段，使用累积的启动积分，并会丢弃获得的超过积分限制的任何积分，导致积分余额减少。在第 4 个时段，实例发挥的积分数少于其获得的积分数。所获得的任何超出限制的积分将丢弃，因此余额保持在其最大值 72 个积分。

在本周期，没有累积的启动积分，余额中累积获得的积分数低于限制。不会丢弃获得的任何积分。此外，实例获得的积分多于使用的积分，导致积分余额增加。



积分使用率	24 小时 28.8 积分 (每小时 1.2 积分 , 2% CPU 利用率 , 40% 积分获得率) — 15 小时 18 积分
积分获得率	每 24 小时 72 积分 (15 小时 45 积分)
积分丢弃率	每 24 小时 0 积分
积分余额	72 积分 (余额按每 24 小时 43.2 积分的速率增加 — 改变率 = 使用率 28.8/24 + 获得率 72/24)

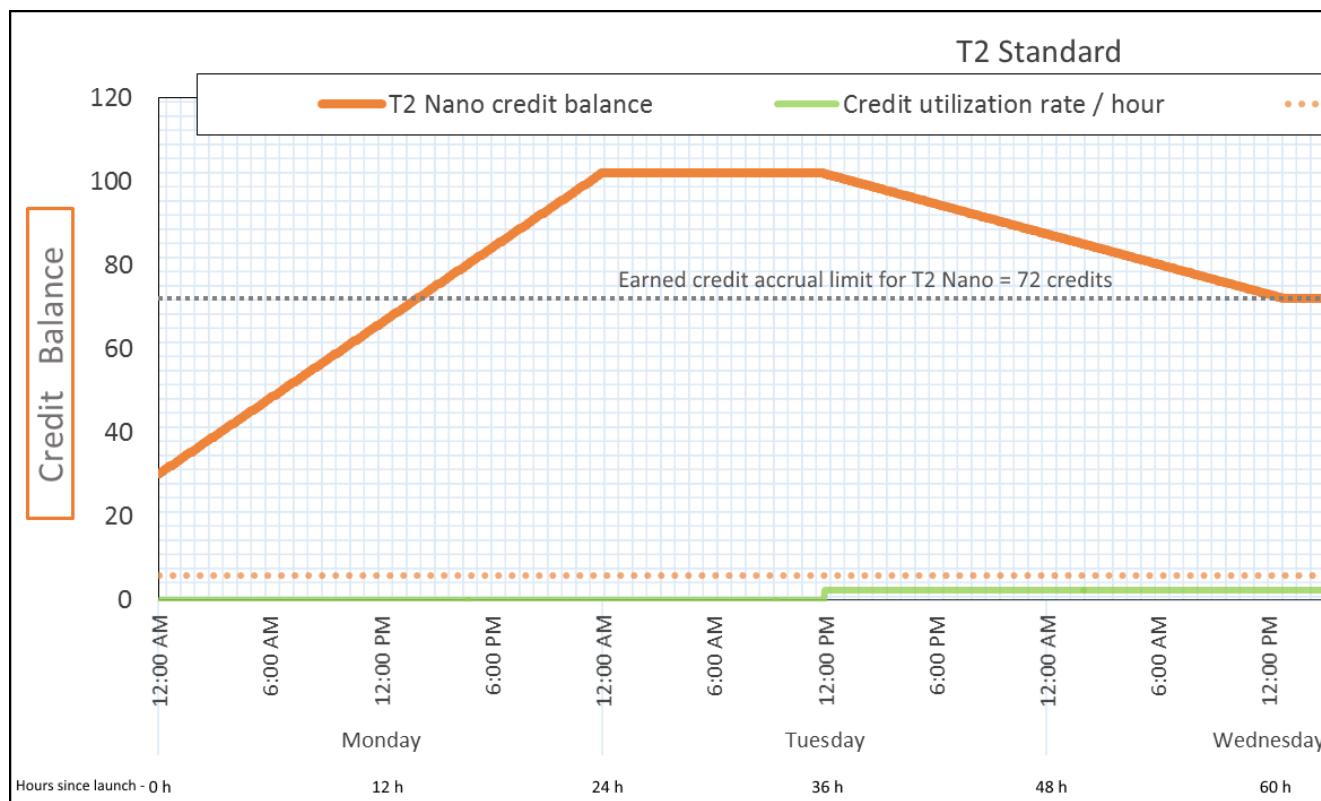
结论

如果实例使用的积分少于获得的积分，则其积分余额将增加。

第 7 个时段 : 91 – 96 小时

在接下来六小时，实例保持闲置状态— (CPU 利用率为 0%)，—不使用任何积分。这与第 2 个时段的 CPU 利用率相同，但积分余额不保持在 102 积分，而保持在 72 积分，—这是实例的积分余额限制。

在第 2 个时段，积分余额中包含累积的 30 启动积分。启动积分在第 3 个时段使用。正在运行的实例无法获得更多启动积分。达到积分余额限制后，会丢弃获得的超过限制的任何积分。



积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	72 积分 (0 启动积分，获得的 72 积分)

结论

如果已达到积分余额限制，实例会继续获得积分，但不会累积更多获得的积分。达到该限制后，会丢弃新获得的积分。积分余额限制由实例在 24 小时内可获得的积分数决定。有关积分余额限制的更多信息，请参阅 [积分表 \(p. 176\)](#)。

使用可突增性能实例

用于启动、监控和修改这些实例的步骤是类似的。主要差别在于它们启动时的默认积分规范。如果您没有更改默认积分规范，则默认值为：

- 默认情况下，T3 和 T3a 实例以 `unlimited` 模式启动。
- T2 实例默认情况下作为 `standard` 启动。

目录

- [以“无限”或“标准”模式启动可突增性能实例 \(p. 196\)](#)
- [使用 Auto Scaling 组以“无限”模式启动可突增性能实例 \(p. 196\)](#)
- [查看可突增性能实例的积分规范 \(p. 197\)](#)
- [修改可突增性能实例的积分规范 \(p. 198\)](#)

- 设置账户的默认积分规范 (p. 199)
- 查看默认积分规范 (p. 199)

以“无限”或“标准”模式启动可突增性能实例

默认情况下，T3 和 T3a 实例以 `unlimited` 模式启动。T2 实例默认情况下作为 `standard` 启动。

有关这些实例的 AMI 和驱动程序要求的更多信息，请参阅[发行说明 \(p. 174\)](#)。

您必须将 Amazon EBS 卷作为根设备以启动实例。有关更多信息，请参阅[Amazon EC2 根设备卷 \(p. 13\)](#)。

您可以使用 Amazon EC2 控制台、AWS 开发工具包、命令行工具或者 Auto Scaling 组，以 `unlimited` 或 `standard` 模式启动实例。有关更多信息，请参阅[使用 Auto Scaling 组以“无限”模式启动可突增性能实例 \(p. 196\)](#)。

以“无限”或“标准”模式启动可突增性能实例（控制台）

1. 按照[使用启动实例向导启动实例 \(p. 375\)](#)过程操作。
2. 在选择一个实例类型页面上，选择一种实例类型，然后选择下一步：配置实例详细信息。
3. 选择积分规范。T3 和 T3a 的默认值为 `unlimited`，T2 的默认值为 `standard`。
 - a. 要以 `standard` 模式启动 T3 或 T3a 实例，请在配置实例详细信息页面上为 T2/T3 无限清除启用。
 - b. 要以 `unlimited` 模式启动 T2 实例，请在配置实例详细信息页面上，对于 T2/T3 无限，选择启用。
4. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。

以“无限”或“标准”模式启动可突增性能实例 (AWS CLI)

使用 `run-instances` 命令启动您的实例。使用 `--credit-specification CpuCredits=` 参数指定积分规范。有效的积分规范为 `unlimited` 和 `standard`。

- 对于 T3 和 T3a，如果不包含 `--credit-specification` 参数，实例默认以 `unlimited` 模式启动。
- 对于 T2，如果不包含 `--credit-specification` 参数，实例默认作为 `standard` 启动。

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t3.micro --key-name MyKeyPair --credit-specification "CpuCredits=unlimited"
```

使用 Auto Scaling 组以“无限”模式启动可突增性能实例

在启动可突增性能实例时，它们需要具有 CPU 积分才能获得良好的引导体验。如果您使用 Auto Scaling 组启动实例，建议您将实例配置为 `unlimited`。如果这样做，实例会在自动启动或者由 Auto Scaling 组重新启动时使用超额积分。使用超额积分可以防止受到性能限制。

创建启动模板

在 Auto Scaling 组中以 `unlimited` 模式启动实例时，您必须使用启动模板。启动配置不支持以 `unlimited` 模式启动实例。

创建以“无限”模式启动实例的启动模板（控制台）

1. 按照[为 Auto Scaling 组创建启动模板](#)的过程操作。
2. 在启动模板内容中，对于实例类型，请选择 T3、T3a 或 T2 实例大小。
3. 要在 Auto Scaling 组中以 `unlimited` 模式启动实例，在高级详细信息中，对于 T2/T3 无限，选择启用。

- 在您完成后，定义启动模板参数，选择创建启动模板。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的[为 Auto Scaling 组创建启动模板](#)。

创建以“无限”模式启动实例的启动模板 (AWS CLI)

使用 [create-launch-template](#) 命令并将 `unlimited` 指定为积分规范。

- 对于 T3 和 T3a，如果不包含 `CreditSpecification={CpuCredits=unlimited}` 值，实例默认以 `unlimited` 模式启动。
- 对于 T2，如果不包含 `CreditSpecification={CpuCredits=unlimited}` 值，实例默认作为 `standard` 启动。

```
aws ec2 create-launch-template --launch-template-name MyLaunchTemplate
--version-description FirstVersion --launch-template-data
ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

将 Auto Scaling 组与启动模板关联

要将启动模板与一个 Auto Scaling 组相关联，请使用启动模板创建 Auto Scaling 组，或者将启动模板添加到现有 Auto Scaling 组中。

使用启动模板创建 Auto Scaling 组（控制台）

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在屏幕顶部的导航栏中，选择在创建启动模板时使用的同一区域。
- 在导航窗格中，依次选择 Auto Scaling 组和创建 Auto Scaling 组。
- 选择启动模板，选择您的启动模板，然后选择下一步。
- 填写 Auto Scaling 组的各个字段。当您在审核页面上完成审核配置设置时，选择创建 Auto Scaling 组。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的[使用启动模板创建 Auto Scaling 组](#)。

使用启动模板创建 Auto Scaling 组 (AWS CLI)

使用 [create-auto-scaling-group](#) AWS CLI 命令并指定 `--launch-template` 参数。

添加启动模板到现有 Auto Scaling 组（控制台）

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在屏幕顶部的导航栏中，选择在创建启动模板时使用的同一区域。
- 在导航窗格中，选择 Auto Scaling Groups。
- 从 Auto Scaling 组列表中选择一个 Auto Scaling 组，然后依次选择操作和编辑。
- 在详细信息选项卡上，对于启动模板，选择一个启动模板，然后选择保存。

添加启动模板到现有 Auto Scaling 组 (AWS CLI)

使用 [update-auto-scaling-group](#) AWS CLI 命令并指定 `--launch-template` 参数。

查看可突增性能实例的积分规范

您可以查看正在运行或停止的实例的积分规范 (`unlimited` 或 `standard`)。

查看可突增实例的积分规范（控制台）

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在左侧导航窗格中，选择实例，然后选择实例。

3. 选择描述，然后查看 T2/T3 Unlimited (T2/T3 无限) 字段。

- 如果值为 Enabled，则您的实例配置为 unlimited。
- 如果值为 Disabled，则您的实例配置为 standard。

描述可突增性能实例的积分规范 (AWS CLI)

使用 [describe-instance-credit-specifications](#) 命令。如果您指定一个或多个实例 ID，则将返回具有积分规范 unlimited 的所有实例，以及以前使用 unlimited 积分规范配置的实例。例如，如果您将 T3 实例大小调整为 M4 实例，而该实例配置为 unlimited，Amazon EC2 将返回 M4 实例。

Example

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

下面是示例输出：

```
{  
    "InstanceCreditSpecifications": [  
        {  
            "InstanceId": "i-1234567890abcdef0",  
            "CpuCredits": "unlimited"  
        }  
    ]  
}
```

修改可突增性能实例的积分规范

您可以随时将正在运行或停止的实例的积分规范在 unlimited 与 standard 之间切换。

修改可突增性能实例的积分规范（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，选择实例，然后选择实例。要一次修改若干个实例的规范，请选择所有适用的实例。
3. 依次选择操作、实例设置、更改 T2/T3 无限。

Note

只有在选择 T3、T3a 或 T2 实例时，才会启用更改 T2/T3 无限选项。

4. 要将积分规范更改为 unlimited，请选择启用。要将积分规范更改为 standard，请选择禁用。实例的当前积分规范将显示在实例 ID 后的括号中。

修改可突增性能实例的积分规范 (AWS CLI)

使用 [modify-instance-credit-specification](#) 命令。请使用 --instance-credit-specification 参数指定实例及其积分规范。有效的积分规范为 unlimited 和 standard。

Example

```
aws ec2 modify-instance-credit-specification --region us-east-1 --instance-credit-specification "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

下面是示例输出：

```
{  
    "SuccessfulInstanceCreditSpecifications": [
```

```
{  
    "InstanceId": "i- 1234567890abcdef0"  
}  
,  
"UnsuccessfulInstanceCreditSpecifications": []  
}
```

设置账户的默认积分规范

您可以在每个 AWS 区域的账户级别设置默认积分规范。您可以指定每个实例系列 (T2、T3 或 T3a) 的默认积分规范。

如果您使用 AWS 管理控制台中的启动实例向导启动实例，则 T2/T3 Unlimited (T2/T3 无限) 的值会覆盖账户级别默认积分规范。如果您使用 AWS CLI 启动实例，则账户中所有新的可突增性能实例都使用默认积分选项启动。现有正在运行或已停止的实例的积分规范不受影响。

`modify-default-credit-specification` API 是一种异步操作，适用于 AWS 区域级别，可修改每个可用区的积分选项。区域中的所有可用区都会在五分钟内更新。但是，如果在此操作期间启动了实例，则在可用区更新之前，它们可能无法获得新的积分选项。要验证是否已发生更新，您可以调用 `get-default-credit-specification` 并检查默认积分规范是否已更新。有关更多信息，请参阅[查看默认积分规范 \(p. 199\)](#)。

Note

实例系列的默认积分规范在 5 分钟滚动周期内只能修改一次，在 24 小时滚动周期内最多可修改四次。

在账户级别设置默认积分规范 (AWS CLI)

使用 `modify-default-credit-specification` 命令。使用 `--cpu-credits` 参数指定 AWS 区域、实例系列和默认积分规范。有效的默认积分规范为 `unlimited` 和 `standard`。

```
aws ec2 modify-default-credit-specification --region us-east-1 --instance-family t2 --cpu-credits unlimited
```

查看默认积分规范

您可以在每个 AWS 区域的账户级别查看可突增性能实例系列的默认积分规范。

在账户级别查看默认积分规范 (AWS CLI)

使用 `get-default-credit-specification` 命令。指定 AWS 区域和实例系列。

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

监控 CPU 积分

您可以在 CloudWatch 控制台 Amazon EC2 每个实例指标中查看各个实例的积分余额。

主题

- 可突增性能实例的其他 CloudWatch 指标 (p. 199)
- 计算使用的 CPU 积分 (p. 201)

可突增性能实例的其他 CloudWatch 指标

T3、T3a 和 T2 实例具有这些额外的 CloudWatch 指标，将每 5 分钟更新一次这些指标：

- `CPUCreditUsage` – 在测量周期内花费的 CPU 积分数。
- `CPUCreditBalance` – 实例产生的 CPU 积分数量。在 CPU 突增以及 CPU 积分的花费速度比获得速度快时，该余额将用完。

- **CPUSurplusCreditBalance** – 在 CPUCreditBalance 值为零时，用于保持 CPU 性能而花费的超额 CPU 积分数。
- **CPUSurplusCreditsCharged** – 超过可在 24 小时内获得的 [CPU 积分数上限 \(p. 176\)](#) 的超额 CPU 积分数，因而会产生额外的费用。

最后两个指标仅适用于配置为 `unlimited` 的实例。

下表描述了可突增性能实例的 CloudWatch 指标。有关更多信息，请参阅[列出实例的可用 CloudWatch 指标 \(p. 539\)](#)。

指标	说明
CPUCreditUsage	<p>实例为保持 CPU 使用率而花费的 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 积分指标仅每 5 分钟提供一次。如果您指定一个大于五分钟的时间段，请使用 <code>Sum</code> 统计数据，而非 <code>Average</code> 统计数据。</p> <p>单位：积分 (vCPU 分钟)</p>
CPUCreditBalance	<p>实例自启动后已累积获得的 CPU 积分数。对于 T2 标准，CPUCreditBalance 还包含已累积的启动积分数。</p> <p>在获得积分后，积分将在积分余额中累积；在花费积分后，将从积分余额中扣除积分。积分余额具有最大值限制，这是由实例大小决定的。在达到限制后，将丢弃获得的任何新积分。对于 T2 标准，启动积分不计入限制。</p> <p>实例可以花费 CPUCreditBalance 中的积分，以便突增到基准 CPU 使用率以上。</p> <p>在实例运行过程中，CPUCreditBalance 中的积分不会过期。在 T3 或 T3a 实例停止时，CPUCreditBalance 值将保留七天。之后，所有累积的积分都将丢失。在 T2 实例停止时，CPUCreditBalance 值不会保留，并且所有累积的积分都将丢失。</p> <p>CPU 积分指标仅每 5 分钟提供一次。</p> <p>单位：积分 (vCPU 分钟)</p>
CPUSurplusCreditBalance	<p>在 CPUCreditBalance 值为零时，<code>unlimited</code> 实例花费的超额积分数。</p> <p>CPUSurplusCreditBalance 值由获得的 CPU 积分支付。如果超额积分数超出实例可在 24 小时周期内获得的最大积分数，则超出最大积分数的已花费超额积分将产生额外费用。</p> <p>单位：积分 (vCPU 分钟)</p>
CPUSurplusCreditsCharged	<p>未由获得的 CPU 积分支付并且会产生额外费用的已花费超额积分数。</p> <p>在出现以下任一情况时，将对花费的超额积分收费：</p> <ul style="list-style-type: none">• 花费的超额积分超出实例可在 24 小时周期内获得的最大积分数。对于超出最大积分数的所花费超额积分，将在该小时结束时向您收费。

指标	说明
	<ul style="list-style-type: none">实例已停止或终止。实例从 <code>unlimited</code> 切换为 <code>standard</code>。 <p>单位 : 积分 (vCPU 分钟)</p>

计算使用的 CPU 积分

实例使用的 CPU 积分使用上表中所述的实例 CloudWatch 指标计算。

Amazon EC2 每 5 分钟向 CloudWatch 发送一次指标。在任何时间点引用的以前 指标值是指 5 分钟前 发送的以前指标值。

计算标准实例使用的 CPU 积分

- 如果 CPU 使用率低于基准，此时花费的积分低于前 5 分钟间隔获得的积分，CPU 积分余额将增加。
- 如果 CPU 使用率高于基准，此时花费的积分超过前 5 分钟间隔获得的积分，CPU 积分余额将减少。

从数学上讲，这是使用以下公式得出的：

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -  
CPUCreditUsage]
```

实例大小确定实例每小时可获得的积分数以及实例可在积分余额中累积获得的积分数。有关每小时获得的积分数的信息，以及每个实例大小的积分余额限制，请参阅[积分表 \(p. 176\)](#)。

示例

该示例使用 `t3.nano` 实例。要计算实例的 `CPUCreditBalance` 值，请按以下方式使用前面的公式：

- `CPUCreditBalance` – 要计算的当前积分余额。
- `prior CPUCreditBalance` – 5 分钟前的积分余额。在该示例中，实例累积了两个积分。
- `Credits earned per hour` – `t3.nano` 实例每小时获得 6 个积分。
- `5/60` – 表示 CloudWatch 指标发布的 5 分钟间隔。将每小时获得的积分乘以 `5/60` (5 分钟) 以计算实例在过去 5 分钟获得的积分数。`t3.nano` 实例每 5 分钟获得 0.5 个积分。
- `CPUCreditUsage` – 实例在过去 5 分钟内花费的积分数。在该示例中，实例在过去 5 分钟内花费 1 个积分。

您可以使用这些值计算 `CPUCreditBalance` 值：

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

计算无限实例使用的 CPU 积分

在 T3、T3a 或 T2 实例需要突增到基准以上时，它始终先花费累积的积分，然后再花费超额积分。在用完累积的 CPU 积分余额时，它会花费超额积分以突增所需的时间。在 CPU 使用率低于基准时，在实例累积获得的积分之前始终先支付超额积分。

我们在以下公式中使用 `Adjusted balance` 项以反映在该 5 分钟间隔内发生的活动。我们使用该值计算 `CPUCreditBalance` 和 `CPUSurplusCreditBalance` CloudWatch 指标的值。

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits earned per hour * (5/60) - CPUCreditUsage]
```

如果 0 的值为 Adjusted balance，表示实例花费获得的所有积分来进行突增，而未花费任何超额积分。因此，CPUCreditBalance 和 CPUSurplusCreditBalance 均设置为 0。

正的 Adjusted balance 值表示实例累积获得了积分，并支付了以前的超额积分（如果有）。因此，将 Adjusted balance 值分配给 CPUCreditBalance，并将 CPUSurplusCreditBalance 设置为 0。实例大小决定了可累积的**最大积分数** (p. 176)。

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]  
CPUSurplusCreditBalance = 0
```

负的 Adjusted balance 值表示实例花费了其累积获得的所有积分，并且还花费了超额积分来进行突增。因此，将 Adjusted balance 值分配给 CPUSurplusCreditBalance，并将 CPUCreditBalance 设置为 0。此外，实例大小决定了它可累积的**最大积分数** (p. 176)。

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]  
CPUCreditBalance = 0
```

如果花费的超额积分超过了实例可累积的最大积分，超额积分余额将设置为最大值，如前面的公式中所示。将对剩余的超额积分收费，如 CPUSurplusCreditsCharged 指标表示。

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

最后，在实例终止时，将对由 CPUSurplusCreditBalance 跟踪的任何超额积分收费。如果实例从 unlimited 切换到 standard，则还会对任何剩余的 CPUSurplusCreditBalance 收费。

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
- 高性能 Web 服务器
- 高性能计算 (HPC)
- 科学建模
- 专用游戏服务器和广告服务引擎
- 机器学习推理和其他计算密集型应用程序

有关更多信息，请参阅 [Amazon EC2 C5 实例](#)。

目录

- [硬件规格 \(p. 203\)](#)
- [实例性能 \(p. 204\)](#)

- 网络性能 (p. 204)
- SSD I/O 性能 (p. 205)
- 实例功能 (p. 205)
- 发行说明 (p. 206)

硬件规格

以下是计算优化型实例的硬件规格摘要。

实例类型	默认 vCPU	内存 (GiB)
c4.large	2	3.75
c4.xlarge	4	7.5
c4.2xlarge	8	15
c4.4xlarge	16	30
c4.8xlarge	36	60
c5.large	2	4
c5.xlarge	4	8
c5.2xlarge	8	16
c5.4xlarge	16	32
c5.9xlarge	36	72
c5.12xlarge	48	96
c5.18xlarge	72	144
c5.24large	96	192
c5.metal	96	192
c5d.large	2	4
c5d.xlarge	4	8
c5d.2xlarge	8	16
c5d.4xlarge	16	32
c5d.9xlarge	36	72
c5d.12xlarge	48	96
c5d.18xlarge	72	144
c5d.24large	96	192
c5d.metal	96	192
c5n.large	2	5.25
c5n.xlarge	4	10.5

实例类型	默认 vCPU	内存 (GiB)
c5n.2xlarge	8	21
c5n.4xlarge	16	42
c5n.9xlarge	36	96
c5n.18xlarge	72	192
c5n.metal	72	192

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 实例类型](#)。

有关指定 CPU 选项的更多信息，请参阅 [优化 CPU 选项 \(p. 480\)](#)。

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。有些计算优化型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅[Amazon EBS 优化的实例 \(p. 863\)](#)。

有些计算优化型实例类型提供了在 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 \(p. 471\)](#)。

网络性能

您可以对受支持的实例类型启用增强联网功能。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 \(p. 616\)](#)。

使用 Elastic Network Adapter (ENA) 来增强网络的实例类型提供较高的每秒数据包数性能，并始终保持较低的延迟。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。使用 ENA 并且使用“最高 10 Gbps”或“最高 25 Gbps”的网络性能记录的实例大小使用一种网络 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。实例在网络带宽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。

以下是支持增强联网的计算优化型实例的网络性能摘要。

实例类型	网络性能	增强联网
c5.4xlarge 及更小 c5d.4xlarge 及更小	最高 10 Gbps	ENA (p. 617)
c5.9xlarge c5d.9xlarge	10Gbps	ENA (p. 617)
c5.12xlarge c5d.12xlarge	12 Gbps	ENA (p. 617)
c5n.4xlarge 和更小	最高 25 Gbps	ENA (p. 617)
c5.18xlarge c5.24xlarge c5.metal c5d.18xlarge c5d.24xlarge c5d.metal	25Gbps	ENA (p. 617)
c5n.9xlarge	50 Gbps	ENA (p. 617)
c5n.18xlarge c5n.metal	100 Gbps	ENA (p. 617)

实例类型	网络性能	增强联网
c4.large	中	Intel 82599 VF (p. 628)
c4.xlarge c4.2xlarge c4.4xlarge	高	Intel 82599 VF (p. 628)
c4.8xlarge	10Gbps	Intel 82599 VF (p. 628)

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，则您可以获得下表所列的 IOPS (4096 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	写入 IOPS
c5d.large *	20000	9,000
c5d.xlarge *	40000	18000
c5d.2xlarge *	80,000	37,000
c5d.4xlarge *	175000	75000
c5d.9xlarge	350,000	170,000
c5d.12xlarge	700,000	340,000
c5d.18xlarge	700,000	340,000
c5d.24xlarge	1400000	680,000
c5d.metal	1400000	680,000

* 对于这些实例，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保留空白间。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。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 \(p. 913\)](#)。

实例功能

计算优化型实例的功能汇总如下：

	仅限于 EBS	NVMe EBS	实例存储	置放群组
C4	是	否	否	是
C5	是	是	否	是
C5d	否	是	NVMe *	是
C5n	是	是	否	是

* 根设备卷必须是 Amazon EBS 卷。

有关更多信息，请参阅下列内容：

- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [置放群组 \(p. 662\)](#)

发行说明

- C4、C5、C5d 和 C5n 实例需要 64 位 EBS 支持的 HVM AMIs。它们具有高内存，需要 64 位操作系统才能利用这一容量。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。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- C5、C5d 和 C5n 实例具有以下要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。

以下 AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 `linux-aws` 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本
- C5、C5d 和 C5n 实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。每个实例至少附加 1 个网络接口。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- C5、C5d 和 C5n 实例要求安装 acpid 以通过 API 请求支持干净关闭。

- 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 实例请求表。](#)

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、R5、R5a、R5ad、R5d、R5dn 和 R5n 实例

这些实例非常适合以下应用：

- 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中数据库 (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。

`r5.metal` 和 `r5d.metal` 实例为应用程序提供对主机服务器的物理资源 (如处理器和内存) 的直接访问。这些实例非常适合：

- 需要访问虚拟环境中不可用或不完整支持的低级硬件功能 (如 Intel VT) 的工作负载
- 需要非虚拟化环境进行许可或支持的应用程序

有关更多信息，请参阅[Amazon EC2 R5 实例](#)。

内存增强型实例

内存增强型实例 (`u-6tb1.metal`、`u-9tb1.metal`、`u-12tb1.metal`、`u-18tb1.metal` 和 `u-24tb1.metal`) 为每个实例提供 6 TiB、9 TiB、12 TiB、18 TiB 和 24 TiB 内存。这些实例用于运行大型内存中数据库，包括 SAP HANA 的生产安装。它们通过直接访问主机硬件提供裸机性能。

X1 实例

这些实例非常适合以下应用：

- 内存中数据库，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。

有关更多信息，请参阅[Amazon EC2 X1 实例](#)。

X1e 实例

这些实例非常适合以下应用：

- 高性能数据库。
- 内存数据库，例如 SAP HANA。有关更多信息，请参阅[AWS 云上的 SAP HANA](#)。
- 内存密集型企业应用程序。

有关更多信息，请参阅[Amazon EC2 X1e 实例](#)。

z1d 实例

这些实例提供高计算能力和高内存容量，非常适合以下应用：

- 电子设计自动化 (EDA)
- 关系数据库工作负载

`z1d.metal` 实例为应用程序提供对主机服务器的物理资源 (如处理器和内存) 的直接访问。这些实例非常适合：

- 需要访问虚拟环境中不可用或不完整支持的低级硬件功能 (如 Intel VT) 的工作负载
- 需要非虚拟化环境进行许可或支持的应用程序

有关更多信息，请参阅 [Amazon EC2 z1d 实例](#)。

目录

- [硬件规格 \(p. 208\)](#)
- [内存性能 \(p. 211\)](#)
- [实例性能 \(p. 211\)](#)
- [网络性能 \(p. 211\)](#)
- [SSD I/O 性能 \(p. 212\)](#)
- [实例功能 \(p. 213\)](#)
- [支持 1 个 vCPU \(p. 214\)](#)
- [发行说明 \(p. 215\)](#)

硬件规格

以下是内存优化型实例的硬件规格摘要。

实例类型	默认 vCPU	内存 (GiB)
r4.large	2	15.25
r4.xlarge	4	30.5
r4.2xlarge	8	61
r4.4xlarge	16	122
r4.8xlarge	32	244
r4.16xlarge	64	488
r5.large	2	16
r5.xlarge	4	32
r5.2xlarge	8	64
r5.4xlarge	16	128
r5.8xlarge	32	256
r5.12xlarge	48	384

实例类型	默认 vCPU	内存 (GiB)
r5.16xlarge	64	512
r5.24xlarge	96	768
r5.metal	96	768
r5a.large	2	16
r5a.xlarge	4	32
r5a.2xlarge	8	64
r5a.4xlarge	16	128
r5a.8xlarge	32	256
r5a.12xlarge	48	384
r5a.16xlarge	64	512
r5a.24xlarge	96	768
r5ad.large	2	16
r5ad.xlarge	4	32
r5ad.2xlarge	8	64
r5ad.4xlarge	16	128
r5ad.12xlarge	48	384
r5ad.24xlarge	96	768
r5d.large	2	16
r5d.xlarge	4	32
r5d.2xlarge	8	64
r5d.4xlarge	16	128
r5d.8xlarge	32	256
r5d.12xlarge	48	384
r5d.16xlarge	64	512
r5d.24xlarge	96	768
r5d.metal	96	768
r5dn.large	2	16
r5dn.xlarge	4	32
r5dn.2xlarge	8	64
r5dn.4xlarge	16	128
r5dn.8xlarge	32	256

实例类型	默认 vCPU	内存 (GiB)
r5dn.12xlarge	48	384
r5dn.16xlarge	64	512
r5dn.24xlarge	96	768
r5n.large	2	16
r5n.xlarge	4	32
r5n.2xlarge	8	64
r5n.4xlarge	16	128
r5n.8xlarge	32	256
r5n.12xlarge	48	384
r5n.16xlarge	64	512
r5n.24xlarge	96	768
u-6tb1.metal	448 *	6,144
u-9tb1.metal	448 *	9,216
u-12tb1.metal	448 *	12,288
u-18tb1.metal	448 *	18432
u-24tb1.metal	448 *	24576
x1.16xlarge	64	976
x1.32xlarge	128	1,952
x1e.xlarge	4	122
x1e.2xlarge	8	244
x1e.4xlarge	16	488
x1e.8xlarge	32	976
x1e.16xlarge	64	1,952
x1e.32xlarge	128	3,904
z1d.large	2	16
z1d.xlarge	4	32
z1d.2xlarge	8	64
z1d.3xlarge	12	96
z1d.6xlarge	24	192
z1d.12xlarge	48	384
z1d.metal	48	384

* 每个逻辑处理器都是 224 个内核上的一个超线程。

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 实例类型](#)。

有关指定 CPU 选项的更多信息，请参阅 [优化 CPU 选项 \(p. 480\)](#)。

内存性能

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。

有关可以为内存优化型实例启用多少 RAM 的更多信息，请参阅 [硬件规格 \(p. 208\)](#)。

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。与内存优化型实例上的半虚拟化 (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 \(p. 87\)](#)。

实例性能

R4 实例具备多达 64 个虚拟 vCPU，采用两个基于 E5-2686v4 的 AWS 自定义 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。

X1e 和 X1 实例最多具有 128 个 vCPU 并采用 4 个 Intel Xeon E7-8880 v3 处理器（具有高内存带宽和更大的 L3 缓存）以提高内存中应用程序的性能。

内存增强型实例（`u-6tb1.metal`、`u-9tb1.metal` 和 `u-12tb1.metal`）是首款由 8 插槽平台提供支持的实例，该平台配备了针对关键任务型企业工作负载优化的最新一代 Intel Xeon Platinum 8176M (Skylake) 处理器。

具有 18 TB 和 24 TB 内存的内存增强型实例（`u-18tb1.metal` 和 `u-24tb1.metal`）是首款由配备第二代 Intel Xeon Scalable 8280L (Cascade Lake) 处理器的 8 插槽平台提供支持的实例。

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 \(p. 471\)](#)。

网络性能

您可以对受支持的实例类型启用增强联网功能。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 \(p. 616\)](#)。

使用 Elastic Network Adapter (ENA) 来增强网络的实例类型提供较高的每秒数据包数性能，并始终保持较低的延迟。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。使用 ENA 并且使用“最高 10 Gbps”或“最高 25 Gbps”的网络性能记录的实例大小使用一种网络 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。实例在网络带宽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。

以下是支持增强联网的内存优化型实例的网络性能摘要。

实例类型	网络性能	增强联网
<code>r4.4xlarge</code> 和更小 <code>r5.4xlarge</code> 和更小 <code>r5a.8xlarge</code> 和更小 <code>r5ad.4xlarge</code> 和更小 <code>r5d.4xlarge</code> 和更小 <code>x1e.8large</code> 和更小 <code>z1d.3xlarge</code> 和更小	最高 10 Gbps	ENA (p. 617)
<code>r4.8xlarge</code> <code>r5.8xlarge</code> <code>r5.12xlarge</code> <code>r5a.12xlarge</code> <code>r5ad.12xlarge</code>	10 Gbps	ENA (p. 617)

实例类型	网络性能	增强联网
r5d.8xlarge r5d.12xlarge x1.16xlarge x1e.16xlarge z1d.6xlarge		
r5a.16xlarge r5ad.16xlarge	12 Gbps	ENa (p. 617)
r5.16xlarge r5a.24xlarge r5ad.24xlarge r5d.16xlarge	20 Gbps	ENa (p. 617)
r5dn.4xlarge 及更小 r5n.4xlarge 及更小	最高 25 Gbps	ENa (p. 617)
r4.16xlarge r5.24xlarge r5.metal r5d.24xlarge r5d.metal r5dn.8xlarge r5n.8xlarge u-6tb1.metal u-9tb1.metal u-12tb1.metal x1.32xlarge x1e.32xlarge z1d.12xlarge z1d.metal	25Gbps	ENa (p. 617)
r5dn.12xlarge r5n.12xlarge	50 Gbps	ENa (p. 617)
r5dn.16xlarge r5n.16xlarge	75 Gbps	ENa (p. 617)
r5dn.24xlarge r5n.24xlarge u-18tb1.metal u-24tb1.metal	100 Gbps	ENa (p. 617)

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，则您可以获得下表所列的 IOPS (4096 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	写入 IOPS
r5ad.large *	30000	15000
r5ad.xlarge *	59,000	29,000
r5ad.2xlarge *	117,000	57,000
r5ad.4xlarge *	234,000	114,000
r5ad.12xlarge	700,000	340,000
r5ad.24xlarge	1400000	680,000
r5d.large *	30000	15000
r5d.xlarge *	59,000	29,000
r5d.2xlarge *	117,000	57,000
r5d.4xlarge *	234,000	114,000
r5d.8xlarge	466666	233333
r5d.12xlarge	700,000	340,000
r5d.16xlarge	933333	466666
r5d.24xlarge	1400000	680,000

实例大小	100% 随机读取 IOPS	写入 IOPS
r5d.metal	1400000	680,000
r5dn.large *	30000	15000
r5dn.xlarge *	59,000	29,000
r5dn.2xlarge *	117,000	57,000
r5dn.4xlarge *	234,000	114,000
r5dn.8xlarge	466666	233333
r5dn.12xlarge	700,000	340,000
r5dn.16xlarge	933333	466666
r5dn.24xlarge	1400000	680,000
z1d.large *	30000	15000
z1d.xlarge *	59,000	29,000
z1d.2xlarge *	117,000	57,000
z1d.3xlarge *	175000	75000
z1d.6xlarge	350,000	170,000
z1d.12xlarge	700,000	340,000
z1d.metal	700,000	340,000

* 对于这些实例，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保留空白间。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。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 \(p. 913\)](#)。

实例功能

内存优化型实例的功能汇总如下。

	仅限于 EBS	NVMe EBS	实例存储	置放群组
R4	是	否	否	是

	仅限于 EBS	NVMe EBS	实例存储	置放群组
R5	是	是	否	是
R5a	是	是	否	是
R5ad	否	是	NVME *	是
R5d	否	是	NVME *	是
R5dn	否	是	NVME *	是
R5n	是	是	否	是
u-6tb1.metal	是	是	否	否
u-9tb1.metal	是	是	否	否
u-12tb1.metal	是	是	否	否
u-18tb1.metal	是	是	否	否
u-24tb1.metal	是	是	否	否
X1	否	否	SSD	是
X1e	否	否	SSD *	是
z1d	否	是	NVME *	是

* 根设备卷必须是 Amazon EBS 卷。

有关更多信息，请参阅下列内容：

- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [置放群组 \(p. 662\)](#)

支持 个 vCPU

内存优化型实例具有大量虚拟 vCPU，可能会在虚拟 vCPU 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 2 \(HVM\)](#)
- [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 2019](#)
- [Windows Server 2016](#)
- [Windows Server 2012 R2](#)
- [Windows Server 2012](#)
- [Windows Server 2008 R2 64 位](#)
- [Windows Server 2008 SP2 64 位](#)

发行说明

- R5 和 R5d 实例配备了 3.1 GHz Intel Xeon Platinum 8000 系列处理器。
- R5a 和 R5ad 实例配备了 2.5 GHz AMD EPYC 7000 系列处理器。
- 以下是高内存、R5、R5a、R5ad、R5d、R5dn、R5n 和 z1d 实例的要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。

以下 AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 linux-aws 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本
- R5、R5a、R5ad、R5d、R5dn、R5n 和 z1d 实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。每个实例至少附加 1 个网络接口。例如，如果在仅限 EBS 的实例上没有附加其他网络接口，您可以附加 27 个 EBS 卷到该实例。
- u-6tb1.metal、u-9tb1.metal 和 u-12tb1.metal 实例支持最多 13 个 EBS 卷。u-18tb1.metal 和 u-24tb1.metal 实例支持最多 19 个 EBS 卷。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 除了 x1.16xlarge 实例之外，您无法使用 Windows Server 2008 SP2 64 位 AMI 启动 X1 实例。
- 您无法使用 Windows Server 2008 SP2 64 位 AMI 启动 X1e 实例。
- 对于 Windows Server 2008 R2 64 位 AMI 的早期版本，您无法启动 r4.large 和 r4.4xlarge 实例。如果遇到此问题，请更新至该 AMI 的最新版本。
- 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 实例请求表](#)。

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 实例非常适合以下应用程序：

- 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

H1 实例

H1 实例非常适合以下应用程序：

- 数据密集型工作负载，例如，MapReduce 和分布式文件系统
- 需要顺序访问直接附加的实例存储上的大量数据的应用程序
- 需要以高吞吐量方式访问大量数据的应用程序

I3 和 I3en 实例

这些实例非常适合以下应用：

- 高频率联机事务处理 (OLTP) 系统
- 关系数据库
- NoSQL 数据库
- 内存中数据库 (例如，Redis) 的缓存
- 数据仓库应用程序
- 分布式文件系统

裸机实例为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。这些实例非常适合：

- 需要访问虚拟环境中不可用或不完整支持的低级硬件功能（如 Intel VT）的工作负载
- 需要非虚拟化环境进行许可或支持的应用程序

有关更多信息，请参阅 [Amazon EC2 I3 实例](#)。

目录

- [硬件规格 \(p. 216\)](#)
- [实例性能 \(p. 217\)](#)
- [网络性能 \(p. 218\)](#)
- [SSD I/O 性能 \(p. 218\)](#)
- [实例功能 \(p. 219\)](#)
- [支持 1 个 vCPU \(p. 220\)](#)
- [发行说明 \(p. 221\)](#)

硬件规格

D2 实例的主要数据存储是 HDD 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 \(p. 903\)](#) 和 [SSD 实例存储卷 \(p. 912\)](#)。

以下是存储优化型实例的硬件规格摘要。

实例类型	默认 vCPU	内存 (GiB)
d2.xlarge	4	30.5
d2.2xlarge	8	61
d2.4xlarge	16	122
d2.8xlarge	36	244
h1.2xlarge	8	32
h1.4xlarge	16	64
h1.8xlarge	32	128
h1.16xlarge	64	256
i3.large	2	15.25
i3.xlarge	4	30.5
i3.2xlarge	8	61
i3.4xlarge	16	122
i3.8xlarge	32	244
i3.16xlarge	64	488
i3.metal	72	512
i3en.large	2	16
i3en.xlarge	4	32
i3en.2xlarge	8	64
i3en.3xlarge	12	96
i3en.6xlarge	24	192
i3en.12xlarge	48	384
i3en.24xlarge	96	768
i3en.metal	96	768

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 实例类型](#)。

有关指定 CPU 选项的更多信息，请参阅 [优化 CPU 选项 \(p. 480\)](#)。

实例性能

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 2 或 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。有些存储优化型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅[Amazon EBS 优化的实例 \(p. 863\)](#)。

有些存储优化型实例类型提供了在 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 \(p. 471\)](#)。

网络性能

您可以对受支持的实例类型启用增强联网功能。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 \(p. 616\)](#)。

使用 Elastic Network Adapter (ENA) 来增强网络的实例类型提供较高的每秒数据包数性能，并始终保持较低的延迟。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。使用 ENA 并且使用“最高 10 Gbps”或“最高 25 Gbps”的网络性能记录的实例大小使用一种网络 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。实例在网络带宽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。

以下是支持增强联网的存储优化型实例的网络性能摘要。

实例类型	网络性能	增强联网
i3.4xlarge 和更小	最高 10 Gbps，使用网络 I/O 积分机制	ENA (p. 617)
i3.8xlarge h1.8xlarge	10Gbps	ENA (p. 617)
i3en.3xlarge 和更小	最高 25 Gbps，使用网络 I/O 积分机制	ENA (p. 617)
i3.16xlarge i3.metal i3en.6xlarge h1.16xlarge	25 Gbps	ENA (p. 617)
i3en.12xlarge	50 Gbps	ENA (p. 617)
i3en.24xlarge	100 Gbps	ENA (p. 617)
d2.xlarge	中	Intel 82599 VF (p. 628)
d2.2xlarge d2.4xlarge	高	Intel 82599 VF (p. 628)
d2.8xlarge	10Gbps	Intel 82599 VF (p. 628)

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，则您可以获得下表所列的 IOPS (4096 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	写入 IOPS
i3.large *	100,125	35000

实例大小	100% 随机读取 IOPS	写入 IOPS
i3.xlarge *	206,250	70,000
i3.2xlarge	412,500	180,000
i3.4xlarge	825,000	360,000
i3.8xlarge	1.65 百万	720,000
i3.16xlarge	3.3 百万	1.4 百万
i3.metal	3.3 百万	1.4 百万
i3en.large *	42,500	32,500
i3en.xlarge *	85,000	65,000
i3en.2xlarge *	170,000	130,000
i3en.3xlarge	250,000	200,000
i3en.6xlarge	500,000	400,000
i3en.12xlarge	1,000,000	800,000
i3en.24xlarge	2,000,000	1,600,000
i3en.metal	2,000,000	1,600,000

* 对于这些实例，您最多可获得指定的性能。

在填充基于 SSD 的实例存储卷时，您获得的 I/O 性能将会下降。这是因为，SSD 控制器必须执行额外的工作以查找可用的空间，重写现有的数据，以及擦除未使用的空间以进行重写。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保留空白间。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。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 \(p. 913\)](#)。

实例功能

存储优化型实例的功能汇总如下：

	仅限于 EBS	实例存储	置放群组
D2	否	HDD	是
H1	否	HDD *	是

	仅限于 EBS	实例存储	置放群组
I3	否	NVMe *	是
I3en	否	NVMe *	是

* 根设备卷必须是 Amazon EBS 卷。

有关更多信息，请参阅下列内容：

- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [置放群组 \(p. 662\)](#)

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 vCPU 的 d2.8xlarge 实例：

- Amazon Linux 2 (HVM)
- Amazon Linux AMI 2018.03 (HVM)
- Ubuntu Server 14.04 LTS (HVM) 或更高版本
- 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 stopped 状态转换原因而更改为 Client.InstanceInitiatedShutdown），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。

发行说明

- 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 \(p. 87\)](#)。
- 以下是 i3en 和 i3.meta1 实例的要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。

以下 AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 linux-aws 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本
- 启动 i3.meta1 实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 如果是 FreeBSD AMI，裸机实例需要近 1 小时才能启动，并且不能完成到本地 NVMe 存储的 I/O。解决方法是将下面的代码行添加到 /boot/loader.conf 并重启：

```
hw.nvme.per_cpu_io_queues="0"
```

- 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 \(p. 220\)](#)。

- 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 实例请求表](#)。

Linux 加速计算实例

如果您需要高处理能力，您可以从使用加速计算实例中获益，这些实例可让您访问基于硬件的计算加速器，如图形处理单元 (GPU) 或现场可编程门阵列 (FPGA)。加速计算实例能在计算密集型工作负载上提供更高的并行度，以实现更高的吞吐量。

基于 GPU 的实例能让您访问具有数千个计算内核的 NVIDIA GPU。可以通过基于 GPU 的加速计算实例来利用 CUDA 或开放计算语言 (OpenCL) 并行计算框架，从而为科学、工程和渲染应用程序加速。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。

基于 FPGA 的实例能让您访问具有数百万并行系统逻辑单元格的 FPGA。您可以通过基于 FPGA 的加速计算实例，利用定义自硬件加速来加速工作负载，例如基因组学、财务分析、实时视频处理、大数据分析和安全工作负载。您可以使用硬件描述语言 (如 Verilog 或 VHDL) 或使用更高级语言 (如 OpenCL 并行计算框架) 来开发这些加速。您可以开发自己的硬件加速代码或通过[AWS Marketplace](#) 购买硬件加速。

Important

基于 FPGA 的实例不支持 Microsoft Windows。

您可以将加速计算实例放入集群置放群组中。集群置放群组可在单个可用区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 \(p. 662\)](#)。

目录

- [加速计算实例系列 \(p. 222\)](#)
- [硬件规格 \(p. 224\)](#)
- [实例性能 \(p. 225\)](#)
- [网络性能 \(p. 225\)](#)
- [实例功能 \(p. 225\)](#)
- [发行说明 \(p. 226\)](#)
- [适用于基于 GPU 的加速计算实例的 AMI \(p. 226\)](#)
- [在 Linux 实例上安装 NVIDIA 驱动程序 \(p. 227\)](#)
- [在 G3 实例上激活 NVIDIA GRID 虚拟应用 \(p. 231\)](#)
- [优化 GPU 设置 \(p. 231\)](#)
- [FPGA 开发入门 \(p. 232\)](#)
- [AWS Inferentia 开发入门 \(p. 232\)](#)

有关 Windows 加速计算实例的信息，请参阅 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、图形处理或数据模式匹配，比在 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。

F1 实例

F1 实例使用 Xilinx UltraScale+ VU9P FPGA 并且专用于加快计算密集型算法，例如不适合通用型 CPU 的数据流或高度并行操作。F1 实例中的每个 FPGA 包含大约 250 万个逻辑单元和大约 6800 个数字信号处理

(DSP) 引擎，连同 64 GiB 的本地 DDR ECC 保护内存一起，通过专用 PCIe Gen3 x16 连接与实例相连。F1 实例提供本地 NVMe SSD 卷。

开发人员可以使用 FPGA 开发人员 AMI 和 AWS 硬件开发人员工具包来创建用于 F1 实例的自定义硬件加速。FPGA 人员开发 AMI 包括云中的用于全周期 FPGA 开发的开发工具。使用这些工具，开发人员可以创建和分享 Amazon FPGA 映像 (AFI)，这些映像可以加载到 F1 实例的 FPGA 上。

有关更多信息，请参阅 [Amazon EC2 F1 实例](#)。

P3 实例

P3 实例使用 NVIDIA Tesla V100 GPU，可用于使用 CUDA 或 OpenCL 编程模型或通过机器学习框架进行的通用 GPU 计算。P3 实例提供了高带宽网络、强大的半精度\单精度\双精度浮点功能以及每 GPU 最高 32 GiB 内存，非常适合用于深度学习、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。Tesla V100 GPU 不支持图形模式。有关更多信息，请参阅 [Amazon EC2 P3 实例](#)。

P3 实例支持 NVIDIA NVLink 对等传输。

要查看有关系统的拓扑信息，请运行以下命令：

```
nvidia-smi topo -m
```

有关更多信息，请参阅 [NVIDIA NVLink](#)。

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 NVIDIA GPUDirect 对等传输。

要查看有关系统的拓扑信息，请运行以下命令：

```
nvidia-smi topo -m
```

有关更多信息，请参阅 [NVIDIA GPUDirect](#)。

G4 实例

G4 实例使用 NVIDIA Tesla GPU，并为使用 CUDA 或机器学习框架的通用 GPU 计算以及使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。G4 实例提供高带宽网络、强大的半精度和单精度浮点功能以及 INT8 和 INT4 精度。每个 GPU 具有 16 GiB GDDR6 内存，从而使 G4 实例非常适合机器学习推理、视频转码以及图形应用程序，例如，远程图形工作站和云中的游戏流。

G4 实例支持 NVIDIA GRID 虚拟工作站。有关更多信息，请参阅 [NVIDIA Marketplace 产品](#)。

G3 实例

G3 实例使用 NVIDIA Tesla M60 GPU，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。G3 实例还提供 NVIDIA GRID 虚拟工作站功能（如 4 个分辨率高达 4096x2160 的监视器）以及 NVIDIA GRID 虚拟应用程序。G3 实例非常适合一些应用程序，例如，3D 可视化、图形密集型远程工作站、3D 渲染、视频编码、虚拟现实以及其他需要大量并行处理能力的服务器端图形工作负载。

G3 实例支持 NVIDIA GRID 虚拟工作站和 NVIDIA GRID 虚拟应用程序。要激活任一功能，请参阅 [在 G3 实例上激活 NVIDIA GRID 虚拟应用 \(p. 231\)](#)。

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。

硬件规格

以下是加速计算实例的硬件规格摘要。

实例类型	默认 vCPU	内存 (GiB)	加速器
p2.xlarge	4	61	1
p2.8xlarge	32	488	8
p2.16xlarge	64	732	16
p3.2xlarge	8	61	1
p3.8xlarge	32	244	4
p3.16xlarge	64	488	8
p3dn.24xlarge	96	768	8
g2.2xlarge	8	15	1
g2.8xlarge	32	60	4
g3s.xlarge	4	30.5	1
g3.4xlarge	16	122	1
g3.8xlarge	32	244	2
g3.16xlarge	64	488	4
g4dn.xlarge	4	16	1
g4dn.2xlarge	8	32	1
g4dn.4xlarge	16	64	1
g4dn.8xlarge	32	128	1
g4dn.12xlarge	48	192	4
g4dn.16xlarge	64	256	1
f1.2xlarge	8	122	1
f1.4xlarge	16	244	2
f1.16xlarge	64	976	8

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 实例类型](#)。

有关指定 CPU 选项的更多信息，请参阅 [优化 CPU 选项 \(p. 480\)](#)。

实例性能

您可以执行多个 GPU 设置优化，以实现实例的最佳性能。有关更多信息，请参阅[优化 GPU 设置 \(p. 231\)](#)。

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。有些加速计算实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅[Amazon EBS 优化的实例 \(p. 863\)](#)。

一些加速计算实例类型提供了在 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 \(p. 471\)](#)。

网络性能

您可以对受支持的实例类型启用增强联网功能。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 \(p. 616\)](#)。

使用 Elastic Network Adapter (ENA) 来增强网络的实例类型提供较高的每秒数据包数性能，并始终保持较低的延迟。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。使用 ENA 并且使用“最高 10 Gbps”或“最高 25 Gbps”的网络性能记录的实例大小使用一种网络 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。实例在网络带宽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。

以下是支持增强联网的加速计算实例的网络性能摘要。

实例类型	网络性能	增强联网
f1.2xlarge f1.4xlarge g3.4xlarge p3.2xlarge	最高 10 Gbps	ENAs (p. 617)
g3s.xlarge g3.8xlarge p2.8xlarge p3.8xlarge	10Gbps	ENAs (p. 617)
g4dn.xlarge g4dn.2xlarge g4dn.4xlarge	最高 25 Gbps	ENAs (p. 617)
f1.16xlarge g3.16xlarge p2.16xlarge p3.16xlarge	25 Gbps	ENAs (p. 617)
g4dn.8xlarge g4dn.12xlarge g4dn.16xlarge	50 Gbps	ENAs (p. 617)
p3dn.24xlarge	100 Gbps	ENAs (p. 617)

实例功能

加速计算实例的特性汇总如下。

	仅限于 EBS	NVMe EBS	实例存储	置放群组
G2	否	否	SSD	是
G3	是	否	否	是

	仅限于 EBS	NVMe EBS	实例存储	置放群组
G4	否	是	NVMe *	是
P2	是	否	否	是
P3	p3dn.24xlarge : 不支持 所有其他大小 : 是	p3dn.24xlarge : 是 所有其他大小 : 否	p3dn.24xlarge : NVMe*	是
F1	否	否	NVMe *	是

* 根设备卷必须是 Amazon EBS 卷。

有关更多信息，请参阅下列内容：

- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [置放群组 \(p. 662\)](#)

发行说明

- 您必须使用 HVM AMI 启动实例。
- 以下是 G4 实例的要求：
 - 必须安装有 NVMe 驱动程序。EBS 卷显示为 [NVMe 块储存设备 \(p. 860\)](#)。
 - 必须安装有 Elastic Network Adapter ([ENA \(p. 617\)](#)) 驱动程序。

以下 AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 `linux-aws` 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本
- 除非安装了 NVIDIA 驱动程序，否则基于 GPU 的实例无法访问 GPU。有关更多信息，请参阅在 [Linux 实例上安装 NVIDIA 驱动程序 \(p. 227\)](#)。
- 每个区域仅限 100 个 AFI。
- 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](#)。

适用于基于 GPU 的加速计算实例的 AMI

为了帮助您开始使用，NVIDIA 和其他公司为基于 GPU 的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。

有关包含 NVIDIA 驱动程序的 AMI 的列表，请搜索 AWS Marketplace，如下所示：

- [NVIDIA P3 AMIs](#)

- NVIDIA Quadro 虚拟工作站 P3 AMI
- NVIDIA P2 AMIs
- NVIDIA GRID G4 AMI
- NVIDIA GRID G3 AMI
- NVIDIA GRID G2 AMI

您可以使用任意 HVM AMI 启动加速计算实例。

Important

这些 AMI 包含由 NVIDIA Corporation 开发、拥有或提供的驱动程序、软件或工具包。使用这些 AMI 即表明您同意仅在包含 NVIDIA 硬件的 Amazon EC2 实例上使用这些 NVIDIA 驱动程序、软件或工具包。

您也可以安装 NVIDIA 驱动程序。有关更多信息，请参阅在 [Linux 实例上安装 NVIDIA 驱动程序 \(p. 227\)](#)。

在 Linux 实例上安装 NVIDIA 驱动程序

基于 GPU 的加速计算实例必须具有相应的 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。

根据实例类型，您可以下载公共 NVIDIA 驱动程序、使用 NVIDIA Marketplace 产品或者从仅对 AWS 客户可用的 Amazon S3 下载驱动程序。

目录

- [公有 NVIDIA 驱动程序 \(p. 227\)](#)
- [适用于 G4 实例的 NVIDIA GRID 驱动程序 \(p. 228\)](#)
- [适用于 G3 实例的 NVIDIA GRID 驱动程序 \(p. 228\)](#)
- [手动安装 NVIDIA 驱动程序 \(p. 229\)](#)
- [使用替代 NVIDIA 驱动程序 \(p. 231\)](#)

公有 NVIDIA 驱动程序

如果是 G3 以外的实例类型，或者您没有在 G3 实例上使用 NVIDIA GRID 功能，您可以下载公有 NVIDIA 驱动程序。

从 <http://www.nvidia.com/Download/Find.aspx> 下载适合您的实例类型的 64 位 NVIDIA 驱动程序。

实例	产品类型	产品系列	产品
G2	GRID	GRID 系列	GRID K520
G4 †	Tesla	T 系列	T4 (418 或更高版本)
P2	Tesla	E 系列	K-80
P3	Tesla	V 系列	V100

† G4 实例需要驱动程序版本 418.87 或更高版本。

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。

适用于 G4 实例的 NVIDIA GRID 驱动程序

可以通过两种方法将 NVIDIA GRID 软件用于 G4 实例上的图形应用程序。您可以下载预装了 GRID 的 AMI，或者从 Amazon S3 下载 NVIDIA GRID vGaming 驱动程序，并将其安装在 G4 实例上。

选项1：将具有 GRID 的 AMI 用于 G4 实例

要查找 AMI，请使用以下链接：[NVIDIA Marketplace 产品](#)。

选项 2：下载 NVIDIA GRID vGaming 驱动程序

此驱动程序仅对 AWS 客户可用。一经下载，即表明您同意仅使用下载的软件开发用于 NVIDIA Tesla T4 硬件的 AMIs。安装软件时，您需要遵循 [NVIDIA GRID Cloud 最终用户许可协议](#) 条款。

如果拥有 GRID 许可证，您应该能够在 G4 实例上使用这些许可证。有关更多信息，请参阅 [NVIDIA GRID 软件快速入门指南](#)。

使用以下过程安装此驱动程序。

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装它们）。
2. 使用以下命令从 Amazon S3 下载并安装 NVIDIA GRID 驱动程序安装实用程序。

```
[ec2-user ~]$ curl -o NVIDIA.run https://s3.amazonaws.com/nvidia-gaming/NVIDIA-Linux-x86_64-435.22-grid.run
```

3. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA.run
```

4. 使用以下命令运行安装程序。

```
[ec2-user ~]$ sudo ./NVIDIA.run
```

5. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

6. 使用以下命令下载并重命名认证文件。

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://s3.amazonaws.com/nvidia-gaming/GridSwCert-Linux.cert"
```

7. 重新启动您的实例。

适用于 G3 实例的 NVIDIA GRID 驱动程序

对于 G3 实例，您可以使用 AWS CLI 或开发工具包从 Amazon S3 下载 NVIDIA GRID 驱动程序。要安装 AWS CLI，请参阅 AWS Command Line Interface 用户指南 中的[安装 AWS Command Line Interface](#)。请务必配置 AWS CLI 以使用您的 AWS 凭证。有关更多信息，请参阅 AWS Command Line Interface 用户指南中的[快速配置](#)。

Important

此下载仅对 AWS 客户可用。下载即表明您同意仅将下载的软件用于开发在 NVIDIA Tesla M60 硬件上使用的 AMIs。安装软件时，您需要遵循 [NVIDIA GRID Cloud 最终用户许可协议](#) 条款。

使用以下 AWS CLI 命令下载最新驱动程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

此存储桶中存储了多个版本的 NVIDIA GRID 驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

手动安装 NVIDIA 驱动程序

如果您使用的是没有所需 NVIDIA 驱动程序的 AMI，则可以在您的实例上安装该驱动程序。

安装 NVIDIA 驱动程序

1. 更新软件包缓存并获取实例的必需软件包更新。

- 对于 Amazon Linux、CentOS 和 Red Hat Enterprise Linux：

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

- 对于 Ubuntu 和 Debian：

```
[ec2-user ~]$ sudo apt-get update -y
```

2. (Ubuntu 16.04 和更高版本，带有 linux-aws 软件包) 升级 linux-aws 软件包以接收最新版本。

```
[ec2-user ~]$ sudo apt-get upgrade -y linux-aws
```

3. 重启实例以加载最新内核版本。

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

4. 重启之后重新连接到实例。

5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

- 对于 Amazon Linux、CentOS 和 Red Hat Enterprise Linux：

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

- 对于 Ubuntu 和 Debian：

```
[ec2-user ~]$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

6. 禁用 NVIDIA 显卡的 nouveau 开源驱动程序。

- 将 nouveau 添加到 /etc/modprobe.d/blacklist.conf 黑名单文件。复制下面的代码块并将其粘贴到终端中。

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- 编辑 /etc/default/grub 文件并添加以下行：

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. 重新生成 Grub 配置。

- 对于 CentOS 和 Red Hat Enterprise Linux :

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- 对于 Ubuntu 和 Debian :

```
[ec2-user ~]$ sudo update-grub
```

7. 按照以下步骤下载之前确定的驱动程序包。

- 对于 P2 和 P3 实例 , 可通过以下命令下载 NVIDIA 驱动程序 , 其中 xxx.xxx 代表 NVIDIA 驱动程序的版本。

```
[ec2-user ~]$ wget http://us.download.nvidia.com/tesla/xxx.xxx/NVIDIA-Linux-x86_64-xxx.xxx.run
```

- 对于 G2 实例 , 可通过以下命令下载 NVIDIA 驱动程序 , 其中 xxx.xxx 代表 NVIDIA 驱动程序的版本。

```
[ec2-user ~]$ wget http://us.download.nvidia.com/XFree86/Linux-x86_64/xxx.xxx/NVIDIA-Linux-x86_64-xxx.xxx.run
```

- 对于 G3 实例 , 您可以使用 AWS CLI 或开发工具包从 Amazon S3 下载驱动程序。要安装 AWS CLI , 请参阅 AWS Command Line Interface 用户指南 中的[安装 AWS Command Line Interface](#)。使用以下 AWS CLI 命令下载最新驱动程序 :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Important

此下载仅对 AWS 客户可用。下载即表明您同意仅将下载的软件用于开发在 NVIDIA Tesla M60 硬件上使用的 AMIs。安装软件时 , 您需要遵循 [NVIDIA GRID Cloud 最终用户许可协议](#) 条款。

此存储桶中存储了多个版本的 NVIDIA GRID 驱动程序。您可以使用以下命令查看所有可用的版本 :

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. 运行自安装脚本 , 安装您在上一个步骤中下载的 NVIDIA 驱动程序。例如 :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

系统提示时 , 接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

9. 重启实例。

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

10. 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
```

11. [仅限 G3 实例] 要启用 NVIDIA GRID 虚拟应用，请完成 [在 G3 实例上激活 NVIDIA GRID 虚拟应用 \(p. 231\)](#) 中的 GRID 激活步骤（默认情况下启用 NVIDIA GRID 虚拟工作站）。
12. 完成[优化 GPU 设置 \(p. 231\)](#)中的优化步骤以实现 GPU 的最佳性能。

使用替代 NVIDIA 驱动程序

Amazon 在 AWS Marketplace 中针对每次官方内核升级向 AMIs 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。

使用该命令卸载 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。

在 G3 实例上激活 NVIDIA GRID 虚拟应用

要激活 G3 实例上的 GRID 虚拟应用程序（默认情况下启用 NVIDIA GRID 虚拟工作站），您必须为注册表 /etc/nvidia/gridd.conf 中文件 定义产品类型。

激活 GRID 虚拟应用程序

1. 从提供的模板文件创建 /etc/nvidia/gridd.conf 文件。

```
[ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

2. 在您常用的文本编辑器中打开 /etc/nvidia/gridd.conf 文件。
3. 找到 FeatureType 行，并将其设置为 0。然后，添加包含 IgnoreSP=TRUE 的行。

```
FeatureType=0
IgnoreSP=TRUE
```

4. 保存文件并退出。
5. 重启实例以接受新配置。

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

优化 GPU 设置

您可以执行几种 GPU 设置优化，以便在 G3、G4、P2、P3 和 P3dn 实例上实现最佳性能。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 GPU 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。

优化 GPU 设置

1. 将 GPU 设置配置为永久。该命令可能需要几分钟才能运行完毕。

```
[ec2-user ~]$ sudo nvidia-persistenced
```

- 禁用实例上所有 GPU 的 autoboot 功能。

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

Note

P3、P3dn 和 G4 实例上的 GPU 不支持 autoboot。

- 将所有 GPU 时钟速度设置为其最大频率。使用以下命令中指定的内存和图形时钟速度。

Note

NVIDIA 驱动程序的某些版本不允许设置应用程序时钟速度，并且将引发 "Setting applications clocks is not supported for GPU ..." 错误 (可忽略)。

- G3 实例：

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

- G4 实例：

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- P2 实例：

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- P3 和 P3dn 实例：

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

FPGA 开发入门

[FPGA 开发人员 AMI](#) 提供了用于开发、测试和构建 AFI 的工具。您可以在任何具有至少 32 GB 系统内存的 EC2 实例上使用 FPGA 开发人员 AMI (例如，C5、M4 和 R4 实例)。

有关更多信息，请参阅 [AWS FPGA 硬件开发人员工具包](#) 的文档。

AWS Inferentia 开发入门

[AWS Deep Learning AMI](#) 提供了使用 AWS Inferentia 开发、测试和构建机器学习应用程序的工具。您可以在任何 Amazon EC2 Inf1 实例上使用深度学习 AMI 进行 AWS Inferentia 开发。

有关更多信息，请参阅 [AWS Neuron](#) 的文档。

查找实例类型

您必须先选择要使用的实例类型，然后才能启动实例。根据将启动的实例的要求，所选的实例类型可能会有所不同。例如，您可能需要考虑以下要求：

- 区域
- 架构：32 位 (i386)、64 位 (x86_64) 或 64 位 ARM (arm64)

- 计算
- 内存
- 存储
- 网络性能

使用 Amazon EC2 控制台查找实例类型

您可以使用 Amazon EC2 控制台查找实例类型。您可以使用 Instance Types (实例类型) 页面搜索所有可用的实例类型。

1. 打开 [Amazon EC2 控制台](#)。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 在导航窗格中，选择 Instance Types (实例类型)。
4. (可选) 选择首选项图标以选择要显示的实例类型属性，例如按需 Linux 定价。或者，您也可以从列表中选择一种实例类型，然后在 Details (详细信息) 窗格中查看所有属性。
5. (可选) 使用 Filter (筛选条件) 选项限定显示的实例类型列表范围，以仅查看您感兴趣的实例类型。例如，您可以列出具有超过 8 个 vCPU 并支持休眠的所有实例类型。
6. (可选) 选择多种实例类型以在 Details (详细信息) 窗格中并排查看所有属性的比较结果。
7. (可选) 要保存实例类型列表以进行进一步检查，请选择 Download list (CSV) (下载列表 (CSV))。将下载一个逗号分隔值 (.csv) 格式的文件。该文件包含与您设置的筛选条件 (如果有) 以及表中显示的所有属性匹配的所有实例类型。

使用 AWS CLI 查找实例类型

您可以在 Amazon EC2 中使用 AWS CLI 命令，以仅列出满足您需求的实例类型。在找到满足您需求的实例类型后，请记下该类型，以便使用它启动实例。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](#)。

`describe-instance-types` 命令支持筛选参数。例如，您可以使用以下筛选条件，以仅显示具有 48 个 vCPU 的实例类型。

```
aws ec2 describe-instance-types --filters "Name=vcpu-info.default-vcpus,Values=48"
```

`describe-instance-type-offerings` 命令支持筛选参数。例如，您可以使用 `--location-type` 参数显示在可用区中提供的实例类型。

```
aws ec2 describe-instance-type-offerings --location-type "availability-zone"
```

您可以将以下筛选条件添加到上一个命令中，以仅显示在 us-east-1a 可用区中提供的实例类型。

```
--filters "Name=location,Values=us-east-1a"
```

更改实例类型

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，您可将其更改为适合工作负载的其他实例类型。

您可能还想从上一代实例类型迁移到最新一代实例类型以利用某些功能，例如 IPv6 支持。

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 \(p. 85\)](#)。

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。对于支持 NVMe 实例存储卷（默认情况下可用）的实例类型，调整大小的实例可能具有其他实例存储卷，具体取决于 AMI。否则，您可以手动将应用程序迁移到具有新实例类型的实例，并指定启动新实例时所需的实例存储卷数。

目录

- [调整大小的实例的兼容性 \(p. 234\)](#)
- [调整由 Amazon EBS 支持的实例的大小 \(p. 235\)](#)
- [迁移实例存储支持的实例 \(p. 235\)](#)
- [迁移到新的实例配置 \(p. 236\)](#)

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 \(p. 87\)](#)。要查看实例的虚拟化类型，请在 Amazon EC2 控制台中查看 Instances (实例) 屏幕的详细信息窗格中的 Virtualization (虚拟化) 字段。
- **Architecture (架构)**：AMI 特定于处理器的架构，因此您必须选择与当前实例类型具有相同处理器架构的实例类型。例如：
 - A1 实例是支持基于 Arm 架构的处理器的唯一实例。如果您要调整其处理器基于 Arm 架构的实例类型的大小，将限于支持基于 Arm 架构的处理器的实例类型。
 - 只有以下实例类型支持 32 位 AMIs : 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。
- **Network (网络)**：较新的实例类型只能在 VPC 中启动。因此，您不能将 EC2-Classic 平台中的实例的大小调整为仅在 VPC 中可用的实例类型，除非您有非默认 VPC。要查看您的实例是否在 VPC 中，请在 Amazon EC2 控制台中查看 Instances (实例) 屏幕的详细信息窗格中的 VPC ID 值。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 \(p. 689\)](#)。
- **增强联网**：支持 [增强联网 \(p. 616\)](#) 的实例类型需要安装必要的驱动程序。例如，A1, C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d 实例类型需要由 EBS 提供支持且安装有 Elastic Network Adapter (ENA) 驱动程序的 AMI。要将现有实例大小调整为支持增强联网的实例类型，则必须先相应地在实例上安装 [ENa 驱动程序 \(p. 617\)](#) 或 [ixgbevf 驱动程序 \(p. 628\)](#)。
- **NVMe**：在 [基于 Nitro 的实例 \(p. 163\)](#) 上，EBS 卷显示为 NVMe 块储存设备。如果将实例类型不支持 NVMe 的实例的大小调整为支持 NVMe 的实例类型，您必须先在实例上安装 [NVMe 驱动程序 \(p. 860\)](#)。此外，您在块储存设备映射中指定的设备的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。因此，要使用 `/etc/fstab` 在启动时挂载文件系统，必须使用 UUID/标签而非设备名称。
- **AMI**：有关支持增强联网和 NVMe 的实例类型所需的 AMI 的信息，请参阅以下文档中的发行说明：
 - [通用实例 \(p. 166\)](#)
 - [计算优化型实例 \(p. 202\)](#)
 - [内存优化型实例 \(p. 207\)](#)

- 存储优化型实例 (p. 215)

调整由 Amazon EBS 支持的实例的大小

您必须先停止由 Amazon EBS 支持的实例，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。
- 如果您的实例处于 Auto Scaling 组中，则 Amazon EC2 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，为组暂停扩展流程。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的[暂停和恢复扩展流程](#)。
- 如果您的实例位于[集群置放群组 \(p. 662\)](#)中，并且在更改实例类型后，实例启动失败，请尝试以下操作：停止集群置放群组中的所有实例，更改受影响实例的实例类型，然后重启集群置放群组中的所有实例。
- 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 \(p. 445\)](#)。

按照以下过程使用 AWS 管理控制台 调整由 Amazon EBS 支持的实例的大小。

调整由 Amazon EBS 支持的实例的大小

1. (可选) 如果新实例类型需要现有实例上未安装的驱动程序，您必须先连接到您的实例并安装驱动程序。有关更多信息，请参阅[调整大小的实例的兼容性 \(p. 234\)](#)。
2. 打开 Amazon EC2 控制台。
3. 在导航窗格中，选择 Instances。
4. 选择所需实例，然后依次选择 Actions、Instance State、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。
6. 在实例处于选中状态时，依次选择 Actions、Instance Settings 和 Change Instance Type。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）。有关更多信息，请参阅[调整大小的实例的兼容性 \(p. 234\)](#)。
 - b. (可选) 如果您选择的实例类型支持 EBS 优化，则选择 EBS-optimized (EBS 优化) 以启用 EBS 优化，或者取消选择 EBS-optimized (EBS 优化) 以禁用 EBS 优化。如果您选择的实例类型默认情况下已经过 EBS 优化，则 EBS 优化已选中，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. (问题排查) 如果您的实例未启动，则可能是新实例类型的某一要求未满足。有关更多信息，请参阅[为什么我的 Linux 实例在更改其类型后无法启动？](#)

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. 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 \(p. 815\)](#)) 或从实例中分离卷，以便您之后可以将其附加到新的实例 (请参阅 [将 Amazon EBS 卷与实例分离 \(p. 810\)](#))。
2. 通过满足先决条件并按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中的过程执行，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。
3. 打开 Amazon EC2 控制台并在导航窗格中选择 AMI。从筛选条件列表中，选择我拥有的，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

如果没有看到上一步创建的 AMI，请确保您已选择在其中创建了 AMI 的区域。

4. 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。

实例进入 running 状态可能需要几分钟时间。

5. (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 (操作)、Instance State (实例状态) 和 Terminate (终止)。

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：

将您的应用程序迁移到兼容实例

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 \(p. 815\)](#)) 或从实例中分离卷，以便您之后可以将其附加到新实例 (请参阅 [将 Amazon EBS 卷与实例分离 \(p. 810\)](#))。
2. 启动新实例，选择下列内容：
 - HVM AMI。
 - 仅限 HVM 的实例类型。
 - 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附加到新实例的任何 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，然后依次选择操作和取消关联地址。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，依次选择操作和关联地址。
 - 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 (操作)、Instance State (实例状态) 和 Terminate (终止)。

获取实例类型建议

AWS 计算优化器 提供了 Amazon EC2 实例建议，以帮助您提高性能和/或节省资金。您可以根据这些建议来决定是否移动到新的实例类型。

为了生成建议，Compute Optimizer 会分析现有实例规范和利用率指标。然后，利用已编译数据来建议哪些 Amazon EC2 实例类型能够最好地处理现有工作负载。建议随每小时实例定价一起返回。

本主题概述了如何通过 Amazon EC2 控制台查看建议。有关更多信息，请参阅[AWS 计算优化器 用户指南](#)。

Note

要从 Compute Optimizer 中获取建议，您必须首先选择加入 Compute Optimizer。有关更多信息，请参阅 AWS 计算优化器 用户指南 中的 [AWS Compute Optimizer 入门](#)。

目录

- [限制 \(p. 237\)](#)
- [结果 \(p. 237\)](#)
- [查看建议 \(p. 237\)](#)
- [评估建议时的注意事项 \(p. 238\)](#)

限制

Compute Optimizer 目前为 M、C、R、T 和 X 实例类型生成建议。Compute Optimizer 不会考虑其他实例类型。如果您使用的是其他实例类型，则不会在 Compute Optimizer 建议视图中列出它们。有关这些实例类型及其他实例类型的信息，请参阅[实例类型 \(p. 160\)](#)。

结果

Compute Optimizer 将其对 EC2 实例的调查结果分类为：

- 预配置不足 – 当您的实例的至少一个规格（如 CPU、内存或网络）没有满足工作负载的性能要求时，将 EC2 实例视为预配置不足。预配置不足的 EC2 实例可能会导致应用程序性能较差。
- 过度预配置 – 当您的实例的至少一个规格（如 CPU、内存或网络）可缩小但仍能满足工作负载的性能要求时，并且没有任何规格处于预配置不足状态时，将 EC2 实例视为过度预配置。过度预配置的 EC2 实例可能会导致不必要的基础设施成本。
- 已优化 – 当您的实例的所有规格（如 CPU、内存和网络）满足工作负载的性能要求且实例未处于过度预配置状态时，将 EC2 实例视为已优化。已优化的 EC2 实例以最佳的性能和基础设施成本运行您的工作负载。对于已优化的实例，Compute Optimizer 有时可能会建议新一代实例类型。
- 无 – 没有对此实例的建议。如果您选择加入 Compute Optimizer 的时间少于 12 小时、实例的运行时间少于 30 小时，或者 Compute Optimizer 不支持实例类型，则可能会发生这种情况。有关更多信息，请参阅前一部分中的 [限制 \(p. 237\)](#)。

查看建议

在选择加入 Compute Optimizer 后，您可以在 EC2 控制台中查看 Compute Optimizer 为 EC2 实例生成的结果。然后，您可以访问 Compute Optimizer 控制台来查看建议。如果您是最近选择加入的，EC2 控制台可能在长达 12 小时内不会反映调查结果。

通过 EC2 控制台查看对 EC2 实例的建议

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择一个实例，然后在 Description (描述) 选项卡上检查 Finding (调查结果) 字段。选择查看详细信息。

实例将在 Compute Optimizer 中打开，在其中，将实例标记为 Current (当前) 实例。最多提供三个不同的实例类型建议，分别标记为 Option 1 (选项 1)、Option 2 (选项 2) 和 Option 3 (选项 3)。窗口的下半部分显示了当前实例的最新 CloudWatch 指标数据：CPU 利用率、内存利用率、网络输入和网络输出。

4. (可选) 在 Compute Optimizer 控制台中，选择设置 () 图标来更改表中的可见列，或查看当前和建议的实例类型的不同购买选项的公开定价信息。

Note

如果您购买了 Reserved Instance，您的按需实例可能会作为 Reserved Instance 进行计费。在更改当前实例类型之前，请首先评估对 Reserved Instance 使用率和覆盖的影响。

确定是否要使用其中某个建议。决定是否要进行优化以便提高性能和/或减少成本。有关更多信息，请参阅 AWS 计算优化器 用户指南 中的 [查看资源建议](#)。

通过 Compute Optimizer 控制台查看对所有区域中的所有 EC2 实例的建议

1. 打开 Compute Optimizer 控制台，网址为 <https://console.aws.amazon.com/compute-optimizer/>。
2. 选择 View recommendations for all EC2 instances (查看对所有 EC2 实例的建议)。
3. 您可以在建议页面上执行以下操作：

- a. 要将建议筛选为一个或多个 AWS 区域，请在 Filter by one or more Regions (按一个或多个区域筛选) 文本框中输入区域名称，或者在显示的下拉列表中选择一个或多个区域。
- b. 要查看其他账户中的资源建议，请选择 Account (账户)，然后选择其他账户 ID。

仅当您登录到组织的主账户并选择加入组织内的所有成员账户时，此选项才可用。

- c. 要清除所选筛选器，请选择 Clear filters (清除筛选器)。
- d. 要更改为当前和建议的实例类型显示的购买选项，请选择设置 () 图标，然后选择 On-Demand Instances (按需实例)、Reserved Instances, standard 1-year no upfront (预留实例，标准 1 年期，无预付费用) 或 Reserved Instances, standard 3-year no upfront (预留实例，标准 3 年期，无预付费用)。
- e. 要查看详细信息（例如，其他建议和利用率指标比较），请选择所需实例旁边列出的调查结果 (Under-provisioned (预配置不足)、Over-provisioned (过度预配置) 或 Optimized (已优化))。有关更多信息，请参阅 AWS 计算优化器 用户指南 中的 [查看资源详细信息](#)。

评估建议时的注意事项

在更改实例类型之前，请考虑以下事项：

- 这些建议不会预测您的使用情况。建议基于您在最近 14 天时间段内的历史使用情况。请务必选择一种预计能够满足您的未来资源需求的实例类型。
- 关注图表指标以确定实际使用量是否低于实例容量。您还可以在 CloudWatch 中查看指标数据（平均值、峰值、百分比），以进一步评估 EC2 实例建议。例如，观察当天 CPU 百分比指标如何变化，以及是否有需要满足的峰值。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [查看可用指标](#)。
- Compute Optimizer 可能会为可突增性能实例（即 T3、T3a 和 T2 实例）提供建议。如果您定期突增至基线之上，请确保您可以基于新实例类型的 vCPU 继续如此。有关更多信息，请参阅 [可突增性能实例的 CPU 积分和基准性能 \(p. 176\)](#)。

- 如果您购买了 Reserved Instance，您的按需实例可能会作为 Reserved Instance 进行计费。在更改当前实例类型之前，请首先评估对 Reserved Instance 使用率和覆盖率的影响。
- 尽可能考虑转换为较新一代实例。
- 在迁移到其他实例系列时，请确保当前实例类型和新实例类型在虚拟化、架构或网络类型等方面兼容。有关更多信息，请参阅 [调整大小的实例的兼容性 \(p. 234\)](#)。
- 最后，请考虑为每个建议提供的性能风险评级。性能风险指示您为了验证建议的实例类型是否满足工作负载的性能要求而可能需要执行的工作量。我们还建议在进行任何更改前后进行严格的负载和性能测试。

调整 EC2 实例大小时，还有其他注意事项。有关更多信息，请参阅 [更改实例类型 \(p. 233\)](#)。

其他资源

- [实例类型 \(p. 160\)](#)
- [AWS 计算优化器 用户指南](#)

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 – 按秒为启动的实例付费。
- Savings Plans – 通过承诺在 1 年或 3 年期限内保持一致的使用量（以美元/小时为单位）来降低您的 Amazon EC2 成本。
- 预留实例 (预留实例) – 通过承诺在 1 年或 3 年期限内提供一致的实例配置（包括实例类型和区域）来降低您的 Amazon EC2 成本。
- 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。
- Spot 实例 (Spot 实例) – 请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。
- 专用主机 – 为完全专用于运行您的实例的物理主机付费，让您现有的按插槽、按内核或按 VM 计费的软件许可证降低成本。
- 专用实例 – 在单一租户硬件上运行的实例按小时付费。
- 容量预留 – 可在特定可用区中为 EC2 实例预留容量，持续时间不限。

如果需要容量预留，请为特定的可用区购买预留实例或容量预留，或者购买计划实例。如果能灵活控制应用程序的运行时间并且应用程序可以中断，Spot 实例就是经济实惠之选。使用专用主机或专用实例，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绑定软件许可证来节省费用。有关更多信息，请参阅 [Amazon EC2 定价](#)。

有关 Savings Plans 的更多信息，请参阅 [AWS Savings Plans 用户指南](#)。

目录

- [确定实例生命周期 \(p. 240\)](#)
- [按需实例 \(p. 240\)](#)
- [预留实例 \(p. 243\)](#)
- [计划的预留实例 \(p. 274\)](#)
- [Spot 实例 \(p. 277\)](#)
- [专用主机 \(p. 333\)](#)
- [专用实例 \(p. 356\)](#)
- [按需容量预留 \(p. 360\)](#)

确定实例生命周期

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将影响实例的生命周期。例如，一个按需实例将在您启动它时运行并在您终止它时结束。只要具有可用的容量，并且您的最高价高于 Spot 价格，Spot 实例就会运行。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，表示实例是 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 Spot 实例。如果值为 scheduled，表示实例是计划内的实例。如果值为 normal，表示实例是个按需实例 或 Reserved Instance。
6. (可选) 如果您购买了 Reserved Instance 并要验证它是否正在被应用，您可以检查 Amazon EC2 的 使用率报告。有关更多信息，请参阅 [Amazon EC2 使用率报告 \(p. 951\)](#)。

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
```

如果实例正在 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 Spot 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，输出不包含 InstanceLifecycle。

按需实例

个按需实例是您按需使用的实例。您可以完全控制其生命周期 — 您确定何时发布、停止、休眠、启动、重启或终止它。

购买按需实例没有长期承诺。您只需要为处于 *running* 状态的按需实例的秒数付费。运行中的个按需实例的每秒的价格固定，在[按需定价](#)页面上列出。

我们建议您为短期的不规则且不能中断的应用程序使用按需实例。

要通过按需实例节省大量费用，请使用 [AWS Savings Plans](#)、[Spot 实例 \(p. 277\)](#)或[预留实例 \(p. 243\)](#)。

目录

- [使用按需实例 \(p. 241\)](#)
- [个按需实例限制 \(p. 241\)](#)
 - [计算您需要的 vCPU 数 \(p. 242\)](#)
 - [申请提高限制 \(p. 243\)](#)
 - [监控个按需实例限制和使用情况 \(p. 243\)](#)
- [查询 AWS 服务的价格 \(p. 243\)](#)

使用按需实例

您可以通过以下方式使用按需实例：

- [启动实例 \(p. 374\)](#)
- [连接到 Linux 实例 \(p. 423\)](#)
- [停止和启动您的实例 \(p. 445\)](#)
- [使 Linux 实例休眠 \(p. 447\)](#)
- [重启您的实例 \(p. 456\)](#)
- [实例停用 \(p. 456\)](#)
- [终止您的实例 \(p. 458\)](#)
- [恢复您的实例 \(p. 463\)](#)
- [配置您的 Amazon Linux 实例 \(p. 464\)](#)
- [识别 EC2 Linux 实例 \(p. 523\)](#)

如果您是 Amazon EC2 的新用户，请参阅[如何开始使用 Amazon EC2 \(p. 1\)](#)。

个按需实例限制

每个区域的每个 AWS 账户运行的按需实例数具有一定的限制。个按需实例限制是根据运行的按需实例使用的虚拟中央处理器 (vCPU) 数进行管理的，而不论实例类型如何。

Note

基于计数的个按需实例限制（根据每种实例类型的实例数进行管理）不再可用。有关更多信息，请参阅[EC2 个按需实例限制](#)。

共有 5 种个按需实例限制，如下表所列。每种限制指定了一个或多个实例系列的 vCPU 限制。有关不同实例系列、实例代和大小的信息，请参阅[Amazon EC2 实例类型](#)。

个按需实例限制名称	默认 vCPU 限制
正在运行的按需标准 (A、C、D、H、I、M、R、T 和 Z) 实例	1152 个 vCPU
正在运行的按需 F 实例	128 个 vCPU
正在运行的按需 G 实例	128 个 vCPU

个按需实例限制名称	默认 vCPU 限制
正在运行的按需 P 实例	128 个 vCPU
正在运行的按需 X 实例	128 个 vCPU

Note

新的 AWS 账户最初设置的限制可能低于此处所述的限制。

对于 vCPU 限制，您可以按照满足您不断变化的应用程序需求的任意实例类型组合所要启动的 vCPU 数来使用限制。例如，对于 256 个 vCPU 的标准实例限制，您可以启动 32 个 m5.2xlarge 实例 (32 x 8 vCPU) 或 16 个 c5.4xlarge 实例 (16 x 16 vCPU)，或者总共有 256 个 vCPU 的任意标准实例类型和大小的组合。有关更多信息，请参阅 [EC2 个按需实例限制](#)。

计算您需要的 vCPU 数

您可以使用 vCPU 限制计算器来确定应用程序需要的 vCPU 数。

以下屏幕截图显示了 vCPU 限制计算器。

The screenshot shows the 'Calculate vCPU limit' tool. At the top, it says 'Calculate number of vCPUs needed' and 'Use this tool to calculate how many vCPUs you need to launch your On-Demand Instances'. Below this, it says 'Select the instance type and the number of instances you require. The calculator will display the number of vCPUs assigned to the selected instances. Use the New Limit value as a guide for requesting a limit increase.' A table lists three instances: m5.2xlarge (32 instances), c5.4xlarge (16 instances), and f1.16xlarge (2 instances). An 'Add instance type' button is available. Below the table, a 'Limits calculation' section shows two rows: 'All Standard (A, C, D, H, I, M, R, T, Z) instances' with a current limit of 1,920 vCPUs and a new limit of 2,432 vCPUs, and 'All F instances' with a current limit of 176 vCPUs and a new limit of 304 vCPUs. Both rows have a 'Request limit increase' button. At the bottom right is a 'Close' button.

您可以查看和使用以下控件和信息：

- 实例类型 – 您添加到 vCPU 限制计算器的实例类型。
- 实例计数 – 您需要的所选实例类型的实例数。
- vCPU 计数 – 与实例计数对应的 vCPU 数。
- 当前限制 – 实例类型所属的限制类型的当前限制。该限制应用到相同限制类型的所有实例类型。例如，在前面的屏幕截图中，m5.2xlarge 和 c5.4xlarge 的当前限制为 1,920 个 vCPU，这是属于所有标准实例限制的所有实例类型的限制。
- 新限制 – 启动您指定的实例数所需的新限制（以 vCPU 数为单位）。

- X – 选择 X 可删除行。
- 添加实例类型 – 选择添加实例类型可将其他实例类型添加到计算器。
- 限制计算 – 显示当前限制、所需 vCPU 以及限制类型的新限制。
 - 实例限制名称 – 您选择的实例类型的限制类型。
 - 当前限制 – 限制类型的当前限制。
- 所需 vCPU – 与您指定的实例数对应的 vCPU 数。对于所有标准实例限制类型，需要的 vCPU 数通过将此限制类型的所有实例类型的 vCPU 计数相加得到。
- 新限制 – 新限制通过将当前限制的值与所需 vCPU 相加得到。
- 选项 – 选择请求提高限制可请求提高对应限制类型的限制。

计算所需 vCPU 数

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择一个区域。
3. 从左侧导航器，选择限制。
4. 选择计算 vCPU 限制。
5. 选择添加实例类型，选择所需实例类型，然后指定所需实例数。要添加更多实例类型，请再次选择添加实例类型。
6. 查看所需新限制的限制计算。
7. 使用完计算器后，选择关闭。

申请提高限制

您可以从 Amazon EC2 控制台的 [限制](#) 页面或 vCPU 限制计算器请求提高各个按需实例限制类型的限制。使用您的用例填写 AWS Support Center [提高限制表单](#) 上的必填字段。对于主实例类型，选择与 vCPU 限制计算器中实例限制名称对应的限制类型。对于新限制值，使用在 vCPU 限制计算器的新限制列中显示的值。有关请求提高限制的更多信息，请参阅 [Amazon EC2 服务限制 \(p. 950\)](#)。

监控个按需实例限制和使用情况

您可以在以下位置查看和管理个按需实例限制：Amazon EC2 控制台中的[“Limits \(限制\)”页面](#)、Services Quotas 控制台中的 [Amazon EC2 Services Quotas 页面](#) 或 AWS Trusted Advisor 控制台中的[“Service Limits \(服务限制\)”页面](#)。有关更多信息，请参阅 Amazon EC2 用户指南 (适用于 Linux 实例) 中的 [Amazon EC2 服务限制 \(p. 950\)](#)、Service Quotas 用户指南中的[查看 Service Quota](#) 以及 [AWS Trusted Advisor](#)。

使用 Amazon CloudWatch 指标集成，您可以根据限制监控 EC2 使用情况。您还可以配置警报以警告即将达到限制。有关更多信息，请参阅 Service Quotas 用户指南中的[使用 Amazon CloudWatch 警报](#)。

查询 AWS 服务的价格

可以使用价目表服务 API 或 AWS 价目表 API 查询 按需实例 的价格。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的[使用 AWS 价目表 API](#)。

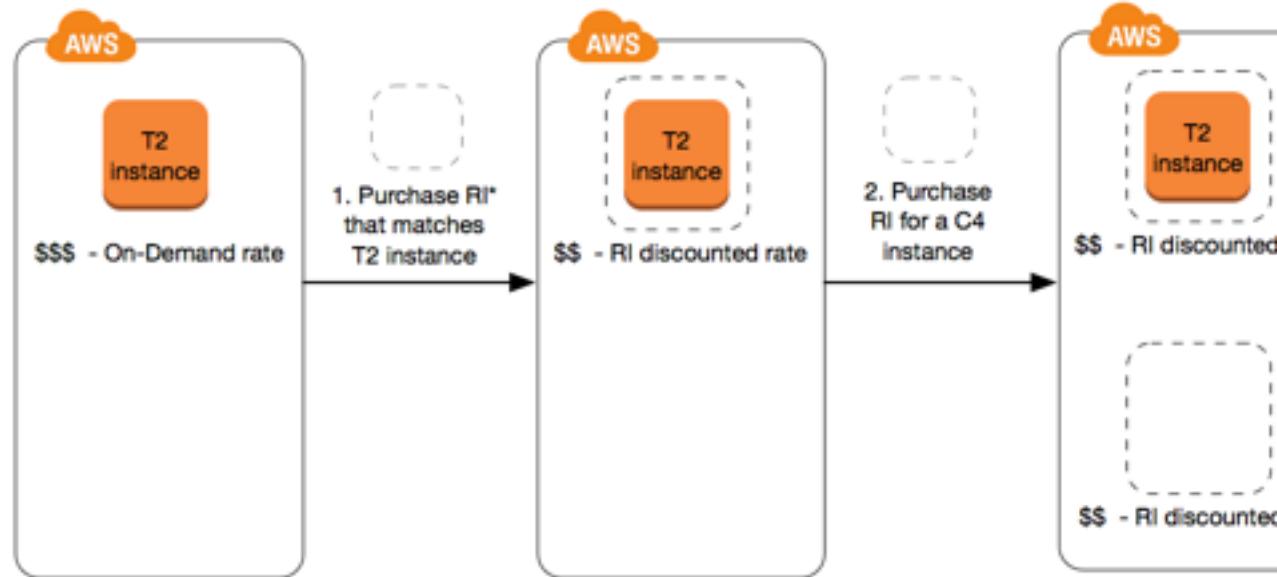
预留实例

与个按需实例定价相比，预留实例为您节省了大量 Amazon EC2 成本。预留实例不是物理实例，而是对账户中的按需实例用量应用的账单折扣。这些按需实例必须与特定属性（例如实例类型和区域）匹配才能享受账单折扣。

与个按需实例定价相比，Savings Plans 还为您节省了大量 Amazon EC2 成本。利用 Savings Plans，您承诺保持一致的使用量（以美元/小时为单位）。这使您能够灵活地使用最能满足您的需求的实例配置，并继续节省费用，而不必对特定实例配置作出承诺。有关更多信息，请参阅 [AWS Savings Plans 用户指南](#)。

Reserved Instance概述

下图是购买和使用预留实例的基本概述。



*RI = Reserved Instance

在此场景中，您的账户中有一个正在运行的按需实例 (T2)，当前您按照按需费率支付。您购买了一个与您正在运行的实例的属性相匹配的Reserved Instance，账单优势立即体现。接下来，您为 C4 实例购买一个 Reserved Instance。您的账户中没有任何正在运行的实例与此Reserved Instance的属性相匹配。在最后的步骤中，您启动了一个与 C4 Reserved Instance的属性相匹配的实例，账单优势立即体现。

决定 Reserved Instance 定价的关键变量

Reserved Instance 定价由以下关键变量决定。

实例属性

Reserved Instance 有四个决定其定价的实例属性。这些属性也决定了 Reserved Instance 应用于您的账户中的运行实例的方式。

- 实例类型：例如，m4.large。这由实例系列 (m4) 和实例大小 (large) 组成。
- 区域：购买Reserved Instance的区域。
- 租赁：您的实例在共享 (默认) 还是单租户 (专用) 硬件上运行。有关更多信息，请参阅[专用实例 \(p. 356\)](#)。
- 平台：操作系统；例如，Windows 或 Linux/Unix。有关更多信息，请参阅[选择平台 \(p. 255\)](#)。

预留实例不会自动续订；当它们过期时，可以继续使用 EC2 实例而不会中断，但要支付按需费率。在上面的示例中，当涵盖 T2 和 C4 实例的 预留实例 过期后，将改为以按需费率支付，直至终止这些实例或者购买与实例属性相匹配的新 预留实例。

期限承诺

您可以承诺购买一年或三年的 Reserved Instance，三年承诺可以获得更大的折扣。

- 一年：一年定义为 31536000 秒 (365 天)。
- 三年：三年定义为 94608000 秒 (1095 天)。

付款选项

针对 预留实例 可使用以下付款选项：

- 预付全费：所有款项于期限开始时支付，无论使用了多少小时数，剩余期限不会再产生其他任何费用或额外按小时计算的费用。
- 预付部分费用：必须预付部分费用，无论是否使用了 Reserved Instance，期限内剩余的小时数都将按照打折小时费率计费。
- 无预付费用：无论是否使用 Reserved Instance，您都将按照期限内的小时数，采用打折小时费率进行付费。无需预付款。

Note

在整个预留期限内，“无预付费用”预留实例需要根据合同义务每月支付费用。因此，账户需要具有成功的账单历史记录才能购买“无预付”预留实例。

一般而言，通过为 预留实例 支付选较高的预付款，可以节省更多成本。在 预留实例市场，也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 \(p. 259\)](#)。

优惠类别

在计算需求发生变化时，您可以根据产品类别修改或交换Reserved Instance。

- 标准：这些提供最大力度的折扣，但只可以修改。
- 可转换：这些相较于标准 预留实例 提供较低的折扣，但可以与具有不同实例属性的可转换 Reserved Instance 进行交换。可转换 预留实例 也可修改。

有关更多信息，请参阅[预留实例的类型 \(提供的类别\) \(p. 246\)](#)。

购买Reserved Instance后，您将不能取消您的购买。但是，如果您需要更改，则可以修改 (p. 265)、[交换 \(p. 270\)](#)或[出售 \(p. 259\)](#)您的 Reserved Instance。

有关定价的更多信息，请参阅[Amazon EC2 预留实例定价](#)。

Reserved Instance限制

您每月可购买的预留实例数存在限制。对于每个区域，您可以为每个可用区购买每月 20 个[区域性 \(p. 247\)](#) 预留实例 以及额外的每月 20 个[地区性 \(p. 247\)](#) 预留实例。

例如，在一个包含三个可用区的区域中，限制为每月 80 个 预留实例：该区域的 20 个区域性 预留实例 加上三个可用区各自的 20 个地区性 预留实例 ($20 \times 3 = 60$)。

区域性 Reserved Instance 账单折扣适用于正在运行的 个按需实例。默认 个按需实例 限制为 20。购买区域性 预留实例 时，不能超出正在运行的 个按需实例 限制。例如，如果您已有 20 个正在运行的 按需实例，并且购买了 20 个区域性 预留实例，则使用 20 个区域性 预留实例 将折扣应用于 20 个正在运行的 按需实例。即使您购买了更多的区域性 预留实例，也无法启动更多的实例，因为已达到 个按需实例 限制。

在购买区域性 预留实例 之前，请确保 个按需实例 限制匹配或超出您打算拥有的区域性 预留实例 的数量。如果需要，请确保在购买更多区域性 预留实例 之前，请求增加 个按需实例 限制。

地区性 Reserved Instance (为特定可用区域购买的 Reserved Instance) 提供容量预留以及折扣。购买地区性 预留实例 时，可以超出 正在运行的 个按需实例 限制。例如，如果您已有 20 个正在运行的 按需实例，并

且购买了 20 个地区性 预留实例，则可以启动另外的 20 个 按需实例，以匹配地区性 预留实例 为您提供总共 40 个正在运行的实例的规范。

Amazon EC2 控制台提供了限制信息。有关更多信息，请参阅 [查看您的当前限制 \(p. 950\)](#)。

区域和可用区 预留实例 (范围)

当您购买 Reserved Instance 时，可决定 Reserved Instance 的范围。范围可以是区域或可用区。

- 区域：当您购买某个区域的 Reserved Instance，该实例称为区域性 Reserved Instance。
- 可用区：当您购买特定可用区的 Reserved Instance 时，该实例称为可用区 Reserved Instance。

区域性或可用区 预留实例 之前的不同

下表重点介绍了区域性 预留实例 和可用区 预留实例 之间的一些主要区别：

	区域性 预留实例	可用区 预留实例
可用区灵活性	Reserved Instance 折扣适用于指定区域的任何可用区中的实例使用。	无可用区灵活性 — Reserved Instance 折扣仅适用于指定可用区中的实例使用。
容量预留	无容量预留 — 区域性 Reserved Instance 不 提供容量预留。	可用区 Reserved Instance 在指定的可用区中提供容量预留。
实例大小灵活性	Reserved Instance 折扣适用于实例系列中的实例使用，无论实例大小如何。只在具有默认租期的 Amazon Linux/Unix 预留实例 上 受支持。有关更多信息，请参阅 实例大小灵活性由标准化因子决定 (p. 247) 。	无实例大小灵活性 — Reserved Instance 折扣仅适用于指定实例类型和大小的实例使用。

有关更多信息以及示例，请参阅 [如何应用预留实例 \(p. 247\)](#)。

预留实例的类型 (提供的类别)

在购买Reserved Instance时，您可以在标准和可转换产品类别之间选择。Reserved Instance 在一个期限内应用于单个实例类型、平台、范围和租期。在计算需求发生变化时，您可以根据产品类别修改或交换 Reserved Instance。产品类别可能会有其他的限制或限制。

以下为标准和可转换产品类别之间的差别。

标准Reserved Instance	可转换预留实例
在期限内可以修改一些属性，例如实例大小；但是，不能修改实例系列。您无法交换标准Reserved Instance，只能修改它。有关更多信息，请参阅 修改预留实例 (p. 265) 。	在期限内可以与具有新属性（包括实例系列、实例类型、平台、范围或租期）的其他可转换预留实例进行交换。有关更多信息，请参阅 交换可转换预留实例 (p. 270) 。您还可以修改可转换预留实例的一些属性。有关更多信息，请参阅 修改预留实例 (p. 265) 。
可以在 预留实例市场 中出售。	不能在 预留实例市场 中出售。

可以购买标准和 可转换预留实例 以应用于特定可用区中的实例（可用区 预留实例）或某个区域中的实例（区域性 预留实例）。有关更多信息以及示例，请参阅 [如何应用预留实例 \(p. 247\)](#)。

如果您想购买每日、每周或每月一次的容量预留，则计划的预留实例可以满足您的需求。有关更多信息，请参阅 [计划的预留实例 \(p. 274\)](#)。

如何应用预留实例

如果您购买了 Reserved Instance 并且已经有正在运行的实例与 Reserved Instance 的规范匹配，账单优势将立即体现。您不必重启您的实例。如果您没有合格的正在运行的实例，请启动实例并确保符合您为 Reserved Instance 指定的相同标准。有关更多信息，请参阅 [使用预留实例 \(p. 259\)](#)。

预留实例 以相同的方式应用，不管产品类型如何（是标准还是可转换），并且将自动应用于具有匹配属性的正在运行的 按需实例。

如何应用区预留实例

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 Reserved Instance 折扣。例如，如果购买可用区 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 Reserved Instance 折扣。正在运行的实例的属性（租期、平台、可用区、实例类型和实例大小）必须与预留实例的属性匹配。

如何应用区域性预留实例

区域性 预留实例 是针对某个区域购买的，可提供可用区灵活性。Reserved Instance 折扣适用于该区域的任何可用区中的实例使用。

区域性 预留实例 还提供实例大小灵活性，Reserved Instance 折扣适用于实例系列中的实例使用，无论实例大小如何。

实例大小灵活性的限制

实例大小灵活性不适用于以下 预留实例：

- 针对特定可用区购买的 预留实例（可用区 预留实例）
- 使用专用租赁的预留实例
- 适用于 Windows Server、装有 SQL Standard 的 Windows Server、装有 SQL Server Enterprise 的 Windows Server、装有 SQL Server Web 的 Windows Server、RHEL 和 SLES 的 预留实例
- 适用于 G4 实例的 预留实例

实例大小灵活性由标准化因子决定

实例大小灵活性取决于实例大小的标准化因子。根据预留的实例大小，区域中的任何可用区中的相同实例系列的运行实例将享受全部或部分折扣。必须匹配的属性仅为实例系列、租期和平台。

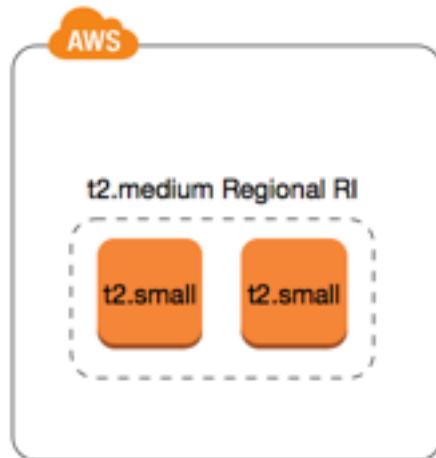
实例大小灵活性基于标准化因子应用于实例系列中各种规模的实例（从最小到最大）。

下表列出了实例系列中的各种大小以及相应的每小时标准化因子。这种比例用于将 预留实例 的折扣费率应用于实例系列的标准化使用。

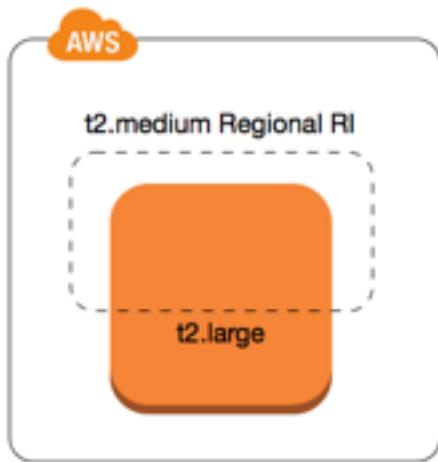
实例大小	标准化因子
nano	0.25

实例大小	标准化因子
微型	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256

例如，t2.medium 实例具有标准化因子 2。如果您在 美国东部（弗吉尼亚北部）中购买了 t2.medium 默认租期 Amazon Linux/Unix Reserved Instance，并且您的账户在该区域中有两个正在运行的 t2.small 实例，则账单优势应用于全部两个实例。



或者，如果您的账户在 美国东部（弗吉尼亚北部）区域有一个 t2.large 实例，则账单优势应用到 50% 的实例使用。



在修改预留实例时，标准化因子也适用。有关更多信息，请参阅[修改预留实例 \(p. 265\)](#)。

裸机实例的标准化因子

实例大小灵活性也适用于实例系列中的裸机实例。如果您具有区域性 Amazon Linux/Unix 预留实例 并对裸机实例使用共享租期，则可以获得在相同实例系列中节省 Reserved Instance 的好处。反过来也是如此：如果您具有区域性 Amazon Linux/Unix 预留实例 并对与裸机实例相同的系列中的实例使用共享租期，则可以在裸机实例中节省 Reserved Instance 的好处。

裸机实例的大小与相同实例系列中的最大实例的大小相同。例如，`i3.metal` 的大小与 `i3.16xlarge` 的大小相同，因此它们具有相同的标准化因子。

Note

`.metal` 实例大小的标准化因子不是单一的。它们会根据特定的实例系列而不同。

裸机实例大小	标准化因子
<code>c5.metal</code>	192
<code>i3.metal</code>	128
<code>r5.metal</code>	192
<code>r5d.metal</code>	192
<code>z1d.metal</code>	96
<code>m5.metal</code>	192
<code>m5d.metal</code>	192

例如，`i3.metal` 实例的标准化因子为 128。如果您购买 美国东部（弗吉尼亚北部）中的 `i3.metal` 默认租期 Amazon Linux/Unix Reserved Instance，则可以获得如下的账单优惠：

- 如果您在该区域的账户中有一个正在运行的 `i3.16xlarge`，则账单优惠全部应用于 `i3.16xlarge` 实例 (`i3.16xlarge` 标准化因子 = 128)。
- 或者，如果您在该区域的账户中有两个正在运行的 `i3.8xlarge` 实例，则账单优惠全部应用于这两个 `i3.8xlarge` 实例 (`i3.8xlarge` 标准化因子 = 64)。
- 或者，如果您在该区域的账户中有四个正在运行的 `i3.4xlarge` 实例，则账单优惠全部应用于所有四个 `i3.4xlarge` 实例 (`i3.4xlarge` 标准化因子 = 32)。

反之亦然。例如，如果您购买 美国东部 (弗吉尼亚北部) 中的两个 `i3.8xlarge` 默认租期 Amazon Linux/Unix 预留实例，并且您在该区域中有一个正在运行的 `i3.metal` 实例，则账单优惠全部应用于 `i3.metal` 实例。

应用预留实例的示例

以下方案涵盖了各种应用预留实例的方式。

Example 方案 1：单个账户中的预留实例

您在账户 A 中运行以下按需实例：

- 4 x `m3.large` Linux，可用区 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

您在账户 A 中购买以下预留实例：

- 4 x `m3.large`，可用区 us-east-1a 中的默认租期 预留实例 (容量为预留)
- 4 x `m4.large` Amazon Linux，区域 us-east-1 中的默认租期 预留实例
- 1 x `c4.large` Amazon Linux，区域 us-east-1 中的默认租期 预留实例

Reserved Instance 优惠以下面方式应用：

- 四个 `m3.large` 地区域性 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` 区域性 预留实例 具备可用区和实例大小灵活性，因为它们是带默认租期的区域性 Amazon Linux 预留实例。

`m4.large` 等效于 4 个标准化单位/小时。

您已购买四个 `m4.large` 区域性 预留实例，它们加起来等效于 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)。这种情况下，四个 `m4.large` 区域性 预留实例 可以降低两个 `m4.xlarge` 实例在完整的一小时内的费用。

- us-east-1 中的 `c4.large` 区域 Reserved Instance 提供了可用区和实例大小灵活性，因为它是带默认租期的区域 Amazon Linux Reserved Instance，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。

在这种情况下，`c4.large` 区域 Reserved Instance 提供了针对 `c4.xlarge` 用量的部分优势。这是因为 `c4.large` Reserved Instance 等效于 4 个标准化单位/小时的用量，而 `c4.xlarge` 实例需要 8 个标准化单位/小时。因此，`c4.large` Reserved Instance 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。

Example 方案 2：关联账户中的区域性预留实例

预留实例首先供购买它们的账户使用，然后供组织中符合条件的任何其他账户使用。有关更多信息，请参阅 [预留实例和整合账单 \(p. 253\)](#)。对于具备大小灵活性的区域性预留实例，这种优势适用于实例系列中各种规模的实例 (从最小到最大)。

您在账户 A (购买账户) 中运行以下按需实例：

- 2 x `m4.xlarge` Linux，可用区 us-east-1a 中的默认租期实例
- 1 x `m4.2xlarge` Linux，可用区 us-east-1b 中的默认租期实例
- 2 x `c4.xlarge` Linux，可用区 us-east-1a 中的默认租期实例

- 1 x c4.2xlarge Linux , 可用区 us-east-1b 中的默认租期实例

另一个客户在账户 B (链接账户) 中运行以下 按需实例 :

- 2 x m4.xlarge Linux , 可用区 us-east-1a 中的默认租期实例

您在账户 A 中购买以下区域性预留实例 :

- 4 x m4.xlarge Linux , 区域 us-east-1 中的默认租期 预留实例
- 2 x c4.xlarge Linux , 区域 us-east-1 中的默认租期 预留实例

区域Reserved Instance优惠以下面方式应用 :

- 四个 m4.xlarge 预留实例 的折扣将由两个 m4.xlarge 实例和账户 A (购买账户) 中的单个 m4.2xlarge 实例使用。所有三个实例均与这些属性相匹配 (实例系列、区域、平台和租期)。折扣将首先应用于购买账户 (账户 A) 中的实例，即使账户 B (链接账户) 具有两个也匹配 预留实例 的 m4.xlarge。由于 预留实例 是区域性 预留实例，因此没有容量预留。
- 两个 c4.xlarge 预留实例 的折扣适用于两个 c4.xlarge , 因为它们比 c4.2xlarge 实例小。由于 预留实例 是区域性 预留实例，因此没有容量预留。

Example 方案 3 : 关联账户中的区预留实例

通常，某个账户拥有的预留实例首先供该账户自用。不过，如果组织的其他账户中有适用于特定可用区、符合条件的未使用 预留实例 (地区性 预留实例)，这些实例将先于账户拥有的区域性 预留实例 应用于账户。这样做是为了确保实现最大Reserved Instance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。

您在账户 A (购买账户) 中运行以下个按需实例 :

- 1 x m4.xlarge Linux , 可用区 us-east-1a 中的默认租期实例

某个客户在关联账户 B 中运行了以下个按需实例 :

- 1 x m4.xlarge Linux , 可用区 us-east-1b 中的默认租期实例

您在账户 A 中购买以下区域性预留实例 :

- 1 x m4.xlarge Linux , 区域 us-east-1 中的默认租期 Reserved Instance

客户还在关联账户 C 中购买了以下区预留实例 :

- 1 x m4.xlarge Linux , 可用区 us-east-1a 中的默认租期 预留实例

Reserved Instance优惠以下面方式应用 :

- 账户 C 拥有的 m4.xlarge 地区性 Reserved Instance 的折扣应用于账户 A 中的 m4.xlarge 用量。
- 账户 A 拥有的 m4.xlarge 区域性 Reserved Instance 的折扣应用于账户 B 中的 m4.xlarge 用量。
- 如果账户 A 拥有的区域性 Reserved Instance 先应用于账户 A 中的用量，则账户 C 拥有的地区性 Reserved Instance 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](#)。

如何计费

与按需定价不同，所有预留实例都提供折扣。使用预留实例时，无论实际使用情况如何，都需要为整个期限付费。您可以根据为 Reserved Instance 指定的[付款选项 \(p. 245\)](#)，为 Reserved Instance 选择预付、部分预付或按月付费。

预留实例过期后，需要根据按需费率支付 EC2 实例使用费用。您最早可以提前三年排队购买 Reserved Instance。这样可以帮助您确保获得不中断的服务。有关更多信息，请参阅[排队购买 \(p. 255\)](#)。

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，然后购买了一个 Reserved Instance，那么将按照标准定价指南付费。有关信息，请参阅[AWS 免费套餐](#)。

目录

- [使用计费 \(p. 252\)](#)
- [查看您的账单 \(p. 253\)](#)
- [预留实例和整合账单 \(p. 253\)](#)
- [Reserved Instance折扣定价套餐 \(p. 253\)](#)

使用计费

在选择的预留实例期限内，无论实例是否运行，预留实例均按小时计费。每时钟小时从标准 24 小时制的整点（该小时经过了零分零秒）开始。例如，1:00:00 到 1:59:59 是一个时钟小时。有关实例状态的更多信息，请参阅[实例生命周期 \(p. 370\)](#)。

Reserved Instance 账单优势适用于按秒收费的运行实例。每秒计费适用于使用开源 Linux 发行版的实例，例如 Amazon Linux 和 Ubuntu。每小时计费用于商业 Linux 发行版，例如 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server。

Reserved Instance 账单优势适用于每小时最多 3600 秒（一小时）的实例使用。您可同时运行多个实例，但每小时只能获得总计 3600 秒的 Reserved Instance 折扣优惠；每小时超出 3600 秒的实例使用将根据按需费率计费。

例如，如果您购买了一个 m4.xlarge Reserved Instance，同时运行 4 个 m4.xlarge 实例 1 小时，则一个实例将按 1 小时的 Reserved Instance 使用收费，其他三个实例将按 3 小时的按需使用收费。

但是，如果您购买一个 m4.xlarge Reserved Instance，在同一小时内运行 4 个 m4.xlarge 实例各 15 分钟（900 秒），那么实例的总运行时间为 1 小时，这将产生 1 小时的 Reserved Instance 使用和 0 小时的按需使用。

	1:00	1:15	1:30	1:45
Instance 1	Orange			
Instance 2		Orange		
Instance 3			Orange	
Instance 4				Orange

如果多个合格实例同时运行，Reserved Instance 账单优势将在一小时内（最多 3600 秒）同时适用于所有实例；在该时间后，根据按需费率收取费用。



使用 [Billing and Cost Management](#) 控制台上的 Cost Explorer (成本管理器) 可以分析运行 按需实例 所节省的成本。[预留实例 常见问题](#)包括标价计算的示例。

如果您关闭 AWS 账户，则您资源的按需计费会停止。不过，如果账户中有任何预留实例，则会继续收到这些实例的账单，直至实例过期。

查看您的账单

您可通过查看 [AWS Billing and Cost Management](#) 控制台来了解您的账户的费用情况。

- 控制面板显示了您的账户的花费汇总。
- 在 Bills (账单) 页面的 Details (详细信息) 下，展开 Elastic Compute Cloud 部分及区域，以了解有关您的预留实例 的账单信息。

您可以在线查看费用，也可以下载 CSV 文件。

您还可以使用 AWS 成本和使用情况报告来跟踪您的Reserved Instance使用情况。有关更多信息，请参阅AWS Billing and Cost Management 用户指南中“成本和使用情况报告”下的 [预留实例](#)。

预留实例和整合账单

如果购买者账户是在一个整合账单付款人账户之下计费的一组账户中的其中之一，则可以共享预留实例定价优惠。每月将在付款人账户中汇总所有成员账户的实例使用量。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Reserved Instance逻辑来计算账单。有关更多信息，请参阅AWS Organizations 用户指南中的[整合账单 和 AWS Organizations](#)。

即使关闭付款人账户，所有享受 预留实例 账单折扣的成员账户将继续享受折扣，直至 预留实例 过期，或者直至该成员账户被删除。

Reserved Instance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Reserved Instance的预付费和实例使用费均自动享受折扣。要取得折扣资格，在该区域内的 预留实例 的标价必须达到 500000 美元或更高。

以下规则适用：

- 定价套餐和相关折扣仅适用于购买 Amazon EC2 标准 预留实例。
- 定价套餐不适用于面向带 SQL Server Standard、SQL Server Web 和 SQL Server Enterprise 的 Windows 的 预留实例。
- 定价套餐不适用于面向带 SQL Server Standard、SQL Server Web 和 SQL Server Enterprise 的 Linux 的 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。
- 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Reserved Instance定价折扣 \(p. 253\)](#)
- [以折扣套餐价格购买 \(p. 254\)](#)
- [跨越定价套餐 \(p. 254\)](#)
- [定价套餐的整合账单 \(p. 255\)](#)

计算Reserved Instance定价折扣

通过计算在区域中的所有 预留实例 的标价，可以确定账户所适用的定价套餐。将每个预留实例的每小时费 用乘以期限的总小时数，再加上购买时 [预留实例 定价页面](#)上所列的未打折预付价格（也称为固定价格）。因

为价目表值基于未打折 (公开) 定价，是否有资格获得批量折扣或者购买预留实例后是否降价均不影响价目表值。

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

例如，对于一年期部分预付 t2.small Reserved Instance，假定预付价格是 60.00 美元，每小时费率为 0.007 美元。这将提供 121.32 美元的标价。

```
121.32 = 60.00 + (0.007 * 8760)
```

使用 Amazon EC2 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. 在导航窗格中，选择 Reserved Instances。
3. 通过选择右上角的 Show/Hide Columns (齿轮状图标) 来显示 Upfront Price 列。

使用命令行查看 预留实例 的固定价格

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeReservedInstances](#) (Amazon EC2 API)

以折扣套餐价格购买

购买 预留实例 时，Amazon EC2 自动将所有折扣应用于所购产品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 工具购买 预留实例。有关更多信息，请参阅[购买预留实例 \(p. 255\)](#)。

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，以后在该区域购买任何 预留实例 都将按打折费率计费。如果在某区域的 预留实例 单项购买额超过折扣套餐阈值，则该项购买超出价格阈值的部分将按打折费率计费。有关在购买过程中创建的临时 Reserved Instance ID 的更多信息，请参阅[跨越定价套餐 \(p. 254\)](#)。

如果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。不过，原来在折扣定价套餐范围内购买的所有 预留实例 将继续享受折扣。

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。

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。

Reserved Instance 服务会生成多个 Reserved Instance 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，由购买 CLI 命令或 API 操作返回的 ID 不同于新预留实例的实际 ID。

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 \(p. 253\)](#)。

购买预留实例

要购买 Reserved Instance，请从 AWS 和第三方卖家搜索 Reserved Instance 产品，调整搜索参数，直至您找到与您的目标完全相符的对象。

在搜索要购买的预留实例时，您将收到一个关于退还产品的成本报价。当您继续购买时，AWS 将自动对购买价格设定一个限定价格。预留实例的总成本不会超过报价金额。

如果价格由于任何原因上升或变动，将不会完成购买。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。

在确认购买之前，请检查您计划购买的Reserved Instance的详细信息，并确保所有参数都是准确的。在您购买 Reserved Instance（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。

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](#)。

任务

- [选择平台 \(p. 255\)](#)
- [排队购买 \(p. 255\)](#)
- [购买标准预留实例 \(p. 256\)](#)
- [购买可转换预留实例 \(p. 257\)](#)
- [查看预留实例 \(p. 258\)](#)
- [取消已排队的购买 \(p. 259\)](#)
- [使用预留实例 \(p. 259\)](#)

选择平台

您购买 Reserved Instance 时，必须选择面向代表您的实例的操作系统的平台的产品。

对于 SUSE Linux 和 RHEL 分配，您必须选择面向这些特定平台的服务产品。对于所有其他 Linux 分配（包括 Ubuntu），选择面向 Linux/UNIX 平台的服务产品。如果您带来现有的 RHEL 订阅，则必须选择 Linux/UNIX 平台的产品，而不是 RHEL 平台的产品。

如果您购买Reserved Instance以应用于从 AMI 启动的带计费产品代码的个按需实例，请确保Reserved Instance具有匹配的计费产品代码。如果您购买不带匹配的计费产品代码的Reserved Instance，则Reserved Instance将不会应用于个按需实例。

排队购买

默认情况下，当您购买 Reserved Instance 时，它会立即执行。或者，您也可以排队预约在将来的某个日期和时间购买。例如，您可以排队预约在现有 Reserved Instance 到期的时间购买。这样可以帮助您确保获得不间断的服务。

您可以排队购买区域 预留实例，但不能排队购买其他卖家的区域 预留实例 或 预留实例。您最早可以提前三年排队购买。在指定日期和时间，将使用默认支付方式进行购买。支付成功后，将体现账单优势。

您可以在 Amazon EC2 控制台中查看已排队的购买。已排队的购买的状态为已排队。在指定时间之前，您随时可以取消已排队的购买。有关详细信息，请参阅 [取消已排队的购买 \(p. 259\)](#)。

购买标准预留实例

您可以购买特定可用区中的标准预留实例从而获得容量预留。或者，您也可以放弃容量预留并购买区域性标准 Reserved Instance。

使用 Amazon EC2 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 (预留实例) 和 Purchase 预留实例 (购买预留实例)。
3. 对于 Offering Class (产品类别)，选择 Standard (标准) 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。要购买区域性 Reserved Instance，请保留复选框未选中。
5. 根据需要选择其他配置并选择 搜索。

要从 预留实例市场 购买标准 Reserved Instance，请在搜索结果的 Seller (卖家) 列中查找 3rd Party (第三方)。Term 列会显示非标准期限。

6. 选择要购买的 预留实例，输入数量，然后选择 Add to Cart (添加购物车)。
7. 要查看已选择的 预留实例 的汇总，请选择 View Cart (查看购物车)。
8. 如果 Order On (订购日期) 为 Now (现在)，则会立即完成购买。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。在浏览器时区选定日期的 00:00 之前，购买将排入队列。
9. 要完成订单，请选择 Order (订单)。

如果在下订单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。

10. 您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 payment-pending 变为 active。当 Reserved Instance 的状态为 active 时即可使用。

Note

如果状态转为 retired，AWS 可能未收到您的付款。

使用 AWS CLI 控制台购买标准 Reserved Instance

1. 使用 [describe-reserved-instances-offerings](#) 命令查找可用 预留实例。为 --offering-class 参数指定 standard 以仅返回标准 预留实例。可以应用更多参数来缩小结果范围；例如，如果仅希望为 Linux/UNIX 购买具有默认租期的一年期区域性 t2.large Reserved Instance：

```
aws ec2 describe-reserved-instances-offerings --instance-type t2.large --offering-class standard --product-description "Linux/UNIX" --instance-tenancy default --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

要仅在 预留实例市场 上查找 预留实例，请使用 marketplace 筛选条件并在请求中不指定持续时间，因为期限可能会短于 1 年期或 3 年期。

```
aws ec2 describe-reserved-instances-offerings --instance-type t2.large --offering-class standard --product-description "Linux/UNIX" --instance-tenancy default --filters Name=marketplace,Values=true
```

当您找到符合需求的 Reserved Instance 时，请记下产品 ID。例如：

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. 使用 [purchase-reserved-instances-offering](#) 命令购买您的 Reserved Instance。您必须指定在上一步中获取的 Reserved Instance 产品 ID，并且必须为预留指定实例数量。

```
aws ec2 purchase-reserved-instances-offering --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 --instance-count 1
```

默认情况下，会立即完成购买。或者，若要排队购买，请在之前的调用中增加以下参数。

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. 使用 [describe-reserved-instances](#) 命令获取您的 Reserved Instance 的状态。

```
aws ec2 describe-reserved-instances
```

或者，使用以下适用于 Windows PowerShell 的 AWS 工具 命令：

- [Get-EC2ReservedInstancesOffering](#)
- [New-EC2ReservedInstance](#)
- [Get-EC2ReservedInstance](#)

购买完成后，如果已有正在运行的与 Reserved Instance 规范匹配的实例，账单优势将立即体现。您不必重启您的实例。如果您没有合适的运行实例，请启动实例并确保符合您为 Reserved Instance 指定的相同标准。有关更多信息，请参阅[使用预留实例 \(p. 259\)](#)。

有关如何将预留实例应用于正在运行的实例的示例，请参阅[如何应用预留实例 \(p. 247\)](#)。

购买可转换预留实例

您可以购买特定可用区中的可转换预留实例从而获得容量预留。或者，您也可以放弃容量预留并购买区域性可转换预留实例。

使用 Amazon EC2 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，依次选择 Reserved Instances (预留实例) 和 Purchase 预留实例 (购买预留实例)。
3. 对于 Offering Class (产品类别)，选择 Convertible (可转换) 以显示 可转换预留实例。
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。要购买区域性 Reserved Instance，请保留复选框未选中。
5. 根据需要选择其他配置并选择 搜索。
6. 选择要购买的 可转换预留实例，输入数量，然后选择 Add to Cart (添加购物车)。
7. 要查看您的选择的摘要，请选择 View Cart。
8. 如果 Order On (订购日期) 为 Now (现在)，则会立即完成购买。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。在浏览器时区选定日期的 00:00 之前，购买将排入队列。
9. 要完成订单，请选择 Order (订单)。

如果在下订单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。

10. 您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 payment-pending 变为 active。当 Reserved Instance 的状态为 active 时即可使用。

Note

如果状态转为 `retired`，AWS 可能未收到您的付款。

使用 AWS CLI 购买 可转换预留实例

1. 使用 `describe-reserved-instances-offerings` 命令查找可用 预留实例。为 `--offering-class` 参数指定 `convertible` 以仅返回 可转换预留实例。可以应用更多参数来缩小结果范围；例如，如果仅希望为 Linux/UNIX 购买具有默认租期的区域性 `t2.large` Reserved Instance：

```
aws ec2 describe-reserved-instances-offerings --instance-type t2.large --offering-class convertible --product-description "Linux/UNIX" --instance-tenancy default --filters Name=scope,Values=Region
```

当您找到符合需求的 Reserved Instance 时，请记下产品 ID。例如：

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. 使用 `purchase-reserved-instances-offering` 命令购买您的 Reserved Instance。您必须指定在上一步中获取的 Reserved Instance 产品 ID，并且必须为预留指定实例数量。

```
aws ec2 purchase-reserved-instances-offering --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 --instance-count 1
```

默认情况下，会立即完成购买。或者，若要排队购买，请在之前的调用中增加以下参数。

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. 使用 `describe-reserved-instances` 命令获取您的 Reserved Instance 的状态。

```
aws ec2 describe-reserved-instances
```

或者，使用以下 适用于 Windows PowerShell 的 AWS 工具 命令：

- `Get-EC2ReservedInstancesOffering`
- `New-EC2ReservedInstance`
- `Get-EC2ReservedInstance`

如果已经有与 Reserved Instance 的规格匹配的运行实例，则将立即体现账单收益。您不必重启您的实例。如果您没有合适的运行实例，请启动实例并确保符合您为 Reserved Instance 指定的相同标准。有关更多信息，请参阅[使用预留实例 \(p. 259\)](#)。

有关如何将 预留实例 应用于正在运行的实例的示例，请参阅[如何应用预留实例 \(p. 247\)](#)。

查看预留实例

您可以使用 Amazon EC2 控制台或命令行工具查看已购买的 预留实例。

在控制台中查看您的预留实例

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. 此时将列出活动的和已停用的预留实例。State 列显示状态。

- 如果您是 预留实例市场 中的卖家，My Listings (我的列表) 选项卡会显示 预留实例市场 (p. 259) 中列出的预留的状态。有关更多信息，请参阅 [Reserved Instance列示状态 \(p. 263\)](#)。

使用命令行查看预留实例

- [describe-reserved-instances \(AWS CLI\)](#)
- [Get-EC2ReservedInstance \(Windows PowerShell 工具\)](#)

取消已排队的购买

您最早可以提前三年排队购买。在指定时间之前，您随时可以取消已排队的购买。

取消已排队的购买

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Reserved Instances。
- 选择一个或多个 预留实例。
- 依次选择 Actions (操作)、Delete Queued Instances (删除已排队的预留实例)。
- 当系统提示进行确认时，选择 Yes, Delete。

使用预留实例

预留实例 将自动应用于正在运行的 按需实例 (前提匹配规范)。如果正在运行的 按需实例 都与 Reserved Instance 的规范不匹配，则不会使用 Reserved Instance，直到您启动具有指定规范的实例。

如果您要启动实例以利用Reserved Instance的账单收益，请确保您在启动期间指定了以下信息：

- 平台**：您必须选择与您的Reserved Instance的平台 (产品说明) 相匹配的 Amazon 系统映像 (AMI)。例如，如果您指定 Linux/UNIX，则可以从 Amazon Linux AMI 或 Ubuntu AMI 启动实例。
- 实例类型**：指定与您的 Reserved Instance 相同的实例类型；例如 t2.large。
- 可用区**：如果您为特定可用区购买了Reserved Instance，则必须在相同的可用区中启动实例。如果您购买了区域性Reserved Instance，则可以在任何可用区中启动实例。
- 租赁**：实例的租赁必须与 Reserved Instance 的租赁匹配；例如 dedicated 或 shared。有关更多信息，请参阅 [专用实例 \(p. 356\)](#)。

有关更多信息，请参阅 [使用启动实例向导启动实例 \(p. 375\)](#)。有关如何将 预留实例 应用于正在运行的实例的示例，请参阅 [如何应用预留实例 \(p. 247\)](#)。

您可以使用 Amazon EC2 Auto Scaling 或其他 AWS 服务来启动使用 Reserved Instance 优惠的 按需实例。有关更多信息，请参阅 [Amazon EC2 Auto Scaling 用户指南](#)。

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，在将实例移到新 AWS 区域中、更改为新实例类型、项目结束但期限仍未到期、业务需求变化或者具有不需要的容量时，您可能希望出售 预留实例。

在 预留实例市场 上销售未使用的 预留实例 必须满足特定资格条件。

目录

- [在 预留实例市场 中出售实例 \(p. 260\)](#)
- [从Reserved Instance市场中购买 \(p. 264\)](#)

在 预留实例市场 中出售实例

只要在 预留实例市场 中列出 预留实例 , 便可供潜在的买方找到。所有预留实例将根据剩余期限及小时价格进行分组。

为满足买方的请求 , AWS 首先出售指定分组中预付价格最低的 Reserved Instance。然后再出售下一个最低价格的 Reserved Instance , 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Reserved Instance出售之前 , 它将归您所有。出售之后 , 您便放弃了容量预留和打折的周期性费用。如果继续使用您的实例 , AWS 将从您的 Reserved Instance 出售的时间开始以按需价格向您收费。

目录

- [限制 \(p. 260\)](#)
- [注册为卖家 \(p. 260\)](#)
- [银行支付账户 \(p. 261\)](#)
- [税务信息 \(p. 261\)](#)
- [为预留实例定价 \(p. 262\)](#)
- [列出预留实例 \(p. 262\)](#)
- [Reserved Instance列示状态 \(p. 263\)](#)
- [实例出售清单的生命周期 \(p. 263\)](#)
- [在Reserved Instance出售后 \(p. 264\)](#)
- [收款 \(p. 264\)](#)
- [与买方共享的信息 \(p. 264\)](#)

限制

您必须先注册为预留实例市场中的卖家 , 然后才能出售未使用的预留。有关信息 , 请参阅 [注册为卖家 \(p. 260\)](#)。

以下限制在出售预留实例时适用 :

- 在 预留实例市场 中只能出售 Amazon EC2 标准 预留实例。不能出售 可转换预留实例。标准Reserved Instance的剩余期限必须至少为一个月。
- 预留实例市场中允许的最低价格为 0.00 美元。
- 您可以在 预留实例市场 中出售“无预付费用”、“预付部分费用”或“预付全费”预留实例。如果存在针对 Reserved Instance 的预付款 , 则只有在 AWS 收到预付款且预留已激活 (被您拥有) 达到至少 30 天之后 , 该实例才能出售。
- 您无法在预留实例市场中直接修改您的列示。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 [为预留实例定价 \(p. 262\)](#)。您也可以在列出预留实例时对其进行修改。有关信息 , 请参阅 [修改预留实例 \(p. 265\)](#)。
- AWS 会向您收取您在 预留实例市场 中出售的每个标准 Reserved Instance 的总预付价格 12% 的服务费。预付价格是卖方对标准Reserved Instance收取的费用。
- 在 预留实例市场 中只能出售 Amazon EC2 标准 预留实例。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。

注册为卖家

Note

只有 AWS 账户根用户才可以将账户注册为卖家。

要在 预留实例市场 中进行销售，您必须先注册为卖家。在注册过程中，您应提供以下信息：

- 银行信息 — 为了支付您出售预留实例时收取的资金，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[银行支付账户 \(p. 261\)](#)。
- 税务信息 — 所有卖方都需要完成税务信息审查以确定任何必要的税务报告义务。有关更多信息，请参阅[税务信息 \(p. 261\)](#)。

在 AWS 收到您已完成的卖家注册后，您会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。

银行支付账户

为了支付您出售 Reserved Instance 时收取的资金，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. 打开[预留实例市场 卖家注册](#)页面并使用您的 AWS 凭证登录。
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 卖家注册](#)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

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，您必须在[卖家注册门户](#)中完成税务审查。此审查将收集税务信息并填充 IRS 表 W-9、W-8BEN 或 W-8BEN-E，后者用于确定任何必要的税务报告义务。

您在税务审查中输入的税务信息可能不同，具体取决于您是作为个人还是企业运营，以及您是否为美国人，您的企业是否为美国实体。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。

根据您的税务审查响应和 IRS 报告阈值，Amazon 可能对表格 1099-K 归档。Amazon 会在您的账户达到阈值级别的那一年的后一年的 1 月 31 日或之前通过电子邮件发送表格 1099-K 的副本。例如，如果您的账户在 2018 年达到阈值，则将在 2019 年 1 月 31 日或之前通过电子邮件发送您的表 1099-K。

有关 IRS 要求和表 1099-K 的更多信息，请参阅 [IRS 网站](#)。

为预留实例定价

预付费用是您可为正在出售的Reserved Instance指定的唯一费用。预付费用是买方在购买Reserved Instance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 销售限制申请表格](#)。
- 最低价格为 0 美元。预留实例市场中允许的最低价格为 0.00 美元。

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。

因为 预留实例 的价值随时间的推移而降低，所以，默认情况下，AWS 可设定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 Reserved Instance 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 Reserved Instance，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。

列出预留实例

注册卖家可以选择销售一个或多个预留实例。您可以选择在一次列出中销售所有实例，或分成多个部分销售。此外，您可以列出任意实例类型、平台和范围配置的预留实例。

控制台将确定建议的价格。它会检查与您的 Reserved Instance 匹配的产品，并与价格最低的产品匹配。否则，它会根据剩余时间的 Reserved Instance 成本计算建议价格。如果计算出的价值小于 1.01 美元，则建议的价格为 1.01 美元。

如果您取消出售清单，且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。

使用 AWS 管理控制台 在 预留实例市场 中列出 Reserved Instance

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. 选择要列出的 预留实例，然后选择 Sell 预留实例 (出售预留实例)。
4. 在 Configure Your Reserved Instance Listing (配置您的预留实例列表) 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. 当您完成列表配置后，请选择 Continue (继续)。
7. 在 Confirm Your Reserved Instance Listing (确认您的预留实例列表) 页面上确认您的列表详细信息；如果对此类信息感到满意，请选择 List Reserved Instance (列出预留实例)。

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. 选择您已列出的 Reserved Instance，然后选择 My Listings (我的列表)。

使用 AWS CLI 管理预留实例市场中的预留实例

1. 使用 `describe-reserved-instances` 命令获取 预留实例 的列表。
2. 记录要列出的 Reserved Instance 的 ID 并调用 `create-reserved-instances-listing`。您必须指定Reserved Instance的 ID、实例数以及价格表。
3. 要查看列表，请使用 `describe-reserved-instances-listings` 命令。
4. 要取消列表，请使用 `cancel-reserved-instances-listings` 命令。

Reserved Instance列示状态

预留实例 页面的 My Listings (我的列表) 选项卡上的 Listing State (列表状态) 显示了列表的当前状态：

Listing State (列表状态) 显示的信息与您在 预留实例市场 中的列表的状态有关。它与 Reserved Instances (预留实例) 页面中的 State (状态) 列显示的状态信息不同。此 State 信息是关于您的预留的。

- active (已激活) — 列表可供购买。
- canceled (已取消) — 列表已取消，并且在 预留实例市场 中不再可供购买。
- closed (已关闭) — Reserved Instance 未列出。Reserved Instance 可能因列表已完成销售而处于 closed 状态。

实例出售清单的生命周期

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。

当列表中只有一部分售出时，AWS 将停用列表中的 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。

将以此方式处理此列表中任何未来预留实例销售。当列表中的所有 预留实例 售出后，AWS 将列表标记为 closed。

例如，您创建一个列表数量为 5 的列表：预留实例 listing 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：

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 0
- 可用 = 5
- 状态 = 已激活

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：

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 2
- 可用 = 3
- 状态 = 已激活

如果您取消您的出售清单，且出售清单的一部分已经售出，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。

在Reserved Instance出售后

当您的 Reserved Instance 售出后，AWS 会向您发送一条电子邮件通知。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，您创建或销售实例出售清单，或者 AWS 将资金发送到您的账户。

要在控制台中跟踪 Reserved Instance 列表的状态，请依次选择 Reserved Instance (预留实例) 和 My Listings (我的列表)。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 [describe-reserved-instances-listings](#) 命令，借助合适的筛选条件来获取您的预留实例出售清单信息。

收款

AWS 从买方收到资金后，会向已售 Reserved Instance 的注册所有者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 Reserved Instance 已售出后的一天到三天内发生。支付每天只发生一次。在发放资金后，您将收到包含支付报告的电子邮件。请记住，在 AWS 从您的银行收到确认信息后，您才能收到付款。这可能需要长达两周的时间。

在查看 预留实例 时，仍会显示已销售的 Reserved Instance。

预留实例 的现金付款通过电汇转账直接进入您的银行账户。AWS 向您收取您在 预留实例市场 中出售的每个 Reserved Instance 的总预付价格 12% 的服务费。

与买方共享的信息

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](#)。

从Reserved Instance市场中购买

您可以从 预留实例市场 向不再需要其 预留实例 的第三方卖方购买 预留实例。您可以使用 Amazon EC2 控制台或命令行工具执行此操作。该过程类似于从 AWS 购买预留实例。有关更多信息，请参阅 [购买预留实例 \(p. 255\)](#)。

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 具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。

- 预留实例类型 — 只能从 预留实例市场 购买 Amazon EC2 标准 预留实例。不能从 预留实例市场 购买 可转换预留实例、Amazon RDS 和 Amazon ElastiCache 预留实例。

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](#)。

修改预留实例

当需求改变时，可以修改标准或可转换预留实例并继续利用账单优势。您可以修改可用区、实例大小 (在相同的实例系列中) 以及 Reserved Instance 的范围等属性。

Note

您还可以将可转换预留实例交换为具有不同配置的其他可转换预留实例。有关更多信息，请参阅[交換可转换预留实例 \(p. 270\)](#)。

可以修改全部或部分预留实例。可以将原始 预留实例 分为两个或更多新的 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 个实例移至 us-east-1b，则修改请求会生成两个新的预留实例 - 一个用于 us-east-1a 中的 5 个实例，另一个用于 us-east-1b 中的 5 个实例。

还可以将两个或更多 预留实例 合并 成单个 Reserved Instance。例如，如果有四个 t2.small 均为 预留实例，则可以将其合并以创建单个 t2.large Reserved Instance。有关更多信息，请参阅[对于修改实例大小的支持 \(p. 266\)](#)。

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。例如，如果您更改预留的可用区，则容量预留和定价优势自动应用到在新可用区中使用的实例。除非您的账户有其他适用的预留，否则将按照按需费率对不再符合新参数的实例收费。

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 [describe-reserved-instances](#) 命令，获取修改后的预留实例的生效日期。
- 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 Reserved Instance 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。
- 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。

如果修改请求失败，预留实例会保持其原始配置，并立即对其他修改请求可用。

修改不会产生任何费用，因此您不会收到任何新账单或发票。

您可以根据自己的需要随时修改预留，但是不能在提交之后更改或取消挂起的修改请求。修改成功完成后，如果需要，您可以提交另一个修改请求，以回滚您所做的任何更改。

目录

- [修改的要求和限制 \(p. 266\)](#)
- [对于修改实例大小的支持 \(p. 266\)](#)
- [提交修改请求 \(p. 269\)](#)
- [修改请求故障排除 \(p. 270\)](#)

修改的要求和限制

您可以按如下方式修改这些属性。

可修改的属性	支持的平台	限制
在相同区域内更改可用区	Linux 和 Windows	-
将范围从可用区更改到区域以及反之	Linux 和 Windows	如果您将范围从可用区更改为区域，则会失去预留容量优势。 如果您将范围从区域更改为可用区，则会失去可用区灵活性和实例大小灵活性（如果适用）。有关更多信息，请参阅 如何应用预留实例 (p. 247) 。
更改相同实例系列内的实例大小	仅限 Linux	预留必须使用默认租赁。某些实例系列不受支持，因为没有其他大小可用。有关更多信息，请参阅 中的 对于修改实例大小的支持 (p. 266) 。
将网络从 EC2-Classic 更改为 Amazon VPC，反之亦然	Linux 和 Windows	网络平台在您的 AWS 账户中必须可用。如果您的 AWS 账户是在 2013 年 12 月 4 日之后创建的，则它不支持 EC2-Classic。

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：

- 在您购买 Reserved Instance 时或在此之前，无法对其进行修改
- Reserved Instance 必须是活动的
- 不能有待处理的修改请求
- 预留实例市场 中未列出 Reserved Instance
- 有效预留的实例大小占用空间必须与目标配置匹配。有关更多信息，请参阅 [对于修改实例大小的支持 \(p. 266\)](#)。
- 输入 预留实例 要么全部是标准 预留实例，要么全部是 可转换预留实例，不能每种类型都有一些
- 输入 预留实例 如果是标准 预留实例，则必须在相同的时间过期

对于修改实例大小的支持

如果您在某个实例系列中的 Amazon Linux 预留有多个大小，则可以修改 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 实例系列属于计算优化型系列，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](#)。

对于以下实例类型，无法修改 预留实例 的实例大小，因为每个实例系列只有一个大小可用。

- cc2.8xlarge

- `cr1.8xlarge`
- `hs1.8xlarge`
- `t1.micro`

每个 Reserved Instance 都有实例大小占用空间，该空间由预留中实例类型的标准化因子和实例数量决定。修改Reserved Instance时，目标配置的占用空间必须与原始配置相匹配，否则不会处理修改请求。

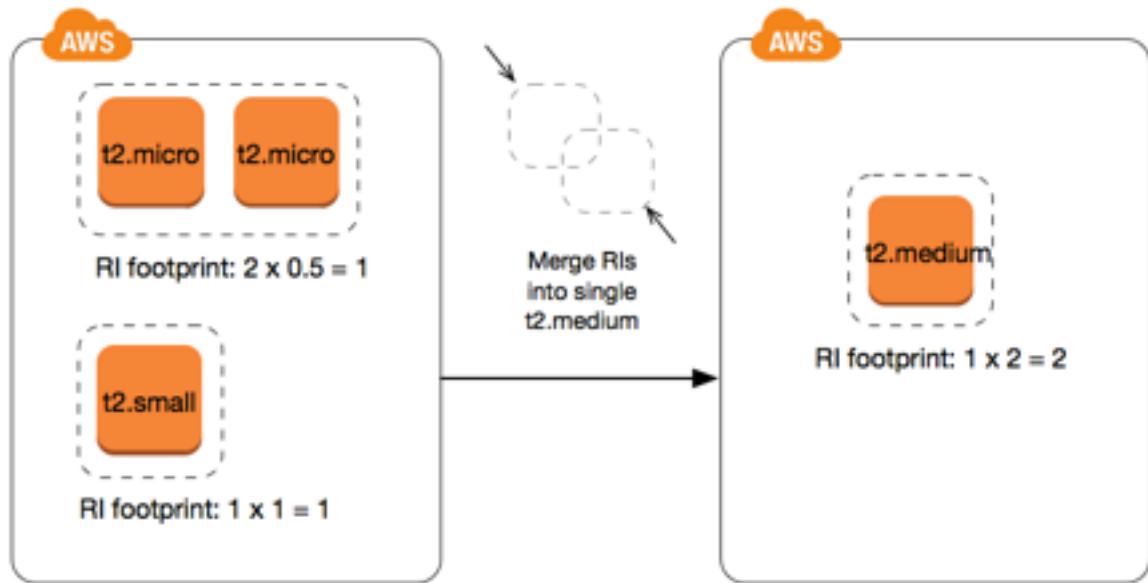
标准化因子基于实例系列中的实例大小（例如，`m1` 实例系列中的 `m1.xlarge` 实例）。这只有在同一实例系列中才有意义。不能跨实例系列修改实例类型。在 Amazon EC2 控制台中，标准化因子用单位数来度量。下表说明在实例系列中应用的标准化因子。

实例大小	标准化因子
<code>nano</code>	0.25
<code>微型</code>	0.5
<code>small</code>	1
<code>medium</code>	2
<code>large</code>	4
<code>xlarge</code>	8
<code>2xlarge</code>	16
<code>4xlarge</code>	32
<code>8xlarge</code>	64
<code>9xlarge</code>	72
<code>10xlarge</code>	80
<code>12xlarge</code>	96
<code>16xlarge</code>	128
<code>18xlarge</code>	144
<code>24xlarge</code>	192
<code>32xlarge</code>	256

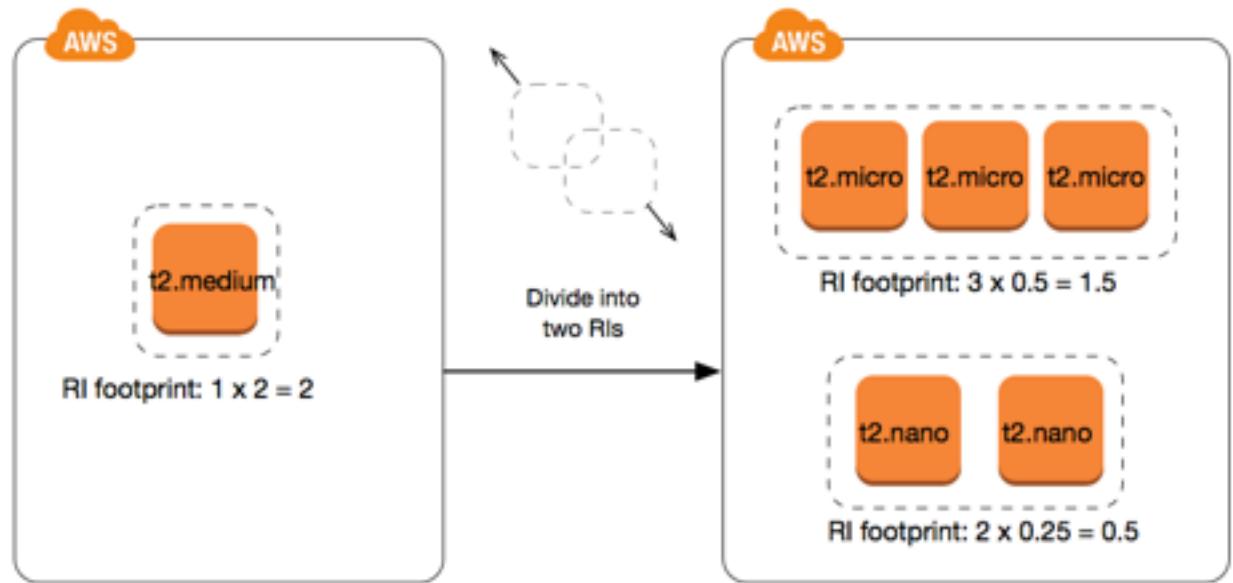
要计算Reserved Instance的实例占用空间大小，请将实例数量乘以标准化因子。例如，`t2.medium` 的标准化因子为 2，因此四个 `t2.medium` 实例的预留具有 8 个单位的占用空间。

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系列（例如 T2 实例系列）中的不同实例大小。例如，您可以将一个 `t2.large` (1×4) 实例的预留划分为四个 `t2.small` (4×1) 实例，也可以将四个 `t2.small` 实例的预留合并为一个 `t2.large` 实例。但是您不能将两个 `t2.small` (2×1) 实例的预留更改为一个 `t2.large` (1×4) 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保留空间。

在以下示例中，您的预留有两个 `t2.micro` 实例（为您带来了占用空间 1）以及带有一个 `t2.small` 实例的预留（为您带来了占用空间 1）。您可以将两个预留合并为带有单个 `t2.medium` 实例的单个预留 — 两个原始预留的组合实例大小占用空间等于修改后预留的占用空间。



您还可以修改预留以将其拆分为多个预留。在以下示例中，您有一个具有 t2.medium 实例的预留。您可以将预留拆分为具有两个 t2.nano 实例的预留，以及具有三个 t2.micro 实例的预留。



裸机实例的标准化因子

您可以将 .metal 预留实例 修改为相同系列中的其他大小，类似地，您可以将相同系列中的其他大小的 预留实例 修改为 .metal 预留实例 的大小。裸机实例的大小与相同实例系列中的最大实例的大小相同。例如，i3.metal 的大小与 i3.16xlarge 的大小相同，因此它们具有相同的标准化因子。

Note

.metal 实例大小的标准化因子不是单一的。它们会根据特定的实例系列而不同。

裸机实例大小	标准化因子
c5.metal	192
i3.metal	128
r5.metal	192
r5d.metal	192
z1d.metal	96
m5.metal	192
m5d.metal	192

例如，i3.metal 实例的标准化因子为 128。如果您购买 i3.metal 默认租期 Amazon Linux/Unix Reserved Instance，则可以按照如下方式划分预留：

- i3.16xlarge 的大小与 i3.metal 实例的大小相同，因此其标准化因子为 128 (128/1)。一个 i3.metal 实例的预留可以修改到一个 i3.16xlarge 实例中。
- i3.8xlarge 的大小是 i3.metal 实例大小的一半，因此其标准化因子为 64 (128/2)。一个 i3.metal 实例的预留可以划分到两个 i3.8xlarge 实例中。
- i3.4xlarge 的大小是 i3.metal 实例大小的四分之一，因此其标准化因子为 32 (128/4)。一个 i3.metal 实例的预留可以划分到四个 i3.4xlarge 实例中。

提交修改请求

在修改预留实例之前，请确保已阅读适用的限制 (p. 266)。在您修改实例大小之前，请计算所要修改的预留的总实例大小占用空间 (p. 266)，并确保该值与目标配置的总实例大小占用空间相匹配。

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 (预留实例) 页面上，选择一个或多个要修改的预留实例，然后依次选择 Actions (操作) 和 Modify Reserved Instances (修改预留实例)。

Note

如果 预留实例 不处于活动状态或无法修改，则 Modify 预留实例 (修改预留实例) 处于禁用状态。

3. 修改表中的第一个条目显示选定预留实例的属性，下方至少有一个目标配置。Units 列显示总实例大小占用空间。单击各个新配置的 Add 以添加。根据需要修改各配置的属性，然后选择继续：
 - Scope (范围)：选择配置是应用于可用区还是整个区域。
 - Availability Zone：选择所需的可用区。不适用于区域性预留实例。
 - 实例类型：选择所需的实例类型。组合配置必须等于原始配置的实例大小占用空间。
 - Count (数量)：指定实例数。要将预留实例拆分为多个配置，请减少数量，选择 Add (添加)，然后为其他配置指定数量。例如，如果单个配置的数量为 10，则可以将其数量更改为 6，并添加数量为 4 的配置。此过程在激活新的预留实例后会停用原始的Reserved Instance。
4. 指定好目标配置之后，若要确认您的修改选择，请选择 Submit Modifications。
5. 您可以在 预留实例 屏幕中通过查看 State (状态) 列来确定修改请求的状态。有以下可能状态。
 - active (活动) (等待修改) — 原始预留实例的转换状态

- 停用 (等待修改) — 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 — 以下选项之一：
 - 从成功的修改请求创建的新预留实例
 - 修改请求失败后的原始预留实例

使用命令行修改预留实例

1. 要修改预留实例，可以使用以下命令之一：
 - [modify-reserved-instances](#) (AWS CLI)
 - [Edit-EC2ReservedInstance](#) (适用于 Windows PowerShell 的 AWS 工具)
2. 要获取修改请求 (processing、fulfilled 或 failed) 的状态，请使用以下命令之一：
 - [describe-reserved-instances-modifications](#) (AWS CLI)
 - [Get-EC2ReservedInstancesModification](#) (适用于 Windows PowerShell 的 AWS 工具)

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。提交请求前，请确保您已阅读适用的限制 ([p. 266](#))。

并非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 Amazon EC2 控制台中的 Reserved Instances (预留实例) 页面，查看预留实例的信息。

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，但无法处理您的任何请求。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，您可能已经为想要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。

交换可转换预留实例

您可以将一个或多个可转换预留实例与具有不同配置的其他可转换预留实例（包括实例系列、操作系统和租期）进行交换。执行交换的次数没有限制，前提是目标可转换预留实例的值等于或高于要交换的可转换预留实例的值。

在交换可转换预留实例时，您当前预留的实例数与目标可转换预留实例的配置的实例数（其涵盖的值相等或更高）进行交换。Amazon EC2 计算您由于交换而可接收的预留实例数。

目录

- [交换可转换预留实例的要求 \(p. 271\)](#)
- [计算可转换预留实例交换 \(p. 271\)](#)
- [合并可转换预留实例 \(p. 272\)](#)
- [交换部分可转换预留实例 \(p. 272\)](#)
- [提交交换请求 \(p. 273\)](#)

交换可转换预留实例的要求

如果满足以下条件，Amazon EC2 将处理您的交换请求。您可转换预留实例必须：

- 处于活动状态
- 没有以前等待处理的交换请求

以下规则适用：

- 可转换预留实例 只能与当前由 AWS 提供的其他 可转换预留实例 交换。
- 可转换预留实例 与特定区域关联，在预留期限内是固定的。您不能将 可转换预留实例 与其他区域中的 可转换预留实例 进行交换。
- 一次只能将一个或多个 可转换预留实例 与一个 可转换预留实例 交换。
- 要交换部分 可转换预留实例，您可以修改它以将其拆分为两个或更多预留，然后将一个或多个预留与新 可转换预留实例 交换。有关更多信息，请参阅[交换部分可转换预留实例 \(p. 272\)](#)。有关修改 预留实例 的更多信息，请参阅[修改预留实例 \(p. 265\)](#)。
- 预付全费的 可转换预留实例 可用来交换预付部分费用的 可转换预留实例，反之亦然。

Note

如果交换所需的总预付款 (调整费用) 少于 0.00 美元，AWS 会自动向您提供可转换预留实例中可确保调整费用大于等于 0.00 美元的实例数。

Note

如果新 可转换预留实例 的总价值 (预付价格 + 每小时价格 * 剩余小时数) 少于交换的 可转换预留实例 的总价值，AWS 会自动向您提供 可转换预留实例 中可确保总价值大于等于交换的 可转换预留实例 的总价值的实例数。

- 要享受更优惠的定价，您可以将无预付费用的 可转换预留实例 交换为预付全费或预付部分费用的 可转换预留实例。
- 不能将预付全费和预付部分费用的 可转换预留实例 交换为无预付费用的 可转换预留实例。
- 仅当新 可转换预留实例 的每小时价格大于等于交换的 可转换预留实例 的每小时价格时，才能将一个无预付费用的 可转换预留实例 交换为另一个无预付费用的 可转换预留实例。

Note

如果新 可转换预留实例 的总价值 (预付价格 + 每小时价格 * 剩余小时数) 少于交换的 可转换预留实例 的总价值，AWS 会自动向您提供 可转换预留实例 中可确保总价值大于等于交换的 可转换预留实例 的总价值的实例数。

- 如果交换到期日期不同的多个 可转换预留实例，则新 可转换预留实例 的到期日期是将来最晚的日期。
- 如果您交换了单个 可转换预留实例，则它必须与新 可转换预留实例 具有相同的期限（1 年或 3 年）。如果合并期限不同的多个 可转换预留实例，则新 可转换预留实例 期限为 3 年。有关更多信息，请参阅[合并可转换预留实例 \(p. 272\)](#)。

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标价。此价目表值与您想要的可转换预留实例的价目表值比较，用于确定您可通过交换收到的实例预留数。

例如：您有 1 个 35 美金标价的可转换预留实例，您希望交换为标价为 10 美金的全新实例类型。

\$35/\$10 = 3.5

您可以将 可转换预留实例 交换为三个 10 美元的 可转换预留实例。无法购买半预留；因此必须购买额外的可转换预留实例才能涵盖剩余部分：

```
3.5 = 3 whole ##### + 1 additional #####.
```

第四个可转换预留实例与其他三个具有相同的结束日期。如果要交换部分或全部预付可转换预留实例，则需要支付第四个预留的调整费用。如果可转换预留实例的剩余预付费用为 500 USD，目标预留通常按比例分摊为 600 USD，则需要支付 100 USD。

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of original reservations = $100 difference.
```

合并可转换预留实例

如果合并两个或更多 可转换预留实例，则新 可转换预留实例 的期限必须与原始 可转换预留实例 的期限相同，或者与原始 可转换预留实例 中的最高期限相同。新可转换预留实例的到期日期是未来有效时间最长的到期日期。

例如，您的账户中有以下可转换预留实例：

Reserved Instance ID	租期	到期日期
aaaa1111	1 年	2018-12-31
bbbb2222	1 年	2018-07-31
cccc3333	3 年	2018-06-30
dddd4444	3 年	2019-12-31

- 您可以合并 aaaa1111 和 bbbb2222 并将它们与 1 年期 可转换预留实例 交换。您无法将它们与 3 年期 可转换预留实例 交换。新可转换预留实例的到期日期为 2018-12-31。
- 您可以合并 bbbb2222 和 cccc3333 并将它们与 3 年期 可转换预留实例 交换。您无法将它们与 1 年期 可转换预留实例 交换。新可转换预留实例的到期日期为 2018-07-31。
- 您可以合并 cccc3333 和 dddd4444 并将它们与 3 年期 可转换预留实例 交换。您无法将它们与 1 年期 可转换预留实例 交换。新可转换预留实例的到期日期为 2019-12-31。

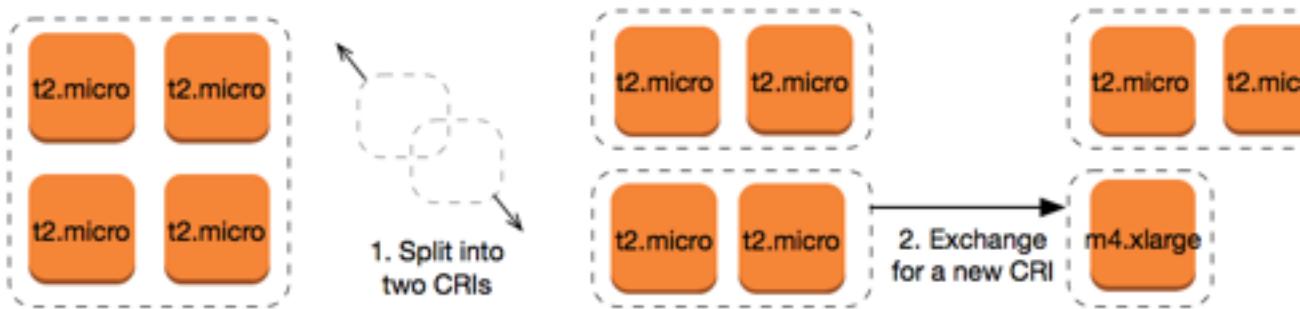
交换部分可转换预留实例

您可以使用修改过程将 可转换预留实例 拆分为较小的预留，然后将一个或多个新预留与新 可转换预留实例 交换。以下示例演示了如何执行此操作。

Example 示例：包含多个实例的可转换预留实例

在本示例中，您有一个在预留中有四个实例的 t2.micro 可转换预留实例。将两个 t2.micro 实例与一个 m4.xlarge 实例交换：

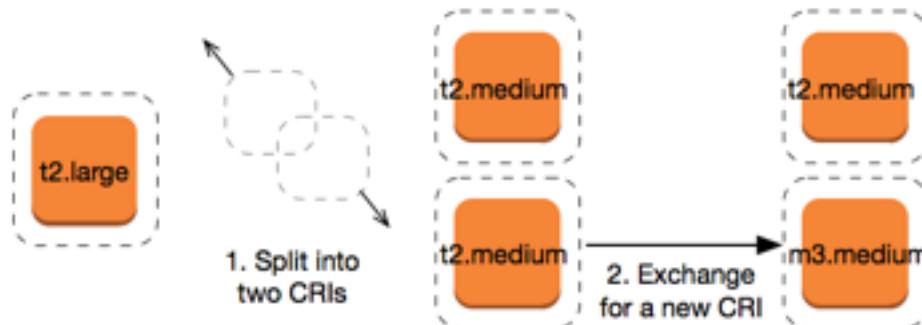
- 修改 t2.micro 可转换预留实例，方法为将其拆分为两个 t2.micro 可转换预留实例，每一个都包含两个实例。
- 将其中一个新 t2.micro 可转换预留实例 与一个 m4.xlarge 可转换预留实例 交换。



Example 示例：包含单个实例的可转换预留实例

在本示例中，您拥有一个 `t2.large` 可转换预留实例。将其更改为一个较小的 `t2.medium` 实例和一个 `m3.medium` 实例：

1. 修改 `t2.large` 可转换预留实例，方法为将其拆分为两个 `t2.medium` 可转换预留实例。单个 `t2.large` 实例具有两个 `t2.medium` 实例相同的实例大小占用空间。
2. 将其中一个新 `t2.medium` 可转换预留实例与一个 `m3.medium` 可转换预留实例交换。



有关更多信息，请参阅 [对于修改实例大小的支持 \(p. 266\)](#) 和 [提交交换请求 \(p. 273\)](#)。

提交交换请求

您可以使用 Amazon EC2 控制台或命令行工具来交换 可转换预留实例。

使用控制台交换可转换预留实例

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 Amazon EC2 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 (预留实例)，选择要交换的 可转换预留实例，然后依次选择 Actions (操作) 和 Exchange Reserved Instance (交换预留实例)。
3. 使用下拉菜单选择所需配置的属性，然后选择 Find Offering。
4. 选择新的 可转换预留实例。Instance Count (实例数量) 列显示通过交换收到的 预留实例 数。当您选择了符合要求的 可转换预留实例 时，请选择 Exchange (交换)。

已交换的 预留实例 将停用，Amazon EC2 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。

使用命令行界面交换可转换预留实例

要交换 可转换预留实例，请首先查找符合您的要求的目标 可转换预留实例：

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#) (Windows PowerShell 工具)

获取交换的报价，这包括通过交换获得的预留实例数以及交换的调整费用：

- [get-reserved-instances-exchange-quote](#) (AWS CLI)
- [GetEC2-ReservedInstancesExchangeQuote](#) (Windows PowerShell 工具)

最后，执行交换：

- [accept-reserved-instances-exchange-quote](#) (AWS CLI)
- [Confirm-EC2ReservedInstancesExchangeQuote](#) (Windows PowerShell 工具)

计划的预留实例

利用计划的预留实例（计划实例），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。

如果需要持续的容量预留，预留实例可能符合这种需求并且可以降低成本。有关更多信息，请参阅[预留实例 \(p. 243\)](#)。如果实例运行时间比较灵活，Spot 实例可能符合这种需求并且可以降低成本。有关更多信息，请参阅[Spot 实例 \(p. 277\)](#)。

目录

- [计划实例如何运行 \(p. 274\)](#)
- [计划实例的服务相关角色 \(p. 275\)](#)
- [购买计划实例 \(p. 275\)](#)
- [启动计划实例 \(p. 276\)](#)
- [计划实例限制 \(p. 276\)](#)

计划实例如何运行

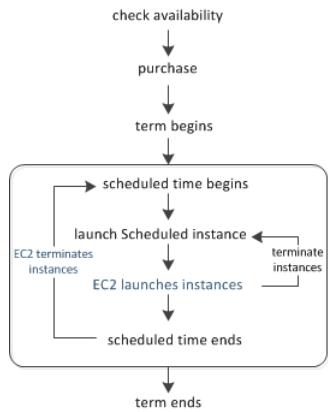
Amazon EC2 在每个可用区内都留下了一些 EC2 实例池以用作计划实例。每个池都支持实例类型、操作系统和网络的一个特定组合。

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。



计划实例的服务相关角色

当您购买计划实例时，Amazon EC2 将创建一个服务相关角色。服务相关角色包含 Amazon EC2 代表您调用其他 AWS 服务所需的一切权限。有关更多信息，请参阅 IAM 用户指南 中的[使用服务相关角色](#)。

Amazon EC2 使用名为 AWSServiceRoleForEC2ScheduledInstances 的服务相关角色完成以下操作：

- `ec2:TerminateInstances` - 在计划实例的计划完成后终止该实例
- `ec2:CreateTags` - 向计划实例添加系统标签

如果您在 2017 年 10 月前购买了计划实例，当 Amazon EC2 开始支持此服务相关角色时，Amazon EC2 在您的 AWS 账户中创建了 AWSServiceRoleForEC2ScheduledInstances 角色。有关更多信息，请参阅 IAM 用户指南中的[我的账户中出现新角色](#)。

如果您不再需要使用计划实例，我们建议您删除 AWSServiceRoleForEC2ScheduledInstances 角色。当此角色从您的账户中删除后，如果您购买计划实例，Amazon EC2 将再次创建此角色。

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（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 INSTANCE 下，选择 Scheduled Instances。如果当前所选的区域不支持计划实例，则该页面不可用。[了解更多 \(p. 276\)](#)
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使用率（每年 1200 个小时）的最短持续时间指定一个值。

Create a schedule

Starting on for duration 4 hours
 +/- 2 hours

Recurring

- 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。

Instance details

Platform Instance type

Availability Zone

- 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。

购买计划实例 (AWS CLI)

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。

启动计划实例 (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。如果当前所选的区域不支持计划实例，则该页面不可用。[了解更多 \(p. 276\)](#)
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。

启动计划实例 (AWS CLI)

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限制：

- 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)。
- 所需的最低使用率为每年 1200 个小时。
- 您最多可以提前三个月购买计划实例。
- 它们在以下区域中提供：美国东部（弗吉尼亚北部）、美国西部（俄勒冈）和欧洲（爱尔兰）。

Spot 实例

Spot 实例是一种未使用的 EC2 实例，以低于按需价格提供。由于 Spot 实例 允许您以极低的折扣请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。Spot 实例的每小时价格称为 Spot 价格。每个可用区中的每种实例类型的价格是由 Amazon EC2 设置的，并根据 Spot 实例 的长期供求趋势逐步调整价格。只要容量可用，并且请求的每小时最高价超过 Spot 价格，Spot 实例就会运行。

如果能灵活控制应用程序的运行时间并且应用程序可以中断，Spot 实例就是经济实惠之选。例如，Spot 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 Spot 实例](#)。

主题

- [概念 \(p. 277\)](#)
- [如何开始 \(p. 278\)](#)
- [相关服务 \(p. 279\)](#)
- [定价和节省 \(p. 279\)](#)

概念

在开始使用 Spot 实例之前，应该熟悉以下概念：

- Spot 实例池 – 一组未使用的 EC2 实例，它们具有相同的实例类型（例如 `m5.large`）、操作系统、可用区和网络平台。
- Spot 价格 – Spot 实例 的当前每小时价格。
- Spot 实例 请求 – 提供您愿意为 Spot 实例 支付的每小时最高价。如果未指定最高价，则默认最高价为按需价格。如果具有可用的容量，并且您的请求的每小时最高价超过 Spot 价格，Amazon EC2 将完成您的请求。Spot 实例 请求可以是一次性 或持久性 请求。Amazon EC2 会在与持久性 Spot 请求关联的 Spot 实例 终止之后自动重新提交该请求。Spot 实例 请求可选择为 Spot 实例 指定一个持续时间。
- Spot 队列 – 一组基于指定条件启动的 Spot 实例。Spot 队列 选择满足您的需要的 Spot 实例 池，并启动 Spot 实例 以满足队列的目标容量。默认情况下，在队列中的 Spot 实例 终止之后，系统会启动替换实例 以保持 Spot 队列 的目标容量。您可以将 Spot 队列 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。您可以在 Spot 队列 请求中包含 个按需实例 请求。
- Spot 实例 中断 – 如果 Spot 价格超过您的请求的最高价，或者不再具有可用的容量，Amazon EC2 将终止、停止或休眠您的 Spot 实例。Amazon EC2 将提供 Spot 实例 中断通知，这会在实例中断之前为其提供两分钟的警告。

Spot 实例 与 按需实例 的主要区别

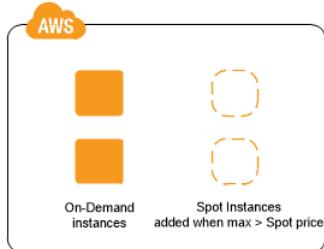
下表列出了 Spot 实例 与 按需实例 之间的主要区别。

	Spot 实例	按需实例
启动时间	只有 Spot 请求处于活动状态并且有可用容量时才能立即启动。	只有发出手动启动请求并且有可用容量时才能立即启动。

	Spot 实例	按需实例
可用容量	如果没有可用容量，则 Spot 请求会继续自动发起启动请求，直到有可用容量为止。	如果在发出启动请求时没有可用容量，您会收到容量不足错误 (ICE)。
每小时价格	Spot 实例的每小时价格根据需求而有所不同。	按需实例的每小时价格是静态的。
实例中断	您无法停止和启动由 Amazon EBS 支持的 Spot 实例；只有 Amazon EC2 Spot 服务可以执行该操作。如果容量不再可用、Spot 价格超出您的最高价或者对 Spot 实例 的需求增加，Amazon EC2 Spot 服务可以中断 (p. 325)个别 Spot 实例。	您可以决定何时中断个按需实例 (停止或终止)。

有关使用 Spot 实例 的策略

一种为应用程序维护最低级别的保障计算资源的策略是，启动一组核心 按需实例，再适机通过 Spot 实例 来进行补充。



另一个策略是启动具有指定持续时间（也称为 Spot 型限制）的 Spot 实例，这些实例不会中断并且会在您选择的持续时间内连续运行。在极少数情况下，Spot 型限制会由于 Amazon EC2 的容量需求而中断。在这种情况下，我们将在终止实例前提供两分钟的警告，即使您使用了此已终止的实例，也无需为其支付费用。有关更多信息，请参阅 [定义 Spot 实例的持续时间 \(p. 290\)](#)。

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 Spot 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 \(p. 18\)](#)
- [Amazon EC2 Linux 实例入门 \(p. 24\)](#)

Spot 基础知识

- [Spot 实例的工作原理 \(p. 280\)](#)
- [Spot 队列的工作原理 \(p. 281\)](#)

使用 Spot 实例

- [准备中断 \(p. 328\)](#)
- [创建Spot 实例请求 \(p. 292\)](#)
- [获取请求状态信息 \(p. 323\)](#)

使用 Spot 队列

- [Spot 队列先决条件 \(p. 297\)](#)
- [创建Spot 队列请求 \(p. 300\)](#)

相关服务

您可以直接使用 Amazon EC2 预置 Spot 实例。也可以使用其他 AWS 服务预置 Spot 实例。有关更多信息，请参阅以下文档。

Amazon EC2 Auto Scaling 和 Spot 实例

您可以用自己愿意支付的最高价创建启动模板或配置，以便 Amazon EC2 Auto Scaling 可以启动 Spot 实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的[在您的 Auto Scaling 组中启动 Spot 实例](#) 和[使用多个实例类型和购买选项](#)。

Amazon EMR 和 Spot 实例

有时候，在 Amazon EMR 集群中运行 Spot 实例 会非常有帮助。有关更多信息，请参阅 Amazon EMR 管理指南中的[Spot 实例](#) 和[什么时候应该使用 Spot 实例](#)。

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 模板可能包含您愿意支付的最高价。有关更多信息，请参阅[EC2 Spot 实例更新 - Auto Scaling 和 CloudFormation 集成](#)。

AWS SDK for Java

可以使用 Java 编程语言来管理 Spot 实例。有关更多信息，请参阅[教程：Amazon EC2 Spot 实例](#) 和[教程：高级 Amazon EC2 Spot 请求管理](#)。

适用于 .NET 的 AWS 开发工具包

可以使用 .NET 编程环境来管理 Spot 实例。有关更多信息，请参阅[教程：Amazon EC2 Spot 实例](#)。

定价和节省

您可以为 Spot 实例 支付 Spot 价格，该价格由 Amazon EC2 设置，并根据 Spot 实例 的长期供求趋势逐步进行调整。如果具有可用的容量，并且您的请求的最高价超过当前 Spot 价格，Amazon EC2 将完成您的请求。您的 Spot 实例 将一直运行，直到您终止这些实例、不再具有可用的容量、Spot 价格超过您的最高价或您的 Amazon EC2 Auto Scaling 组在[缩减](#)期间终止这些实例。

具有预定义持续时间的 Spot 实例 使用的固定每小时价格在 Spot 实例 运行时仍然有效。

如果您或 Amazon EC2 中断正在运行的 Spot 实例，您将按使用的秒数或整个小时付费，或者您不收取任何费用，具体取决于所使用的操作系统以及 Spot 实例的中断方。有关更多信息，请参阅[中断的 Spot 实例 的计费 \(p. 330\)](#)。

查看价格

要查看各个 AWS 区域和实例类型的当前（每 5 分钟更新一次）最低 Spot 价格，请参阅[Spot 实例定价](#)页面。

要查看过去三个月的 Spot 价格历史记录，请使用 Amazon EC2 控制台或 `describe-spot-price-history` 命令 (AWS CLI)。有关更多信息，请参阅[Spot 实例定价历史记录 \(p. 287\)](#)。

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。

查看节省

您可以查看单个 Spot 队列或所有 Spot 实例通过使用 Spot 实例节省的费用。您可以查看过去一小时或过去三天的节省，还可以查看每 vCPU 小时和每内存 (GiB) 小时的平均费用。节省是估算的，因为未算入您使用期间的计费调整，所以可能与实际的节省有所差异。有关查看节省信息的更多信息，请参阅[通过购买 Spot 实例 实现节省 \(p. 287\)](#)。

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](#)。

Spot 实例的工作原理

要使用 Spot 实例，请创建一个 Spot 实例 请求 或 Spot 队列 请求。该请求可能包含您愿意为每个实例支付的每小时最高价 (默认为按需价格) 以及其他限制 (如实例类型和可用区)。如果您的最高价超过指定实例的当前 Spot 价格，并且具有可用的容量，则会立即完成您的请求。否则，只要最高价超过 Spot 价格，并且具有可用的容量，就会完成该请求。Spot 实例将一直运行，直到您终止这些实例或 Amazon EC2 必须中断这些实例 (也称为Spot 实例 中断) 。

使用 Spot 实例 时，必须做好应对中断的准备。如果 Spot 实例 需求增加或 Spot 实例 供应减少，在 Spot 价格超过您的最高价时，Amazon EC2 可能会中断您的 Spot 实例。在 Amazon EC2 中断 Spot 实例 时，将提供 Spot 实例 中断通知，这会在 Amazon EC2 终止该实例之前为其提供两分钟的警告。无法为 Spot 实例 启用终止保护。有关更多信息，请参阅[Spot 实例中断 \(p. 325\)](#)。

如果由 Amazon EBS 支持的实例是 Spot 实例，您无法停止和启动该实例 (只有 Spot 服务才能停止和启动 Spot 实例)，但可以重新引导或终止 Spot 实例。

目录

- [在启动组中启动 Spot 实例 \(p. 280\)](#)
- [在可用区组中启动 Spot 实例 \(p. 280\)](#)
- [在 VPC 中启动 Spot 实例 \(p. 281\)](#)

在启动组中启动 Spot 实例

在 Spot 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 Spot 实例时才启动该组。此外，如果 Spot 服务必须终止启动组中的某个实例 (例如，如果 Spot 价格超过您的最高价)，它必须终止所有实例。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。

尽管此选项有用处，但是添加此约束会减少完成 Spot 实例 请求的几率并且增加 Spot 实例 被终止的几率。例如，启动组包括多个可用区中的实例。如果其中一个可用区中的容量减少且不再可用，则 Amazon EC2 会终止启动组的所有实例。

如果您创建了另一个成功的Spot 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 Spot 实例

在 Spot 实例 请求中指定可用区组，可以通知 Spot 服务在同一可用区中启动一组 Spot 实例。Amazon EC2 不需要同时中断某个可用区组中的所有实例。如果 Amazon EC2 必须中断可用区组中的某个实例，剩余的实例仍保持运行。

虽然此选项非常有用，但添加此约束会减少完成您的Spot 实例请求的几率。

如果您指定了可用区组，但未在 Spot 实例 请求中指定可用区，则具体结果将取决于您所指定的网络。

默认 VPC

Amazon EC2 使用指定子网的可用区。如果您未指定子网，它会为您选择一个可用区及其默认子网，但不一定是价格最低的可用区。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 Spot 实例

按照为 按需实例 指定子网的相同方法，为您的 Spot 实例 指定子网。

- 您应该使用默认最高价 (按需价格)，或者根据 VPC 中的 Spot 实例的 Spot 价格历史记录指定最高价。
- [默认 VPC] 如果希望在特定的低价格可用区中启动您的 Spot 实例，您必须在 Spot 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 Spot 价格不一定是最低的。
- [非默认 VPC] 您必须为您的Spot 实例指定子网。

Spot 队列的工作原理

Spot 队列 是 Spot 实例 和可选的 按需实例 的集合或队列。

Spot 队列 会尝试启动适当数量的 Spot 实例 和 按需实例，以满足在 Spot 队列 请求中指定的目标容量要求。如果具有可用的容量，并且在 Spot 实例请求中指定的最高价格超过当前 Spot 价格，则会完成该请求。如果 Spot 实例中断，Spot 队列还会尝试保持其目标容量队列。

也可以设置您愿意为队列支付的每小时最大金额，Spot 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

Spot 实例 池 是一组未使用的 EC2 实例，具有相同的实例类型（例如 m5.large）、操作系统、可用区和网络平台。在您发出Spot 队列请求时，您可以指定多个启动规范（因实例类型、AMI、可用区或子网而异）。Spot 队列 会基于 Spot 队列 请求中包含的启动规范以及 Spot 队列 的配置来选择用于执行请求的 Spot 实例 池。Spot 实例来自所选的池。

目录

- [Spot 队列中的按需容量 \(p. 281\)](#)
- [Spot 实例分配策略 \(p. 282\)](#)
- [Spot 价格覆盖 \(p. 283\)](#)
- [控制支出 \(p. 283\)](#)
- [Spot 队列实例权重 \(p. 284\)](#)
- [演练：将 Spot 队列 与实例权重结合使用 \(p. 285\)](#)

Spot 队列中的按需容量

为确保始终拥有实例容量，您可以在 Spot 队列请求中包含按需容量请求。在 Spot 队列请求中，您需要指定所需的目标容量以及该容量中有多少必须是按需容量。余量由 Spot 容量组成，后者在有可用的 Amazon EC2 容量并且可用时启动。例如，如果您在 Spot 队列 请求中指定目标容量为 10，按需容量为 8，则 Amazon EC2 启动 8 个容量单位作为按需实例，启动 2 个容量单位 (10-8=2) 作为 Spot 实例。

针对按需容量优化实例类型

Spot 队列 尝试满足您的按需容量时，它会默认首先启动价格最低的实例类型。如果 OnDemandAllocationStrategy 设置为 prioritized，Spot 队列 使用优先级来确定首先使用什么实例类型来满足按需容量。优先级分配给启动模板覆盖，优先级最高的最先启动。

例如，您可以配置三个启动模板覆盖，每个覆盖具有不同的实例类型：c3.large、c4.large 和 c5.large。c5.large 的按需价格低于 c4.large。c3.large 价格最低。如果您不使用优先级来确定顺序，则机群按照从 c3.large 开始、然后 c5.large 的顺序满足按需容量。由于您的 c4.large 经常会有未使用的预留实例，您可以设置启动模板覆盖优先级，这样其顺序就是 c4.large、c3.large、c5.large。

Spot 实例分配策略

Spot 队列中 Spot 实例的分配策略决定了如何根据启动规范从可能的 Spot 实例池执行 Spot 队列请求。以下是您在 Spot 队列请求中可以指定的分配策略：

`lowestPrice`

Spot 实例来自价格最低的池。这是默认策略。

`diversified`

Spot 实例分布在所有池中。

`capacityOptimized`

Spot 实例来自为启动的实例数量提供最佳容量的池。

`InstancePoolsToUseCount`

Spot 实例分布在您指定数量的 Spot 池中。此参数仅在与 `lowestPrice` 结合使用时有效。

维持目标容量

在 Spot 实例因 Spot 实例池的 Spot 价格或可用容量发生变化而终止之后，`maintain` 类型的 Spot 队列会启动替换 Spot 实例。如果分配策略是 `lowestPrice`，则队列在当前具有最低 Spot 价格的池中启动替换实例。如果分配策略是 `diversified`，则队列在其余池间分配替换 Spot 实例。如果分配策略是 `lowestPrice` 与 `InstancePoolsToUseCount` 的组合，则队列选择具有最低价格的 Spot 池并跨您指定数量的 Spot 池启动 Spot 实例。

配置 Spot 队列，实现成本优化

要优化 Spot 实例使用成本，请指定 `lowestPrice` 分配策略，以便 Spot 队列自动基于当前 Spot 价格部署实例类型和可用区的最低成本组合。

对于个按需实例目标容量，Spot 队列始终根据公开按需价格选择成本最低的实例类型，同时对 Spot 实例继续按照策略（`lowestPrice`、`capacityOptimized` 或 `diversified`）执行分配。

配置 Spot 队列以实现成本优化和多元化

要以低成本且多元化的方式创建 Spot 实例队列，请将 `lowestPrice` 分配策略与 `InstancePoolsToUseCount` 结合使用。Spot 队列基于您指定数量的 Spot 池中的当前 Spot 价格，自动部署实例类型和可用区的最低成本组合。此组合可用于避免最昂贵的 Spot 实例。

配置 Spot 队列以实现容量优化

使用 Spot 实例，定价会根据长期供需趋势缓慢发生变化，但容量会实时波动。`capacityOptimized` 策略通过查看实时容量数据并预测可用性最高的池，自动在可用性最高的池中启动 Spot 实例。这适用于与中断相关的重启工作和检查点成本较高的工作负载，例如大数据和分析、图像和媒体渲染、机器学习以及高性能计算。通过实现更低的中断可能性，`capacityOptimized` 策略可以降低您工作负载的整体成本。

选择合适的分配策略

您可以基于自己的使用案例来优化 Spot 队列。

如果您的队列较小或只是短时间运行，则您的 Spot 实例实例中断的可能性较低（即使所有实例都在同一个 Spot 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。

如果队列较大或长时间运行，则可以通过在多个池间分配 Spot 实例来提高队列的可用性。例如，如果 Spot 队列请求指定 10 个池，目标容量为 100 个实例，则队列会在每个池中启动 10 个 Spot 实例。如果某个池的 Spot 价格超过您在该池中的最高价，您的队列仅 10% 受到影响。使用此策略还可降低您的队列对单个池的 Spot 价格随时间上涨的敏感度。

使用 `diversified` 策略时，Spot 队列不在 Spot 价格等于或高于按需价格的任何池中启动 Spot 实例。

要创建低成本且多元化的机群，请将 `lowestPrice` 策略与 `InstancePoolsToUseCount` 结合使用。您可以使用少量或大量的 Spot 池以在其中分配您的 Spot 实例。例如，如果您运行批处理，我们建议指定少量的 Spot 池（例如，`InstancePoolsToUseCount=2`）以确保队列始终具有计算容量，同时尽可能节省成本。如果您运行 Web 服务，我们建议指定较大量数的 Spot 池（例如，`InstancePoolsToUseCount=10` 个）以最大限度减少 Spot 实例池暂时不可用造成的影响。

如果您的队列运行的工作负载可能会因重启工作和检查点而导致更高的中断成本，则使用 `capacityOptimized` 策略。此策略提供更低的中断可能性，这可以降低您工作负载的整体成本。

Spot 价格覆盖

每个 Spot 队列 请求可能包含全局最高价，或者使用默认价格（按需价格）。Spot 队列 将该价格作为每个启动规范的默认最高价。

您可以选择在一个或多个启动规范中指定最高价。该价格是启动规范特有的。如果启动规范包含特定的价格，则 Spot 队列 使用该最高价以覆盖全局最高价。不包含特定最高价的任何其他启动规范仍使用全局最高价。

控制支出

在达到目标容量或您愿意支付的最大金额时，Spot 队列 停止启动实例。要控制您每小时为队列支付的金额，您可以为 Spot 实例指定 `SpotMaxTotalPrice` 并为按需实例指定 `OnDemandMaxTotalPrice`。在达到最高总价时，即使未达到目标容量，Spot 队列 也会停止启动实例。

以下示例显示了两个不同的方案。在第一个方案中，在达到目标容量时，Spot 队列 停止启动实例。在第二个方案中，在达到您愿意支付的最大金额时，Spot 队列 停止启动实例。

示例：在达到目标容量时，停止启动实例

假设发出 `m4.large` 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- `OnDemandTargetCapacity`：10
- `OnDemandMaxTotalPrice`：1.50 美元

Spot 队列 启动 10 个按需实例，因为总价 1.00 美元（10 个实例 × 0.10 美元）不超过 `OnDemandMaxTotalPrice`（1.50 美元）。

示例：在达到最高总价时，停止启动实例

假设发出 `m4.large` 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- `OnDemandTargetCapacity`：10
- `OnDemandMaxTotalPrice`：0.80 美元

如果 Spot 队列 启动按需目标容量（10 个按需实例），则每小时的总成本为 1.00 美元。该值超过了为 `OnDemandMaxTotalPrice` 指定的金额（0.80 美元）。为了防止支出超过您愿意支付的金额，Spot 队列 仅启动 8 个按需实例（低于按需目标容量），因为启动更多实例将超过 `OnDemandMaxTotalPrice`。

Spot 队列实例权重

在请求 Spot 实例队列时，可以使用实例权重 定义每种实例类型为应用程序能贡献的容量单位，并相应地为每个 Spot 实例池调整最高价。

默认情况下，您指定的价格是每实例小时 价格。在使用实例权重功能时，您指定的价格是每单位小时 价格。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价格。Spot 队列 将目标容量除以实例权重以计算要启动的 Spot 实例 数。如果结果不是整数，则 Spot 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。Spot 队列 可以选择您在启动规范中指定的任意池，即使所启动实例的容量超过请求的目标容量也是如此。

下表提供了确定目标容量为 10 的 Spot 队列请求的每单位价格的计算示例。

实例类型	实例权重	每实例小时价格	每单位小时价格	启动的实例数
r3.xlarge	2	0.05 美元	0.025 (0.05 除以 2)	5 (10 除以 2)

实例类型	实例权重	每实例小时价格	每单位小时价格	启动的实例数
r3.8xlarge	8	0.10 美元	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 Spot 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 Spot 队列设置目标容量。
2. 设置每单位价格。
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 Spot 队列请求：

- 目标容量为 24
- 一个实例类型为 r3.2xlarge 且权重为 6 的启动规范
- 一个实例类型为 c3.xlarge 且权重为 5 的启动规范

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动规范提供了最低的每单位价格（r3.2xlarge 每实例小时价格除以 6），Spot 队列将启动其中的四个实例（24 除以 6）。

如果第二个启动规范提供了最低的每单位价格（c3.xlarge 每实例小时价格除以 5），则 Spot 队列会启动 5 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 Spot 队列请求：

- 目标容量为 30
- 一个实例类型为 c3.2xlarge 且权重为 8 的启动规范
- 一个实例类型为 m3.xlarge 且权重为 8 的启动规范
- 一个实例类型为 r3.xlarge 且权重为 8 的启动规范

Spot 队列会启动四个实例 (30 除以 8，结果向上舍入)。在使用 `lowestPrice` 策略时，所有四个实例均来自提供最低每单位价格的池。使用 `diversified` 策略时，Spot 队列会在所有三个池中各启动一个实例，并在三个池中提供最低每单位价格的那个池中启动第四个实例。

演练：将 Spot 队列与实例权重结合使用

该演练使用一个名为 Example Corp 的虚构公司说明使用实例权重请求Spot 队列的过程。

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[Spot 最佳实践](#)。然后，Example Corp 确定了他们的Spot 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Spot 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Spot 队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时价格

Example Corp 将每实例小时[按需价格](#)作为其价格的起点。他们也可以使用最近的 Spot 价格或两者的组合。为了计算每单位小时价格，他们将每实例小时起始价格除以权重。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 美元	1	0.7 美元

实例类型	按需价格	实例权重	每单位小时价格
r3.4xLarge	1.4 美元	2	0.7 美元
r3.8xLarge	2.8 美元	4	0.7 美元

Example Corp 可能会使用每单位小时全局价格 0.7 美元，这对于所有三种实例类型来说是非常有竞争力的。他们可能还会使用每单位小时全局价格 0.7 美元，并在 `r3.8xlarge` 启动规范中使用特定的每单位小时价格 0.9 美元。

验证权限

在创建 Spot 队列 请求之前，Example Corp 会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[Spot 队列先决条件 \(p. 297\)](#)。

创建请求

Example Corp 为其 Spot 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/aws-ec2-spot-fleet-tagging-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 Spot 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[Spot 队列请求 \(p. 296\)](#)。

执行

分配策略确定 Spot 实例所来自的 Spot 实例池。

在使用 `lowestPrice` 策略 (这是默认策略) 时，Spot 实例来自在完成请求时具有最低每单位价格的池。为了提供 20 个单位的容量，Spot 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)。

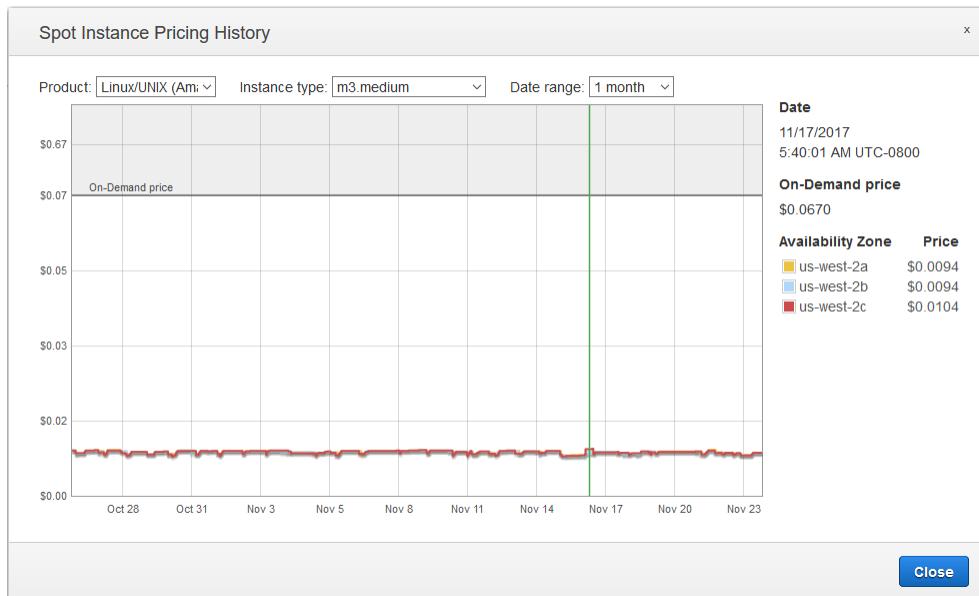
如果 Example Corp 使用 *diversified* 策略，则 Spot 实例来自所有三个池。Spot 队列会启动 6 个 *r3.2xlarge* 实例（提供 6 个单位）、3 个 *r3.4xlarge* 实例（提供 6 个单位）和 2 个 *r3.8xlarge* 实例（提供 8 个单位），总共 20 个单位。

Spot 实例定价历史记录

在请求 Spot 实例时，建议使用默认最高价（按需价格）。如果要指定最高价，我们建议您在这样做之前查看 Spot 价格历史记录。您可以查看最近 90 天的 Spot 价格历史记录，并按照实例类型、操作系统和可用区筛选。

查看 Spot 价格历史记录（控制台）

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 Spot 实例，您将看到欢迎页面。选择试用，滚动到屏幕底部，然后选择取消。
4. 选择 Pricing History。
5. 选择操作系统（Product（产品））、Instance type（实例类型）和要查看价格历史记录的 Date range（日期范围）。将指针移动到图形上可显示选定日期范围内的特定时间的价格。



- 6.（可选）要查看特定可用区的 Spot 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 Spot 价格历史记录

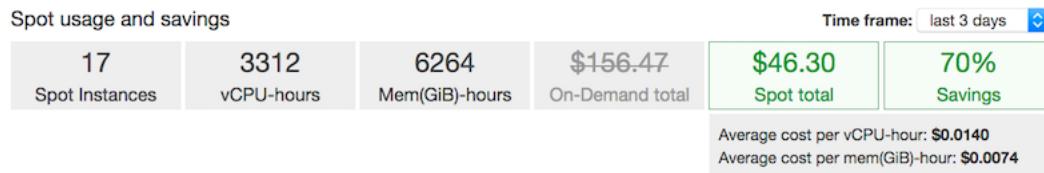
您可以使用以下任一命令。有关更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-spot-price-history](#) (AWS CLI)
- [Get-EC2SpotPriceHistory](#) (适用于 Windows PowerShell 的 AWS 工具)

通过购买 Spot 实例 实现节省

您可以在每个队列级别或针对所有正在运行的 Spot 实例，查看 Spot 实例的用量和节省信息。在每个队列级别，用量和节省信息包括该队列启动和终止的所有实例。您可以查看过去一小时或过去三天的此信息。

来自“Spot Requests (Spot 请求)”页面的以下屏幕截图显示了 Spot 队列的 Spot 用量和节省信息。



Details					
c3.large (8)	1152 vCPU-hours	2160 mem(GiB)-hours	\$16.82 total	72% savings	
c4.xlarge (6)	1728 vCPU-hours	3240 mem(GiB)-hours	\$26.48 total	69% savings	
t2.medium (3)	432 vCPU-hours	864 mem(GiB)-hours	\$3.00 total	70% savings	

您可查看以下用量和节省信息：

- Spot 实例 – Spot 队列 所启动和终止的 Spot 实例 数。在查看节省摘要时，该数字表示您的所有正在运行的 Spot 实例。
- vCPU-hours (vCPU 小时数) – 在所选时间范围内所有 Spot 实例 使用的 vCPU 小时数。
- Mem(GiB)-hours (内存 (GiB) 小时数) – 在所选时间范围内所有 Spot 实例 使用的 GiB 小时数。
- On-Demand total (按需总额) – 您在将这些实例作为 按需实例 启动后，在所选时间范围内支付的总额。
- Spot total (Spot 总额) – 您在所选时间范围内支付的总额。
- Savings (节省) – 您通过未支付按需价格而节省的百分比。
- Average cost per vCPU-hour (每 vCPU 小时的平均费用) – 在所选时间范围内所有 Spot 实例 使用 vCPU 的平均小时费用，其计算方式如下：每 vCPU 小时的平均费用 = Spot 总额 / vCPU 小时数。
- Average cost per mem(GiB)-hour (每内存 (GiB) 小时的平均费用) – 在所选时间范围内所有 Spot 实例 使用 GiB 的平均小时费用，其计算方式如下：每内存 (GiB) 小时的平均费用 = Spot 总额 / 内存 (GiB) 小时数。
- Details (详细信息) 表 – 构成 Spot 队列 的各种实例类型 (每个实例类型的实例数括在圆括号中)。在查看节省摘要时，这些数字涵盖了您的所有正在运行的 Spot 实例。

节省信息只能使用 Amazon EC2 控制台查看。

查看 Spot 队列 的节省信息 (控制台)

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. 选择一个 Spot 队列 请求，然后选择 Savings (节省)。
4. 默认情况下，该页面显示过去三天的用量和节省信息。您可以选择 last hour (过去一小时) 或 last three days (过去三天)。对于不到一小时之前启动的 Spot 队列，该页面显示这一小时的预计节省。

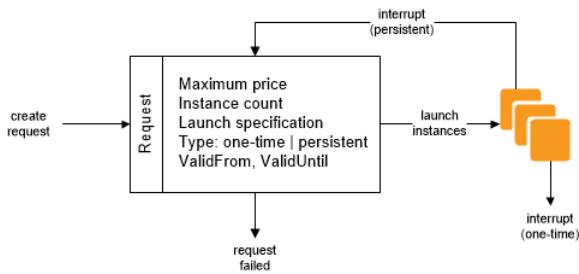
查看所有正在运行的 Spot 实例 的节省信息 (控制台)

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 Savings Summary (节省摘要) 选项卡。

Spot 实例请求

要使用 Spot 实例，您需要创建 Spot 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实例小时支付的最高价。如果具有可用的容量，并且您的最高价超过当前 Spot 价格，Amazon EC2 将立即完成您的请求。否则，Amazon EC2 将等待直至可以完成您的请求，或者直至您取消请求。

以下演示了 Spot 请求的运行方式。请注意，为 Spot 实例中断执行的操作取决于请求类型 (一次性还是持久性) 和中断行为 (休眠、停止或终止)。如果请求是持久性请求，则在Spot 实例中断之后将重新打开请求。



目录

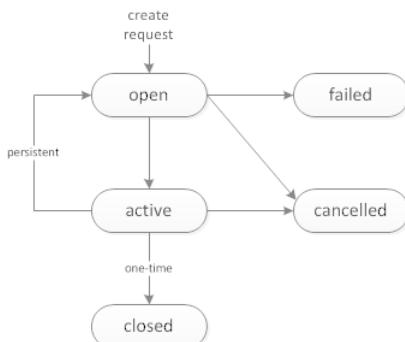
- [Spot 实例请求状态 \(p. 289\)](#)
- [定义 Spot 实例的持续时间 \(p. 290\)](#)
- [指定 Spot 实例的租期 \(p. 290\)](#)
- [Spot 实例请求的服务相关角色 \(p. 291\)](#)
- [创建Spot 实例请求 \(p. 292\)](#)
- [查找正在运行的 Spot 实例 \(p. 293\)](#)
- [标记Spot 实例请求 \(p. 293\)](#)
- [取消Spot 实例请求 \(p. 294\)](#)
- [终止 Spot 实例 \(p. 294\)](#)
- [Spot 请求示例启动规范 \(p. 294\)](#)

Spot 实例请求状态

Spot 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 Spot 实例。
- **failed** – 请求的一个或多个参数错误。
- **closed** – Spot 实例被中断或终止。
- **cancelled** – 您取消了请求或请求已过期。

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 Spot 实例请求在 Amazon EC2 启动 Spot 实例、请求过期前或者您取消请求前保持有效。如果 Spot 价格超过您的最高价或容量不可用，将终止您的 Spot 实例并关闭 Spot 实例请求。

持久性Spot 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。如果 Spot 价格超过您的最高价或没有可用的容量，您的Spot 实例将会中断。在您的实例中断后，在最高价超过 Spot 价格或再次具

有可用的容量时，将会启动 Spot 实例（如果已停止）或将其恢复（如果已休眠）。如果 Spot 实例已终止，则会重新打开 Spot 实例请求，并且 Amazon EC2 会启动一个新 Spot 实例。

您可以跟踪 Spot 实例请求的状态以及通过该状态启动的 Spot 实例的状态。有关更多信息，请参阅 [Spot 请求状态 \(p. 320\)](#)。

定义 Spot 实例的持续时间

具有定义的持续时间（也称为 Spot 型限制）的 Spot 实例不会中断并且会在您选择的持续时间内连续运行。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。

您可以使用 1、2、3、4、5 或 6 小时的持续时间。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 [Spot 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 Spot 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。不足一个实例小时的部分的计费将精确到秒。

在您的 Spot 请求中定义持续时间时，每个 Spot 实例的持续时间段将在该实例收到其实例 ID 后立即开始。Spot 实例将运行，直到您终止它或其持续时间段结束。在持续时间期间结束后，Amazon EC2 将 Spot 实例标记为终止并提供一个 Spot 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。在极少数情况下，Spot 型限制会由于 Amazon EC2 的容量需求而中断。在这种情况下，我们将在终止实例前提供两分钟的警告，即使您使用了此已经终止的实例，也无需为其支付费用。

启动具有定义的持续时间的 Spot 实例（控制台）

有关更多信息，请参阅 [创建Spot 队列请求 \(p. 300\)](#)。

启动具有定义的持续时间的 Spot 实例 (AWS CLI)

要为您的 Spot 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，下面的命令创建一个 Spot 请求，用于启动运行时间为两小时的 Spot 实例：

```
aws ec2 request-spot-instances --instance-count 5 --block-duration-minutes 120 --type "one-time" --launch-specification file:///specification.json
```

检索具有定义的持续时间的 Spot 实例的费用 (AWS CLI)

使用 `describe-spot-instance-requests` 命令可检索具有指定持续时间的 Spot 实例的固定费用。该信息位于 `actualBlockHourlyPrice` 字段中。

指定 Spot 实例的租期

您可以在单租户硬件上运行 Spot 实例。专用 Spot 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 \(p. 356\)](#) 和 [Amazon EC2 专用实例](#) 产品页面。

要运行专用 Spot 实例，请执行以下操作之一：

- 在创建 Spot 实例请求时，指定租期 `dedicated`。有关更多信息，请参阅 [创建Spot 实例请求 \(p. 292\)](#)。
- 在 VPC 中请求实例租期为 `dedicated` 的 Spot 实例。有关更多信息，请参阅 [创建有专用实例租期的 VPC \(p. 358\)](#)。如果您在 VPC 中请求实例租期为 `dedicated` 的 Spot 实例，则无法请求租期为 `default` 的此类实例。

以下实例类型支持专用 Spot 实例。

最新一代

- `c4.8xlarge`
- `d2.8xlarge`

- i3.16xlarge
- m4.10xlarge
- m4.16xlarge
- p2.16xlarge
- r4.16xlarge
- x1.32xlarge

上一代

- c3.8xlarge
- cc2.8xlarge
- cr1.8xlarge
- g2.8xlarge
- i2.8xlarge
- r3.8xlarge

Spot 实例请求的服务相关角色

Amazon EC2 使用服务相关角色获取代表您调用其他 AWS 服务所需的权限。服务相关角色是一种独特类型的 IAM 角色，它与 AWS 服务直接相关。服务相关角色提供了一种将权限委托给 AWS 服务的安全方式，因为只有相关服务才能代入服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的[使用服务相关角色](#)。

Amazon EC2 使用名为 AWSServiceRoleForEC2Spot 的服务相关角色代表您启动和管理 Spot 实例。

AWSServiceRoleForEC2Spot 授予的权限

Amazon EC2 使用 AWSServiceRoleForEC2Spot 完成以下操作：

- ec2:DescribeInstances – 描述 Spot 实例
- ec2:StopInstances – 停止 Spot 实例
- ec2:StartInstances – 启动 Spot 实例

创建服务相关角色

在大多数情况下，您无需手动创建服务相关角色。在首次使用控制台请求 Spot 实例时，Amazon EC2 创建 AWSServiceRoleForEC2Spot 服务相关角色。

如果在 2017 年 10 月之前具有活动 Spot 实例请求（此时 Amazon EC2 开始支持该服务相关角色），则 Amazon EC2 在您的 AWS 账户中创建了 AWSServiceRoleForEC2Spot 角色。有关更多信息，请参阅 IAM 用户指南中的[我的账户中出现新角色](#)。

在使用 AWS CLI 或 API 请求 Spot 实例之前，请确保该角色存在。要创建该角色，请如下使用 IAM 控制台。

手动创建 AWSServiceRoleForEC2Spot 服务相关角色

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Roles。
3. 选择创建角色。
4. 在 Select type of trusted entity (选择受信任实体的类型) 页面上，依次选择 EC2、EC2 - Spot Instances (EC2 - Spot 实例) 和 Next: Permissions (下一步：权限)。
5. 在下一页上，选择 Next:Review (下一步：审核)。
6. 在 Review (审核) 页面上，选择 Create role (创建角色)。

如果您不再需要使用 Spot 实例，我们建议您删除 AWSServiceRoleForEC2Spot 角色。从账户中删除该角色后，如果您请求 Spot 实例，Amazon EC2 将再次创建该角色。

授予用于加密的 AMI 和 EBS 快照的 CMK 的访问权限

如果为 Spot 实例指定[加密的 AMI \(p. 134\)](#) 或[加密的 Amazon EBS 快照 \(p. 851\)](#)，并且您使用客户托管客户主密钥 (CMK) 进行加密，则必须为 AWSServiceRoleForEC2Spot 角色授予使用 CMK 的权限，以便 Amazon EC2 可以代表您启动 Spot 实例。为此，您必须在 CMK 中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[使用授权](#)和[在 AWS KMS 中使用密钥策略](#)。

为 AWSServiceRoleForEC2Spot 角色授予使用 CMK 的权限

- 使用 `create-grant` 命令在 CMK 中添加授权，并指定授予权限的委托人 (AWSServiceRoleForEC2Spot 服务相关角色) 以执行授权允许的操作。CMK 是由 `key-id` 参数和 CMK 的 ARN 指定的。委托人是由 `grantee-principal` 参数和 AWSServiceRoleForEC2Spot 服务相关角色的 ARN 指定的。

以下示例设置了相应的格式以便于阅读。

```
aws kms create-grant \
--region us-east-1 \
--key-id arn:aws:kms:us-east-1:44445556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Spot \
--operations "Decrypt" "Encrypt" "GenerateDataKey" "GenerateDataKeyWithoutPlaintext" \
"CreateGrant" "DescribeKey" "ReEncryptFrom" "ReEncryptTo"
```

创建Spot 实例请求

请求 Spot 实例的过程与启动一个按需实例的过程相似。在提交 Spot 实例请求后，您无法更改该请求的参数，包括您的最高价。

如果您一次请求了多个 Spot 实例，Amazon EC2 将创建单独的 Spot 实例，这样您可以分别跟踪各个请求的状态。有关跟踪 Spot 实例请求的更多信息，请参阅[Spot 请求状态 \(p. 320\)](#)。

先决条件

在开始之前，请确定最高价、所需的 Spot 实例数以及要使用的实例类型。要查看 Spot 价格趋势，请参阅[Spot 实例定价历史记录 \(p. 287\)](#)。

创建 Spot 实例 请求 (控制台)

有关更多信息，请参阅[创建Spot 队列请求 \(p. 300\)](#)。

创建 Spot 实例 请求 (AWS CLI)

使用以下 `request-spot-instances` 命令可创建一次性请求：

```
aws ec2 request-spot-instances --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 --instance-count 5 --type "persistent" --launch-
specification file://specification.json
```

有关要用于这些命令的启动规范文件的示例，请参阅[Spot 请求示例启动规范 \(p. 294\)](#)。如果您从控制台下载启动规范文件，必须改为使用 `request-spot-fleet` 命令（控制台使用 Spot 队列指定 Spot 请求）。

在最高价超过 Spot 价格并具有可用的容量时，Amazon EC2 会启动您的 Spot 实例。Spot 实例将一直运行，直到该实例中断，或者您自行终止该实例。使用以下 [describe-spot-instance-requests](#) 命令可监控您的 Spot 实例 请求：

```
aws ec2 describe-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

查找正在运行的 Spot 实例

在最高价超过 Spot 价格并具有可用的容量时，Amazon EC2 会启动 Spot 实例。Spot 实例将一直运行，直到该实例中断，或者您自行终止该实例。如果您的最高价与 Spot 价格完全相同，根据需求情况，您的 Spot 实例 可能会保持运行状态。

查找正在运行的 Spot 实例（控制台）

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 Spot 实例 请求和 Spot 队列 请求。如果 Spot 实例 请求已执行，那么 Capacity (容量) 就是 Spot 实例 的 ID。对于 Spot 队列，Capacity (容量) 表示已执行的请求容量。要查看 Spot 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 (实例)。

Note

Spot 实例请求不会立即被标记，过一段时间后，可能会与 Spot 队列请求 (SFR) 分开显示出 来。

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。

查找正在运行的 Spot 实例 (AWS CLI)

要枚举您的 Spot 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 Spot 实例，如下所示：

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

标记Spot 实例请求

要对您的Spot 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。有关更多信息，请参阅[标记您的 Amazon EC2 资源 \(p. 940\)](#)。

您可以在创建Spot 实例请求之后为其分配标签。您为Spot 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 Spot 服务为完成请求所启动的Spot 实例中。在 Spot 实例 启动后，您必须自己将标签添加到 Spot 实例。

使用 AWS CLI 向您的 Spot 实例 请求或 Spot 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Spot 实例请求

如果您不再需要 Spot 请求，您可以将其取消。您只能取消 open 或 active 的 Spot 实例请求。当您的请求未执行，且实例没有启动时，您的 Spot 请求处于 open 状态。当您的请求完成且 Spot 实例因此已启动时，您的 Spot 请求处于 active 状态。如果您的 Spot 请求处于 active 状态，且关联的 Spot 实例正在运行，那么取消请求不会终止该实例。有关终止 Spot 实例的更多信息，请参阅下一节。

取消 Spot 实例 请求 (AWS CLI)

- 使用以下 [cancel-spot-instance-requests](#) 命令可取消指定的 Spot 请求：

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

终止 Spot 实例

如果您的 Spot 请求处于 active 状态，且关联的 Spot 实例正在运行，那么取消请求不会终止该实例；您必须手动终止正在运行的 Spot 实例。如果您终止的运行中 Spot 实例是由持久性 Spot 请求启动的，则 Spot 请求会返回 open 状态，这样就可以启动新的 Spot 实例。要取消持久性 Spot 请求并终止其 Spot 实例，您必须先取消 Spot 请求，然后终止 Spot 实例。否则，持久性 Spot 请求可以启动新实例。有关取消 Spot 实例请求的更多信息，请参阅上一节。

手动终止 Spot 实例 (AWS CLI)

- 使用以下 [terminate-instances](#) 命令可手动终止 Spot 实例：

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Spot 请求示例启动规范

以下示例显示了可与 [request-spot-instances](#) 命令结合使用来创建 Spot 实例 请求的启动配置。有关更多信息，请参阅[创建Spot 实例请求 \(p. 292\)](#)。

- 启动 Spot 实例 ([p. 294](#))
- 在指定的可用区中启动 Spot 实例 ([p. 295](#))
- 在指定的子网中启动 Spot 实例 ([p. 295](#))
- 启动专用 Spot 实例 ([p. 295](#))

示例 1：启动 Spot 实例

以下示例不包含可用区或子网。Amazon EC2 会为您选择可用区。Amazon EC2 在所选可用区的默认子网中实例。

```
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],  
    "InstanceType": "m3.medium",  
}
```

```
"IamInstanceProfile": {  
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
}  
}
```

示例 2：在指定的可用区中启动 Spot 实例

以下示例包含一个可用区。Amazon EC2 在该指定可用区的默认子网中启动实例。

```
{  
    "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 Spot 实例

以下示例包含一个子网。Amazon EC2 在该指定子网中启动实例。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。指定网络接口时，您必须包含使用网络接口（而不是使用示例 3 中所示的 `SubnetId` 和 `SecurityGroupIds` 字段）的子网 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 Spot 实例

以下示例请求租期为 `dedicated` 的 Spot 实例。专用 Spot 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"  
    }  
}
```

Spot 队列请求

要使用 Spot 队列，请创建一个 Spot 队列 请求，其中包括目标容量、可选的按需比例、实例的一个或多个启动规范以及您愿意支付的最高价。当 Spot 价格发生更改时，Amazon EC2 将尝试保持 Spot 队列 的目标容量。有关更多信息，请参阅 [Spot 队列的工作原理 \(p. 281\)](#)。

有两种类型的 Spot 队列 请求：`request` 和 `maintain`。您可以创建Spot 队列，以针对所需容量提交一次性能请求，或者要求其随着时间的推移保持目标容量。两种请求类型都可以使用Spot 队列的分配策略。

在发出一次性请求时，Spot 队列 将提出所需的请求，但在容量减少时不会尝试补充 Spot 实例。如果没有可用的容量，则Spot 队列 不会在其他 Spot 池中提交请求。

为了保持目标容量，Spot 队列将提出请求以满足目标容量，并自动补充任何中断的实例。

提交一次性请求后，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。

Spot 队列请求在过期或您取消它之前保持有效。取消 Spot 队列 请求时，可以指定取消 Spot 队列 请求是否会终止 Spot 队列 中的 Spot 实例。

每个启动规范包括 Amazon EC2 启动实例所需的信息，如 AMI、实例类型、子网或可用区、一个或多个安全组。

目录

- [Spot 队列请求状态 \(p. 296\)](#)
- [Spot 队列先决条件 \(p. 297\)](#)
- [Spot 队列 和 IAM 用户 \(p. 297\)](#)
- [Spot 队列运行状况检查 \(p. 298\)](#)
- [计划Spot 队列请求 \(p. 299\)](#)
- [Spot 队列请求的服务相关角色 \(p. 299\)](#)
- [创建Spot 队列请求 \(p. 300\)](#)
- [监控 Spot 队列 \(p. 303\)](#)
- [修改Spot 队列请求 \(p. 304\)](#)
- [取消Spot 队列请求 \(p. 305\)](#)
- [Spot 队列示例配置 \(p. 305\)](#)

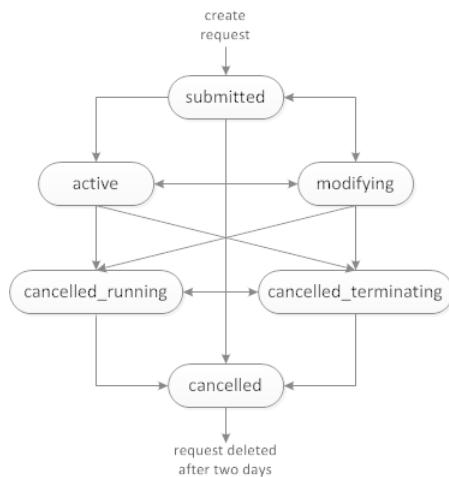
Spot 队列请求状态

Spot 队列请求可以处于以下某种状态：

- `submitted` – 正在评估 Spot 队列 请求，并且 Amazon EC2 正准备启动目标数量的 Spot 实例。
- `active` – 已验证 Spot 队列，并且 Amazon EC2 正在尝试保持目标数量的正在运行的 Spot 实例。请求会保持此状态，直到修改或取消它。
- `modifying` – 正在修改 Spot 队列请求。请求将保持该状态，直到完全处理修改或取消了 Spot 队列。无法修改一次性 `request`，并且这一状态不适用于此类 Spot 请求。

- `cancelled_running` – Spot 队列 已取消并且不会启动额外的 Spot 实例。其现有 Spot 实例继续运行，直至被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。
 - `cancelled_terminating` – 已取消 Spot 队列，并且其 Spot 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` – Spot 队列 已取消，并且没有运行的 Spot 实例。Spot 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。如果超出 Spot 队列限制，将会立即取消请求。



Spot 队列先决条件

如果您使用 Amazon EC2 控制台创建 Spot 队列，将创建一个名为 `aws-ec2-spot-fleet-tagging-role` 的角色，以便为 Spot 队列 授予代表您请求、启动、终止和标记实例的权限。创建Spot 队列请求时，选择此角色。如果您改用 AWS CLI 或 API，则必须确保此角色存在。您可以使用请求 Spot 实例 向导（角色在您前进到该向导的第二页时创建）或使用 IAM 控制台，如下所示。

为 Spot 队列 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. 在 Select type of trusted entity (选择受信任实体的类型) 页面上，依次选择 AWS service (AWS 服务)、EC2、EC2 - Spot Fleet Tagging (EC2 - Spot 队列标记) 和 Next: Permissions (下一步: 权限)。
 4. 在 Attached permissions policy 页面上，选择 Next: Review。
 5. 在 Review (审核) 页面上，键入角色的名称（例如 **aws-ec2-spot-fleet-tagging-role**），然后选择 Create role (创建角色)。

Spot 队列 和 IAM 用户

如果您的 IAM 用户将创建或管理 Spot 队列，请确保为其授予所需的权限，如下所示。

向 IAM 用户授予 Spot 队列权限

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、Create policy。
 3. 在 Create policy (创建策略) 页面上，选择 JSON，将文本替换为以下内容，然后选择 Review policy (查看策略)。

{

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:/*"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam>ListRoles",
            "iam>PassRole",
            "iam>ListInstanceProfiles"
        ],
        "Resource": "*"
    }
]
```

`ec2:*` 为 IAM 用户授予调用所有 Amazon EC2 API 操作的权限。要将用户限制到特定 Amazon EC2 API 操作，请改为指定这些操作。

IAM 用户必须具有相应权限，可以调用 `iam>ListRoles` 操作以枚举现有 IAM 角色、调用 `iam>PassRole` 操作以指定 Spot 队列角色以及调用 `iam>ListInstanceProfiles` 操作以枚举现有实例配置文件。

(可选) 要使 IAM 用户能够使用 IAM 控制台创建角色或实例配置文件，您必须向该策略添加以下操作：

- `iam>AddRoleToInstanceProfile`
- `iam>AttachRolePolicy`
- `iam>CreateInstanceProfile`
- `iam>CreateRole`
- `iam>GetRole`
- `iam>ListPolicies`

4. 在 Review policy (查看策略) 页面上，键入策略名称和描述，然后选择 Create policy (创建策略)。
5. 在导航窗格中，选择用户，然后选择相应用户。
6. 选择 Permissions、Add permissions。
7. 选择直接附加现有策略。选择之前创建的策略，然后选择 Next: Review (下一步：查看)。
8. 选择 Add permissions (添加权限)。

Spot 队列运行状况检查

Spot 队列每 2 分钟检查一次队列中 Spot 实例的运行状况。实例的运行状况为 `healthy` 或 `unhealthy`。Spot 队列使用 Amazon EC2 所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 \(p. 528\)](#)。

您可以配置Spot 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。在替换运行状况不佳的实例时，Spot 队列的容量可能在几分钟内降至其目标容量之下。

要求

- 只有保持目标容量的 Spot 队列（而非一次性 Spot 队列）支持运行状况检查替换。

- 您可以将 Spot 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。

计划Spot 队列请求

在创建 Spot 队列 请求前，请查看 [Spot 最佳实践](#)。使用这些最佳实践规划您的Spot 队列请求，以便以可能的最低价格预置需要的实例类型。还建议执行以下操作：

- 确定您要创建的Spot 队列是针对所需目标容量提交一次性请求，还是随着时间推移维持目标容量。
- 确定满足您的应用程序要求的实例类型。
- 确定您的Spot 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[Spot 队列实例权重 \(p. 284\)](#)。
- 确定 Spot 队列目标容量的大部分必须是按需容量。可以将按需容量指定为 0。
- 确定您的每单位价格 (如果使用实例权重)。要计算每单位价格，请将每实例小时价格除以该实例表示的单位数 (或权重)。如果不使用实例权重，则默认每单位价格为每实例小时价格。
- 查看用于您的Spot 队列请求的可能选项。关于更多信息，请参阅 AWS CLI Command Reference 中的 `request-spot-fleet` 命令。有关其他示例，请参阅 [Spot 队列示例配置 \(p. 305\)](#)。

Spot 队列请求的服务相关角色

Amazon EC2 使用服务相关角色获取代表您调用其他 AWS 服务所需的权限。服务相关角色是一种独特类型的 IAM 角色，它与 AWS 服务直接相关。服务相关角色提供了一种将权限委托给 AWS 服务的安全方式，因为只有相关服务才能代入服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的 [使用服务相关角色](#)。

Amazon EC2 使用名为 `AWSServiceRoleForEC2SpotFleet` 的服务相关角色代表您启动和管理 Spot 实例。

[AWSServiceRoleForEC2SpotFleet 授予的权限](#)

Amazon EC2 使用 `AWSServiceRoleForEC2SpotFleet` 完成以下操作：

- `ec2:RequestSpotInstances` - 请求 Spot 实例
- `ec2:TerminateInstances` - 终止 Spot 实例
- `ec2:DescribeImages` - 描述 Spot 实例 的 Amazon 系统映像 (AMI)
- `ec2:DescribeInstanceStatus` - 描述 Spot 实例 的状态
- `ec2:DescribeSubnets` - 描述 Spot 实例 的子网
- `ec2:CreateTags` - 向 Spot 实例 添加系统标签

[创建服务相关角色](#)

在大多数情况下，您无需手动创建服务相关角色。在首次使用控制台创建 Spot 队列时，Amazon EC2 创建 `AWSServiceRoleForEC2SpotFleet` 服务相关角色。

如果在 2017 年 10 月之前具有活动 Spot 队列请求（此时 Amazon EC2 开始支持该服务相关角色），则 Amazon EC2 在您的 AWS 账户中创建了 `AWSServiceRoleForEC2SpotFleet` 角色。有关更多信息，请参阅 IAM 用户指南中的 [我的账户中出现新角色](#)。

确保此角色存在，然后才使用 AWS CLI 或 API 来创建 Spot 队列。要创建该角色，请如下使用 IAM 控制台。

[手动创建 AWS ServiceRoleForEC2SpotFleet 服务相关角色](#)

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Roles。
3. 选择创建角色。

4. 在 Select type of trusted entity (选择受信任实体的类型) 页面上，依次选择 EC2、EC2 - Spot Fleet (EC2 - Spot 队列) 和 Next: Permissions (下一步: 权限)。
5. 在下一页上，选择 Next:Review (下一步 : 审核)。
6. 在 Review (审核) 页面上，选择 Create role (创建角色)。

如果您不再需要使用 Spot 队列，我们建议您删除 AWSServiceRoleForEC2SpotFleet 角色。从账户中删除该角色后，如果您请求 Spot 队列，Amazon EC2 将再次创建该角色。

授予用于加密的 AMI 和 EBS 快照的 CMK 的访问权限

如果在 Spot 队列请求中指定[加密的 AMI \(p. 134\)](#) 或[加密的 Amazon EBS 快照 \(p. 851\)](#)，并且您使用客户托管客户主密钥 (CMK) 进行加密，则必须为 AWSServiceRoleForEC2SpotFleet 角色授予使用 CMK 的权限，以便 Amazon EC2 可以代表您启动 Spot 实例。为此，您必须在 CMK 中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[使用授权](#)和[在 AWS KMS 中使用密钥策略](#)。

为 AWSServiceRoleForEC2SpotFleet 角色授予使用 CMK 的权限

- 使用 `create-grant` 命令在 CMK 中添加授权，并指定授予权限的委托人 (AWSServiceRoleForEC2SpotFleet 服务相关角色) 以执行授权允许的操作。CMK 是由 `key-id` 参数和 CMK 的 ARN 指定的。委托人是由 `grantee-principal` 参数和 AWSServiceRoleForEC2SpotFleet 服务相关角色的 ARN 指定的。

以下示例设置了相应的格式以便于阅读。

```
aws kms create-grant
--region us-east-1
--key-id arn:aws:kms:us-east-1:44445556666:key/1234abcd-12ab-34cd-56ef-1234567890ab
--grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2SpotFleet
--operations "Decrypt" "Encrypt" "GenerateDataKey" "GenerateDataKeyWithoutPlaintext"
"CreateGrant" "DescribeKey" "ReEncryptFrom" "ReEncryptTo"
```

创建Spot 队列请求

使用 AWS 管理控制台 快速创建 Spot 队列 请求，只需选择您的应用程序或任务需要及最低计算规格即可。Amazon EC2 会配置一个最符合您需求并遵循 Spot 最佳实践的队列。有关更多信息，请参阅[快速创建 Spot 队列 请求 \(控制台\) \(p. 300\)](#)。否则，您可以修改任意默认设置。有关更多信息，请参阅[使用已定义的参数创建 Spot 队列 请求 \(控制台\) \(p. 301\)](#)。

快速创建 Spot 队列 请求 (控制台)

按照以下步骤快速创建 Spot 队列 请求。

使用推荐设置创建 Spot 队列 请求 (控制台)

1. 在 <https://console.aws.amazon.com/ec2spot> 处打开 Spot 控制台。
2. 如果您是首次接触 Spot，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot 实例 (请求 Spot 实例)。
3. 对于 Tell us your application or task need (告诉我们您的应用程序或任务需要)，选择 Flexible workloads (灵活工作负载)、Load balancing workloads (负载均衡工作负载)、Big data workloads (大数据工作负载) 或 Defined duration workloads (已定义持续时间的工作负载)。
4. 在 Configure your instances (配置您的实例) 下，对于 Minimum compute unit (最小计算单位) 选择您的应用程序或任务所需的最低硬件规格 (vCPU、内存和存储)，即 as specs (按规格) 或 as an instance type (按实例类型)。

- 对于 as specs (按规格) , 指定所需的 vCPUs 数和内存量。
 - 对于 as an instance type (按实例类型) , 接受默认实例类型 , 或者选择 Change instance type (更改实例类型) 以选择其他实例类型。
5. 对于 Tell us how much capacity you need (告诉我们您需要多少容量) 下 , 对于 Total target capacity (总目标容量) , 指定要请求的目标容量单位数。您可以选择实例或 vCPU。
 6. 根据您的应用程序或任务选择 , 查看推荐的 Fleet request settings (队列请求设置) , 然后选择 Launch (启动)。

使用已定义的参数创建 Spot 队列 请求 (控制台)

您可以使用自己定义的参数创建 Spot 队列。

使用已定义的参数创建 Spot 队列 请求 (控制台)

1. 在 <https://console.aws.amazon.com/ec2spot> 处打开 Spot 控制台。
2. 如果您是首次接触 Spot , 则会看到一个欢迎页面 ; 请选择 Get started。否则 , 请选择 Request Spot 实例 (请求 Spot 实例)。
3. 对于 Tell us your application or task need (告诉我们您的应用程序或任务需要) , 选择 Flexible workloads (灵活工作负载)、Load balancing workloads (负载均衡工作负载)、Big data workloads (大数据工作负载) 或 Defined duration workloads (已定义持续时间的工作负载)。
4. 对于 Configure your instances (配置您的实例) , 执行以下操作 :
 - a. (可选) 对于启动模板 , 请选择一个启动模板。启动模板必须指定 Amazon 系统映像 (AMI) , 因为如果您指定启动模板 , 则不能使用 Spot 队列覆盖 AMI。

Important

如果您打算指定 Optional On-Demand portion (可选的按需部分) , 则必须选择一个启动模板。

- b. 对于 AMI , 选择 AWS 提供的一个基本 AMI , 或者选择 Search for AMI (搜索 AMI) 以使用来自我们用户社区的 AMI、AWS Marketplace 或您自己的一个 AMI。
- c. 对于 Minimum compute unit (最小计算单位) , 选择您的应用程序或任务所需的最低硬件规格 (vCPU、内存和存储) , 即 as specs (按规格) 或 as an instance type (按实例类型)。
 - 对于 as specs (按规格) , 指定所需的 vCPUs 数和内存量。
 - 对于 as an instance type (按实例类型) , 接受默认实例类型 , 或者选择 Change instance type (更改实例类型) 以选择其他实例类型。

- d. (可选) 对于 Network (网络) , 选择现有 VPC 或新建一个。

[现有 VPC] 选择所需的 VPC。

[新 VPC] 选择 Create new VPC (新建 VPC) 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。

- e. (可选) 对于 Availability Zone (可用区) , 让 AWS 为 Spot 实例 选择可用区 , 或者指定一个或多个可用区。

如果您在一个可用区中有多个子网 , 则请从 Subnet (子网) 中选择合适的子网。要添加子网 , 请选择 Create new subnet (新建子网) 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。

- f. (可选) 对于 Key pair name (密钥对名称) , 选择现有密钥对或新建一个密钥对。

[现有密钥对] 选择所需的密钥对。

[新密钥对] 选择 Create new key pair (新建密钥对) 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。

5. (可选) 对于 Additional configurations (其他配置)，执行以下操作：
 - a. (可选) 要添加存储，请根据实例类型指定实例存储卷或 Amazon EBS 卷。
 - b. (可选) 要启用 Amazon EBS 优化，请对 EBS-optimized (EBS 优化) 选择 Launch EBS-optimized instances (启动 EBS 优化实例)。
 - c. (可选) 要为实例添加临时性块级存储，请对 Instance store (实例存储) 选择 Attach at launch (启动时附加)。
 - d. (可选) 默认情况下，已为您的实例启用基本监控。要启用详细监控，请对 监控 选择 启用 CloudWatch 详细监控。
 - e. (可选) 要替换运行状况不佳的实例，请为 Health check (运行状况检查) 选择 Replace unhealthy instances (替换运行状况不佳的实例)。要启用此选项，您必须先选择 Maintain target capacity (保持目标容量)。
 - f. (可选) 要运行专用 Spot 实例，请为 Tenancy (租期) 选择 Dedicated - run a dedicated instance (专用 - 运行专用实例)。
 - g. (可选) 对于 Security groups (安全组)，选择一个或多个安全组，或者新建一个。

[现有安全组] 选择一个或多个所需的安全组。

[新安全组] 选择 Create new security group (新建安全组) 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。

- h. (可选) 要能够通过 Internet 访问实例，请对 Auto-assign IPv4 Public IP (自动分配 IPv4 公有 IP) 选择 Enable (启用)。
 - i. (可选) 要使用 IAM 角色启动 Spot 实例，请对 IAM 实例配置文件选择角色。
 - j. (可选) 要运行启动脚本，请将其复制到 User data。
 - k. (可选) 要添加标签，请选择 Add new tag (添加新标签)，然后输入该标签的键和值。对每个标签重复此操作。

6. 对于 Tell us how much capacity you need (告诉我们您需要多少容量)，执行以下操作：

- a. 对于 Total target capacity (总目标容量)，指定要请求的目标容量单位数。您可以选择实例或 vCPU。要将目标容量指定为 0 以便以后可增加容量，请选择 Maintain target capacity (保持目标容量)。
- b. (可选) 对于 Optional On-Demand portion (可选的按需部分)，指定要请求的按需单位数。该数字必须小于 Total target capacity (总目标容量)。Amazon EC2 会计算差值，并将差值分配给要请求的 Spot 单位。

Important

要指定可选的按需部分，您必须先选择一个启动模板。

- c. (可选) 默认情况下，在 Spot 实例中断时，Spot 服务将终止这些实例。要保持目标容量，请选择 Maintain target capacity (保持目标容量)。这样，您就可以指定 Spot 服务在 Spot 实例中断时终止、停止或休眠这些实例。为此，请从中断行为中选择相应的选项。

7. 对于 Fleet request settings (队列请求设置)，执行以下操作：

- a. 根据您的应用程序或任务选择，查看队列请求和队列分配策略。要更改实例类型或分配策略，请清除 Apply recommendations (应用推荐设置)。
- b. (可选) 要删除实例类型，请对 Fleet request (队列请求) 选择 Remove (删除)。要添加实例类型，请选择 Select instance types (选择实例类型)。
- c. (可选) 对于 Fleet allocation strategy (队列分配策略)，选择满足您需求的策略。有关更多信息，请参阅[Spot 实例分配策略 \(p. 282\)](#)。

8. 对于 Additional request details (其他请求详细信息)，执行以下操作：

- a. 查看其他请求详细信息。要进行更改，请清除 Apply defaults (应用默认设置)。
- b. (可选) 对于 IAM fleet role (IAM 队列角色)，您可以使用默认角色或选择其他角色。要在更改角色后使用默认角色，请选择 Use default role (使用默认角色)。

- c. (可选) 对于 Maximum price (最高价) , 您可以使用默认最高价 (按需价格) , 也可以指定您愿意支付的最高价。如果最高价低于所选实例类型的 Spot 价格 , 则不会启动 Spot 实例。
 - d. (可选) 要创建仅在特定时间段内有效的请求 , 请编辑请求有效起始时间和请求有效截止时间。
 - e. (可选) 默认情况下 , 我们会在请求过期时终止 Spot 实例。要保持这些实例在请求过期后继续运行 , 请清除 Terminate the instances when the request expires (请求到期时终止实例)。
 - f. (可选) 要向负载均衡器注册 Spot 实例 , 请选择 Receive traffic from one or more load balancers (从一个或多个负载均衡器接收流量) , 然后选择一个或多个 Classic Load Balancer 或目标组。
9. (可选) 要下载一个启动配置副本以用于 AWS CLI , 请选择 JSON config (JSON 配置)。
10. 选择 Launch。

Spot 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。

使用 AWS CLI 创建 Spot 队列 请求

- 使用以下 [request-spot-fleet](#) 命令可创建 Spot 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 [Spot 队列示例配置 \(p. 305\)](#)。

下面是示例输出 :

```
{  
    "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

监控 Spot 队列

在最高价超过 Spot 价格并具有可用的容量时 , Spot 队列 会启动 Spot 实例。Spot 实例 将一直运行 , 直到这些实例中断 , 或者您终止这些实例。

监控 Spot 队列 (控制台)

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Spot 队列请求。要查看配置详细信息 , 请选择 Description (描述)。
4. 要列出 Spot 队列 的 Spot 实例 , 请选择 Instances (实例) 选项卡。
5. 要查看 Spot 队列 的历史记录 , 请选择 History (历史记录) 选项卡。

监控 Spot 队列 (AWS CLI)

使用以下 [describe-spot-fleet-requests](#) 命令可描述 Spot 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 Spot 队列 的 Spot 实例 :

```
aws ec2 describe-spot-fleet-instances --spot-fleet-request-id sfr-73fb2ce-  
aa30-494c-8788-1cee4EXAMPLE
```

使用以下 [describe-spot-fleet-request-history](#) 命令可描述指定 Spot 队列 请求的历史记录：

```
aws ec2 describe-spot-fleet-request-history --spot-fleet-request-id sfr-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2015-05-18T00:00:00Z
```

修改Spot 队列请求

您可以修改活动的Spot 队列请求以完成以下任务：

- 提高目标容量和按需部分
- 降低目标容量和按需部分

Note

您无法修改一次性 Spot 队列请求。您只能在创建 Spot 队列 请求时选择了 Maintain target capacity (保持目标容量) 的情况下修改 Spot 队列 请求。

当您提高目标容量时，Spot 队列启动其他 Spot 实例。当您提高按需部分时，Spot 队列启动其他按需实例。

当您提升目标容量时，Spot 队列 会根据其 Spot 队列 请求的分配策略来启动额外的 Spot 实例。如果分配策略是 lowestPrice，则 Spot 队列 从 Spot 队列 请求中价格最低的 Spot 实例 池启动实例。如果分配策略是 diversified，则 Spot 队列 在 Spot 队列 请求中的池间分配实例。

在减少目标容量时，Spot 队列 将取消超过新目标容量的任何打开的请求。您可以请求 Spot 队列终止 Spot 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 Spot 队列 会终止每单位价格最高的实例。如果分配策略是 diversified，则 Spot 队列 会在池间终止实例。或者，您可以请求 Spot 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 Spot 实例。

当 Spot 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 Spot 实例 中断通知。

修改 Spot 队列 请求 (控制台)

- 在 <https://console.aws.amazon.com/ec2spot/home/fleet> 处打开 Spot 控制台。
- 选择您的Spot 队列 请求。
- 依次选择 Actions (操作) 和 Modify target capacity (修改目标容量)。
- 在 Modify target capacity 中，执行以下操作：
 - 输入新的目标容量和按需部分。
 - (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，请清除 Terminate instances (终止实例)。
 - 选择 Submit。

使用 AWS CLI 修改 Spot 队列 请求

使用以下 [modify-spot-fleet-request](#) 命令可更新指定 Spot 队列 请求的目标容量：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 20
```

可以按如下所示修改前面的命令，以减少指定 Spot 队列 的目标容量而不因此终止任何 Spot 实例：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 10 --excess-capacity-termination-policy NoTermination
```

取消Spot 队列请求

在使用完 Spot 队列后，可以取消 Spot 队列 请求。这将取消与 Spot 队列 关联的所有 Spot 请求，从而不会为您的 Spot 队列 启动任何新的 Spot 实例。必须指定 Spot 队列 是否应终止其 Spot 实例。如果终止这些实例，则 Spot 队列 请求进入 `cancelled_terminating` 状态。否则，Spot 队列 请求将进入 `cancelled_running` 状态，并且实例将继续运行直至它们中断或您手动终止它们。

取消 Spot 队列 请求 (控制台)

1. 在 <https://console.aws.amazon.com/ec2spot/home/fleet> 处打开 Spot 控制台。
2. 选择您的Spot 队列 请求。
3. 依次选择 Actions (操作) 和 Cancel spot request (取消 Spot 请求)。
4. 在 Cancel spot request (取消 spot 请求) 中，确认是否要取消 Spot 队列。要使队列保持其当前大小，请清除 Terminate instances (终止实例)。如果准备就绪，请选择 Confirm。

使用 AWS CLI 取消 Spot 队列 请求

使用以下 `cancel-spot-fleet-requests` 命令可取消指定的 Spot 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Spot 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": []  
}
```

Spot 队列示例配置

以下各示例显示了可与 `request-spot-fleet` 命令结合使用以创建 Spot 队列 请求的启动配置。有关更多信息，请参阅 [创建Spot 队列请求 \(p. 300\)](#)。

1. 使用区域中价格最低的可用区或子网启动 Spot 实例 (p. 306)
2. 使用指定列表中价格最低的可用区或子网启动 Spot 实例 (p. 306)
3. 使用指定列表中价格最低的实例类型启动 Spot 实例 (p. 307)
4. 覆盖请求的价格 (p. 308)
5. 使用多样化分配策略启动 Spot 队列 (p. 310)
6. 使用实例权重启动 Spot 队列 (p. 312)
7. 启动具有按需容量的 Spot 队列 (p. 313)

示例 1：使用区域中价格最低的可用区或子网启动 Spot 实例

以下示例指定一个没有可用区或子网的启动规范。Spot 队列会在具有默认子网且价格最低的可用区中启动实例。您支付的价格不得超过按需价格。

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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 Spot 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 相同的两种启动规范。

Availability Zones (可用区)

Spot 队列会在价格最低的指定可用区的默认子网中启动实例。

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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 (子网)

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。Spot 服务会在位于价格最低的可用区的子网中启动实例。

您无法在Spot 队列请求中指定来自相同可用区的不同子网。

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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。在启动规范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。指定网络接口时，您必须包括使用网络接口的子网 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 Spot 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。Spot 队列使用价格最低的指定实例类型启动实例。

可用区

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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. 覆盖请求的价格

我们建议您使用默认最高价 (这是按需价格)。如果愿意，您可以为队列请求以及各个启动规范指定最高价。

以下示例为队列请求以及两个启动规范 (共三个) 指定最高价。队列请求的最高价用于未指定最高价的任何启动规范。Spot 队列使用价格最低的实例类型启动实例。

可用区

```
{  
    "SpotPrice": "1.00",  
    "TargetCapacity": 30,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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/aws-ec2-spot-fleet-tagging-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Spot 队列

以下示例使用 diversified 分配策略。启动规范具有不同的实例类型，但具有相同的 AMI 和可用区或子网。Spot 队列在 3 个启动规范间分配 30 个实例，以便每种类型有 10 个实例。有关更多信息，请参阅 [Spot 实例分配策略 \(p. 282\)](#)。

可用区

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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/aws-ec2-spot-fleet-tagging-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"  
        }  
    ]  
}
```

在其中一个可用区中断的情况下，增加 EC2 容量可以满足 Spot 请求的几率的最佳实践是跨区域实现多样化。对于这种情况，请在启动规范中包含每个对您可用的可用区。并且，不是每次使用同一个子网，而是使用三个唯一的子网（每个子网映射到不同的区域）。

可用区

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2a"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2c"  
            }  
        }  
    ]  
}
```

子网

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "SubnetId": "subnet-2a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-3a2b3c4d"  
        }  
    ]  
}
```

示例 6：使用实例权重启动Spot 队列

以下示例使用实例权重，这意味着价格是每单位小时价格，而不是每实例小时价格。每个启动配置列出不同的实例类型和不同的权重。Spot 队列选择每单位小时价格最低的实例类型。Spot 队列通过将目标容量除以实例权重，计算出要启动的 Spot 实例数。如果结果不是整数，则Spot 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 请求成功，Spot 将预置其中的 4 个实例。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 请求成功，Spot 将预置其中的 7 个实例。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 [Spot 队列实例权重 \(p. 284\)](#)。

可用区

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-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/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "WeightedCapacity": 6  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.xlarge",  
            "SubnetId": "subnet-1a2b3c4d",  
            "WeightedCapacity": 3  
        }  
    ]  
}
```

示例 7：启动具有按需容量的 Spot 队列

为确保始终拥有实例容量，您可以在 Spot 队列请求中包含按需容量请求。如果具有容量，则将始终执行按需请求。目标容量的余量将在具有容量且可用的情况下作为 Spot 容量执行。

以下示例将所需的目标容量指定为 10，其中 5 个必须为按需容量。未指定 Spot 容量；它由目标容量减去按需容量的余量隐含指定。Amazon EC2 启动 5 个容量单位作为按需容量，并在有可用的 Amazon EC2 容量并且可用时，启动 5 个容量单位 (10-5=5) 作为 Spot 容量。

有关更多信息，请参阅[Spot 队列中的按需容量 \(p. 281\)](#)。

```
{  
    "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",  
    "AllocationStrategy": "lowestPrice",  
    "TargetCapacity": 10,  
    "SpotPrice": null,  
    "ValidFrom": "2018-04-04T15:58:13Z",  
    "ValidUntil": "2019-04-04T15:58:13Z",  
    "TerminateInstancesWithExpiration": true,  
    "LaunchSpecifications": [],  
    "Type": "maintain",  
    "OnDemandTargetCapacity": 5,  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",  
                "Version": "2"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "t2.medium",  
                    "WeightedCapacity": 1,  
                    "SubnetId": "subnet-d0dc51fb"  
                }  
            ]  
        }  
    ]  
}
```

Spot 队列 的 CloudWatch 指标

Amazon EC2 提供了可用来监控 Spot 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 \(p. 538\)](#)。

有关 Amazon EC2 提供的 CloudWatch 指标的更多信息，请参阅[使用 CloudWatch 监控您的实例 \(p. 538\)](#)。

Spot 队列 指标

AWS/EC2Spot 命名空间包含以下指标以及针对队列中的 Spot 实例的 CloudWatch 指标。有关更多信息，请参阅[实例指标 \(p. 540\)](#)。

AWS/EC2Spot 命名空间包括以下指标。

指标	说明
AvailableInstancePoolsCount	Spot 队列 请求中指定的 Spot 实例 池。

指标	说明
	单位 : 计数
BidsSubmittedForCapacity	Amazon EC2 已提交 Spot 队列 请求的容量。 单位 : 计数
EligibleInstancePoolCount	在 Amazon EC2 可以完成请求的 Spot 队列 请求中指定的 Spot 实例 池。在您愿意为 Spot 实例 支付的最高价格低于 Spot 价格或 Spot 价格高于 按需实例 价格的池中 , Amazon EC2 不会完成请求。 单位 : 计数
FulfilledCapacity	Amazon EC2 已执行的容量。 单位 : 计数
MaxPercentCapacityAllocation	Spot 队列 请求中指定的所有 Spot 队列 池间的 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 Spot 实例 池分配的容量。要 获取所有 Spot 实例 池间记录的最大值 , 请使用 MaxPercentCapacityAllocation。 单位 : 百分比
TargetCapacity	Spot 队列 请求的目标容量。 单位 : 计数
TerminatingCapacity	因预置容量大于目标容量而终止的容量。 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。

Spot 队列 维度

要筛选您的 Spot 队列 的数据 , 请使用以下维度。

维度	描述
AvailabilityZone	按照可用区筛选数据。
FleetRequestId	按照 Spot 队列请求筛选数据。
InstanceType	按实例类型筛选数据。

查看 Spot 队列的 CloudWatch 指标

可使用 Amazon CloudWatch 控制台查看 Spot 队列的 CloudWatch 指标。这些指标显示为监控图表。如果 Spot 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 Spot 队列请求 ID、实例类型或可用区来查看所有 Spot 队列指标或 Spot 队列指标组。

查看 Spot 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 (队列请求指标) — 按 Spot 队列 请求分组
- By Availability Zone (按可用区) — 按 Spot 队列 请求和可用区分组
- By Instance Type (按实例类型) — 按 Spot 队列 请求和实例类型分组
- By Availability Zone/Instance Type (按可用区/实例类型) — 按 Spot 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。

The screenshot shows the CloudWatch Metrics interface for the EC2 Spot fleet. The top navigation bar includes 'EC2 Spot' and a search bar. Below the search bar are several filter buttons: 'Fleet Request Metrics' (which is selected), 'By Availability Zone', 'By Instance Type', and 'By Availability Zone/Instance Type'. A message below the filters states 'Showing all results (18) for EC2 Spot > Fleet Request Metrics. For more results expand your search to All EC2 Spot Metrics.' There are two buttons at the bottom of this section: 'Select All' and 'Clear'. The main content area is titled 'EC2 Spot > Fleet Request Metrics' and lists metrics with their corresponding Fleet Request IDs. The metrics listed are:

FleetRequestId	Metric Name
sfr-4a707781-8fac-459b-a5ae-4701fce47d7	AvailableInstancePoolsCount
sfr-4a707781-8fac-459b-a5ae-4701fce47d7	BidsSubmittedForCapacity
<input checked="" type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fce47d7	CPUUtilization
sfr-4a707781-8fac-459b-a5ae-4701fce47d7	DiskReadBytes

Spot 队列的自动扩展

自动扩展 是根据需求自动增加或减少 Spot 队列 目标容量的能力。Spot 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）。

Spot 队列 支持以下类型的自动扩展：

- [目标跟踪扩展 \(p. 317\)](#) – 根据特定指标的目标值，增加或减少队列的当前容量。这与恒温器保持家里温度的方式类似—您选择一个温度，恒温器将完成所有其他工作。
- [步进扩展 \(p. 317\)](#) – 根据一组扩展调整，增加或减小队列的当前容量，这些调整称为步进调整，将根据警报严重程度发生变化。
- [计划扩展 \(p. 319\)](#) – 根据日期和时间增加或减少队列的当前容量。

如果使用[实例权重 \(p. 284\)](#)，请记住，Spot 队列 可以根据需要超出目标容量。执行容量可以是浮点数，但目标容量必须是整数，因此 Spot 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，自动扩展过程将 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Spot 队列为执行容量为 12 的实例预置权重为 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，则自动扩展过程将 12 减 12*0.2 得到 9.6，然后将其向上取整为 10，因此不执行扩展操作。

您为 Spot 队列 创建的扩展策略支持冷却时间。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，自动扩展将立即扩大您的可扩展目标。

建议将随实例指标扩展的频率设置为 1 分钟，这可确保更快地响应使用率变化。如果将随指标扩展的频率设置为 5 分钟，可能会导致响应时间变慢，并且可能导致系统依据陈旧的指标数据进行扩展。要每隔 1 分钟向 CloudWatch 发送一次实例的指标数据，您必须专门启用详细监控。有关更多信息，请参阅 [对您的实例启用或禁用详细监控 \(p. 538\)](#) 和 [使用已定义的参数创建 Spot 队列 请求 \(控制台 \) \(p. 301\)](#)。

有关为 Spot 队列配置扩展的更多信息，请参阅以下资源：

- AWS CLI Command Reference 的 [application-autoscaling](#) 部分
- [Application Auto Scaling API 参考](#)
- [Application Auto Scaling 用户指南](#)

Spot 队列 Auto Scaling 所需的 IAM 权限

通过结合使用 Amazon EC2、Amazon CloudWatch 和 Application Auto Scaling API 可实现 Spot 队列的自动扩展。通过 Amazon EC2 可创建 Spot 队列请求，通过 CloudWatch 可创建警报，通过 Application Auto Scaling 可创建扩展策略。

除了 [Spot 队列的 IAM 权限 \(p. 297\)](#) 和 Amazon EC2，访问队列扩展设置的 IAM 用户必须具有支持动态扩展的服务的适当权限。IAM 用户必须具有使用以下示例策略中所示操作的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "application-autoscaling:*",  
                "ec2:DescribeSpotFleetRequests",  
                "ec2:ModifySpotFleetRequest",  
                "cloudwatch:DeleteAlarms",  
                "cloudwatch:DescribeAlarmHistory",  
                "cloudwatch:DescribeAlarms",  
                "cloudwatch:DescribeAlarmsForMetric",  
                "cloudwatch:GetMetricStatistics",  
                "cloudwatch>ListMetrics",  
                "cloudwatch:PutMetricAlarm",  
                "cloudwatch:DisableAlarmActions",  
                "cloudwatch:EnableAlarmActions",  
                "iam>CreateServiceLinkedRole",  
                "sns>CreateTopic",  
                "sns:Subscribe",  
                "sns:Get*",  
                "sns>List*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

您还可以创建自己的 IAM 策略，从而使 Application Auto Scaling API 调用获得更精细的权限。有关更多信息，请参阅 Application Auto Scaling 用户指南中的 [身份验证和访问控制](#)。

Application Auto Scaling 服务还需要描述 Spot 队列和 CloudWatch 警报的权限，以及代表您修改 Spot 队列目标容量的权限。如果您为 Spot 队列启用自动扩展功能，它将创建一个名为

`AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest` 的服务相关角色。此服务相关角色授予 Application Auto Scaling 权限，以描述策略警报、监控队列的当前容量以及修改队列的容量。Application Auto Scaling 的原托管 Spot 队列角色为 `aws-ec2-spot-fleet-autoscale-role`，但今后已不再需要。此服务相关角色是 Application Auto Scaling 的默认角色。有关更多信息，请参阅 Application Auto Scaling 用户指南 中的 [服务相关角色权限](#)。

使用目标跟踪策略扩展Spot 队列

在使用目标跟踪扩展策略时，可以选择一个指标并设置一个目标值。Spot 队列 创建和管理触发扩展策略的 CloudWatch 警报，并根据指标和目标值计算扩展调整。扩展策略根据需要增加或减少容量，将指标保持在指定的目标值或接近指定的目标值。除了将指标保持在目标值附近以外，目标跟踪扩展策略还会根据由于负载模式波动而造成的指标波动进行调节，并最大限度减少队列容量发生快速波动的情况。

您可以为Spot 队列创建多个目标跟踪扩展策略，但前提是它们分别使用不同的指标。队列根据提供最大队列容量的策略进行扩展。这样，您就可以涵盖多种方案，并确保始终具有足够的容量以处理您的应用程序工作负载。

为了确保应用程序可用性，队列针对指标尽快按比例向外扩展，但会逐渐向内扩展。

当 Spot 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 Spot 实例 中断通知。

请勿编辑或删除 Spot 队列 为目标跟踪扩展策略管理的 CloudWatch 警报。在删除目标跟踪扩展策略时，Spot 队列 将自动删除警报。

限制

- Spot 队列 请求必须使用 `maintain` 作为请求类型。一次性请求或 Spot 型限制不支持自动扩展。

配置目标跟踪策略（控制台）

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 Spot 队列 请求，然后选择 Auto Scaling。
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. 在 Policy name 中键入策略的名称。
7. 选择一个目标指标。
8. 为该指标键入一个目标值。
9. (可选) 设置冷却时间以修改默认冷却时间。
10. (可选) 选择禁用向内扩展以禁止根据当前配置创建向内扩展策略。您可以使用不同的配置创建一个向内扩展策略。
11. 选择 Save。

使用 AWS CLI 配置目标跟踪策略

1. 使用 `register-scalable-target` 命令将 Spot 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。

使用步进扩展策略扩展Spot 队列

在使用步进扩展策略时，您可以指定 CloudWatch 警报以触发扩展过程。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。

在创建步进扩展策略时，您必须指定以下扩展调整类型之一：

- Add (增加) – 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 (移走) – 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 (设定为) – 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，自动扩展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。触发警报时，自动扩展过程为 10 增加 1 得到 11，因此 Spot 队列 将启动 1 个实例。

当 Spot 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 Spot 实例 中断通知。

限制

- Spot 队列 请求必须使用 `maintain` 作为请求类型。一次性请求或 Spot 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)。

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 (创建警报)。
4. 在 Specify metric and conditions (指定指标和条件) 页面上，选择 Select metric (选择指标)。
5. 选择 EC2 Spot、Fleet Request Metrics (队列请求指标)，选择一个指标 (例如 CPUUtilization)，然后选择 Select metric (选择指标)。

这将显示 Specify metric and conditions (指定指标和条件) 页面，其中显示一个图表以及有关所选指标的其他信息。

6. 在 Period (周期) 下，选择警报的评估周期，例如 1 分钟。评估警报时，每个周期都聚合到一个数据点。

Note

周期越短，创建的警报越敏感。

7. 在 Conditions (条件) 下，通过定义阈值条件来定义警报。例如，您可以定义一个阈值，在指标值大于或等于 80% 时触发警报。
8. 在 Additional configuration (附加配置) 下，对于 Datapoints to alarm (触发警报的数据点数)，指定必须有多少个数据点 (评估期) 处于 ALARM 状态才会触发警报，例如，1 个或 2 个 (共 3 个) 评估期。这将创建一个警报，如果多个连续周期超出阈值，该警报将进入 ALARM (警报) 状态。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的 [评估警报](#)。
9. 对于 Missing data treatment (缺失数据处理)，选择某个选项 (或保留 Treat missing data as missing (将缺失的数据视为缺失) 的默认值)。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的 [配置 CloudWatch 警报处理缺少数据的方式](#)。
10. 选择 Next。
11. (可选) 要接收扩展事件的通知，在 Notification (通知) 中，您可以选择或创建要用于接收通知的 Amazon SNS 主题。当然，您也可以立即删除通知，之后按需添加通知。
12. 选择 Next。

13. 在 Add a description (添加描述) 下，输入警报的名称和描述，然后选择 Next (下一步)。
14. 选择 Create alarm (创建警报)。

为您的 Spot 队列 配置分步扩展策略 (控制台)

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 Spot 队列 请求，然后选择 Auto Scaling。
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 (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 (策略触发器)，可以选择现有的警报，或选择 Create new alarm (新建警报) 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 (冷却时间) 中选择一个数字。
8. 选择 Save。

使用 AWS CLI 为 Spot 队列 配置步进扩展策略

1. 使用 `register-scalable-target` 命令将 Spot 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` 命令创建触发扩展策略的警报。

使用计划扩展功能扩展 Spot 队列

按计划扩展使您可以按照可预测的需求变化来扩展应用程序。要使用计划扩展，请创建指示 Spot 队列 在特定时间执行扩展活动的计划操作。创建计划操作时，您可以指定 Spot 队列、执行扩展活动的时间、最小容量和最大容量。您可以创建仅扩展一次或按重复计划扩展的计划操作。

限制

- Spot 队列 请求必须使用 `maintain` 作为请求类型。一次性请求或 Spot 型限制不支持自动扩展。

创建一次性计划操作

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 Spot 队列 请求，然后选择 Scheduled Scaling (计划扩展)。
4. 选择 Create Scheduled Action (创建计划扩展)。
5. 对于 Name (名称)，指定计划操作的名称。
6. 对于 Minimum capacity (最小容量) 和/或 Maximum capacity (最大容量)，输入所需的值。
7. 对于 Recurrence (重复次数)，选择 Once (一次)。

8. (可选) 对于 Start time (开始时间) 和/或 End time (结束时间) , 选择所需的日期和时间。
9. 选择 Submit。

按照重复计划扩展

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 Spot 队列 请求 , 然后选择 Scheduled Scaling (计划扩展)。
4. 对于 Recurrence (重复次数) , 选择预定义计划之一 (例如 Every day (每天)) , 或者选择 Custom (自定义) 并键入 cron 表达式。有关计划扩展所支持的 cron 表达式的更多信息 , 请参阅 Amazon CloudWatch Events 用户指南 中的 [cron 表达式](#)。
5. (可选) 对于 Start time (开始时间) 和/或 End time (结束时间) , 选择所需的日期和时间。
6. 选择 Submit。

编辑计划操作

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 Spot 队列 请求 , 然后选择 Scheduled Scaling (计划扩展)。
4. 选择所需的计划操作 , 然后依次选择 Actions (操作) 和 Edit (编辑)。
5. 进行所需的更改 , 然后选择 Submit (提交)。

删除计划操作

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 Spot 队列 请求 , 然后选择 Scheduled Scaling (计划扩展)。
4. 选择所需的计划操作 , 然后依次选择 Actions (操作) 和 Delete (删除)。
5. 当系统提示进行确认时 , 选择 Delete。

使用 AWS CLI 管理计划扩展

使用以下命令 :

- [put-scheduled-action](#)
- [describe-scheduled-actions](#)
- [delete-scheduled-action](#)

Spot 请求状态

要帮助跟踪 Spot 实例 请求和规划 Spot 实例 的使用 , 请使用 Amazon EC2 提供的请求状态。例如 , 请求状态可以提供尚未完成 Spot 请求的原因 , 或者列出妨碍完成 Spot 请求的限制。

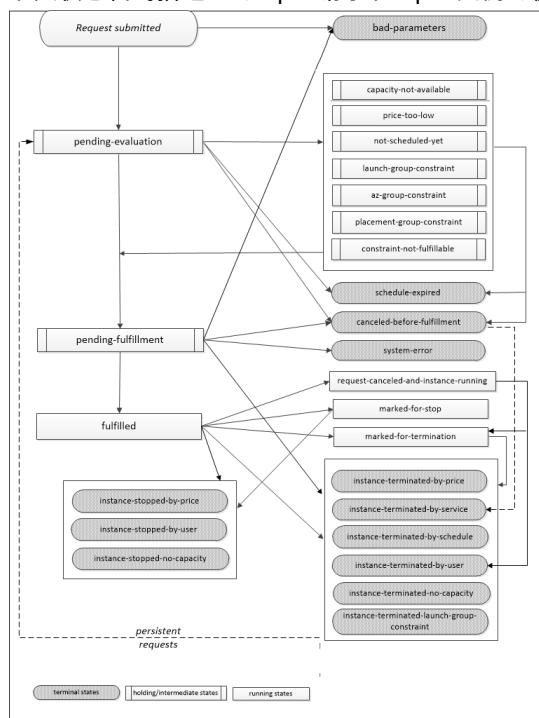
在此过程 (也称为 Spot 请求生命周期) 中的每一步 , 都有特定事件确定连续的请求状态。

目录

- [Spot 请求的生命周期 \(p. 321\)](#)
- [获取请求状态信息 \(p. 323\)](#)
- [Spot 请求状态代码 \(p. 324\)](#)

Spot 请求的生命周期

以下图表显示您的 Spot 请求在其整个生命周期 (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 Spot 请求和 Spot 实例的状态。



待评估

当您提交 Spot 实例 请求之后，除非一个或多个请求参数无效 (bad-parameters)，否则该请求就会进入 pending-evaluation 状态。

状态代码	请求状态	实例状态
pending-evaluation	open	不适用
bad-parameters	closed	不适用

备用

如果一个或多个请求限制有效但目前无法满足，或者如果没有足够的容量，那么请求将进入暂挂状态，等待满足限制。请求选项影响请求完成的可能性。例如，如果您指定的最高价低于当前 Spot 价格，您的请求将保持暂挂状态，直到 Spot 价格低于您的最高价。如果您指定了可用区组，则该请求将保持为暂挂状态，直至满足可用区的限制。

如果其中一个可用区中断，则可能会影响其他可用区中可用于 Spot 实例请求的备用 EC2 容量。

状态代码	请求状态	实例状态
capacity-not-available	open	不适用
price-too-low	open	不适用

状态代码	请求状态	实例状态
not-scheduled-yet	open	不适用
launch-group-constraint	open	不适用
az-group-constraint	open	不适用
placement-group-constraint	open	不适用
constraint-not-fulfillable	open	不适用

等待评估/最终执行

如果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，则您的 Spot 实例请求可能会进入 `terminal` 状态。如果您取消请求，或者出现系统错误，请求也可能会进入该状态。

状态代码	请求状态	实例状态
<code>schedule-expired</code>	<code>cancelled</code>	不适用
<code>canceled-before-fulfillment*</code>	<code>cancelled</code>	不适用
<code>bad-parameters</code>	<code>failed</code>	不适用
<code>system-error</code>	<code>closed</code>	不适用

* 如果您取消请求。

等待履行

如果满足指定的限制 (如果有) 并且您的最高价等于或高于当前 Spot 价格，您的 Spot 请求将会进入 `pending-fulfillment` 状态。

此时，Amazon EC2 已经准备好为您预置您请求的实例。如果该过程在此时停止，则可能是因为用户在启动 Spot 实例之前取消了请求。也可能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>	不适用

已完成

当您的 Spot 实例所有规格都得到满足时，Spot 请求将会执行。Amazon EC2 会启动 Spot 实例，这可能需要几分钟时间。如果 Spot 实例在中断时休眠或停止，它将保持该状态，直到可以再次完成该请求或取消该请求。

状态代码	请求状态	实例状态
<code>fulfilled</code>	<code>active</code>	<code>pending → running</code>
<code>fulfilled</code>	<code>active</code>	<code>stopped → running</code>

执行的最终

只要最高价等于或高于 Spot 价格，实例类型具有可用的容量，并且您未终止 Spot 实例，这些实例就会继续运行。如果 Spot 价格或可用容量变化要求 Amazon EC2 终止 Spot 实例，Spot 请求将进入终止状态。如果取消 Spot 请求或终止 Spot 实例，请求也将进入终止状态。

状态代码	请求状态	实例状态
request-canceled-and-instance-running	cancelled	running
marked-for-stop	active	running
marked-for-termination	closed	running
instance-stopped-by-price	disabled	stopped
instance-stopped-by-user	disabled	stopped
instance-stopped-no-capacity	disabled	stopped
instance-terminated-by-price	closed (一次性), open (持久性)	terminated
instance-terminated-by-schedule	closed	terminated
instance-terminated-by-service	cancelled	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-launch-group-constraint	closed (一次性), open (持久性)	terminated

† 只有当用户从实例运行关闭命令时，Spot 实例 才能到达此状态。我们不建议您这样做，因为 Spot 服务可能会重新启动实例。

* 如果您终止实例但未取消请求，则请求状态为 closed。如果您终止实例并取消请求，则请求状态为 cancelled。即使您在取消实例请求之前终止了 Spot 实例，Amazon EC2 检测您的 Spot 实例 已终止的过程可能会有延迟。在这种情况下，请求状态可能是 closed 或 cancelled。

持久性请求：

当您的 Spot 实例 终止 (由您或由 Amazon EC2) 时，如果 Spot 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 Spot 实例。

获取请求状态信息

您可以使用 AWS 管理控制台或命令行工具获取请求状态信息。

获取请求状态信息 (控制台)

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 (Spot 请求)，然后选择所需的 Spot 请求。
3. 要查看状态，请依次选择 Description (描述) 和 Status (状态)。

使用命令行获取请求状态信息

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)

Spot 请求状态代码

Spot 请求状态信息包含状态代码、更新时间以及状态消息。这些信息帮助您确定如何处理 Spot 请求。

下面是 Spot 请求状态代码：

`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 Spot 请求的一个或多个参数无效 (例如，您指定的 AMI 不存在)。状态消息指示哪个参数无效。

`canceled-before-fulfillment`

在完成前，用户取消了竞价请求。

`capacity-not-available`

您请求的实例没有足够的容量可用。

`constraint-not-fulfillable`

由于一个或多个限制无效 (例如，可用区不存在)，Spot 请求无法完成。状态消息指示哪个限制无效。

`fulfilled`

Spot 请求处于 `active` 状态，Amazon EC2 正在启动您的 Spot 实例。

`instance-stopped-by-price`

您的实例已停止，因为 Spot 价格超出了您的最高价格。

`instance-stopped-by-user`

您的实例已停止，因为用户从实例运行了 `shutdown -h`。

`instance-stopped-no-capacity`

您的实例已停止，因为实例不再有足够的 Spot 容量可用。

`instance-terminated-by-price`

您的实例已终止，因为 Spot 价格超出了您的最高价格。如果您的请求是持久性的，该过程将重新开始，因此，您的请求将等待进行评估。

`instance-terminated-by-schedule`

Spot 实例在其计划持续时间结束时终止。

`instance-terminated-by-service`

您的实例从停止状态终止。

`instance-terminated-by-user` 或者 `spot-instance-terminated-by-user`

您终止了已完成的 Spot 实例，因此，请求状态为 `closed`（除非这是持久性请求），实例状态为 `terminated`。

`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限制。

`instance-terminated-no-capacity`

您的实例已终止，因为实例不再有足够的 Spot 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。有关这些限制以及如何请求提高限制的更多信息，请参阅 Amazon Web Services 一般参考中的 [Amazon EBS 限制](#)。

`marked-for-stop`

您的 Spot 实例被标记为停止。

`marked-for-termination`

您的 Spot 实例被标记为终止。

`not-scheduled-yet`

您的 Spot 请求在指定日期之前不会被评估。

`pending-evaluation`

当您提交 Spot 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 正尝试预置 Spot 实例。

`placement-group-constraint`

因为 Spot 实例目前不能添加到置放群组中，因此尚无法完成 Spot 请求。

`price-too-low`

由于您的最高价低于 Spot 价格，无法完成请求。在这种情况下，不会启动任何实例，并且您的请求保持 `open` 状态。

`request-canceled-and-instance-running`

在 Spot 实例仍在运行时，您取消了 Spot 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，Spot 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 AWS Support 以获取帮助。

Spot 实例中断

对 Spot 实例的需求可能因时间不同而有显著的差异，Spot 实例的可用性也会因为有多少未使用 EC2 实例可用而差别巨大。始终可能会中断您的 Spot 实例。因此，必须确保应用程序针对 Spot 实例中断做好准备。

不能中断在 EC2 队列或 Spot 队列中指定的个按需实例。

目录

- [中断原因 \(p. 326\)](#)
- [中断行为 \(p. 326\)](#)
- [准备中断 \(p. 328\)](#)
- [准备将实例休眠 \(p. 328\)](#)
- [Spot 实例中断通知 \(p. 329\)](#)
- [中断的 Spot 实例的计费 \(p. 330\)](#)

中断原因

下面列出了 Amazon EC2 中断您的 Spot 实例 的可能原因：

- 价格 – Spot 价格高于您的最高价。
- 容量 – 如果没有足够的未使用 EC2 实例，无法满足 Spot 实例 的需求，则 Amazon EC2 会中断 Spot 实例。实例的中断顺序是由 Amazon EC2 确定的。
- 约束 – 如果您的请求包含约束（如启动组或可用区组），则当不再满足约束时，这些 Spot 实例 将成组终止。

中断行为

您可以指定在 Spot 实例 中断时 Amazon EC2 应将其休眠、停止还是终止。您可以选择满足您的需求的中断行为。默认方式是在 Spot 实例中断时将其终止。要更改中断行为，请在创建 Spot 请求时从控制台的 Interruption behavior(中断行为) 中选择一个选项，或者在启动配置或启动模板中指定 InstanceInterruptionBehavior。要在创建 Spot 请求时在控制台中更改中断行为，请选择 Maintain target capacity(维护目标容量)。如果您选择此选项，Interruption behavior(中断行为) 将出现，并且您随后可指定 Spot 服务在中断时终止、停止 Spot 实例或使其休眠。

停止中断的 Spot 实例

您可以更改中断行为，以便在满足以下要求时，Amazon EC2 停止中断的 Spot 实例。

要求

- 对于 Spot 实例请求，类型必须是 persistent。您不能在Spot 实例请求中指定启动组。
- 对于 EC2 队列或 Spot 队列请求，类型必须是 maintain。
- 根卷必须是 EBS 卷，而不是实例存储卷。

在 Spot 服务停止一个 Spot 实例后，只有 Spot 服务才能重新启动 Spot 实例，而且必须使用同一启动规范。

对于由 persistent Spot 实例请求启动的 Spot 实例，Spot 服务会在容量在同一可用区中可用且适用于已停止的实例的同一实例类型时重新启动已停止的实例。

如果 EC2 队列或 Spot 队列中的实例已停止并且队列类型为 maintain，则 Spot 服务启动替换实例以保持目标容量。Spot 服务基于指定的分配策略 (lowestPrice、diversified 或 InstancePoolsToUseCount) 查找最优池；它不会使用早期已停止的实例确定池的优先级。稍后，如果分配策略产生了包含早期已停止的实例的池，则 Spot 实例会重新启动已停止的实例以满足目标容量。

例如，考虑使用 lowestPrice 分配策略的 Spot 队列。初始启动时，c3.large 池满足启动规范的 lowestPrice 条件。稍后，当中断 c3.large 实例时，Spot 服务会停止实例并从符合 lowestPrice 策略的其他池中补充容量。此时，该池正好是一个 c4.large 池，并且 Spot 服务会启动 c4.large 实例以满足目标容量。同样，Spot 队列下次可以移动到 c5.large 池。在这些转换的每个转换中，Spot 服务不会使

用早期已停止的实例确定池的优先级，但会仅在指定的分配策略上确定优先级。`lowestPrice` 策略可以返回到包含早期已停止的实例的池。例如，如果实例在 `c5.large` 池中被中断且 `lowestPrice` 策略将其返回到 `c3.large` 或 `c4.large` 池，则早期已停止的实例会重新启动以满足目标容量。

在 Spot 实例停止后，您可以修改其部分实例属性，但不能修改实例类型。如果您分离或删除一个 EBS 卷，则在 Spot 实例启动时不会附加该卷。如果您分离根卷，并且 Spot 服务尝试启动 Spot 实例，则该实例将启动失败，并且 Spot 服务将终止已停止的实例。

当 Spot 实例停止时，您可以将其终止。如果取消 Spot 请求、EC2 队列或 Spot 队列，Spot 服务将终止任何停止的关联 Spot 实例。

在 Spot 实例停止后，您只需为保留的 EBS 卷付费。对于 EC2 队列和 Spot 队列，如果具有很多停止的实例，则可能会超出您的账户的 EBS 卷数限制。

休眠中断的 Spot 实例

您可以更改中断行为，以便在满足以下要求时，Amazon EC2 在 Spot 实例 中断时将其休眠。

要求

- 对于 Spot 实例请求，类型必须是 `persistent`。您不能在 Spot 实例请求中指定启动组。
- 对于 EC2 队列或 Spot 队列请求，类型必须是 `maintain`。
- 根卷必须是 EBS 卷，而不是实例存储卷，并且它必须足够大以在休眠期间存储实例内存 (RAM)。
- 支持以下实例：`C3`、`C4`、`C5`、`M4`、`M5`、`R3` 和 `R4`，并且内存少于 100 GB。
- 支持以下操作系统：Amazon Linux 2、Amazon Linux AMI、AWS 优化的 Ubuntu 内核 (`linux-aws`) 高于 4.4.0-1041 的 Ubuntu 以及 Windows Server 2008 R2 和更高版本。
- 在支持的操作系统上安装休眠代理，或者使用已包含该代理的以下 AMI 之一：
 - Amazon Linux 2
 - Amazon Linux AMI 2017.09.1 或更高版本
 - Ubuntu Xenial 16.04 20171121 或更高版本
 - Windows Server 2008 R2 AMI 2017.11.19 或更高版本
 - Windows Server 2012 或 Windows Server 2012 R2 AMI 2017.11.19 或更高版本
 - Windows Server 2016 AMI 2017.11.19 或更高版本
 - Windows Server 2019
- 启动该代理。我们建议您使用用户数据在实例启动时启动该代理。或者，您也可以手动启动该代理。

建议

- 我们强烈建议您将加密的 Amazon EBS 卷作为根卷，因为在休眠期间实例内存存储在根卷上。这确保在卷上静态存储数据以及在实例和卷之间移动数据时，将加密内存 (RAM) 内容。可以使用以下三个选项之一，以确保根卷是加密的 Amazon EBS 卷：
 - EBS“单步加密”：在单个 `run-instances` API 调用中，您可以从未加密的 AMI 中启动 EBS 支持的加密 EC2 实例。有关更多信息，请参阅 [将加密与 EBS 支持的 AMI 结合使用 \(p. 134\)](#)。
 - EBS 默认加密：您可以启用 EBS 默认加密，以确保加密在您的 AWS 账户中创建的所有新的 EBS 卷。有关更多信息，请参阅 [默认加密 \(p. 853\)](#)。
 - 加密的 AMI：您可以使用加密的 AMI 启动实例以启用 EBS 加密。如果 AMI 没有加密的根快照，则可以将其复制到新的 AMI 并请求加密。有关更多信息，请参阅 [在复制过程中将未加密映像加密 \(p. 137\)](#) 和 [复制 AMI \(p. 141\)](#)。

在 Spot 服务将 Spot 实例休眠时，将保留 EBS 卷并在根卷上保留实例内存 (RAM)。还会保留实例的私有 IP 地址。不会保留实例存储卷和公有 IP 地址 (非弹性 IP 地址)。在实例休眠时，仅向您收取 EBS 卷费用。对于 EC2 队列和 Spot 队列，如果具有很多休眠的实例，则可能会超出您的账户的 EBS 卷数限制。

在实例从 Spot 服务收到指令时，该代理将提示操作系统休眠。如果未安装该代理，则底层操作系统不支持休眠，或者没有足够的卷空间以保存实例内存，休眠将失败并且 Spot 服务停止该实例。

在 Spot 服务将 Spot 实例 休眠时，将收到一条中断通知，但不会在 Spot 实例 中断之前留出两分钟的时间。将立即开始休眠。在实例进行休眠过程中，实例运行状况检查可能会失败。在休眠过程完成时，实例状态为 stopped。

在 Spot 服务将Spot 实例休眠后，只能由 Spot 服务恢复该实例。如果 Spot 价格低于您指定的最高价，并且具有可用的容量，Spot 服务将恢复该实例。

有关更多信息，请参阅 [准备将实例休眠 \(p. 328\)](#)。

有关将按需实例休眠的信息，请参阅[使 Linux 实例休眠 \(p. 447\)](#)。

准备中断

下面是在使用 Spot 实例时可以遵循的一些最佳实践：

- 使用默认最高价 (这是按需价格)。
- 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 Spot 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Spot 实例中断通知监控您的 Spot 实例的状态。
- 虽然我们尽一切努力尽快提供此警告，但您的 Spot 实例 可能会在我们提供此警告之前被终止。测试您的应用程序，确保它很好地处理了意外的实例终止，即使您正在针对中断通知进行测试。您可以使用 个按需实例 来运行应用程序，然后自行终止该 个按需实例，以便确认这一点。

准备将实例休眠

您必须在您的实例上安装休眠代理，除非您使用已包含该代理的 AMI。您必须在实例启动时运行该代理，无论该代理是包含在您的 AMI 中，还是您自行安装的。

下列步骤帮助您准备 Linux 实例。有关准备 Windows 实例的说明，请参阅Amazon EC2 用户指南 (适用于 Windows 实例) 中的[准备将实例休眠](#)。

准备 Amazon Linux 实例

1. 确认您的内核支持休眠，并在必要时更新内核。
2. 如果您的 AMI 不包含该代理，请使用以下命令安装代理。

```
sudo yum update; sudo yum install hibagent
```

3. 将以下命令添加到用户数据中：

```
#!/bin/bash
/usr/bin/enable-ec2-spot-hibernation
```

准备 Ubuntu 实例

1. 如果您的 AMI 不包含该代理，请使用以下命令安装代理。休眠代理仅在 Ubuntu 16.04 或更高版本上可用。

```
sudo apt-get install hibagent
```

2. 将以下命令添加到用户数据中。

```
#!/bin/bash
/usr/bin/enable-ec2-spot-hibernation
```

Spot 实例中断通知

防范 Spot 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 Spot 实例 中断通知，该通知可在 Amazon EC2 必须停止或终止您的 Spot 实例 时，提前两分钟发出警告。建议您每 5 秒检查一次这些警告。

此警告作为 CloudWatch 事件以及 Spot 实例 上[实例元数据 \(p. 499\)](#)中的项目提供。

如果您将休眠指定为中断行为，则会收到中断通知，但由于休眠过程立即开始，因此您不会提前两分钟收到警告。

EC2 Spot 实例 Interruption Notice

在 Amazon EC2 将要中断 Spot 实例时，它在实际中断之前两分钟发出一个事件。Amazon CloudWatch Events 可以检测该事件。有关更多信息，请参阅 [Amazon CloudWatch Events 用户指南](#)。

以下是Spot 实例中断事件的示例。instance-action 的可能值为 hibernate、stop 和 terminate。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

instance-action

如果 Spot 实例 标记为由 Spot 服务停止或终止，将在您的实例元数据中包含 instance-action 项。如果没有，则不显示。您可以按如下方式检索 instance-action。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/spot/instance-action
```

instance-action 项目指定操作及其大致执行时间 (采用 UTC 格式)。

以下示例指示将停止此实例的时间：

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

以下示例指示将终止此实例的时间：

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

如果 Amazon EC2 未准备停止或终止实例，或者您自己终止了实例，则 instance-action 不存在且您会收到 HTTP 404 错误。

termination-time

为向后兼容而保留此项目；您应改为使用 `instance-action`。

如果 Spot 实例 标记为由 Spot 服务终止，则您的实例元数据中将显示 `termination-time` 项目。如果没有，则不显示。您可以按如下方式检索 `termination-time`。

```
[ec2-user ~]$ if curl -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*z; then echo terminated; fi
```

`termination-time` 项目指定实例将收到关闭信号的大致时间（用 UTC 表示）。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 Spot 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。

如果 Amazon EC2 无法终止实例，请求状态将设置为 `fulfilled`。`termination-time` 值会将实例元数据保持原始大致时间（现已成为过去时间）。

中断的 Spot 实例的计费

当 Spot 实例（不在 Spot 块中）被中断时，将向您收费，如下所示。

Spot 实例的中断方	操作系统	在第一个小时内中断	在第一个小时后的任一小时内中断
如果您中断 Spot 实例	Linux（不包括 RHEL 和 SUSE）	按使用的秒数收费	按使用的秒数收费
	Windows、RHEL、SUSE	按完整小时收费（即使您的使用时间是部分小时也是如此）	按使用的完整小时数收费，对于中断的部分完整小时，按完整小时收费
如果 Amazon EC2 中断 Spot 实例	Linux（不包括 RHEL 和 SUSE）	免费	按使用的秒数收费
	Windows、RHEL、SUSE	免费	按使用的完整小时数收费，对于中断的部分小时，不收费

当 Spot 实例（在 Spot 块中）被中断时，将向您收费，如下所示。

Spot 实例的中断方	操作系统	在第一个小时内中断	在第一个小时后的任一小时内中断
如果您中断 Spot 实例	Linux（不包括 RHEL 和 SUSE）	按使用的秒数收费	按使用的秒数收费
	Windows、RHEL、SUSE	按完整小时收费（即使您的使用时间是部分小时也是如此）	按使用的完整小时数收费，对于中断的部分完整小时，按完整小时收费
如果 Amazon EC2 中断 Spot 实例	Linux（不包括 RHEL 和 SUSE）	免费	免费
	Windows、RHEL、SUSE	免费	免费

Spot 实例数据源

为了帮助您了解 Spot 实例 费用情况 , Amazon EC2 通过提供的数据源说明 Spot 实例 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 Spot 实例 运行 , 则您不会收到该小时的数据源文件。

目录

- [数据源文件名和格式 \(p. 331\)](#)
- [Amazon S3 存储桶要求 \(p. 332\)](#)
- [订阅您的Spot 实例数据源 \(p. 332\)](#)
- [删除您的Spot 实例数据源 \(p. 332\)](#)

数据源文件名和格式

Spot 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 `aws-s3-bucket1` 并且前缀为 `myprefix` , 则您的文件名类似如下 :

```
aws-s3-bucket1.s3.amazonaws.com/myprefix/111122223333.2014-03-17-20.001.pwBdGTJG.gz
```

Spot 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	描述
Timestamp	时间戳 , 其用于确定针对此实例使用收取的费用。
UsageType	指示使用类型和被收取费用的实例类型。对于 <code>m1.small</code> Spot 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> 。
Operation	指示被收取费用的产品。对于 Linux Spot 实例 , 此字段设置为 <code>RunInstances</code> 。对于 Windows Spot 实例 , 此字段设置为 <code>RunInstances:0002</code> 。Spot 使用情况按照可用区分组。
InstanceID	生成此实例使用的Spot 实例的 ID。
MyBidID	生成此实例使用的Spot 实例请求的 ID。
MyMaxPrice	为此Spot 实例请求指定的最高价。
MarketPrice	在 <code>Timestamp</code> 字段中指定的时刻的 Spot 价格。
Charge	针对此实例使用收取的费用。
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：

- 您必须拥有存储桶的 FULL_CONTROL 权限，其中包括 s3:GetBucketAcl 和 s3:PutBucketAcl 操作的权限。
如果您是存储桶拥有者，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。
- 在您订阅数据源时，这些权限用于更新存储桶 ACL，以向 AWS 数据源账户提供 FULL_CONTROL 权限。AWS 数据源账户会将数据源文件写入存储桶。如果您的账户没有所需权限，则数据源文件无法写入存储桶。

Note

如果您更新 ACL 并删除 AWS 数据源账户的权限，则数据源文件无法写入存储桶。您必须重新订阅数据源以接收数据源文件。

- 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。AWS 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 AWS 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 Spot 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 aws-s3-bucket1 [--prefix myprefix]
```

下面是示例输出：

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "111122223333",  
        "Prefix": "myprefix",  
        "Bucket": "aws-s3-bucket1",  
        "State": "Active"  
    }  
}
```

删除您的 Spot 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
```

Spot 实例限制

Spot 实例请求受以下限制的约束：

限制

- [Spot 请求限制 \(p. 333\)](#)
- [Spot 队列限制 \(p. 333\)](#)
- [T3 实例 \(p. 333\)](#)
- [T2 实例 \(p. 333\)](#)

Spot 请求限制

默认情况下，每个区域的账户限制为 20 个 Spot 实例。如果您终止了 Spot 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。

Spot 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可以逐渐增加。此外，您的账户对特定 Spot 实例类型可能存在一些限制。如果您提交 Spot 实例请求，并且收到错误 `Max spot instance count exceeded`，您可以填写 AWS 支持中心[创建案例](#)表单以请求增加 Spot 实例限制。对于 Limit type (限制类型)，选择 EC2 Spot Instances (EC2 Spot 实例)。有关更多信息，请参阅 [Amazon EC2 服务限制 \(p. 950\)](#)。

Spot 队列限制

常用的 Amazon EC2 限制适用于 Spot 队列或 EC2 队列，例如，Spot 请求价格限制、实例限制和卷限制。此外，以下限制将适用：

- 每个区域的活动 Spot 队列 和 EC2 队列 的数量：1000*
- 每个队列的启动规范的数量：50*
- 启动规范中的用户数据的大小：16 KB*
- 每个 Spot 队列或 EC2 队列的目标容量：10000
- 区域中所有 Spot 队列和 EC2 队列的目标容量：100000
- Spot 队列请求或 EC2 队列请求不能跨区域。
- Spot 队列请求或 EC2 队列请求不能跨同一可用区内的不同子网。

如果您需要增加目标容量的默认限制，请填写 AWS 支持中心[创建案例](#)表格请求增加限制。对于 Limit type (限制类型)，选择 EC2 Fleet (EC2 队列)，选择区域，然后选择 Target Fleet Capacity per Fleet (in units) (每个队列的目标队列容量(单位)) 和/或 Target Fleet Capacity per Region (in units) (每个区域的目标队列容量(单位))。

*这些是硬限制。您不能请求提高这些限制。

T3 实例

如果您打算立即或短期内使用 T3 Spot 实例，没有空闲时间累积 CPU 积分，我们建议您以 [standard \(p. 185\)](#) 模式启动 T3 Spot 实例 以避免支付更多的费用。

如果您以 [unlimited \(p. 178\)](#) 模式启动 T3 Spot 实例 并立即突增 CPU，您将会为突增花费超额积分。如果您在短期内使用实例，实例没有时间累积 CPU 积分来支付超额积分，则您将在终止实例时为超额积分付费。

只有实例的运行时间较长，足以累积进行突增的 CPU 积分时，针对 T3 Spot 实例的 Unlimited 模式才适用。否则，为超额积分付费会使 T3 Spot 实例比 M5 或 C5 实例的费用更高。

T2 实例

通过提供足够的计算资源来配置实例，启动积分旨在为 T2 实例提供有成效的初始启动体验。不允许重复启动 T2 实例以访问新的启动积分。如果您需要持续的 CPU，您可以赚取积分 (通过空转一段时间)，使用 [T2 Unlimited \(p. 178\)](#)，或将实例类型和专用 CPU (例如 c4.large) 一起使用。

专用主机

Amazon EC2 专用主机是 EC2 实例容量完全专供您使用的物理服务器。专用主机允许您使用按插槽、按内核或按虚拟机授权的现有软件许可证，包括 Windows Server、Microsoft SQL Server、SUSE 和 Linux Enterprise Server。

目录

- [专用主机与专用实例的区别 \(p. 334\)](#)
- [自带许可 \(p. 334\)](#)
- [专用主机实例容量 \(p. 335\)](#)
- [专用主机限制 \(p. 335\)](#)
- [定价和计费 \(p. 335\)](#)
- [使用专用主机 \(p. 336\)](#)
- [使用共享专用主机 \(p. 348\)](#)
- [主机恢复 \(p. 351\)](#)
- [跟踪配置更改 \(p. 355\)](#)

专用主机与专用实例的区别

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。下表重点介绍专用主机和专用实例之间的一些重要区别：

	专用主机	专用实例
计费	按主机计费	按实例计费
套接字、内核和主机 ID 的可见性	提供套接字数和物理内核数的可见性	无可见性
主机和实例关联	允许您在一段时间内将您的实例一致地部署到同一物理服务器	不支持
定向实例置放	提供额外可见性以及对在物理服务器上放置实例的方式的控制	不支持
自动实例恢复	支持。有关更多信息，请参阅 主机恢复 (p. 351) 。	支持
自带许可 (BYOL)	支持	不支持

自带许可

专用主机允许使用现有的按插槽、按内核或按虚拟机软件的许可证。如果自带许可，您有责任管理自己的许可证。不过，Amazon EC2 具有一些帮助您保持许可证合规性的功能，例如实例关联和定向置放。

要将您自己的卷许可的计算机镜像引入到 Amazon EC2 中，需要执行以下常规步骤。

1. 验证控制您的系统映像使用的许可证条款是否允许在虚拟化云环境中使用系统映像。
2. 在确认可在 Amazon EC2 中使用系统映像后，使用 VM Import/Export 导入该映像。有关如何导入系统映像的信息，请参阅 [VM Import/Export 用户指南](#)。
3. 在导入系统映像后，可以在您的账户中的活动专用主机上从该映像中启动实例。
4. 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 服务器激活这些实例。

Note

要跟踪您的映像在 AWS 中的使用方式，请在 AWS Config 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[跟踪配置更改 \(p. 355\)](#)。

专用主机实例容量

AWS Nitro 系统支持的专用主机可以支持同一实例系列中的多种实例类型。例如，在分配 r5 专用主机时，您可以使用一个具有 2 个插槽和 48 个物理内核的主机，可以在该主机上运行不同的实例类型，例如 r5.2xlarge 和 r5.4xlarge。您可以运行任意数量的实例，直到与该主机关联的内核容量用尽。例如，下表显示了您可以在专用主机上运行的不同实例类型组合。

实例系列	实例类型组合示例
R5	<ul style="list-style-type: none">示例 1 : 4 x r5.4xlarge + 4 x r5.2xlarge示例 2 : 1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large
C5	<ul style="list-style-type: none">示例 1 : 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge示例 2 : 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large
M5	<ul style="list-style-type: none">示例 1 : 4 x m5.4xlarge + 4 x m5.2xlarge示例 2 : 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large

对于 AWS Nitro 系统不支持的实例系列，您只能为特定的实例类型配置专用主机。有关专用主机上支持的所有实例系列和实例类型配置的列表，请参阅[Amazon EC2 专用主机定价](#)。

专用主机限制

在分配专用主机之前，请注意以下限制：

- RHEL、SUSE Linux 和 Windows AMI (无论由 AWS 提供还是在 AWS Marketplace 上提供) 无法用于专用主机。
- 最多可以为每个区域的每个实例系列分配两个按需专用主机。可以请求提高限制：[请求提高 Amazon EC2 专用主机的分配限制](#)。
- 在专用主机上运行的实例只能在 VPC 中启动。
- 在使用指定主机资源组的启动模板时，支持 Auto Scaling 组。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的[为 Auto Scaling 组创建启动模板](#)。
- 不支持 Amazon RDS 实例。
- AWS 免费使用套餐不适用于专用主机。
- 实例置放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。

定价和计费

专用主机的价格因付款选项而异。

付款选项

- [按需专用主机 \(p. 336\)](#)

- [专用主机预留 \(p. 336\)](#)
- [Savings Plans \(p. 336\)](#)

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。

专用主机的按需价格因实例系列和区域而异。您需按专用主机的小时费率付费，无论您选择在专用主机上启动的实例的数量或大小如何。换句话说，您需要为整个专用主机而不是您选择在其中运行的单个实例付费。有关按需定价的更多信息，请参阅 [Amazon EC2 专用主机按需定价](#)。

您可以随时释放按需专用主机以停止产生费用。有关释放专用主机的信息，请参阅 [释放专用主机 \(p. 345\)](#)。

专用主机预留

与运行按需 专用主机 相比，专用主机预留 可提供账单折扣。预留提供三种付款选项：

- 无预付费用 — 无预付费用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，无需额外将来付费。

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。如果有三个不同实例大小的专用主机 (`m4.xlarge`、`m4.medium` 和 `m4.large`)，则可以将一个 `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之关联的专用主机的实例系列和区域相匹配。

当预留与专用主机关联后，将无法释放专用主机，直到预留期限结束。

有关预留定价的更多信息，请参阅 [Amazon EC2 专用主机定价](#)。

Savings Plans

Savings Plans 是通过按需实例提供大幅优惠的灵活定价模式。在使用 Savings Plans 时，您承诺在一年或三年期限内保持一致的使用量（以美元/小时为单位）。这使您能够灵活地使用最能满足您的需求的专用主机，并继续节省费用，而不必对特定专用主机做出承诺。有关更多信息，请参阅 [AWS Savings Plans 用户指南](#)。

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主机 租赁，在主机上启动实例。您必须选择在其中启动实例的特定主机，或者您可以允许实例在任何已启用自动置放且匹配其实例类型的主机上启动。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 该主机。

专用主机也与 AWS License Manager 相集成。使用 License Manager，您可以创建主机资源组，该组是作为单个实体进行管理的专用主机的集合。创建主机资源组时，可以为专用主机指定主机管理首选项，如自动分配和自动释放。这允许您在专用主机上启动实例，而无需手动分配和管理这些主机。有关更多信息，请参阅 AWS License Manager 用户指南 中的 [主机资源组](#)。

目录

- [分配专用主机 \(p. 337\)](#)
- [在专用主机上启动实例 \(p. 338\)](#)

- 在主机资源组中启动实例 (p. 339)
- 了解自动置放与关联 (p. 340)
- 修改专用主机自动置放 (p. 340)
- 修改支持的实例类型 (p. 341)
- 修改实例租赁和关联 (p. 342)
- 查看专用主机 (p. 343)
- 标记专用主机 (p. 344)
- 监控专用主机 (p. 345)
- 释放专用主机 (p. 345)
- 购买 专用主机预留 (p. 346)
- 查看专用主机预留 (p. 347)
- 标记 专用主机预留 (p. 348)

分配专用主机

要开始使用专用主机，您必须使用 Amazon EC2 控制台或命令行工具在您的账户中分配专用主机。

在分配专用主机后，将在您的账户中立即提供专用主机容量，您可以开始在专用主机上启动实例。

使用 Amazon EC2 控制台分配专用主机

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机、分配 专用主机。
3. 对于 Instance family (实例系列)，为专用主机选择实例系列。
4. 指定专用主机是支持选定实例系列中的多种实例类型，还是仅支持特定的实例类型。请执行以下任一操作。
 - 要将专用主机配置为支持选定实例系列中的多种实例类型，请选择 Support multiple instance types (支持多种实例类型)。通过启用该选项，您可以在专用主机上启动同一实例系列中的不同实例类型。例如，如果您选择 m5 实例系列并选择该选项，则可以在专用主机上启动 m5.xlarge 和 m5.4xlarge 实例。可以将以下实例系列配置为支持多种实例类型：A1, C5, C5n, M5, M5n, R5, and R5n。
 - 要将专用主机配置为支持选定实例系列中的特定实例类型，请清除 Support multiple instance types (支持多种实例类型)，然后为 Instance type (实例类型) 选择要支持的实例类型。通过启用该选项，您可以在专用主机上启动一种实例类型。例如，如果选择该选项并将 m5.4xlarge 指定为支持的实例类型，则只能在专用主机上启动 m5.4xlarge 实例。
5. 对于 Availability Zone (可用区)，选择要在其中分配专用主机的可用区。
6. 要允许专用主机接受与其实例类型匹配的非定向实例启动，请为实例自动置放选择启用。有关自动置放的更多信息，请参阅[了解自动置放与关联 \(p. 340\)](#)。
7. 要为专用主机启用主机恢复，请为主机恢复选择启用。有关更多信息，请参阅[主机恢复 \(p. 351\)](#)。
8. 对于 Quantity (数量)，输入要分配的专用主机数量。
9. (可选) 选择添加标签，然后输入标签键和标签值。
10. 选择 Allocate host。

使用命令行工具分配专用主机

使用以下命令之一。

以下命令分配一个专用主机，它在 us-east-1a 可用区中支持 m5 实例系列中的多种实例类型。该主机还启用了主机恢复，并禁用了自动置放。

- [allocate-hosts \(AWS CLI\)](#)

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --auto-placement "off" --host-recovery "on" --quantity 1
```

- [New-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -AutoPlacement Off -HostRecovery On -Quantity 1
```

以下命令分配一个在 eu-west-1a 可用区中支持非定向 m4.large 实例启动的专用主机，启用主机恢复，并应用一个具有键 purpose 和值 production 的标签。

- [allocate-hosts \(AWS CLI\)](#)

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a" --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

- [New-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

TagSpecification 参数用于在创建时标记专用主机，需要一个指定所标记资源类型、标签键和标签值的对象。以下命令创建所需对象。

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

以下命令分配专用主机并应用在 \$tagspec 对象中指定的标签。

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

在专用主机上启动实例

在分配一个专用主机后，您可以在其中启动实例。对于您启动的实例类型，如果没有具有足够可用容量的活动专用主机，则无法启动具有 host 租赁的实例。

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 [专用主机限制 \(p. 335\)](#)。

从专用主机页面中在特定专用主机上启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 在 专用主机 页面上，选择一个主机，选择 Actions (操作)，然后选择 Launch Instance(s) onto Host (在主机上启动实例)。
4. 从列表中选择一个 AMI。Windows、SUSE 和 Amazon EC2 提供的 RHEL AMI 无法用于专用主机。
5. 在 Choose an Instance Type (选择实例类型) 页面上，选择要启动的实例类型，然后选择 Next: Configure Instance Details (下一步：配置实例详细信息)。

如果专用主机仅支持一种实例类型，则默认选择支持的实例类型，而无法进行更改。

如果专用主机支持多种实例类型，您必须根据专用主机的可用实例容量在支持的实例系列中选择一种实例类型。建议您首先启动较大的实例大小，然后根据需要用较小的实例大小填充剩余的实例容量。

6. 在配置实例详细信息页面上，配置实例设置以满足需求，然后为关联选择下列选项之一：

- 关闭 — 实例在指定的主机上启动，但不保证停止后仍在同一专用主机上重新启动。
- 主机 — 如果停止，实例将始终在此特定主机上重新启动。

有关关联的更多信息，请参阅[了解自动置放与关联 \(p. 340\)](#)。

租赁和主机选项是根据您选择的主机预配置的。

7. 选择 Review and Launch。
8. 在 Review Instance Launch 页面上，选择 Launch。
9. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

使用启动实例向导在专用主机上启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择实例、启动实例。
3. 从列表中选择一个 AMI。Windows、SUSE 和 Amazon EC2 提供的 RHEL AMI 无法用于专用主机。
4. 选择要启动的实例类型，然后选择下一步：配置实例详细信息。
5. 在配置实例详细信息页面上，配置实例设置以满足需求，然后配置以下专用主机特定的设置：
 - 租赁 — 选择专用主机 – 在专用主机上启动此实例。
 - 主机 — 选择使用自动置放可在任何已启用自动置放的专用主机或在列表中选择特定的专用主机上启动实例。该列表仅显示支持选定实例类型的专用主机。
 - 关联 — 请选择下列选项之一：
 - 关闭 — 实例在指定的主机上启动，但不保证停止后仍在其上重新启动。
 - 主机 — 如果停止，实例将始终在指定主机上重新启动。

有关更多信息，请参阅[了解自动置放与关联 \(p. 340\)](#)。

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. 选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

使用命令行工具在专用主机上启动实例

使用以下命令之一并在 Placement 请求参数中指定实例关联、租赁和主机：

- [run-instances \(AWS CLI\)](#)
- [New-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在主机资源组中启动实例

在包含具有可用实例容量的专用主机的主机资源组中启动实例时，Amazon EC2 将在该主机上启动实例。如果主机资源组没有包含具有可用实例容量的主机，Amazon EC2 将自动分配主机资源组中的新主机，然后在该主机上启动实例。有关更多信息，请参阅 AWS License Manager 用户指南 中的[主机资源组](#)。

在主机资源组中启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择实例、启动实例。
3. 从列表中选择一个 AMI。Windows、SUSE 和 Amazon EC2 提供的 RHEL AMI 无法用于专用主机。
4. 选择要启动的实例类型，然后选择下一步：配置实例详细信息。
5. 在配置实例详细信息页面上，配置实例设置以满足需求，然后执行以下操作：
 - a. 对于租赁，选择专用主机。
 - b. 对于 Host resource group (主机资源组)，选择 Launch instance into a host resource group (在主机资源组中启动实例)。
 - c. 对于 Host resource group name (主机资源组名称)，选择要在其中启动实例的主机资源组。

您无法通过选择主机 ID 来定位特定主机，并且无法在主机资源组中启动实例时启用实例关联。

6. 选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

了解自动置放与关联

专用主机的置放控制是在实例级别和主机级别进行的。

自动置放

自动置放是在主机级别配置的。通过使用该功能，您可以管理启动的实例是在特定主机上启动，还是在具有匹配配置的任何可用主机上启动。

如果专用主机的自动置放已禁用，则它仅接受指定其唯一主机 ID 的主机租赁实例启动。这是新专用主机的默认设置。

如果专用主机的自动置放已启用，则它接受任何匹配其实例类型配置的非定向实例启动。

在启动实例时，您需要配置其租赁。如果在专用主机上启动实例而不提供特定 HostId，则将允许实例在任何已启用自动置放且匹配其实例类型的专用主机上启动。

主机关联

在实例级别配置主机关联。它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。

如果关联设置为 Off，并且您停止并重新启动实例，则实例可在任何可用主机上重新启动。但是，它将尝试在上次运行它的专用主机上启动(尽最大努力)。

修改专用主机自动置放

在将专用主机分配给 AWS 账户后，可以修改专用主机的自动置放设置。

使用 Amazon EC2 控制台修改专用主机的自动置放

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。

3. 在专用主机页面上，选择一个主机，然后依次选择操作、修改自动置放。
4. 在“修改自动置放”窗口中，对于允许自动置放，选择是以启用自动置放，或选择否以禁用自动置放。有关更多信息，请参阅[了解自动置放与关联 \(p. 340\)](#)。
5. 选择 Save。

使用命令行工具修改专用主机的自动置放

使用以下命令之一。以下示例为指定专用主机启用自动置放。

- [modify-hosts \(AWS CLI\)](#)

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

- [Edit-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

修改支持的实例类型

您可以修改专用主机以更改它支持的实例类型。如果它当前支持一种实例类型，您可以对其进行修改以支持该实例系列中的多种实例类型。类似地，如果它当前支持多种实例类型，您可以对其进行修改以仅支持特定的实例类型。

要修改专用主机以支持多种实例类型，您必须先停止主机上正在运行的所有实例。完成修改大约需要 10 分钟。在进行修改时，专用主机将转变为 pending 状态。在处于 pending 状态时，您无法在专用主机上启动停止的实例或启动新实例。可以修改以下实例系列以支持多种实例类型：A1, C5, C5n, M5, M5n, R5, and R5n。

要将支持多种实例类型的专用主机修改为仅支持特定的实例类型，则主机不能具有运行中的实例，或者运行中的实例必须是您希望主机支持的实例类型。例如，要将支持 m5 实例系列中的多种实例类型的主机修改为仅支持 m5.large 实例，则专用主机不能具有正在运行的实例，或者只能在主机上运行 m5.large 实例。

使用 Amazon EC2 控制台修改专用主机支持的实例类型

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 专用主机。
3. 选择要修改的专用主机，然后依次选择 Actions (操作) 和 Modify Supported Instance Types (修改支持的实例类型)。
4. 根据专用主机的当前配置，执行以下其中一项操作。
 - 如果专用主机当前支持特定的实例类型，则为 Support multiple instance types (支持多种实例类型) 选择 No (否)。要修改主机以支持当前实例系列中的多种类型，请为 Support multiple instance types (支持多种实例类型) 选择 Yes (是)。

您必须先停止主机上正在运行的所有实例，然后再修改主机以支持多种实例类型。

- 如果专用主机当前支持实例系列中的多种实例类型，则为 Support multiple instance types (支持多种实例类型) 选择 Yes (是)，Instance family (实例系列) 将显示支持的实例系列。要修改主机以支持特定的实例类型，请为 Support multiple instance types (支持多种实例类型) 选择 No (否)，然后为 Instance type (实例类型) 选择要支持的特定实例类型。

您无法更改专用主机支持的实例系列。

5. 选择 Save。

使用命令行工具修改专用主机支持的实例类型

可以使用 [modify-hosts](#) (AWS CLI) 或 [Edit-EC2Host](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

以下命令修改专用主机以支持 m5 实例系列中的多种实例类型。

- [modify-hosts](#) (AWS CLI)

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

- [Edit-EC2Host](#) (适用于 Windows PowerShell 的 AWS 工具)

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

以下命令修改专用主机以仅支持 m5.xlarge 实例。

- [modify-hosts](#) (AWS CLI)

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-ids h-012a3456b7890cdef
```

- [Edit-EC2Host](#) (适用于 Windows PowerShell 的 AWS 工具)

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

修改实例租赁和关联

在启动实例后，您可以将其租赁从 `dedicated` 更改为 `host` 或从 `host` 更改为 `dedicated`。您也可以修改实例与主机之间的关联。要修改实例租赁或关联，实例必须处于 `stopped` 状态。

使用 Amazon EC2 控制台修改实例租赁或关联

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择实例并选择要修改的实例。
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. 在修改实例置放页面上，配置以下项：
 - 租赁 — 选择下列项之一：
 - 运行专用硬件实例 — 将实例作为专用实例启动。有关更多信息，请参阅[专用实例 \(p. 356\)](#)。
 - 在专用主机上启动实例 — 在具有可配置关联的专用主机上启动实例。
 - 关联 — 选择下列项之一：
 - 此实例可以在任一主机上运行 — 实例在您的账户中支持该实例类型的任何可用专用主机上启动。
 - 此实例只能在选定的主机上运行 — 实例只能在为目标主机选择的专用主机上运行。
 - 目标主机 — 选择实例必须在其中运行的专用主机。如果未列出目标主机，则账户中可能没有可用的兼容专用主机。

有关更多信息，请参阅 [了解自动置放与关联 \(p. 340\)](#)。

6. 选择 Save。

使用命令行工具修改实例租赁或关联

使用以下命令之一。以下示例将指定实例的关联从 `default` 更改为 `host`，并指定与实例关联的专用主机。

- [modify-instance-placement \(AWS CLI\)](#)

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host --  
host-id h-012a3456b7890cdef
```

- [Edit-EC2InstancePlacement \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -  
HostId h-012a3456b7890cdef
```

查看专用主机

您可以查看有关专用主机及其中的单个实例的详细信息。

使用 Amazon EC2 控制台查看专用主机的详细信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 在 专用主机 页面上，选择一个主机。
4. 有关主机的信息，请选择描述。Available vCPUs (可用的 vCPU) 指示专用主机上可用于启动新实例的 vCPU。例如，如果专用主机支持 c5 实例系列中的多种实例类型，并且没有在上面运行实例，则它具有 72 个可用的 vCPU。这意味着，您可以在专用主机上启动不同的实例类型组合，以使用 72 个可用的 vCPU。

有关主机上运行的实例的信息，请选择实例。

使用命令行工具查看专用主机上的实例的详细信息

使用以下命令之一：

- [describe-hosts \(AWS CLI\)](#)

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

- [Get-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

使用命令行工具查看专用主机的实例容量

使用以下命令之一：

- [describe-hosts \(AWS CLI\)](#)

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

- [Get-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

以下示例使用 [describe-hosts \(AWS CLI\)](#) 命令查看支持 c5 实例系列中的多种实例类型的专用主机的可用实例容量。已在专用主机上运行两个 c5.4xlarge 实例和 4 个 c5.2xlarge 实例。

```
$ aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [  
    { "AvailableCapacity": 2,  
      "InstanceType": "c5.xlarge",  
      "TotalCapacity": 18 },  
    { "AvailableCapacity": 4,  
      "InstanceType": "c5.large",  
      "TotalCapacity": 36 }  
],  
"AvailableVCpus": 8
```

标记专用主机

您可以为现有专用主机分配自定义标签，以不同的方式对它们分类，例如按用途、所有者或环境。这有助于根据分配的自定义标签快速查找特定的专用主机。也可以将专用主机标签用于成本分配跟踪。

您还可以在创建时向专用主机应用标签。有关更多信息，请参阅[分配专用主机 \(p. 337\)](#)。

您可使用 Amazon EC2 控制台和命令行工具标记专用主机。

使用控制台标记专用主机

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 选择要标记的专用主机，然后选择标签。
4. 选择添加/编辑标签。
5. 在添加/编辑标签对话框中，选择创建标签，然后指定该标签的键和值。
6. (可选) 选择创建标签以将其他标签添加到专用主机。
7. 选择 Save。

使用命令行标记专用主机

使用以下命令之一：

- [create-tags \(AWS CLI \)](#)

以下命令将使用 Owner=TeamA 标记指定 专用主机。

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

- [New-EC2Tag \(适用于 Windows PowerShell 的 AWS 工具 \)](#)

New-EC2Tag 命令需要 Tag 对象，此对象指定要用于专用主机标签的键值对。以下命令使用 Owner 和 TeamA 键值对创建一个名为 \$tag 的 Tag 对象。

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag  
PS C:\> $tag.Key = "Owner"  
PS C:\> $tag.Value = "TeamA"
```

以下命令使用 \$tag 对象标记指定的专用主机。

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

监控专用主机

Amazon EC2 持续监控专用主机的状态。将在 Amazon EC2 控制台上显示更新的状态。您也可以使用命令行工具获取有关专用主机的信息。

使用 Amazon EC2 控制台查看专用主机的状态

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 在列表中找到专用主机，并查看状态列中的值。

使用命令行工具查看专用主机的状态

使用以下命令之一，然后查看 state 响应元素的 hostSet 属性：

- [describe-hosts \(AWS CLI\)](#)

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

- [Get-EC2Host \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

下表说明了可能的专用主机状态。

状态	描述
available	AWS 未检测到专用主机问题。不会安排维护或修复。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。如果必须采取措施，系统将通过 AWS 管理控制台或电子邮件通知您。无法在处于该状态的专用主机上启动实例。
pending	无法使用专用主机启动新的实例。正在对其进行 修改以支持多种实例类型 (p. 341) ，或者正在进行 主机恢复 (p. 351) 。
permanent-failure	检测到了一个不可恢复的故障。您将通过您的实例和通过电子邮件接收到一个移出通知。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。AWS 不会在此状态下重新启动实例。无法在处于该状态的专用主机上启动实例。
released-permanent-failure	AWS 永久释放已发生故障的专用主机，不再在这些主机上运行实例。专用主机 ID 不再可供使用。

释放专用主机

必须先停止专用主机上运行的所有实例，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。这些步骤只适用于按需专用主机。

使用 Amazon EC2 控制台释放专用主机

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

2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择要释放的专用主机。
4. 选择 Actions、Release Hosts。
5. 选择释放以确认。

使用命令行工具释放专用主机

使用以下命令之一：

- [release-hosts](#) (AWS CLI)

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

- [Remove-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

在释放专用主机后，您无法再次重新使用同一主机或主机 ID，并将不再根据按需账单费率向您收费。专用主机的状态将变为 `released`，您无法在该主机上启动任何实例。

Note

如果最近释放了专用主机，可能需要一些时间才会停止将其计入限制。在这段时间内，如果尝试分配新的专用主机，可能会出现 `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。

购买 专用主机预留

您可以使用 Amazon EC2 控制台或命令行工具购买预留。

使用 Amazon EC2 控制台购买预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 专用主机、专用主机预留 和 Purchase 专用主机预留 (购买专用主机预留)。
3. 在购买专用主机预留屏幕上，您可以使用默认设置搜索可用的产品，也可以为以下内容指定自定义值：
 - 主机实例系列 — 列出的选项对应于您的账户中尚未分配给预留的专用主机。
 - 可用区 — 您的账户中尚未分配给预留的专用主机的可用区。
 - 付款选项 — 产品的付款选项。
 - 期限 — 预留期限，可以是一年或三年。
4. 选择查找产品，并选择符合您要求的产品。
5. 选择要与预留关联的专用主机，然后选择审核。
6. 审核您的订单，然后选择 Order (订单)。

使用命令行工具购买预留

1. 使用以下命令之一列出符合您需求的可用产品。以下示例列出了支持 m4 实例系列中的实例并具有一年期限的产品。

Note

期限以秒为单位指定。一年期限包括 31536000 秒，三年期限包括 94608000 秒。

- [describe-host-reservation-offerings \(AWS CLI\)](#)

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4  
--max-duration 31536000
```

- [Get-EC2HostReservationOffering \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

这两条命令都返回符合您条件的产品的列表。记下要购买的产品的 offeringId。

2. 使用以下命令之一可购买产品并提供上一步骤中记下的 offeringId。以下示例购买指定的预留，并将其与 AWS 账户中已分配的特定专用主机关联。

- [purchase-host-reservation \(AWS CLI\)](#)

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --host-id-  
set h-013abcd2a00cbd123
```

- [New-EC2HostReservation \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -  
HostIdSet h-013abcd2a00cbd123
```

查看专用主机预留

您可以查看有关与预留关联的专用主机的信息，包括：

- 预留期限
- 付款选项
- 开始和结束日期

使用 Amazon EC2 控制台查看预留的详细信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择专用主机预留，然后从提供的列表中选择预留。
4. 有关预留的信息，请选择 Details。
5. 如需与预留关联的专用主机的信息，请选择主机。

使用命令行工具查看预留的详细信息

使用以下命令之一：

- [describe-host-reservations \(AWS CLI\)](#)

```
aws ec2 describe-host-reservations
```

- [Get-EC2HostReservation \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> Get-EC2HostReservation
```

标记 专用主机预留

可以为您的 专用主机预留 分配自定义标签以便按不同的方式将它们分类，例如按用途、拥有者或环境分类。这有助于根据分配的自定义标签快速查找特定的专用主机预留。

您仅可以使用 AWS CLI 标记 专用主机预留。

使用命令行标记 专用主机预留

使用以下命令之一：

- [create-tags \(AWS CLI \)](#)

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

- [New-EC2Tag \(适用于 Windows PowerShell 的 AWS 工具 \)](#)

New-EC2Tag 命令需要 Tag 参数来指定要用于 专用主机预留 标签的键值对。以下命令创建 Tag 参数。

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag  
PS C:\> $tag.Key = "Owner"  
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

使用共享专用主机

专用主机共享使专用主机拥有者能够与其他 AWS 账户或在 AWS 组织内共享其专用主机。这使您能够集中创建和管理专用主机，并跨多个 AWS 账户或在 AWS 组织内共享专用主机。

在此模型中，拥有专用主机的 AWS 账户（拥有者）将与其他 AWS 账户（使用者）共享它。使用者可以在与其共享的专用主机上启动实例，所用方式与他们在自己的账户中分配的专用主机上启动实例的方式相同。拥有者负责管理专用主机以及在其上启动的实例。拥有者无法修改使用者在共享的专用主机上启动的实例。使用者负责管理在与其共享的专用主机上启动的实例。使用者无法查看或修改其他使用者或专用主机拥有者所拥有的实例，也无法修改与其共享的专用主机。

专用主机拥有者可与以下对象共享专用主机：

- 其 AWS 组织内部或外部的特定 AWS 账户
- 其 AWS 组织内的组织部门
- 其整个 AWS 组织

目录

- [共享专用主机的先决条件 \(p. 349\)](#)
- [相关服务 \(p. 349\)](#)
- [跨可用区共享 \(p. 349\)](#)
- [共享专用主机 \(p. 349\)](#)
- [将已共享的专用主机取消共享 \(p. 350\)](#)
- [标识共享的专用主机 \(p. 350\)](#)

- [查看在共享专用主机上运行的实例 \(p. 350\)](#)
- [共享的专用主机权限 \(p. 351\)](#)
- [计费和计量 \(p. 351\)](#)
- [专用主机限制 \(p. 351\)](#)
- [主机恢复和专用主机共享 \(p. 351\)](#)

共享专用主机的先决条件

- 要共享专用主机，您必须在您的 AWS 账户中拥有它。您无法共享已与您共享的专用主机。
- 要与您的 AWS 组织或 AWS 组织内的组织部门共享专用主机，您必须允许与 AWS Organizations 共享。
有关更多信息，请参阅 AWS RAM 用户指南 中的[允许与 AWS Organizations 共享](#)。

相关服务

AWS Resource Access Manager

专用主机共享与 AWS Resource Access Manager (AWS RAM) 集成。AWS RAM 是一项服务，允许您与任何 AWS 账户或通过 AWS Organizations 共享 AWS 资源。利用 AWS RAM，您可通过创建资源共享 来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用者可以是单个 AWS 账户或 AWS Organizations 中的组织部门或整个组织。

有关 AWS RAM 的更多信息，请参阅 [AWS RAM 用户指南](#)。

跨可用区共享

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名称。这可能会导致账户之间的可用区命名差异。例如，您的 AWS 账户的可用区 us-east-1a 可能与另一 AWS 账户的 us-east-1a 不在同一位置。

要确定专用主机相对于账户的位置，您必须使用可用区 ID (AZ ID)。可用区 ID 是跨所有 AWS 账户的可用区的唯一且一致的标识符。例如，use1-az1 是 us-east-1 区域的可用区 ID，它在每个 AWS 账户中的位置均相同。

查看账户中的可用区的可用区 ID

1. 从 <https://console.aws.amazon.com/ram> 打开 AWS RAM 控制台。
2. 当前区域的可用区 ID 显示在屏幕右侧的 Your AZ ID (您的 AZ ID) 面板中。

共享专用主机

当所有者共享专用主机时，它允许使用者在主机上启动实例。使用者可以在共享主机上启动其可用容量允许的任意数量的实例。

如果您共享启用了自动放置的专用主机，请记住以下内容，因为它可能导致意外的专用主机使用：

- 如果使用者启动具有专用主机租赁的实例，但他们的账户中拥有的专用主机上没有容量，则会自动在共享的专用主机上启动实例。

要共享专用主机，您必须将它添加到资源共享。资源共享是一项 AWS RAM 资源，可让您跨 AWS 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。您可以将专用主机添加到现有资源，也可以将其添加到新的资源共享。

如果您是 AWS Organizations 中某组织的一部分并且已在您的组织中启用共享，组织中的使用者将自动获得对共享专用主机的访问权限。否则，使用者会收到加入资源共享的邀请，并在接受邀请后获得对共享专用主机的访问权限。

Note

共享专用主机后，使用者可能需要几分钟的时间才能访问它。

您可以使用 AWS RAM 控制台或 AWS CLI 共享您拥有的专用主机。

使用 AWS RAM 控制台共享您拥有的专用主机

请参阅 AWS RAM 用户指南 中的[创建资源共享](#)。

使用 AWS CLI 共享您拥有的专用主机

使用 [create-resource-share](#) 命令。

将已共享的专用主机取消共享

专用主机拥有者可以随时将共享的专用主机取消共享。在将共享的专用主机取消共享时，以下规则将适用：

- 与之共享专用主机的使用者不再能够在专用主机上启动新实例。
- 取消共享时在专用主机上运行的使用者所拥有的实例将继续运行，但计划[停用](#)。消费者将收到实例的停用通知，他们有两周时间对通知采取措施。但是，如果在停用通知期内与使用者重新共享专用主机，则将取消实例停用。

要取消共享您拥有的已共享专用主机，必须从资源共享中将其删除。您可以使用 AWS RAM 控制台或 AWS CLI 来执行此操作。

使用 AWS RAM 控制台取消共享您拥有的已共享专用主机

请参阅 AWS RAM 用户指南 中的[更新资源共享](#)。

使用 AWS CLI 取消共享您拥有的已共享专用主机

使用 [disassociate-resource-share](#) 命令。

标识共享的专用主机

拥有者和使用者可以使用 Amazon EC2 控制台和 AWS CLI 标识共享的专用主机。

使用 Amazon EC2 控制台标识共享的专用主机

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择专用主机。屏幕列出了您拥有的专用主机以及与您共享的专用主机。拥有者列显示专用主机拥有者的 AWS 账户 ID。

使用 AWS CLI 标识共享的专用主机

可以使用 [describe-hosts](#) 命令。该命令返回您拥有的专用主机以及与您共享的专用主机。

查看在共享专用主机上运行的实例

拥有者和使用者可以随时使用 Amazon EC2 控制台和 AWS CLI 查看在共享专用主机上运行的实例。

使用 Amazon EC2 控制台查看在共享专用主机上运行的实例

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择专用主机。
- 选择要查看其实例的专用主机，然后选择实例。该选项卡列出了在主机上运行的实例。拥有者可以查看在主机上运行的所有实例，包括使用者启动的实例。使用者只能查看他们在主机上启动的正在运行的实例。拥有者列显示启动实例的账户的 AWS 账户 ID。

使用 AWS CLI 查看在共享专用主机上运行的实例

可以使用 [describe-hosts](#) 命令。该命令返回在每个专用主机上运行的实例。拥有者可以查看在主机上运行的所有实例。使用者只能查看他们在共享主机上启动的正在运行的实例。`InstanceOwnerId` 显示实例拥有者的 AWS 账户 ID。

共享的专用主机权限

拥有者的权限

拥有者负责管理其共享的专用主机以及在专用主机上启动的实例。拥有者可以查看在共享专用主机上运行的所有实例，包括使用者启动的实例。但是，拥有者不能对使用者启动的正在运行的实例采取任何操作。

使用者的权限

使用者负责管理他们在共享的专用主机上启动的实例。使用者不能以任何方式修改共享的专用主机，也不能查看或修改由其他使用者或专用主机拥有者启动的实例。

计费和计量

共享专用主机不会产生额外的费用。

拥有者需要为他们共享的专用主机付费。使用者不需要为他们在共享的专用主机上启动的实例付费。

专用主机预留继续为共享的专用主机提供账单折扣。只有专用主机拥有者可以为他们拥有的共享专用主机购买专用主机预留。

专用主机限制

共享的专用主机仅计入拥有者的专用主机限制。使用者的专用主机限制不受已与他们共享的专用主机的影响。同样，使用者在共享的专用主机上启动的实例不计入其实例限制。

主机恢复和专用主机共享

主机恢复可恢复由专用主机拥有者以及与之共享专用主机的使用者启动的实例。将替换专用主机分配给拥有者的账户。它会添加到与原始专用主机相同的资源共享，并与相同的使用者共享。

有关更多信息，请参阅 [主机恢复 \(p. 351\)](#)。

主机恢复

如果在专用主机上检测到故障，主机恢复自动在新的替换主机上重新启动实例。主机恢复减少了人工干预的需求，并降低了发生意外专用主机故障时的运营负担。

此外，如果进行主机恢复，与 AWS License Manager 的内置集成自动跟踪和管理您的许可证。

Note

仅在提供了 AWS License Manager 的区域中支持 AWS License Manager 集成。

目录

- [主机恢复基础知识 \(p. 352\)](#)
- [配置主机恢复 \(p. 352\)](#)
- [主机恢复状态 \(p. 354\)](#)
- [支持的实例配置 \(p. 354\)](#)
- [手动恢复不支持的实例 \(p. 354\)](#)
- [相关服务 \(p. 354\)](#)
- [定价 \(p. 355\)](#)

主机恢复基础知识

主机恢复使用主机级运行状况检查以评估专用主机可用性，以及检测基本系统故障。可能导致主机级运行状况检查失败的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的硬件或软件问题

在专用主机上检测到系统故障时，将启动主机恢复，并且 Amazon EC2 自动分配替换专用主机。替换专用主机收到新的主机 ID，但保留与原始专用主机相同的属性，包括：

- 可用区
- 实例类型
- 标签
- 自动置放设置

在分配替换专用主机后，实例将恢复到替换专用主机上。恢复的实例保留与原始实例相同的属性，包括：

- 实例 ID
- 私有 IP 地址
- 弹性 IP 地址
- EBS 卷附加
- 所有实例元数据

如果实例与受损专用主机之间具有主机关联关系，恢复的实例将与替换专用主机建立主机关联。

在所有实例已恢复到替换专用主机时，将释放受损专用主机并且替换专用主机变为可用。

在启动了主机恢复时，将通过电子邮件和 AWS Personal Health Dashboard 事件通知 AWS 账户所有者。在成功完成主机恢复后，将发送第二个通知。

停止的实例不会恢复到替换专用主机上。如果您尝试启动将受损专用主机作为目标的停止实例，实例启动将失败。我们建议您修改停止的实例以将不同的专用主机作为目标，或者在任何可用的专用主机上启动并启用匹配的配置和自动置放。

具有实例存储的实例不会恢复到替换专用主机上。作为一项纠正措施，将受损专用主机标记为停用，并且您在主机恢复完成后收到停用通知。在指定的时间段内，按照停用通知中所述的纠正步骤手动恢复受损专用主机上的其余实例。

如果使用 AWS License Manager 跟踪您的许可证，AWS License Manager 根据许可证配置限制为替换专用主机分配新的许可证。如果由于主机恢复而违反许可证配置的硬限制，则不允许执行恢复过程，并通过 Amazon SNS 通知向您通知主机恢复失败。如果由于主机恢复而违反许可证配置的软限制，则允许继续执行恢复，并通过 Amazon SNS 通知向您通知违反了限制。有关更多信息，请参阅 AWS License Manager 用户指南 中的[使用许可证配置](#)。

配置主机恢复

您可以在分配专用主机时配置主机恢复，也可以在分配后使用 Amazon EC2 控制台或 AWS Command Line Interface (CLI) 配置主机恢复。

目录

- [启用主机恢复 \(p. 353\)](#)
- [禁用主机恢复 \(p. 353\)](#)

- [查看主机恢复配置 \(p. 353\)](#)

启用主机恢复

您可以在分配专用主机时或分配后启用主机恢复。

有关在分配专用主机时启用主机恢复的更多信息，请参阅[分配专用主机 \(p. 337\)](#)。

在分配后启用主机恢复 (控制台)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 选择要启用主机恢复的专用主机，选择操作，然后选择修改主机恢复。
4. 对于主机恢复，请选择启用，然后选择保存。

在分配后启用主机恢复 (AWS CLI)

可以使用 `modify-hosts` 命令并指定 `host-recovery` 参数。

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

禁用主机恢复

您可以在分配专用主机后随时禁用主机恢复。

在分配后禁用主机恢复 (控制台)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 选择要禁用主机恢复的专用主机，选择操作，然后选择修改主机恢复。
4. 对于主机恢复，请选择禁用，然后选择保存。

在分配后禁用主机恢复 (AWS CLI)

可以使用 `modify-hosts` 命令并指定 `host-recovery` 参数。

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

查看主机恢复配置

您可以随时查看专用主机的主机恢复配置。

查看专用主机的主机恢复配置 (控制台)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择专用主机。
3. 选择专用主机，然后在描述选项卡中查看主机恢复字段。

查看专用主机的主机恢复配置 (AWS CLI)

可以使用 `describe-hosts` 命令。

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

HostRecovery 响应元素指示是启用还是禁用主机恢复。

主机恢复状态

在检测到专用主机故障时，受损专用主机将进入 `under-assessment` 状态，并且所有实例进入 `impaired` 状态。在处于 `under-assessment` 状态时，您无法在受损的专用主机上启动实例。

在分配替换专用主机后，它进入 `pending` 状态。它保持该状态，直到主机恢复过程完成。在处于 `pending` 状态时，您无法在替换专用主机上启动实例。在恢复过程中，在替换专用主机上恢复的实例保持 `impaired` 状态。

在主机恢复完成后，替换专用主机进入 `available` 状态，并且恢复的实例恢复为 `running` 状态。在进入 `available` 状态后，您可以在替换专用主机上启动实例。将永久释放原始受损专用主机，并且它进入 `released-permanent-failure` 状态。

如果受损专用主机具有不支持主机恢复的实例（例如，具有实例存储支持的卷的实例），则不会释放专用主机。相反，它标记为停用并进入 `permanent-failure` 状态。

支持的实例配置

只有具有支持配置的实例才支持主机恢复。要恢复不支持的实例，请参阅[手动恢复不支持的实例 \(p. 354\)](#)。

不支持以下实例配置：

- 实例存储卷
 - C5d、G4、I3en、M5ad、M5d、M5dn、P3dn、R5ad、R5d、R5dn 和 z1d 实例
 - D2、F1、HS1、I2、I3、X1 和 X1e 实例

手动恢复不支持的实例

主机恢复不支持恢复使用实例存储卷的实例。请按照以下说明手动恢复无法自动恢复的任何实例。

Warning

在停止或终止实例时，实例存储卷上的数据将会丢失。这包括附加到使用 EBS 卷作为根设备的实例的实例存储卷。要保留实例存储卷中的数据，请在停止或终止实例之前将其备份到持久性存储中。

手动恢复 EBS 支持的实例

对于无法自动恢复的 EBS 支持的实例，我们建议您手动停止并启动实例以将其恢复到新的专用主机上。有关停止实例以及在停止实例后对实例配置进行的更改的更多信息，请参阅[停止和启动您的实例 \(p. 445\)](#)。

手动恢复实例存储支持的实例

有关无法自动恢复的实例存储支持的实例，我们建议您执行以下操作：

1. 在新的专用主机上从最新的 AMI 中启动替换实例。
2. 将所需的所有数据迁移到替换实例中。
3. 终止受损专用主机上的原始实例。

相关服务

专用主机与以下 AWS 服务集成在一起：

- AWS License Manager — 在 Amazon EC2 专用主机之间跟踪许可证（仅在提供了 AWS License Manager 的区域中支持）。有关更多信息，请参阅[AWS License Manager 用户指南](#)。

定价

使用主机恢复不会收取额外的费用，但会收取正常的专用主机费用。有关更多信息，请参阅 [Amazon EC2 专用主机定价](#)。

一旦启动了主机恢复，将不再对受损专用主机计费。仅在进入 `available` 状态后，才会开始对替换专用主机计费。

如果使用按需费率对受损专用主机进行计费，还会使用按需费率对替换专用主机进行计费。如果受损专用主机具有有效专用主机预留，则会将其转移到替换专用主机。

跟踪配置更改

您可以使用 AWS Config 记录专用主机的配置更改，以及记录在主机上启动、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，并通过关系将这些信息配对。具有三种报告条件：

- AWS Config 记录状态 — 当其状态为开启时，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 — 当其状态为启用时，将记录专用主机的配置信息。
- 实例记录状态 — 当其状态为启用时，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。对于其中的任何实例，您还可以查找其 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 (按插槽或按内核授予许可) 的许可。

您可以使用以下任一方式查看配置历史记录：

- 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，请选择专用主机页面的配置时间线列中的灰色图标。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 中获取所有专用主机的列表，请运行 CLI 命令，如下所示。

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

要从 AWS Config 中获取专用主机的配置历史记录，请运行 CLI 命令，如下所示。

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --  
resource-id i-1234567890abcdef0
```

使用控制台管理 AWS Config 设置

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在专用主机页面上，选择编辑配置记录。
3. 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[查看配置详细信息 \(AWS CLI\)](#)。
- 要使用 Amazon EC2 API，请参阅[GetResourceConfigHistory](#)。

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。属于不同 AWS 账户的专用实例在硬件层面上物理隔离。此外，属于链接到单个付款人账户的 AWS 账户的专用实例也在硬件层面上物理隔离。不过，专用实例可与来自同一 AWS 账户但非专用实例的其他实例共享硬件。

Note

专用主机也是一种专供您使用的物理服务器。使用 专用主机，您可以查看和控制在服务器上放置实例的方式。有关更多信息，请参阅[专用主机 \(p. 333\)](#)。

专用实例基础知识

您在 VPC 内启动的每项实例都有一个租赁属性。此属性有以下值。

租赁值	描述
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。

在启动实例后，要想更改其租赁属性，有一定限制。

- 在启动实例后，不能将其租赁属性从 default 改为 dedicated 或 host。
- 在启动实例后，不能将其租赁属性从 dedicated 或 host 改为 default。

在启动实例后，可以将其租赁属性从 dedicated 改为 host，或从 host 改为 dedicated。有关更多信息，请参阅[更改实例的租期 \(p. 360\)](#)。

每个 VPC 都有相关的实例租期属性。此属性有以下值。

租赁值	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，除非您在实例启动时显式指定为 host 租赁。在实例启动期间，您无法指定 default 租户。

在创建 VPC 之后，可以将其租赁属性从 dedicated 改为 default。不能将 VPC 的实例租赁改为 dedicated。

要创建专用实例，可以执行以下操作：

- 创建实例租赁设置为 dedicated 的 VPC (在该 VPC 内启动的所有实例均为专用实例)。
- 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

当启动 Amazon EBS 支持的专用实例时，EBS 卷不会在单一租户硬件上运行。

使用专用租赁的预留实例

要确保足够的容量来启动专用实例，可以购买专用预留实例。有关更多信息，请参阅 [预留实例 \(p. 243\)](#)。

如果购买专用 Reserved Instance，可以按相当优惠的使用价同时购买到在 VPC 中启动专用实例的容量；而这种优惠的使用价只有在您启动专用租赁实例时才适用。当您购买具有默认租期的 Reserved Instance 时，它仅适用于具有 default 租期的运行实例；它不适用于具有 dedicated 租期的运行实例。

您在购买 Reserved Instance 之后将无法使用修改过程来更改其租赁。但是，您可以将可转换预留实例换成具有不同租赁的新可转换预留实例。

专用实例的自动扩展

您可以使用 Amazon EC2 Auto Scaling 启动专用实例。有关更多信息，请参阅 [Amazon EC2 Auto Scaling 用户指南 中的在 VPC 中启动 Auto Scaling 实例](#)。

专用实例 的自动恢复

如果 专用实例 因需要 AWS 参与才能修复的基础硬件故障或问题而受损，您可以为它配置自动恢复。有关更多信息，请参阅 [恢复您的实例 \(p. 463\)](#)。

专用 Spot 实例

创建 Spot 实例请求时，您可以通过指定租赁 dedicated 来运行专用 Spot 实例。有关更多信息，请参阅 [指定 Spot 实例的租期 \(p. 290\)](#)。

专用实例定价

专用实例的定价不同于按需实例的定价。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 `dedicated` 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 \(p. 358\)](#)
- [在 VPC 中启动专用实例 \(p. 358\)](#)
- [显示租期信息 \(p. 359\)](#)
- [更改实例的租期 \(p. 360\)](#)
- [更改 VPC 的租赁 \(p. 360\)](#)

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。如果使用 Amazon VPC 控制台，可以使用 VPC 向导或您的 VPC 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。

使用命令行在创建 VPC 时设置租赁选项

- `create-vpc` (AWS CLI)
- `New-EC2Vpc` (适用于 Windows PowerShell 的 AWS 工具)

如果在实例租赁已设置为 `dedicated` 的 VPC 中启动实例，则无论实例的租赁如何，实例都将自动为专用实例。

在 VPC 中启动专用实例

可以使用 Amazon EC2 启动实例向导来启动专用实例。

使用控制台在默认租赁 VPC 中启动专用实例

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

确保选择作为专用实例受支持的实例类型。有关更多信息，请参阅 [Amazon EC2 专用实例](#)。

5. 在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。检查完核查实例启动页面上的选项后，选择启动以选择一个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 \(p. 338\)](#)。

使用命令行在启动过程中设置实例的租赁选项

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

显示租期信息

使用控制台显示您的 VPC 的租赁信息

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。

使用控制台显示您的实例的租赁信息

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. 如果未显示 Tenancy (租期) 栏，您可以执行以下操作：
 - 在 Show/Hide Columns 对话框中选择 Show/Hide Columns (齿轮形状的图标)、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。

使用命令行描述您的 VPC 的租赁

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行描述您的实例的租赁

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

使用命令行描述Reserved Instance的租赁值

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行描述Reserved Instance产品的租赁值

- [describe-reserved-instances-offerings \(AWS CLI\)](#)
- [Get-EC2ReservedInstancesOffering \(适用于 Windows PowerShell 的 AWS 工具\)](#)

更改实例的租期

根据您的实例类型和平台，您可以在启动一个已停止的专用实例之后将其租赁更改为 host。下次该实例启动时，会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以及可以在专用主机上使用的实例类型的更多信息，请参阅[使用专用主机 \(p. 336\)](#)。同样，您也可以在启动一个已停止的专用主机实例后将其租赁更改为 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。

使用控制台更改实例的租赁

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、Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 在租赁列表中，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。

使用命令行修改实例的租赁值

- [modify-instance-placement \(AWS CLI\)](#)
- [Edit-EC2InstancePlacement \(适用于 Windows PowerShell 的 AWS 工具\)](#)

更改 VPC 的租赁

可以将 VPC 的实例租赁属性从 dedicated 改为 default。修改 VPC 的实例租赁不会影响 VPC 中任何现有实例的租赁。下次在 VPC 中启动一个实例时，该实例将具有 default 租赁，除非您在启动过程中另有指定。

不能将 VPC 的实例租赁属性更改为 dedicated。

可以使用 AWS CLI、AWS 开发工具包或仅使用 Amazon EC2 API 修改 VPC 的实例租赁属性。

使用 AWS CLI 修改 VPC 的实例租赁属性

- 使用 [modify-vpc-tenancy](#) 命令指定 VPC 的 ID 和实例租赁值。default 是唯一受支持的值。

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

按需容量预留

通过使用按需容量预留，您可以在特定可用区中为 Amazon EC2 实例预留容量达任意持续时间。这使您能够独立于 Savings Plans 或区域预留实例提供的账单折扣来创建和管理容量预留。通过创建容量预留，可以确保您始终能够在需要时访问 EC2 容量。您随时可以创建容量预留，而无需作出一年或三年期限承诺，并且可以立即使用该容量。当您不再需要预留时，可以取消容量预留以停止产生费用。

在创建容量预留时，您将指定：

- 在其中预留容量的可用区
- 为其预留容量的实例的数量
- 实例属性，包括实例类型、租期和平台/操作系统

容量预留只能由匹配其属性的实例使用。默认情况下，这些容量由与属性匹配的运行中实例使用。如果您没有任何正在运行的实例与容量预留的容量匹配，则这些容量将保持未使用的状态，直至启动具有匹配属性的实例。

此外，您可以将 Savings Plans 和区域预留实例与您的容量预留配合使用，以享受账单折扣。当容量预留的属性与 Savings Plans 或区域 Reserved Instance 的属性匹配时，AWS 会自动应用您的折扣。有关更多信息，请参阅[账单折扣 \(p. 362\)](#)。

目录

- 容量预留、预留实例和 Savings Plans 之间的区别 (p. 361)
- 容量预留限制 (p. 361)
- 容量预留定价 (p. 362)
- 容量预留定价和计费 (p. 362)
- 使用容量预留 (p. 363)
- 使用共享容量预留 (p. 367)

容量预留、预留实例和 Savings Plans 之间的区别

下表重点介绍了容量预留、预留实例和 Savings Plans 之间的主要区别：

	容量预留	可用区 预留实例	区域性 预留实例	Savings Plans
期限	没有承诺用量。可以根据需要创建和取消。	需要固定的一年或三年使用承诺		
容量优势	在特定可用区中预留容量。		不在某个可用区中预留容量。	
账单折扣	无账单折扣。在容量预留中启动的实例按照其标准按需费率收费。不过，您可以将 Savings Plans 或区域预留实例与容量预留结合使用，以享受账单折扣。区域预留实例不适用于容量预留。	提供账单折扣		
实例限制	限制为您的每区域个按需实例限额。	限制为每可用区 20 个。可以请求提高限制。	限制为每区域 20 个。可以请求提高限制。	无限制。

有关更多信息，请参阅下列内容：

- [预留实例 \(p. 243\)](#)
- [AWS Savings Plans 用户指南](#)

容量预留限制

允许您预留容量的实例数基于您账户的个按需实例限制。您可以在限制允许的数量减去已经运行的实例数量范围内，为任意数量的实例预留容量。

容量预留限制

在创建容量预留之前，请注意以下限制。

- 活动和未使用的容量预留会计入您的个按需实例限制中
- 容量预留无法从一个 AWS 账户转移到另一个账户
- 区域Reserved Instance账单折扣不适用于容量预留
- 无法在置放群组中创建容量预留
- 容量预留不能与专用主机一起使用
- 容量预留不能用于自带许可 (BYOL)

容量预留定价和计费

容量预留的价格因付款选项而异。

定价

当容量预留 处于活动状态时，不论您是否运行实例，您均需要支付等同的按需费用。如果您没有使用预留，这将在您的 EC2 账单中显示为未使用的预留。如果您运行的实例属性与预留匹配，则您只需要为该实例付费，不需要为预留付费。没有任何预付费用或额外收费。

例如，如果您为 20 个 m4.large Linux 实例创建容量预留并在同一个可用区中运行 15 个 m4.large Linux 实例，则会向您收取 15 个活动的实例和预留中 5 个未使用的实例的费用。

Savings Plans 和区域预留实例的账单折扣适用于容量预留。有关更多信息，请参阅[账单折扣 \(p. 362\)](#)。

有关 Amazon EC2 定价的更多信息，请参阅 [Amazon EC2 定价](#)。

计费

容量预留以秒为单位计费。这意味着会向您收取不足一小时的费用。例如，如果您账户中的预留保持活动状态 24 小时 15 分钟，则会向您收取 24.25 个预留小时的费用。

下面的示例说明如何对容量预留计费。为一个 m4.large Linux 实例创建了容量预留，其按需费率为每使用一小时 0.10 美元。在此实例中，账户内的容量预留活动了五个小时。第一个小时未使用容量预留，因此按照 m4.large 实例类型的标准按需费率计入一小时未使用费用。从第二个小时到第五个小时，m4.large 实例占用了容量预留。在这段时间内，容量预留不会产生任何费用，改为向账户收取占用这部分容量的 m4.large 实例的费用。在第六个小时取消了容量预留，并在预留容量之外正常运行 m4.large 实例。对于一个小时，将以 m4.large 实例类型的按需费率进行收费。

Hour	1	2	3	4	5	
Unused Capacity Reservation	\$0.10	\$0.00	\$0.00	\$0.00	\$0.00	\$
On-demand Instance Usage	\$0.00	\$0.10	\$0.10	\$0.10	\$0.10	\$
Hourly cost	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$

账单折扣

Savings Plans 和区域预留实例的账单折扣适用于容量预留。AWS 自动将这些折扣应用于具有匹配属性的容量预留。当容量预留由某个实例使用时，折扣将适用于该实例。折扣将优先适用于已产生的实例使用量，然后再用于未使用的容量预留。

区域预留实例的账单折扣不适用于容量预留。

有关更多信息，请参阅下列内容：

- [预留实例 \(p. 243\)](#)
- [AWS Savings Plans 用户指南](#)

查看您的账单

您可以在 AWS Billing and Cost Management 控制台上查看您账户的费用情况。

- 控制面板显示了您的账户的花费汇总。
- 在 Bills (账单) 页面上的 Details (详细信息) 下，展开 Elastic Compute Cloud 部分及区域，以获取有关您的容量预留的账单信息。

您可以在线查看费用，也可以下载 CSV 文件。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的 [容量预留行项目](#)。

使用容量预留

要开始使用容量预留，您可以在所需的可用区中创建容量预留。然后，您可以在预留容量中启动实例，实时查看其容量使用情况，以及根据需要增加或减少其容量。

默认情况下，容量预留自动将新实例与具有匹配属性（实例类型、平台和可用区）的运行中实例进行匹配。这意味着，任何具有匹配属性的实例都将自动在容量预留中运行。不过，您还可以将容量预留定位到特定工作负载。这使您可以明确控制允许哪些实例在预留容量中运行。

您可以指定预留如何结束。您可以选择手动取消容量预留或者在指定时间自动结束它。如果您指定结束时间，则容量预留在指定时间的一小时之内取消。例如，如果您指定“5/31/2019, 13:30:55”，则容量预留可确保在 2019 年 5 月 31 日的 13:30:55 到 14:30:55 之间结束。预留结束后，您无法再将实例定位到容量预留中。在预留容量中运行的实例继续运行，不会中断。如果定位到容量预留中的实例停止，在您删除其容量预留定位首选项或者将其配置为定位到其他容量预留之前，无法重新启动这些实例。

目录

- [创建容量预留 \(p. 363\)](#)
- [在现有容量预留中启动实例 \(p. 364\)](#)
- [修改容量预留 \(p. 365\)](#)
- [修改实例的容量预留设置 \(p. 365\)](#)
- [查看容量预留 \(p. 366\)](#)
- [取消容量预留 \(p. 366\)](#)

创建容量预留

创建容量预留之后，容量立即可用。只要容量预留活动，该容量就为您预留，您可以随时在其中启动实例。如果容量预留处于开放状态，具有匹配属性的新实例和现有实例自动使用容量预留的容量运行。如果容量预留处于 targeted 状态，只有专门定位到其中的实例才能在预留容量中运行。

如果出现以下情况之一，创建容量预留的请求会失败：

- Amazon EC2 没有足够的容量来满足请求。请稍后重试、尝试不同的可用区或者尝试较小的容量。如果您的应用程序灵活地跨实例类型和大小，请尝试不同的实例属性。
- 请求的数量超过选定实例系列的个按需实例限制。增加该实例系列的个按需实例限制，然后重试。有关更多信息，请参阅 [个按需实例限制 \(p. 241\)](#)。

使用控制台创建容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 容量预留 (容量预留) , 然后选择 Create 容量预留 (创建容量预留)。
3. 在“Create a 容量预留 (创建容量预留)”页面上的实例详细信息部分中，配置以下设置。您启动的实例的实例类型、平台和可用区必须与您在此处指定的实例类型、平台和可用区匹配，否则将不会应用容量预留。例如，如果开放的容量预留不匹配，则明确针对此容量预留的实例启动将失败。
 - a. 实例类型 — 在预留容量中启动的实例类型。
 - b. 启动 EBS 优化的实例 — 指定是否为 EBS 优化的实例预留容量。一些实例类型默认情况下会选中此选项。有关 EBS 优化实例的更多信息，请参阅 [Amazon Elastic Block Store \(p. 782\)](#)。
 - c. 启动时附加实例存储 — 指定在容量预留中启动的实例是否使用临时块级别存储。实例存储卷上的数据仅在相关实例的生命周期内保留。
 - d. 平台 — 实例的操作系统。
 - e. 可用区 — 在其中预留容量的可用区。
 - f. 租赁 — 指定要在共享硬件 (默认) 还是专用实例上运行。
 - g. Quantity (数量) – 为其预留容量的实例的数量。如果指定的数量超过了选定实例类型的剩余个按需实例限制，将拒绝该请求。
4. 在预留详细信息部分中配置以下设置：
 - a. 预留结束 — 选择以下选项之一：
 - 手动 — 容量将预留，直至您明确取消。
 - Specific time (特定时间) – 在指定的日期和时间自动取消容量预留。
 - b. 实例资格 — 选择以下选项之一：
 - 开放 (默认值) – 容量预留匹配任意具有匹配属性 (实例类型、平台和可用区) 的实例。如果您启动具有匹配属性的实例，则会自动将其放置到预留容量中。
 - targeted (定位) – 容量预留仅接受具有匹配属性 (实例类型、平台和可用区) 并明确针对预留的实例。
5. 选择请求预留。

使用 AWS CLI 创建容量预留

使用 `create-capacity-reservation` 命令：

```
aws ec2 create-capacity-reservation --instance-type instance_type --instance-platform platform_type --availability-zone az --instance-count quantity
```

在现有容量预留中启动实例

您可在任意具有匹配属性 (实例类型、平台和可用区) 和充足容量的现有容量预留中启动实例。在容量预留中启动实例会将其可用容量减去所启动实例的数量。例如，如果您启动 3 个实例，容量预留的可用容量将减去 3。

使用控制台在现有容量预留中启动实例

1. 通过从控制面板或实例选择启动实例来打开启动实例向导。
2. 选择 Amazon 系统映像 (AMI) 和实例类型。
3. 完成配置实例详细信息页面。对于容量预留，请选择下列选项之一：
 - 开放 — 在具有匹配属性以及对于所选实例数具有足够容量的任意容量预留中启动实例。如果没有匹配的容量预留具有足够容量，实例使用按需容量。

- <容量预留> – 在此特定容量预留中启动实例。如果此容量预留没有足够的容量用于所选实例数量，则实例启动失败。
 - 无 — 阻止实例在容量预留中启动。
4. 完成剩余步骤以启动实例。

使用 AWS CLI 在现有容量预留中启动实例

使用 `run-instances` 命令并指定 `--capacity-reservation-specification` 参数。

以下示例在任意具有匹配属性和可用容量的开放容量预留中启动 `t2.micro` 实例。

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --  
key-name MyKeyPair --availability-zone us-east-1b --capacity-reservation-specification  
CapacityReservationPreference=open
```

以下示例在 `targeted` 容量预留中启动 `t2.micro` 实例：

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --  
key-name MyKeyPair --availability-zone us-east-1b --capacity-reservation-specification  
CapacityReservationTarget=[{CapacityReservationId=cr-a1234567}]
```

修改容量预留

在创建之后，您可以更改活动容量预留的属性。在某个容量预留过期后，或者您明确取消后，您无法对其进行修改。

修改容量预留时，您只能增加或减少数量以及更改释放容量的方式。无法更改容量预留的实例类型、EBS 优化、实例存储设置、平台、可用区或实例资格。如果您需要修改任意这些属性，我们建议您取消预留，然后使用所需属性创建新的预留。

如果指定的新数量超过了选定实例类型的剩余个按需实例限制，更新将失败。

使用控制台修改容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择容量预留，选择要修改的容量预留，然后选择编辑。
3. 根据需要修改数量或预留结束选项，然后选择保存更改。

使用 AWS CLI 修改 容量预留

使用 `modify-capacity-reservations` 命令：

```
aws ec2 modify-capacity-reservation --capacity-reservation-id reservation_id --instance-  
count quantity --end-date-type limited/unlimited --end-date expiration_date
```

修改实例的容量预留设置

您随时可以为已停止实例修改以下容量预留设置：

- 在具有匹配属性（实例类型、平台和可用区）以及可用容量的任意容量预留上启动。
- 在特定容量预留中启动实例。
- 阻止实例在容量预留中启动。

使用控制台修改实例的容量预留设置

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择实例并选择要修改的实例。停止实例（如果尚未停止）。
3. 依次选择操作和修改容量预留设置。
4. 对于容量预留，请选择下列选项之一：
 - 放开 — 在任意具有匹配属性（实例类型、平台和可用区）以及可用容量的开放容量预留上启动实例。如果没有匹配的容量预留具有可用容量，实例使用按需容量。
 - <容量预留> – 在特定容量预留中运行实例。如果实例属性（实例类型、平台和可用区）与容量预留的属性不匹配，或者如果所选容量预留没有足够的容量，则实例启动失败。
 - 无 — 阻止实例在容量预留中运行。

使用 AWS CLI 修改实例的容量预留设置

使用 `modify-instance-capacity-reservation-attributes` 命令：

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id instance_id --  
capacity-reservation-specification 'CapacityReservationPreference=none|open'
```

查看容量预留

容量预留可能具有以下几种状态：

- `active` — 容量可供使用。
- `expired` — 容量预留已在您预留请求中指定的日期和时间自动失效。预留容量不再可供您使用。
- `cancelled` — 已手动取消容量预留。预留容量不再可供您使用。
- `pending` — 容量预留请求已成功，但容量预配置仍待处理。
- `failed` — 容量预留请求失败。请求可能由于无效的请求参数、容量限制或实例限制等约束条件失败。您可以查看 60 分钟内的失败请求。

使用控制台查看容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择容量预留并选择要查看的容量预留。
3. 选择查看此预留已启动的实例。

使用 AWS CLI 查看容量预留

使用 `describe-capacity-reservations` 命令：

```
aws ec2 describe-capacity-reservations
```

取消容量预留

如果不在需要预留容量，您可以随时取消容量预留。取消容量预留之后，该容量将立即释放，不再保留供您使用。

您可以取消空容量预留以及具有正在运行的实例的容量预留。如果您取消具有正在运行的实例的容量预留，这些实例将继续在容量预留之外正常运行并应用标准个按需实例费率；或者，如果您有匹配的 Savings Plan 或区域 Reserved Instance，则应用折扣费率。

取消容量预留之后，定位到其中的实例无法再启动。修改这些实例，使其定位到不同容量预留、启动到任意处于“开放”状态且具有匹配属性和充足容量的容量预留，或者避免将其启动到容量预留中。有关更多信息，请参阅[修改实例的容量预留设置 \(p. 365\)](#)。

使用控制台取消容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择容量预留，然后选择要取消的容量预留。
3. 依次选择取消预留、取消预留。

使用 AWS CLI 取消容量预留

使用 `cancel-capacity-reservation` 命令：

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id reservation_id
```

使用共享容量预留

容量预留共享使容量预留拥有者能够与其他 AWS 账户或在 AWS 组织内共享其预留容量。这使您能够集中创建和管理容量预留，并跨多个 AWS 账户或在 AWS 组织内共享预留容量。

在此模型中，拥有容量预留的 AWS 账户（拥有者）将与其他 AWS 账户（使用者）共享它。使用者可以在与其共享的容量预留中启动实例，所用方式与他们在自己的账户中拥有的容量预留中启动实例的方式相同。容量预留拥有者负责管理容量预留以及它们启动到其中的实例。拥有者无法修改使用者启动到已共享的容量预留中的实例。使用者负责管理启动到与其共享的容量预留中的实例。使用者无法查看或修改由其他使用者或容量预留拥有者拥有的实例。

容量预留拥有者可与以下对象共享容量预留：

- 其 AWS 组织内部或外部的特定 AWS 账户
- 其 AWS 组织内的组织部门
- 其整个 AWS 组织

目录

- [共享容量预留的先决条件 \(p. 367\)](#)
- [相关服务 \(p. 368\)](#)
- [跨可用区共享 \(p. 368\)](#)
- [共享容量预留 \(p. 368\)](#)
- [将已共享的容量预留取消共享 \(p. 369\)](#)
- [标识共享的容量预留 \(p. 369\)](#)
- [查看共享的容量预留的使用情况 \(p. 370\)](#)
- [共享的容量预留权限 \(p. 370\)](#)
- [计费和计量 \(p. 370\)](#)
- [实例限制 \(p. 370\)](#)

共享容量预留的先决条件

- 要共享容量预留，您必须在您的 AWS 账户拥有它。无法共享已与您共享的容量预留。
- 您只能为共享租赁实例共享容量预留。您无法为专用租赁实例共享容量预留。

- 容量预留共享不适用于新的 AWS 账户或具有有限账单历史记录的 AWS 账户。链接到合格主（付款人）账户或通过 AWS 组织链接的新账户不受此限制的约束。
- 要与您的 AWS 组织或 AWS 组织内的组织部门共享容量预留，您必须允许与 AWS Organizations 共享。有关更多信息，请参阅 AWS RAM 用户指南中的[允许与 AWS Organizations 共享](#)。

相关服务

容量预留共享与 AWS Resource Access Manager (AWS RAM) 集成。AWS RAM 是一项服务，允许您与任何 AWS 账户或通过 AWS Organizations 共享 AWS 资源。利用 AWS RAM，您可通过创建资源共享来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用者可以是单个 AWS 账户或 AWS Organizations 中的组织部门或整个组织。

有关 AWS RAM 的更多信息，请参阅 [AWS RAM 用户指南](#)。

跨可用区共享

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名称。这可能会导致账户之间的可用区命名差异。例如，您的 AWS 账户的可用区 us-east-1a 可能与另一 AWS 账户的 us-east-1a 不在同一位置。

要确定容量预留相对于账户的位置，您必须使用可用区 ID (AZ ID)。AZ ID 是跨所有 AWS 账户的可用区的唯一且一致的标识符。例如，use1-az1 是 us-east-1 区域的 AZ ID，它在每个 AWS 账户中的位置均相同。

查看账户中的可用区的 AZ ID

1. 从 <https://console.aws.amazon.com/ram> 打开 AWS RAM 控制台。
2. 当前区域的 AZ ID 显示在屏幕右侧的 Your AZ ID (您的 AZ ID) 面板中。

共享容量预留

在与其他 AWS 账户共享您拥有的容量预留时，您必须启用它们以便将实例启动到预留容量中。如果您共享开放容量预留，请记住以下内容，因为它可能导致意外的容量预留使用：

- 如果使用者拥有与容量预留的属性匹配的运行中实例、已将 CapacityReservationPreference 参数设置为 open 且尚未在预留容量中运行，他们将自动使用共享容量预留。
- 如果使用者启动具有匹配属性（实例类型、平台和可用区）的实例，并且已将 CapacityReservationPreference 参数设置为 open，它们将自动启动到共享容量预留中。

要共享容量预留，您必须将它添加到资源共享。资源共享是一项 AWS RAM 资源，可让您跨 AWS 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。在使用 Amazon EC2 控制台共享容量预留时，必须将它添加到现有资源共享。要将容量预留添加到新的资源共享，您必须使用 [AWS RAM 控制台](#) 创建资源共享。

如果您是 AWS Organizations 中某组织的一部分并且已在您的组织中启用共享，组织中的使用者将自动获得对共享容量预留的访问权限。否则，使用者会收到加入资源共享的邀请，并在接受邀请后获得对共享容量预留的访问权限。

您可以使用 Amazon EC2 控制台、AWS RAM 控制台或 AWS CLI 共享您拥有的容量预留。

使用 Amazon EC2 控制台共享您拥有的容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择容量预留。

3. 选择要共享的容量预留，然后选择操作、共享预留。
4. 选择要将容量预留添加到的资源共享，然后选择共享容量预留。

使用者可能需要几分钟的时间才能访问共享容量预留。

使用 AWS RAM 控制台共享您拥有的容量预留

请参阅 AWS RAM 用户指南 中的[创建资源共享](#)。

使用 AWS CLI 共享您拥有的容量预留

使用 `create-resource-share` 命令。

将已共享的容量预留取消共享

容量预留拥有者可以随时将共享的容量预留取消共享。在将共享的容量预留取消共享时，以下规则将适用：

- 在取消共享时在共享容量中运行的使用者所拥有的实例继续在预留容量之外正常运行，并且根据 Amazon EC2 容量可用性将容量还原到容量预留。
- 与之共享容量预留的使用者不再能够在预留容量中启动新实例。

要取消共享您拥有的已共享容量预留，则必须从资源共享中将其删除。您可以使用 Amazon EC2 控制台、AWS RAM 控制台或 AWS CLI 完成此操作。

使用 Amazon EC2 控制台取消共享您拥有的已共享容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择容量预留。
3. 选择要取消共享的容量预留，然后选择共享选项卡。
4. 共享选项卡列出了已将容量预留添加到的资源共享。选择要从中删除容量预留的资源共享，然后选择从资源共享中删除。

使用 AWS RAM 控制台取消共享您拥有的已共享容量预留

请参阅 AWS RAM 用户指南 中的[更新资源共享](#)。

使用 AWS CLI 取消共享您拥有的已共享容量预留

使用 `disassociate-resource-share` 命令。

标识共享的容量预留

拥有者和使用者可以使用 Amazon EC2 控制台和 AWS CLI 标识共享的容量预留

使用 Amazon EC2 控制台标识共享的容量预留

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择容量预留。屏幕列出了您拥有的容量预留以及与您共享的容量预留。拥有者列显示了容量预留拥有者的 AWS 账户 ID。AWS 账户 ID 旁边的 (me) 指示您是拥有者。

使用 AWS CLI 标识共享的容量预留

使用 `describe-capacity-reservations` 命令。此命令返回您拥有的容量预留以及与您共享的容量预留。`OwnerId` 显示容量预留拥有者的 AWS 账户 ID。

查看共享的容量预留的使用情况

共享的容量预留的拥有者可随时使用 Amazon EC2 控制台和 AWS CLI 查看其使用情况。

使用 Amazon EC2 控制台查看容量预留的使用情况

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择容量预留。
3. 选择要查看其使用情况的容量预留，然后选择使用情况选项卡。

AWS 账户 ID 列显示了当前使用容量预留的使用者的账户 ID。启动的实例列显示了每个使用者当前在预留容量中运行的实例数。

使用 AWS CLI 查看容量预留的使用情况

使用 `get-capacity-reservation-usage` 命令。`AccountId` 显示使用容量预留的账户的 ID。`UsedInstanceCount` 显示使用者当前在预留容量中运行的实例数。

共享的容量预留权限

拥有者的权限

拥有者负责管理和取消其共享的容量预留。拥有者无法修改由其他账户拥有的共享容量预留中运行的实例。拥有者仍然负责管理其启动到共享的容量预留中的实例。

使用者的权限

使用者负责管理其正在运行共享的容量预留的实例。使用者不能以任何方式修改共享的容量预留，也不能查看或修改由其他使用者或容量预留拥有者拥有的实例。

计费和计量

共享容量预留不会产生额外的费用。

容量预留拥有者需要为他们在容量预留内部运行的实例以及未使用的预留容量付费。使用者需要为他们在共享的容量预留中运行的实例付费。

实例限制

所有容量预留使用量都计入容量预留拥有者的个按需实例限制。这包括：

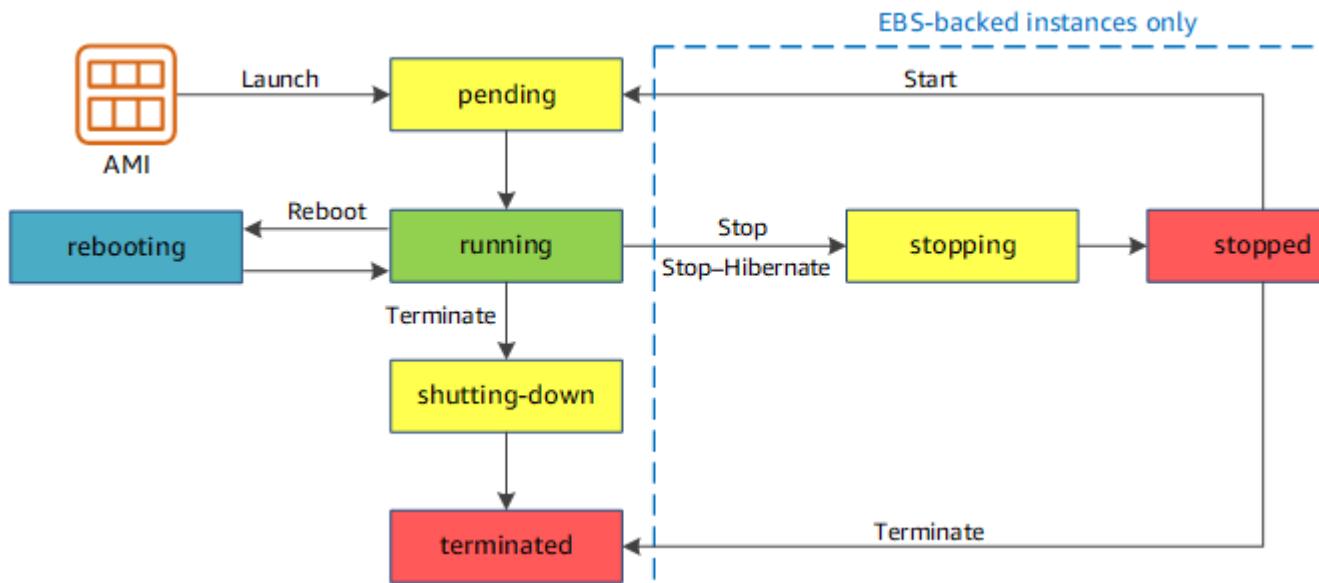
- 未使用的预留容量
- 容量预留拥有者拥有的实例的使用情况
- 使用者拥有的实例的使用情况

使用者在共享容量中启动的实例将计入容量预留拥有者的个按需实例限制。使用者的实例限制是他们自己的个按需实例限制和他们可以访问的共享容量预留中的可用容量的总和。

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 \(p. 85\)](#)。



下表提供了每个实例状态的简短说明，并指示它是否已计费。

Note

该表仅指示用于实例使用率的计费。一些 AWS 资源（如 Amazon EBS 卷和弹性 IP 地址）无论实例的状态如何，都将产生费用。有关更多信息，请参阅[AWS Billing and Cost Management 用户指南](#)中的[避免意外费用](#)。

实例状态	描述	实例使用率计费
pending	实例正准备进入 running 状态。实例在首次启动时进入 pending 状态，或者在处于 stopped 状态后启动。	不计费
running	实例正在运行，并且做好了使用准备。	已计费
stopping	实例正准备处于停止状态或休眠停止状态。	如果准备停止，则不计费 如果准备休眠，则计费
stopped	实例已关闭，不能使用。可随时启动实例。	不计费
shutting down	实例正准备终止。	不计费
terminated	实例已永久删除，无法启动。	<p>不计费</p> <p>Note</p> <p>应用于已终止实例的预留实例将按照其付款选项进行计费，直到其期限结束。有关更多信息，请参阅预留实例 (p. 243)。</p>

Note

重新启动实例不会启动新的实例计费周期，因为实例停留在 `running` 状态。

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的实例的主机硬件。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，您就需要为实例运行的每个秒，至少一分钟付费；即使实例处于闲置状态并且您并未连接到实例也是如此。

有关更多信息，请参阅[启动实例 \(p. 374\)](#)和[连接到 Linux 实例 \(p. 423\)](#)。

实例停止和启动 (仅限 Amazon EBS 支持的实例)

如果您的实例无法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。）如果您停止并启动实例，将丢失先前主机的实例存储卷上的所有数据。

您的实例会保留其私有 IPv4 地址，这意味着与该私有 IPv4 地址或网络接口关联的弹性 IP 地址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，我们都按每秒，您每次启动实例时至少一分钟。

有关更多信息，请参阅[停止和启动您的实例 \(p. 445\)](#)。

实例休眠 (仅限 Amazon EBS 支持的实例)

当您使实例休眠时，我们向操作系统发出信号来执行休眠 (`suspend-to-disk`)，这会将实例内存 (RAM) 中的内容保存到您的 Amazon EBS 根卷。我们保留实例的 Amazon EBS 根卷以及任何附加的 Amazon EBS 数据卷。当您启动实例时，Amazon EBS 根卷将还原到其之前的状态，并且 RAM 内容将重新加载。之前附加的数据卷会重新附加，实例也会保留其实例 ID。

当您将实例休眠时，它会进入 `stopping` 状态，然后进入 `stopped` 状态。当已休眠的实例处于 `stopped` 状态时，我们不会对其收取使用费，但是这些实例处于 `stopping` 状态时，这与您[停止实例 \(p. 372\)](#)而未将其休眠时不同，我们会对其进行收费。我们不收取数据传输费，但我们会对所有 Amazon EBS 卷的存储（包括 RAM 数据的存储）收费。

当您启动已休眠的实例时，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。

您的实例会保留其私有 IPv4 地址，这意味着与该私有 IPv4 地址或网络接口关联的弹性 IP 地址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。

有关更多信息，请参阅[使 Linux 实例休眠 \(p. 447\)](#)。

实例重启

您可以使用 Amazon EC2 控制台、命令行工具和 Amazon EC2 API 来重启实例。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。

重启实例相当于重启操作系统。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周期；将继续按秒计费，不再收取最低一分钟的费用。

有关更多信息，请参阅[重启您的实例 \(p. 456\)](#)。

实例停用

实例计划在 AWS 检测到托管实例的基础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 \(p. 456\)](#)。

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。

如果您启用终止保护，则无法使用控制台、CLI 或 API 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。您无法连接到或恢复已终止的实例。

Amazon EBS 支持的每个实例都支持 `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 上使用 `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 \(p. 458\)](#)。

重启、停止、休眠与终止之间的区别

下表总结了重启、停止、休眠与终止实例之间的主要区别。

特征	重启	停止/启动 (仅限 Amazon EBS 支持的实例)	休眠 (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	在许多情况下，我们会将该实例移动到新主机。您的实例可能驻留在同一主机上，前提是此主机正常。	在许多情况下，我们会将该实例移动到新主机。您的实例可能驻留在同一主机上，前提是此主机正常。	无
私有和公有 IPv4 地址	这些地址保持不变	实例保留其私有 IPv4 地址。实例将获取新的公有 IPv4 地址，除非它具有弹性 IP 地址（该地址在停止/启动过程中不更改）。	实例保留其私有 IPv4 地址。实例将获取新的公有 IPv4 地址，除非它具有弹性 IP 地址（该地址在停止/启动过程中不更改）。	无
弹性 IP 地址 (IPv4)	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址不再与实例相关联

特征	重启	停止/启动 (仅限 Amazon EBS 支持的实例)	休眠 (仅限 Amazon EBS 支持的实例)	终止
IPv6 地址	地址保持不变	实例保留其 IPv6 地址	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	数据将擦除
根设备卷	卷将保留	卷将保留	卷将保留	默认情况下将删除卷
RAM (内存中的内容)	RAM 将擦除	RAM 将擦除	RAM 将保存到根卷上的某一文件	RAM 将擦除
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。实例每次从 <code>stopped</code> 转换为 <code>running</code> 时，我们都会启动新的实例计费周期，您每次启动实例时，最低收取一分钟费用。	当实例处于 <code>stopping</code> 状态时，将会产生费用；但实例处于 <code>stopped</code> 状态时，将会停止产生费用。实例每次从 <code>stopped</code> 转换为 <code>running</code> 时，我们都会启动新的实例计费周期，您每次启动实例时，最低收取一分钟费用。	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。

操作系统的关闭命令始终会终止实例存储支持的实例。您可以控制操作系统关闭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 \(p. 460\)](#)。

启动实例

实例在 AWS 云中充当虚拟服务器。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，免费启动和使用微型实例 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] 使用启动实例向导指定启动参数。	使用启动实例向导启动实例 (p. 375)
[Amazon EC2 控制台] 创建启动模板并通过启动模板启动实例。	通过启动模板启动实例 (p. 379)
[Amazon EC2 控制台] 将现有实例作为基础。	使用现有实例中的参数启动实例 (p. 388)
[Amazon EC2 控制台] 使用您创建的 Amazon EBS 快照。	从备份启动 Linux 实例 (p. 389)
[Amazon EC2 控制台] 使用从 AWS Marketplace 购买的 AMI。	启动 AWS Marketplace 实例 (p. 389)
[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。	来自适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2
[AWS CLI] 使用 EC2 队列跨不同的 EC2 实例类型和可用区以及跨一个按需实例、Reserved Instance 和 Spot 实例购买模式预置容量。	启动 EC2 队列 (p. 391)

当您启动实例时，可以在与以下一项资源关联的子网中启动实例：

- 可用区 - 此选项为默认选项。
- 本地区域 - 要在本地区域中启动实例，您必须选择加入该功能。有关更多信息，请参阅[选择加入本地区域](#)。
- Outpost - 要在 Outpost 中启动实例，您必须创建 Outpost。有关如何创建 Outpost 的信息，请参阅 AWS Outposts 用户指南中的[AWS Outposts 入门](#)。

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。实例将获得一个公有 DNS 名称，您可使用此名称通过 Internet 与实例通信。实例还会获得一个私有 DNS 名称，相同 VPC 网络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 Linux 实例 \(p. 423\)](#)。

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 \(p. 458\)](#)。

使用启动实例向导启动实例

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 \(p. 18\)](#)。

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 可能包含充当 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（例如，美国东部（俄亥俄州））。为实例选择一个满足您需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
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。要选择符合免费套餐条件的 AMI，请在左侧窗格中选择 Free tier only。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。要查看已与您共享的 AMI，请在左侧窗格中选择与我共享。

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 \(p. 389\)](#)。

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 (根设备类型)。请注意哪些 AMI 是您需要的类型，即 ebs (由 Amazon EBS 支持) 或 instance-store (由实例存储支持)。有关更多信息，请参阅[根设备存储 \(p. 85\)](#)。
 - 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。有关更多信息，请参阅[Linux AMI 虚拟化类型 \(p. 87\)](#)。
 - 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 \(p. 160\)](#)。

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[可突增性能实例 \(p. 175\)](#)。

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

要快速设置实例以便进行测试，请选择 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。
 - (可选) 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 (启动至 Auto Scaling 组) 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[Amazon EC2 Auto Scaling 用户指南](#)。
 - Purchasing option (购买选项)：选择 Request Spot instances (请求 Spot 实例) 以启动 Spot 实例。这将在此页面中添加和删除选项。设置您的最高价，并选择性地更新请求类型、中断行为和请求有效性。有关更多信息，请参阅[创建Spot 实例请求 \(p. 292\)](#)。
 - 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。
 - 子网：您可以在与可用区、本地区域或 Outpost 关联的子网中启动实例。

要在可用区中启动实例，请选择要在其中启动实例的子网。您可以选择 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。

要在本地区域中启动实例，请选择您在本地区域中创建的子网。

要在 Outpost 中启动实例，请在 VPC 中选择与 Outpost 关联的子网。

- 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 \(p. 575\)](#)。
- 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[您的 VPC 和子网](#)。
- 容量预留：指定是将实例启动到共享容量还是现有容量预留。有关更多信息，请参阅[在现有容量预留中启动实例 \(p. 364\)](#)。
- IAM role (IAM 角色)：选择要与实例关联的 AWS Identity and Access Management (IAM) 角色。有关更多信息，请参阅[适用于 Amazon EC2 的 IAM 角色 \(p. 749\)](#)。
- CPU options (CPU 选项)：选择 Specify CPU options (指定 CPU 选项) 可在实例启动期间指定自定义 vCPU 数。设置 CPU 内核数和每内核线程数。有关更多信息，请参阅[优化 CPU 选项 \(p. 480\)](#)。
- 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 \(p. 460\)](#)。
- Stop - Hibernate behavior (停止 - 休眠行为)：要启用休眠，请选中该复选框。只有当实例满足休眠先决条件时，此选项才可用。有关更多信息，请参阅[使 Linux 实例休眠 \(p. 447\)](#)。
- Enable termination protection (启用终止保护)：要防止意外终止，请选中该复选框。有关更多信息，请参阅[为实例启用终止保护 \(p. 459\)](#)。
- 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 \(p. 538\)](#)。
- EBS-Optimized instance (EBS 优化的实例)：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。如果实例类型支持此功能，请选中此复选框来启动该功能。将收取额外费用。有关更多信息，请参阅[Amazon EBS 优化的实例 \(p. 863\)](#)。
- Tenancy：如果您要在 VPC 内启动实例，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 \(p. 356\)](#) 和 [专用主机 \(p. 333\)](#)。
- T2/T3 Unlimited (T2/T3 无限)：选中此复选框可允许应用程序突增到基准以上所需的时间。可能收取额外费用。有关更多信息，请参阅[可突增性能实例 \(p. 175\)](#)。
- 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 可添加辅助网络接口。辅助网络接口可以与 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 \(p. 595\)](#)。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，如果您为 eth0 指定某个现有网络接口，则无法使用 Auto-assign Public IP 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 \(p. 578\)](#)。

- Kernel ID (内核 ID)：(仅对半虚拟化 (PV) AMIs 有效) 除非您想使用某个特定内核，否则选择 Use default (使用默认值)。
- RAM disk ID (RAM 磁盘 ID)：(仅对半虚拟化 (PV) AMIs 有效) 除非您想使用某个特定 RAM 磁盘，否则选择 Use default (使用默认值)。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。
- 置放组：置放组确定您的实例的置放策略。选择现有置放群组或创建新组。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 \(p. 662\)](#)。

- 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. 您选择的 AMI 包含一个或多个存储卷，包括根设备卷。在添加存储页面上，您可以选择添加新卷来指定要附加到实例的其他卷。如下所示配置每个卷，然后选择 Next: Add Tags (下一步：添加标记)。
- 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 \(p. 903\)](#) 和 [Amazon EBS 卷 \(p. 783\)](#)。
 - 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可用的共享快照和公有快照。快照描述区分大小写。
 - Size (大小)：对于 EBS 卷，您可以指定存储大小。即使您选择了有资格享用免费套餐的 AMI 和实例，若要享用免费套餐，您必须将总存储大小保持为 30 GiB 以下。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。
 - 卷类型：对于 EBS 卷，请选择卷类型。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 785\)](#)。
 - 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 \(p. 461\)](#)。
 - 加密：如果实例类型支持 EBS 加密，则可以指定卷的加密状态。如果默认情况下在此区域中启用了加密，则将为您选择默认的 CMK。您可以选择其他密钥或禁用加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 851\)](#)。
8. 在 Add Tags 页面上，通过提供键和值组合来指定 [标签 \(p. 940\)](#)。您可以标记实例、卷或两者。对于 Spot 实例，只能标记 Spot 实例请求。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 \(p. 768\)](#)。) 按如下所示选择或创建安全组，然后选择 Review and Launch。
- a. 要选择现有安全组，请选择 Select an existing security group (选择现有安全组)，然后选择您的安全组。您无法编辑现有安全组的规则，但是可以通过选择 Copy to new (复制到新项目) 将它们复制到新组。随后您可以按下一步所述添加规则。
 - b. 要创建新安全组，请选择 Create a new security group (创建新安全组)。向导会自动定义 launch-wizard-x 安全组并创建入站规则，以允许您通过 SSH (端口 22) 连接到实例。
 - c. 您可以根据需要添加规则。例如，如果您的实例是 Web 服务器，请打开端口 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。

Warning

在本次简短练习中，可以接受启用所有 IP 地址 (0.0.0.0/0) 以通过 SSH 或 RDP 访问您实例的规则，但这种规则在生产环境中不安全。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。

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。

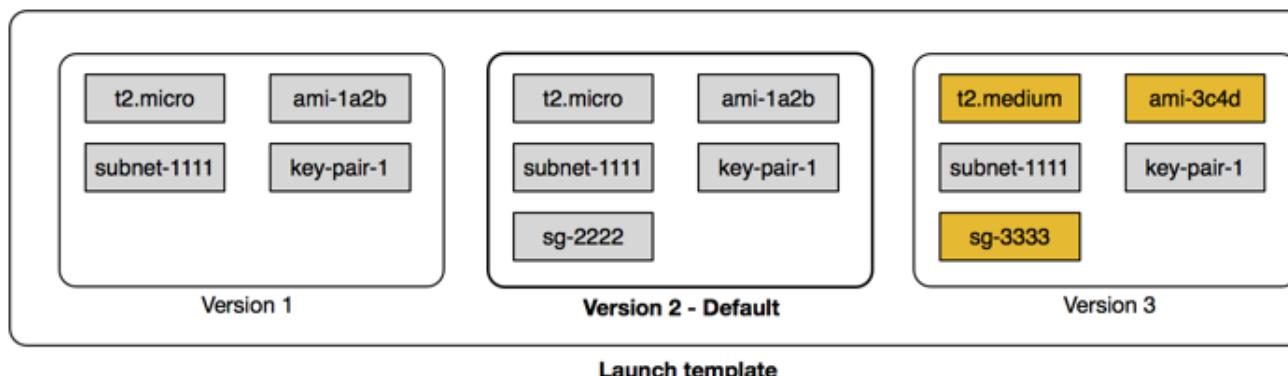
12. (可选) 您可以为实例创建一个状态检查警报 (可能需要额外付费)。(如果您不确定，您可以随时在以后添加。) 在确认屏幕上，选择 Create status check alarms 并按照指示操作。有关更多信息，请参阅[创建和编辑状态检查警报 \(p. 530\)](#)。
13. 如果实例无法启动或状态立即转至 terminated 而非 running，请参阅[排查实例启动问题 \(p. 953\)](#)。

通过启动模板启动实例

您可以创建一个启动模板，其中包含用于启动实例的配置信息。您可以在启动模板中存储启动参数，而无需在每次启动实例时都指定这些参数。例如，启动模板可能包含您通常用于启动实例的 AMI ID、实例类型和网络设置。在使用 Amazon EC2 控制台、AWS 软件开发工具包或命令行工具启动实例时，您可以指定要使用的启动模板。

对于每个启动模板，您可以创建一个或多个编号的启动模板版本。每个版本可能具有不同的启动参数。在通过启动模板启动实例时，您可以使用任何版本的启动模板。如果未指定版本，则使用默认版本。您可以将任何启动模板版本设置为默认版本 — 默认情况下，这是启动模板的第一个版本。

下图显示了具有三个版本的启动模板。第一个版本指定用于启动实例的实例类型、AMI ID、子网和密钥对。第二个版本基于第一个版本，并且还为实例指定了一个安全组。第三个版本在某些参数中使用不同的值。版本 2 设置为默认版本。如果通过该启动模板启动实例，并且未指定任何其他版本，则使用版本 2 中的启动参数。



目录

- [启动模板限制 \(p. 380\)](#)
- [使用启动模板控制启动参数 \(p. 380\)](#)
- [控制如何使用启动模板 \(p. 380\)](#)
- [创建启动模板 \(p. 380\)](#)
- [管理启动模板版本 \(p. 385\)](#)
- [通过启动模板启动实例 \(p. 386\)](#)
- [将启动模板与 Amazon EC2 Auto Scaling 一起使用 \(p. 387\)](#)
- [将启动模板与 EC2 队列一起使用 \(p. 387\)](#)
- [将启动模板与 Spot 队列一起使用 \(p. 387\)](#)
- [删除启动模板 \(p. 387\)](#)

启动模板限制

以下规则适用于启动模板和启动模板版本：

- 您最多可以为每个区域创建 5,000 个启动模板，并且每个启动模板最多具有 10,000 个版本。
- 启动模板参数是可选的。不过，您必须确保启动实例的请求包含所需的所有参数。例如，如果启动模板不包含 AMI ID，您必须在启动实例时指定启动模板和 AMI ID。
- 在创建启动模板时，不会验证启动模板参数。确保您为参数指定正确的值，并使用支持的参数组合。例如，要在置放群组中启动实例，您必须指定一种支持的实例类型。
- 您可以标记启动模板，但无法标记启动模板版本。
- 启动模板版本是按创建顺序编号的。在创建启动模板版本时，您无法自行指定版本号。

使用启动模板控制启动参数

启动模板可以包含用于启动实例的全部或部分参数。在使用启动模板启动实例时，您可以覆盖启动模板中指定的参数。或者，也可以指定在启动模板中不包含的额外参数。

Note

您无法在启动期间删除启动模板参数（例如，无法为参数指定空值）。要删除某个参数，请创建不包含该参数的新启动模板版本，并使用该版本启动实例。

要启动实例，IAM 用户必须有权使用 `ec2:RunInstances` 操作。您还必须有权创建或使用创建或与该实例关联的资源。您可以使用 `ec2:RunInstances` 操作的资源级权限控制用户可以指定的启动参数。或者，您可以为用户授予使用启动模板启动实例的权限。这样，您就可以在启动模板中管理启动参数，而不是在 IAM 策略中管理，并将启动模板作为授权方法以启动实例。例如，您可以指定用户只能使用启动模板启动实例，并且他们只能使用特定的启动模板。您还可以控制用户可以在启动模板中覆盖的启动参数。有关示例策略，请参阅 [启动模板 \(p. 734\)](#)。

控制如何使用启动模板

默认情况下，IAM 用户无权使用启动模板。您可以创建一个 IAM 用户策略，以便为用户授予创建、修改、描述和删除启动模板和启动模板版本的权限。您还可以将资源级权限应用于某些启动模板操作，以控制用户能否在这些操作中使用特定的资源。有关更多信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 712\)](#) 以及以下示例策略：[示例：使用启动模板 \(p. 740\)](#)。

在为用户授予使用 `ec2:CreateLaunchTemplate` 和 `ec2:CreateLaunchTemplateVersion` 操作的权限时，应格外小心。这些操作不支持资源级权限，您无法控制用户可以在启动模板中指定哪些资源。要限制用于启动实例的资源，请确保仅为相应的管理员授予创建启动模板和启动模板版本的权限。

创建启动模板

使用定义的参数创建新的启动模板，或者将现有的启动模板或实例作为基础以创建新的启动模板。

使用定义的参数创建新启动模板（控制台）

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择启动模板，然后选择创建启动模板。
3. 对于设备模板名称，请为您的启动模板输入描述性名称。要在创建时标记启动模板，请选择显示标签、添加标签，然后输入标签键/值对。
4. 对于模板版本说明，提供启动模板版本的简短说明。
5. 对于 Launch template contents（启动模板内容），请提供以下信息：
 - AMI ID：要从中启动实例的 AMI。要搜索所有可用 AMI，请选择 Search for AMI（搜索 AMI）。要选择常用的 AMI，请选择 Quick Start（快速入门）。或者，选择 AWS Marketplace 或 Community AMIs（社区 AMI）。您可以使用自己的 AMI 或 [查找合适的 AMI \(p. 88\)](#)。

- Instance type (实例类型) : 确保实例类型与指定的 AMI 兼容。有关更多信息 , 请参阅[实例类型 \(p. 160\)](#)。
 - Key pair name (密钥对名称) : 实例的密钥对。有关更多信息 , 请参阅[Amazon EC2 密钥对 \(p. 759\)](#)。
 - Network type (网络类型) : 如果适用 , 选择是将实例启动到 VPC 还是 EC2-Classic。如果选择 VPC , 请在 Network interfaces (网络接口) 部分中指定子网。如果选择 Classic , 请确保在 EC2 Classic 中支持指定的实例类型 , 并为实例指定可用区。
 - Security Groups (安全组) : 一个或多个要与实例关联的安全组。有关更多信息 , 请参阅[Linux 实例的 Amazon EC2 安全组 \(p. 768\)](#)。
6. 对于网络接口 , 您可以为实例最多指定两个[网络接口 \(p. 595\)](#)。
- Device (设备) : 网络接口的设备号 ; 例如 , eth0 表示主网络接口。如果将该字段保留空白 , AWS 将创建主网络接口。
 - Network interface (网络接口) : 网络接口的 ID , 或者保留空白以让 AWS 创建新的网络接口。
 - Description (描述) : (可选) 新网络接口的描述。
 - Subnet (子网) : 要在其中创建新网络接口的子网。对于主网络接口 (eth0) , 这是在其中启动实例的子网。如果为 eth0 输入了现有的网络接口 , 将在该网络接口所在的子网中启动实例。
 - Auto-assign public IP (自动分配公有 IP) : 指定是否自动为设备索引为 eth0 的网络接口分配公有 IP 地址。只能为单个新网络接口启用该设置。
 - Primary IP (主要 IP) : 您的子网范围内的一个私有 IPv4 地址。保留空白会让 AWS 为您选择一个私有 IPv4 地址。
 - Secondary IP (辅助 IP) : 您的子网范围内的一个辅助私有 IPv4 地址。保留空白会让 AWS 为您选择一个辅助私有 IPv4 地址。
 - (仅限 IPv6) IPv6 IP : 子网范围内的一个 IPv6 地址。
 - Security group ID (安全组 ID) : 您的 VPC 中与网络接口关联的安全组的 ID。
 - Delete on termination (终止时删除) : 选择在删除实例时是否删除网络接口。
 - Elastic Fabric Adapter : 指示网络接口是否为 Elastic Fabric Adapter。有关更多信息 , 请参阅 [Elastic Fabric Adapter](#)。
7. 对于存储 (卷) , 除了 AMI 指定的卷以外 , 还可以指定要附加到实例的卷。
- Volume type (卷类型) : 与实例关联的实例存储或 Amazon EBS 卷。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 \(p. 903\)](#) 和 [Amazon EBS 卷 \(p. 783\)](#)。
 - Device name (设备名称) : 卷的设备名称。
 - Snapshot (快照) : 用于创建卷的快照的 ID。
 - Size (大小) (对于 Amazon EBS 卷) 存储大小。
 - Volume type (卷类型) : (对于 Amazon EBS 卷) 卷类型。有关更多信息 , 请参阅 [Amazon EBS 卷类型 \(p. 785\)](#)。
 - IOPS : (对于 预配置 IOPS SSD 卷类型) 卷可支持的每秒 I/O 操作数。
 - Delete on termination (终止时删除) : 对于 Amazon EBS 卷 , 选择在终止实例时是否删除卷。有关更多信息 , 请参阅 [在实例终止时保留 Amazon EBS 卷 \(p. 461\)](#)。
 - 加密 : 如果实例类型支持 EBS 加密 , 则可以为卷启用加密。如果默认情况下在此区域中启用了加密 , 则会为您启用加密。有关更多信息 , 请参阅 [Amazon EBS Encryption \(p. 851\)](#)。
 - Key (密钥) : 要用于 EBS 加密的 CMK。您可以指定您使用 AWS Key Management Service 创建的任何客户主密钥 (CMK) 的 ARN。如果指定 CMK , 还必须使用加密来启用加密。
8. 对于标签 , 请提供键和值组合以指定[标签 \(p. 940\)](#)。您可以标记实例、卷或两者。
9. 对于高级详细信息 , 请展开该部分以查看字段并为实例指定任何其他参数。
- Purchasing option (购买选项) : 购买模式。选择 Request Spot instances (请求 Spot 实例) 可按照 Spot 价格请求 Spot 实例 , 以按需价格为上限 ; 而选择 Customize Spot parameters (自定义 Spot 参数) 可更改默认 Spot 实例 设置。如果您未请求 Spot 实例 , 则默认情况下 EC2 会启动 个按需实例。有关更多信息 , 请参阅[Spot 实例 \(p. 277\)](#)。

- IAM instance profile (IAM 实例配置文件)：要与实例关联的 AWS Identity and Access Management (IAM) 实例配置文件。有关更多信息，请参阅[适用于 Amazon EC2 的 IAM 角色 \(p. 749\)](#)。
- Shutdown behavior (关闭操作)：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 \(p. 460\)](#)。
- Stop - Hibernate behavior (停止 - 休眠操作)：选择是否为实例启用休眠。此字段仅适用于满足休眠先决条件的实例。有关更多信息，请参阅[使 Linux 实例休眠 \(p. 447\)](#)。
- Termination protection (终止保护)：选择是否禁止意外终止。有关更多信息，请参阅[为实例启用终止保护 \(p. 459\)](#)。
- Monitoring (监控)：选择是否使用 Amazon CloudWatch 启用实例详细监控。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 \(p. 538\)](#)。
- T2/T3 Unlimited (T2/T3 无限)：选择是否允许应用程序突增到基准以上所需的时间。此字段仅适用于 T2 和 T3 实例。可能收取额外费用。有关更多信息，请参阅[可突增性能实例 \(p. 175\)](#)。
- Placement group name (置放群组名称)：指定要在其中启动实例的置放群组。并非可以在置放群组中启动所有实例类型。有关更多信息，请参阅[置放群组 \(p. 662\)](#)。
- EBS-optimized instance (EBS 优化的实例)：为 Amazon EBS I/O 提供额外的专用容量。并非所有实例类型都支持该功能，并且会产生额外的费用。有关更多信息，请参阅[Amazon EBS 优化的实例 \(p. 863\)](#)。
- Tenancy (租期)：选择是在共享硬件 (Shared (共享))、隔离的专用硬件 (Dedicated (专用))，还是在专用主机 (Dedicated host (专用主机)) 上运行您的实例。如果您选择在专用主机上启动实例，则可以指定是否在主机资源组中启动实例，也可以定位特定专用主机。可能收取额外费用。有关更多信息，请参阅[专用实例 \(p. 356\)](#) 和 [专用主机 \(p. 333\)](#)。
- RAM 磁盘 ID：实例的 RAM 磁盘。如果您指定了一个内核，则可能需要指定带有可支持该内核的驱动程序的某个特定 RAM 磁盘。仅对半虚拟化 (PV) AMIs 有效。
- 内核 ID：实例的内核。仅对半虚拟化 (PV) AMIs 有效。
- 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。有关更多信息，请参阅[启动时在 Linux 实例上运行命令 \(p. 494\)](#)。

10. 选择创建启动模板。

通过现有启动模板创建启动模板 (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 Launch Templates。
3. 选择创建启动模板。提供启动模板的名称、描述和标签。
4. 对于源模板，请选择新启动模板所基于的启动模板。
5. 对于源模板版本，请选择新启动模板版本所基于的启动模板版本。
6. 根据需要，调整任何启动参数，然后选择创建启动模板。

通过实例创建启动模板 (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 Instances (实例)。
3. 选择所需实例，然后依次选择 Actions (操作) 和 Create Template From Instance (从实例创建模板)。
4. 提供名称、描述和标签，然后根据需要调整启动参数。

Note

通过实例创建启动模板时，该实例的网络接口 ID 和 IP 地址将不包含在模板中。

5. 选择 Create Template From Instance (从实例创建模板)。

创建启动模板 (AWS CLI)

- 使用 [create-launch-template](#) (AWS CLI) 命令。下面的示例创建一个指定以下内容的启动模板：
 - 启动模板的标签 (`purpose=production`)
 - 要启动的实例类型 (`r4.4xlarge`) 和 AMI (`ami-8c1be5f6`)
 - 总共 8 个 vCPU 的内核数 (4) 和每内核线程数 (2) (4 个内核 x 2 个线程)
 - 要在其中启动实例的子网 (`subnet-7b16de0c`)

该模板会向实例分配一个公有 IP 地址和一个 IPv6 地址，并为实例创建一个标签 (`Name=webserver`)。

```
aws ec2 create-launch-template --launch-template-name TemplateForWebServer
--version-description WebVersion1 --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' --launch-template-data file://template-
data.json
```

以下是 `template-data.json` 文件示例：

```
{
  "NetworkInterfaces": [
    {
      "AssociatePublicIpAddress": true,
      "DeviceIndex": 0,
      "Ipv6AddressCount": 1,
      "SubnetId": "subnet-7b16de0c"
    }
  ],
  "ImageId": "ami-8c1be5f6",
  "InstanceType": "r4.4xlarge",
  "TagSpecifications": [
    {
      "ResourceType": "instance",
      "Tags": [
        {
          "Key": "Name",
          "Value": "webserver"
        }
      ]
    }
  ],
  "CpuOptions": {
    "CoreCount": 4,
    "ThreadsPerCore": 2
  }
}
```

下面是示例输出。

```
{
  "LaunchTemplate": {
    "LatestVersionNumber": 1,
    "LaunchTemplateId": "lt-01238c059e3466abc",
    "LaunchTemplateName": "TemplateForWebServer",
    "DefaultVersionNumber": 1,
    "CreatedBy": "arn:aws:iam::123456789012:root",
    "CreateTime": "2017-11-27T09:13:24.000Z"
  }
}
```

获取启动模板的实例数据 (AWS CLI)

- 使用 `get-launch-template-data` (AWS CLI) 命令，并指定实例 ID。您可以将输出作为基础以创建新的启动模板或启动模板版本。默认情况下，输出包含一个顶级 `LaunchTemplateData` 对象，无法在启动模板数据中指定该对象。请使用 `--query` 选项排除该对象。

```
aws ec2 get-launch-template-data --instance-id i-0123d646e8048babc --query "LaunchTemplateData"
```

下面是示例输出。

```
{  
    "Monitoring": {},  
    "ImageId": "ami-8c1be5f6",  
    "BlockDeviceMappings": [  
        {  
            "DeviceName": "/dev/xvda",  
            "Ebs": {  
                "DeleteOnTermination": true  
            }  
        }  
    ],  
    "EbsOptimized": false,  
    "Placement": {  
        "Tenancy": "default",  
        "GroupName": "",  
        "AvailabilityZone": "us-east-1a"  
    },  
    "InstanceType": "t2.micro",  
    "NetworkInterfaces": [  
        {  
            "Description": "",  
            "NetworkInterfaceId": "eni-35306abc",  
            "PrivateIpAddresses": [  
                {  
                    "Primary": true,  
                    "PrivateIpAddress": "10.0.0.72"  
                }  
            ],  
            "SubnetId": "subnet-7b16de0c",  
            "Groups": [  
                "sg-7c227019"  
            ],  
            "Ipv6Addresses": [  
                {  
                    "Ipv6Address": "2001:db8:1234:1a00::123"  
                }  
            ],  
            "PrivateIpAddress": "10.0.0.72"  
        }  
    ]  
}
```

您可以将输出直接写入到一个文件中，例如：

```
aws ec2 get-launch-template-data --instance-id i-0123d646e8048babc --query "LaunchTemplateData" >> instance-data.json
```

管理启动模板版本

您可以为特定启动模板创建启动模板版本，设置默认版本以及删除不再需要的版本。

任务

- [创建启动模板版本 \(p. 385\)](#)
- [设置默认启动模板版本 \(p. 385\)](#)
- [删除启动模板版本 \(p. 386\)](#)

创建启动模板版本

在创建启动模板版本时，您可以指定新的启动参数，或者将现有版本作为基础以创建新的版本。有关启动参数的更多信息，请参阅[创建启动模板 \(p. 380\)](#)。

创建启动模板版本（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 Launch Templates。
3. 选择创建启动模板。
4. 对于您要做什么，选择创建新模板版本
5. 对于启动模板名称，从列表中选择现有启动模板的名称。
6. 对于模板版本说明，键入启动模板版本的说明。
7. (可选) 选择启动模板的版本或其他启动模板的版本，以用作新启动模板版本的基础。新启动模板版本从此启动模板版本继承启动参数。
8. 根据需要修改启动参数，然后选择创建启动模板。

创建启动模板版本 (AWS CLI)

- 使用 `create-launch-template-version` (AWS CLI) 命令。您可以指定新版本所基于的源版本。新版本从此版本继承启动参数，您可以使用 `--launch-template-data` 覆盖参数。以下示例根据启动模板的版本 1 创建新的版本并指定不同的 AMI ID。

```
aws ec2 create-launch-template-version --launch-template-id lt-0abcd290751193123 --version-description WebVersion2 --source-version 1 --launch-template-data "ImageId=ami-c998b6b2"
```

设置默认启动模板版本

您可以设置启动模板的默认版本。如果通过启动模板启动实例并且未指定版本，将使用默认版本的参数启动实例。

设置默认启动模板版本（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 Launch Templates。
3. 选择启动模板，然后依次选择操作和设置默认版本。
4. 对于默认版本，请选择版本号，然后选择设置为默认版本。

设置默认启动模板版本 (AWS CLI)

- 使用 `modify-launch-template` (AWS CLI) 命令，并指定要设置为默认版本的版本。

```
aws ec2 modify-launch-template --launch-template-id lt-0abcd290751193123 --default-version 2
```

删除启动模板版本

如果不再需要某个启动模板版本，您可以将其删除。在删除该版本后，无法替换版本号。您无法删除启动模板的默认版本；您必须先分配一个不同的版本以作为默认版本。

删除启动模板版本（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 Launch Templates。
3. 选择启动模板，然后依次选择操作、删除模板版本。
4. 选择要删除的版本，然后选择删除启动模板版本。

删除启动模板版本 (AWS CLI)

- 使用 `delete-launch-template-versions` (AWS CLI) 命令，并指定要删除的版本号。

```
aws ec2 delete-launch-template-versions --launch-template-id lt-0abcd290751193123 --versions 1
```

通过启动模板启动实例

您可以使用启动模板中包含的参数启动实例。在启动实例之前，您可以选择覆盖或添加启动参数。

将自动为使用启动模板启动的实例分配两个具有 `aws:ec2launchtemplate:id` 和 `aws:ec2launchtemplate:version` 键的标签。您无法删除或编辑这些标签。

通过启动模板启动实例（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 Launch Templates。
3. 选择启动模板，然后依次选择操作、从模板启动实例。
4. 选择要使用的启动模板版本。
5. (可选) 您可以在实例详细信息部分中更改和添加参数以覆盖或添加启动模板参数。
6. 选择通过模板启动实例。

通过启动模板启动实例 (AWS CLI)

- 使用 `run-instances` AWS CLI 命令，并指定 `--launch-template` 参数。可以选择指定要使用的启动模板版本。如果未指定版本，则使用默认版本。

```
aws ec2 run-instances --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- 要覆盖启动模板参数，请在 `run-instances` 命令中指定该参数。以下示例覆盖在启动模板（如果有）中指定的实例类型。

```
aws ec2 run-instances --launch-template LaunchTemplateId=lt-0abcd290751193123 --instance-type t2.small
```

- 如果指定复杂结构包含的嵌套参数，则使用启动模板中指定的复杂结构以及您指定的任何其他嵌套参数启动实例。

在以下示例中，将使用标签 Owner=TeamA 以及在启动模板中指定的任何其他标签启动实例。如果启动模板包含具有 Owner 键的现有标签，该值将替换为 TeamA。

```
aws ec2 run-instances --launch-template LaunchTemplateId=lt-abcd290751193123 --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

在以下示例中，将使用具有设备名称 /dev/xvdb 的卷以及在启动模板中指定的任何其他块储存设备映射启动实例。如果启动模板为 /dev/xvdb 定义了一个现有的卷，它的值将替换为指定的值。

```
aws ec2 run-instances --launch-template LaunchTemplateId=lt-abcd290751193123 --block-device-mappings "DeviceName=/dev/xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

如果实例无法启动或状态立即转至 terminated 而非 running，请参阅 [排查实例启动问题 \(p. 953\)](#)。

将启动模板与 Amazon EC2 Auto Scaling 一起使用

您可以创建一个 Auto Scaling 组，并指定一个用于该组的启动模板。在 Amazon EC2 Auto Scaling 启动 Auto Scaling 组中的实例时，它使用关联的启动模板中定义的启动参数。

有关更多信息，请参阅 [Amazon EC2 Auto Scaling 用户指南中的使用启动模板创建 Auto Scaling 组](#)。

通过启动模板创建或更新 Amazon EC2 Auto Scaling 组 (AWS CLI)

- 使用 [create-auto-scaling-group](#) 或 [update-auto-scaling-group](#) AWS CLI 命令，并指定 --launch-template 参数。

将启动模板与 EC2 队列一起使用

您可以创建一个 EC2 队列请求，并在实例配置中指定一个启动模板。在 Amazon EC2 完成 EC2 队列 请求时，它使用关联的启动模板中定义的启动参数。您可以覆盖启动模板中指定的某些参数。

有关更多信息，请参阅 [创建 EC2 队列 \(p. 407\)](#)。

通过启动模板创建 EC2 队列 (AWS CLI)

- 使用 [create-fleet](#) AWS CLI 命令。请使用 --launch-template-configs 参数指定启动模板，并为启动模板指定任何覆盖值。

将启动模板与 Spot 队列一起使用

您可以创建一个 Spot 队列请求，并在实例配置中指定一个启动模板。在 Amazon EC2 完成 Spot 队列 请求时，它使用关联的启动模板中定义的启动参数。您可以覆盖启动模板中指定的某些参数。

有关更多信息，请参阅 [Spot 队列请求 \(p. 296\)](#)。

通过启动模板创建 Spot 队列 请求 (AWS CLI)

- 使用 [request-spot-fleet](#) AWS CLI 命令。请使用 LaunchTemplateConfigs 参数指定启动模板，并为启动模板指定任何覆盖值。

删除启动模板

如果不再需要某个启动模板，您可以将其删除。如果删除启动模板，则会删除该模板的所有版本。

删除启动模板 (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 Launch Templates。
3. 选择启动模板，然后依次选择操作、删除模板。
4. 选择删除启动模板。

删除启动模板 (AWS CLI)

- 使用 `delete-launch-template` (AWS CLI) 命令，并指定启动模板。

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

使用现有实例中的参数启动实例

Amazon EC2 控制台提供了一个 Launch More Like This (启动更多类似项) 向导选项，允许将当前实例作为基础来启动其他实例。该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。

或者，创建一个 [启动模板 \(p. 379\)](#) 以存储您的实例的启动参数。

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 \(p. 575\)](#)。
- 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：

- 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。
4. 如果实例无法启动或状态立即转至 terminated 而非 running，请参阅 [排查实例启动问题 \(p. 953\)](#)。

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。

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 \(p. 922\)](#)。
 - 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 \(p. 87\)](#)。
 - (仅限 PV 虚拟化类型) Kernel ID 和 RAM disk ID：从列表中选择 AKI 和 ARI。如果您选择默认 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一个 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 \(p. 848\)](#)。
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 [使用启动实例向导启动实例 \(p. 375\)](#)。

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 \(p. 99\)](#)。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 \(p. 101\)](#)。

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 仪表板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) (选择一个 Amazon 系统映像 (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[使用启动实例向导启动实例 \(p. 375\)](#)。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。

9. 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 Linux 实例 \(p. 423\)](#)。

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 \(p. 101\)](#)。

10. 如果实例无法启动或状态立即转至 terminated 而非 running，请参阅[排查实例启动问题 \(p. 953\)](#)。

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。

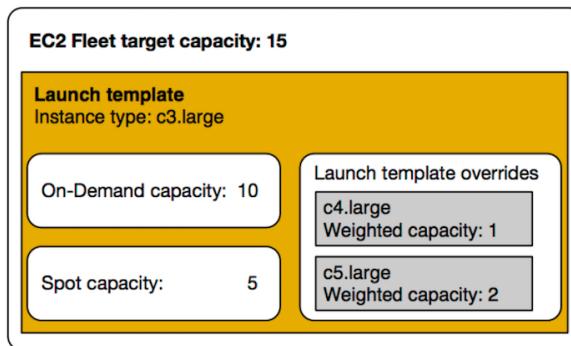
启动 EC2 队列

EC2 队列 包含用于启动实例队列（或实例组）的配置信息。在单个 API 调用中，队列可同时使用按需实例、Reserved Instance 和 Spot 实例购买选项来跨多个可用区启动多种类型的实例。通过使用 EC2 队列，您可以：

- 定义单独的按需和 Spot 容量目标以及您愿意每小时支付的最大金额
- 指定最适合您的应用程序的实例类型
- 指定 Amazon EC2 应如何在每个购买选项中分配您的队列容量

也可以设置您愿意为队列支付的每小时最大金额，EC2 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

EC2 队列会尝试启动适当数量的实例，以满足在您的请求中指定的目标容量要求。如果您指定了每小时最高总价，它将满足容量要求，直至达到您愿意支付的最大金额。如果 Spot 实例中断，队列还可能会尝试保持其目标 Spot 容量。有关更多信息，请参阅[Spot 实例的工作原理 \(p. 280\)](#)。



您可以为每个 EC2 队列指定无限数量的实例类型。那些实例类型可以使用按需和 Spot 购买选项进行预配置。您也可以指定多个可用区，为每个实例指定不同的最高 Spot 价格，并为每个队列选择其他 Spot 选项。当队列启动时，Amazon EC2 使用指定选项来预配置容量。

当队列运行时，如果 Amazon EC2 因价格上涨或实例失败而回收 Spot 实例，EC2 队列会尝试将实例替换为您指定的任何实例类型的实例。这使得可在 Spot 价格高峰期间更轻松地重新获取容量。您可以为每个队列制定灵活的弹性资源配置策略。例如，在特定的队列中，您可以用成本较低的 Spot 容量（如果可用）按需补充主容量。

如果有预留实例，并且在队列中指定按需实例，EC2 队列会使用预留实例。例如，如果队列指定 c4.large 个按需实例，而您有 c4.large 预留实例，则采用 Reserved Instance 定价。

使用 EC2 队列 不收取任何额外费用。您只需为队列为您启动的 EC2 实例付费。

目录

- [EC2 队列限制 \(p. 391\)](#)
- [EC2 队列限制 \(p. 392\)](#)
- [EC2 队列配置策略 \(p. 392\)](#)
- [管理 EC2 队列 \(p. 400\)](#)

EC2 队列限制

以下限制适用于 EC2 队列。

- EC2 队列仅可通过 API 或 AWS CLI 使用。
- EC2 队列请求不能跨 AWS 区域。您需要为每个区域创建单独的 EC2 队列。

- EC2 队列请求不能跨同一可用区内的不同子网。

EC2 队列限制

常用的 Amazon EC2 限制适用于 EC2 队列启动的实例，例如，Spot 请求价格限制、实例限制和卷限制。此外，以下限制将适用：

- 每个 AWS 区域的活动 EC2 队列数量：1,000 * †
- 每个队列的启动规范数：50 †
- 启动规范中的用户数据大小：16 KB †
- 每个 EC2 队列的目标容量：10000
- 区域中所有 EC2 队列的目标容量：100000 *

如果您需要增加目标容量的默认限制，请填写 AWS 支持中心[创建案例](#)表格请求增加限制。对于 Limit type (限制类型)，选择 EC2 Fleet (EC2 队列)，选择区域，然后选择 Target Fleet Capacity per Fleet (in units) (每个队列的目标队列容量(单位)) 和/或 Target Fleet Capacity per Region (in units) (每个区域的目标队列容量(单位))。

* 这些限制同时适用于您的 EC2 队列和 Spot 队列。

† 这些是硬限制。您不能请求提高这些限制。

T3 实例

如果您打算立即或短期内使用 T3 Spot 实例，没有空闲时间累积 CPU 积分，我们建议您以 [standard \(p. 185\)](#) 模式启动 T3 Spot 实例以避免支付更多的费用。

如果您以 [unlimited \(p. 178\)](#) 模式启动 T3 Spot 实例 并立即突增 CPU，您将会为突增花费超额积分。如果您在短期内使用实例，实例没有时间累积 CPU 积分来支付超额积分，则您将在终止实例时为超额积分付费。

只有实例的运行时间较长，足以累积进行突增的 CPU 积分时，针对 T3 Spot 实例的 Unlimited 模式才适用。否则，为超额积分付费会使 T3 Spot 实例比 M5 或 C5 实例的费用更高。

T2 实例

通过提供足够的计算资源来配置实例，启动积分旨在为 T2 实例提供有成效的初始启动体验。不允许重复启动 T2 实例以访问新的启动积分。如果您需要持续的 CPU，您可以赚取积分 (通过空转一段时间)，使用 [T2 Unlimited \(p. 178\)](#)，或将实例类型和专用 CPU (例如 c4.large) 一起使用。

EC2 队列配置策略

EC2 队列 是一组按需实例和 Spot 实例。

EC2 队列 尝试启动适当数量的实例，以满足您在队列请求中指定的目标容量要求。队列可能仅包含按需实例，仅包含 Spot 实例或包含按需实例和 Spot 实例的组合。如果具有可用的容量，并且您的请求的每小时最高价格超过 Spot 价格，则会满足 Spot 实例请求。如果 Spot 实例中断，队列还会尝试保持其目标容量。

也可以设置您愿意为队列支付的每小时最大金额，EC2 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

Spot 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。在您创建 EC2 队列时，可以指定多个启动规范 (因实例类型、可用区、子网以及最高价而异)。该队列会基于请求中包含的启动规范以及请求的配置来选择用于执行请求的 Spot 实例池。Spot 实例来自所选的池。

EC2 队列 让您能基于核心或实例数量或内存量预配置适合于您的应用程序的大量 EC2 容量。例如，您可以指定 EC2 队列启动 200 个实例的目标容量，其中 130 个是按需实例，其余是 Spot 实例。也可以请求 1000 个内核，每个内核至少有 2 GB RAM。该队列确定 Amazon EC2 选项的组合，以便以绝对最低的成本启动此容量。

使用适当的配置策略创建满足您的需求的EC2 队列。

目录

- [规划 EC2 队列 \(p. 393\)](#)
- [EC2 队列请求类型 \(p. 393\)](#)
- [Spot 实例的分配策略 \(p. 394\)](#)
- [配置 EC2 队列，以便进行按需备份 \(p. 395\)](#)
- [最高价覆盖 \(p. 395\)](#)
- [控制支出 \(p. 396\)](#)
- [EC2 队列实例权重 \(p. 396\)](#)
- [教程：将 EC2 队列与实例权重一起使用 \(p. 397\)](#)
- [教程：使用 EC2 队列并将按需作为主容量 \(p. 399\)](#)

规划 EC2 队列

规划 EC2 队列时，建议执行以下操作：

- 确定您要创建的 EC2 队列是针对所需目标容量提交同步或异步一次性请求，还是随着时间推移保持目标容量。有关更多信息，请参阅[EC2 队列请求类型 \(p. 393\)](#)。
- 确定满足您的应用程序要求的实例类型。
- 如果计划在 EC2 队列中包含 Spot 实例，在创建队列之前，请查看 [Spot 最佳实践](#)。使用这些最佳实践规划您的队列，以便以可能的最低价预配置实例。
- 确定您的 EC2 队列的目标容量。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[EC2 队列实例权重 \(p. 396\)](#)。
- 确定 EC2 队列目标容量的大部分必须是按需容量和 Spot 容量。您可以为按需容量和/或 Spot 容量指定 0。
- 确定您的每单位价格（如果使用实例权重）。要计算每单位价格，请将每实例小时价格除以该实例表示的单位数（或权重）。如果不使用实例权重，则默认每单位价格为每实例小时价格。
- 确定您愿意为队列支付的每小时最大金额。有关更多信息，请参阅[控制支出 \(p. 396\)](#)。
- 查看可用于您的 EC2 队列的可能选项。有关更多信息，请参阅[EC2 队列 JSON 配置文件参考 \(p. 405\)](#)。有关 EC2 队列配置示例，请参阅[EC2 队列示例配置 \(p. 413\)](#)。

EC2 队列请求类型

EC2 队列请求有三种类型：

instant

如果您将请求类型配置为 instant，EC2 队列会针对所需容量发出同步一次性请求。在 API 响应中，它返回启动的实例以及那些无法启动实例的错误。

request

如果您将请求类型配置为 request，EC2 队列针对所需容量发出异步一次性请求。此后，如果由于 Spot 中断导致容量减少，队列不会尝试补充 Spot 实例，也不会当容量不可用时在其他 Spot 实例容量池中提交请求。

maintain

（默认）如果您将请求类型配置为 maintain，EC2 队列针对所需容量发出异步请求，并自动补充任何中断的 Spot 实例以保持容量。

在提交 instant 或 request EC2 队列请求后，您无法修改该请求的目标容量。要更改 instant 或 request 队列请求的目标容量，请删除队列并创建新队列。

所有三种请求类型都可通过分配策略获益。有关更多信息，请参阅[Spot 实例的分配策略 \(p. 394\)](#)。

Spot 实例的分配策略

EC2 队列的分配策略决定了如何根据启动规范从可能的 Spot 实例池满足 Spot 实例请求。以下是可在队列中指定的分配策略：

`lowest-price`

Spot 实例来自价格最低的池。这是默认策略。

`diversified`

Spot 实例分布在所有池中。

`capacity-optimized`

Spot 实例来自为启动的实例数量提供最佳容量的池。

`InstancePoolsToUseCount`

Spot 实例分布在您指定数量的 Spot 池中。此参数仅在与 `lowest-price` 结合使用时有效。

维持目标容量

在 Spot 实例因 Spot 价格或 Spot 实例池的可用容量发生变化而终止之后，`maintain` 类型的 EC2 队列会启动替换 Spot 实例。如果分配策略是 `lowest-price`，则队列在当前具有最低 Spot 价格的池中启动替换实例。如果分配策略是 `lowest-price` 与 `InstancePoolsToUseCount` 的组合，则队列选择具有最低价格的 Spot 池并跨所指定数量的 Spot 池启动 Spot 实例。如果分配策略是 `capacity-optimized`，则队列在当前具有最多可用 Spot 实例容量的池中启动替换实例。如果分配策略是 `diversified`，则队列在其余池间分配替换 Spot 实例。

配置 EC2 队列，实现成本优化

要优化 Spot 实例的使用成本，请指定 `lowest-price` 分配策略，以便 EC2 队列自动基于当前 Spot 价格部署实例类型和可用区的最低成本组合。

对于按需实例目标容量，EC2 队列始终根据公开按需价格选择成本最低的实例类型，同时对 Spot 实例继续按照策略 (`lowest-price`、`capacity-optimized` 或 `diversified`) 执行分配。

配置 EC2 队列以实现成本优化和多元化

要以低成本且多元化的方式创建 Spot 实例队列，请将 `lowest-price` 分配策略与 `InstancePoolsToUseCount` 结合使用。EC2 队列基于所指定数量的 Spot 池中的当前 Spot 价格，自动部署实例类型和可用区的最低成本组合。此组合可用于避免最昂贵的 Spot 实例。

配置 EC2 队列以实现容量优化

使用 Spot 实例，定价会根据长期供需趋势缓慢发生变化，但容量会实时波动。`capacity-optimized` 策略通过查看实时容量数据并预测可用性最高的池，自动在可用性最高的池中启动 Spot 实例。这适用于与中断相关的重启工作和检查点成本较高的工作负载，例如大数据和分析、图像和媒体渲染、机器学习以及高性能计算。通过实现更低的中断可能性，`capacity-optimized` 策略可以降低您工作负载的整体成本。

选择合适的分配策略

您可以基于您的使用案例来优化队列。

如果队列较小或运行较短时间，则 Spot 实例中断的可能性较小，即使所有实例位于单个 Spot 实例池中。因此，`lowest-price` 策略可能会满足您的需求，同时提供最低的成本。

如果队列较大或长时间运行，则可以通过在多个池间分配 Spot 实例来提高队列的可用性。例如，如果 EC2 队列指定 10 个池，目标容量为 100 个实例，则队列会在每个池中启动 10 个 Spot 实例。如果某个池的 Spot

价格超过您在该池中的最高价，您的队列仅 10% 受到影响。使用此策略还可降低您的队列对单个池的 Spot 价格随时间上涨的敏感度。

使用 `diversified` 策略时，EC2 队列不在 Spot 价格等于或高于 [按需价格](#) 的任何池中启动 Spot 实例。

要创建低成本且多元化的机群，请将 `lowest-price` 策略与 `InstancePoolsToUseCount` 结合使用。您可以使用少量或大量的 Spot 池以在其中分配您的 Spot 实例。例如，如果您运行批处理，我们建议指定少量的 Spot 池（例如，`InstancePoolsToUseCount=2`）以确保队列始终具有计算容量，同时尽可能节省成本。如果您运行 Web 服务，我们建议指定较大量数的 Spot 池（例如，`InstancePoolsToUseCount=10` 个）以最大限度减少 Spot 实例池暂时不可用造成的影响。

如果您的队列运行的工作负载可能会因重启工作和检查点而导致更高的中断成本，则使用 `capacity-optimized` 策略。此策略提供更低的中断可能性，这可以降低您工作负载的整体成本。

配置 EC2 队列，以便进行按需备份

如果有紧急而不可预测的扩展需要，如在发生重大新闻事件或比赛期间必须扩展的新闻网站，建议为按需实例指定备用实例类型，以备首选选项没有足够可用容量时所需。例如，您可能首选 `c5.2xlarge` 按需实例，但是如果没有足够的可用容量，在负载高峰期，您会愿意使用一些 `c4.2xlarge` 实例。在这种情况下，EC2 队列尝试使用 `c5.2xlarge` 实例满足所有目标容量要求，但如果没有任何容量，则会自动启动 `c4.2xlarge` 实例以满足目标容量要求。

针对按需容量优化实例类型

EC2 队列 尝试满足您的按需容量时，它会默认首先启动价格最低的实例类型。如果 `AllocationStrategy` 设置为 `prioritized`，EC2 队列使用优先级来确定首先使用什么实例类型来满足按需容量。优先级分配给启动模板覆盖，优先级最高的最先启动。

例如，您可以配置三个启动模板覆盖，每个覆盖具有不同的实例类型：`c3.large`、`c4.large` 和 `c5.large`。`c5.large` 的按需价格低于 `c4.large` 的价格。`c3.large` 是最便宜的。如果您不使用优先级来确定顺序，则机群按照从 `c3.large` 开始、然后 `c5.large` 的顺序满足按需容量。由于您的 `c4.large` 经常会有未使用的预留实例，您可以设置启动模板覆盖优先级，这样其顺序就是 `c4.large`、`c3.large`、`c5.large`。

对按需实例 使用 容量预留

可以通过将容量预留的使用策略配置为 `use-capacity-reservations-first` 来将队列配置为在启动按需实例时首先使用按需容量预留。可以将此设置与按需实例的分配策略（`lowest-price` 或 `prioritized`）结合使用。

在将未使用的容量预留用于实现按需容量时：

- 队列使用未使用的容量预留来实现按需容量，最多可达到目标按需容量。
- 如果多个实例池具有未使用的容量预留，则应用按需分配策略（`lowest-price` 或 `prioritized`）。
- 如果未使用的容量预留数少于按需目标容量，则将根据按需分配策略（`lowest-price` 或 `prioritized`）启动剩余的按需目标容量。

只能将未使用的按需容量预留用于 `instant` 类型的队列。

有关如何将队列配置为使用容量预留来实现按需容量的示例，请参阅 [EC2 队列示例配置 \(p. 413\)](#)。有关更多信息，请参阅 [按需容量预留 \(p. 360\)](#) 和 [按需容量预留常见问题](#)。

最高价覆盖

每个 EC2 队列可以包含全局最高价格，或使用默认值（按需价格）。队列将该价格作为每个启动规范的默认最高价。

您可以选择在一个或多个启动规范中指定最高价。该价格是启动规范特有的。如果启动规范包含特定的价格，则 EC2 队列使用该最高价以覆盖全局最高价。不包含特定最高价的任何其他启动规范仍使用全局最高价。

控制支出

在达到以下参数之一时，EC2 队列停止启动实例：TotalTargetCapacity 或 MaxTotalPrice（您愿意支付的最大金额）。要控制您每小时为队列支付的金额，您可以指定 MaxTotalPrice。在达到最高总价时，即使未达到目标容量，EC2 队列也会停止启动实例。

以下示例显示了两个不同的方案。在第一个方案中，在达到目标容量时，EC2 队列停止启动实例。在第二个方案中，在达到您愿意支付的最大金额 (MaxTotalPrice) 时，EC2 队列停止启动实例。

示例：在达到目标容量时，停止启动实例

假设发出 m4.large 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- OnDemandTargetCapacity：10
- MaxTotalPrice：1.50 美元

EC2 队列启动 10 个按需实例，因为按需实例的总价 1.00 美元（10 个实例 × 0.10 美元）不超过 MaxTotalPrice（1.50 美元）。

示例：在达到最高总价时，停止启动实例

假设发出 m4.large 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- OnDemandTargetCapacity：10
- MaxTotalPrice：0.80 美元

如果 EC2 队列启动按需目标容量（10 个按需实例），则每小时的总成本为 1.00 美元。这超过了为按需实例的 MaxTotalPrice 指定的金额（0.80 美元）。为了防止支出超过您愿意支付的金额，EC2 队列仅启动 8 个按需实例（低于按需目标容量），因为启动更多实例将超过按需实例的 MaxTotalPrice。

EC2 队列实例权重

在创建 EC2 队列时，您可以定义每种实例类型为应用程序性能贡献的容量单位。然后，您可以使用实例权重调整每个启动规范的最高价格。

默认情况下，您指定的价格是每实例小时 价格。在使用实例权重功能时，您指定的价格是每单位小时 价格。您可以通过将实例类型价格除以它代表的单位数来计算每单位小时价格。EC2 队列将目标容量除以实例权重以计算要启动的实例数。如果结果不是整数，则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。队列可以选择您在启动规范中指定的任意池，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 EC2 队列请求确定每单位出价的计算示例。

实例类型	实例权重	目标容量	启动的实例数	每实例小时价格	每单位小时价格
r3.xlarge	2	10	5 (10 除以 2)	0.05 美元 (0.05 除以 2)	0.025 美元 (0.05 除以 2)
r3.8xlarge	8	10	2 (10 除以 8， 结果向上舍入)	0.10 美元 (0.10 除以 8)	0.0125 美元 (0.10 除以 8)

按如下所示使用 EC2 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 EC2 队列设置目标容量。
2. 设置每单位价格。
3. 为每个启动规范指定权重，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 EC2 队列请求：

- 目标容量为 24
- 一个实例类型为 `r3.2xlarge` 且权重为 6 的启动规范
- 一个实例类型为 `c3.xlarge` 且权重为 5 的启动规范

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动规范提供了最低的每单位价格（`r3.2xlarge` 每实例小时价格除以 6），则 EC2 队列会启动 4 个这样的实例（24 除以 6）。

如果第二个启动规范提供了最低的每单位价格（`c3.xlarge` 每实例小时价格除以 5），则 EC2 队列会启动 5 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 EC2 队列请求：

- 目标容量为 30 个 Spot 实例
- 一个实例类型为 `c3.2xlarge` 且权重为 8 的启动规范
- 一个实例类型为 `m3.xlarge` 且权重为 8 的启动规范
- 一个实例类型为 `r3.xlarge` 且权重为 8 的启动规范

EC2 队列会启动四个实例（30 除以 8，结果向上舍入）。在使用 `lowest-price` 策略时，所有四个实例均来自提供最低每单位价格的池。使用 `diversified` 策略时，队列会在所有三个池中各启动一个实例，并在三个池中提供最低每单位价格的那个池中启动第四个实例。

教程：将 EC2 队列与实例权重一起使用

该教程使用名为 Example Corp 的虚构公司说明使用实例权重请求 EC2 队列的过程。

目标

Example Corp 是一家医药公司，该公司想要使用 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[Spot 最佳实践](#)。然后，Example Corp 确定了他们的 EC2 队列的要求。

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
<code>r3.2xlarge</code>	61	8

实例类型	内存 (GiB)	vCPU
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）作为一个单位，Example Corp 确定，此数量的 20 倍应可满足其需求。因此该公司将其 EC2 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 EC2 队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时价格

Example Corp 将每实例小时 [按需价格](#) 作为其价格的起点。他们也可以使用最近的 Spot 价格或两者的组合。为了计算每单位小时价格，他们将每实例小时起始价格除以权重。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 美元	1	0.7 美元
r3.4xLarge	1.4 美元	2	0.7 美元
r3.8xLarge	2.8 美元	4	0.7 美元

Example Corp 可能会使用每单位小时全局价格 0.7 美元，这对于所有三种实例类型来说是非常有竞争力的。他们可能还会使用每单位小时全局价格 0.7 美元，并在 r3.8xlarge 启动规范中使用特定的每单位小时价格 0.9 美元。

验证权限

在创建 EC2 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[EC2 队列先决条件 \(p. 401\)](#)。

创建 EC2 队列

Example Corp 为其 EC2 队列创建一个具有以下配置的文件 (config.json)。

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-07b3bc7625cdab851",  
                "Version": "1"  
            },  
        }  
    ]  
}
```

```
"Overrides": [
    {
        "InstanceType": "r3.2xlarge",
        "SubnetId": "subnet-482e4972",
        "WeightedCapacity": 1
    },
    {
        "InstanceType": "r3.4xlarge",
        "SubnetId": "subnet-482e4972",
        "WeightedCapacity": 2
    },
    {
        "InstanceType": "r3.8xlarge",
        "MaxPrice": "0.90",
        "SubnetId": "subnet-482e4972",
        "WeightedCapacity": 4
    }
]
},
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
}
}
```

Example Corp 使用以下 [create-fleet](#) 命令创建 EC2 队列。

```
aws ec2 create-fleet --cli-input-json file://config.json
```

有关更多信息，请参阅 [创建 EC2 队列 \(p. 407\)](#)。

执行

分配策略确定 Spot 实例所来自的 Spot 实例池。

使用 `lowest-price` 策略（这是默认策略）时，Spot 实例来自在执行时具有最低每单位价格的池。为了提供 20 个单位的容量，EC2 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 Spot 实例来自所有三个池。EC2 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。

教程：使用 EC2 队列并将按需作为主容量

该教程使用名为 ABC Online 的虚构公司说明请求 EC2 队列并将按需作为主容量和 Spot 容量（如果可用）的过程。

目标

ABC Online 是一家餐饮送货公司，想要能够跨 EC2 实例类型和购买选项预配置 Amazon EC2 容量，以实现其预期的扩展、性能和成本。

计划

ABC Online 需要在高峰期内有固定容量运行，但也想要以较低价格增加容量，从而获益。ABC Online 确定了其 EC2 队列的以下要求：

- 一个按需实例容量 – ABC Online 需要使用 15 个按需实例，以确保它们可以处理高峰期的流量。
- Spot 实例 容量 – ABC Online 希望能够以较低的价格预配置 5 个 Spot 实例来提高性能。

验证权限

在创建 EC2 队列之前，ABC Online 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[EC2 队列先决条件 \(p. 401\)](#)。

创建 EC2 队列

ABC Online 为其 EC2 队列创建一个具有以下配置的文件 (`config.json`)。

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-07b3bc7625cdab851",  
                "Version": "2"  
            }  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 20,  
        "OnDemandTargetCapacity": 15,  
        "DefaultTargetCapacityType": "spot"  
    }  
}
```

ABC Online 使用以下 `create-fleet` 命令创建 EC2 队列。

```
aws ec2 create-fleet --cli-input-json file://config.json
```

有关更多信息，请参阅[创建 EC2 队列 \(p. 407\)](#)。

执行

分配策略确定按需容量始终得到满足，而目标容量的余额将在具有容量且可用的情况下作为 Spot 容量执行。

管理 EC2 队列

要使用 EC2 队列，请创建一个请求，其中包括总目标容量、按需容量、Spot 容量、实例的一个或多个启动规范以及您愿意支付的最高价。队列请求必须包括队列启动实例所需信息（例如 AMI、实例类型、子网或可用区、一个或多个安全组）的启动模板。您可以为愿意支付的实例类型、子网、可用区以及您愿意支付的最高价指定启动规范覆盖，而且，您可以为每个启动规范覆盖分配权重容量。

如果队列包括 Spot 实例，Amazon EC2 将尝试在 Spot 价格变化时保持队列的目标容量。

EC2 队列请求在过期或您删除它之前一直有效。在删除队列时，您可以指定删除操作是否会终止该队列中的实例。

目录

- [EC2 队列请求状态 \(p. 401\)](#)
- [EC2 队列先决条件 \(p. 401\)](#)
- [EC2 队列运行状况检查 \(p. 403\)](#)
- [生成 EC2 队列 JSON 配置文件 \(p. 404\)](#)
- [创建 EC2 队列 \(p. 407\)](#)
- [标记 EC2 队列 \(p. 410\)](#)
- [监控 EC2 队列 \(p. 400\)](#)

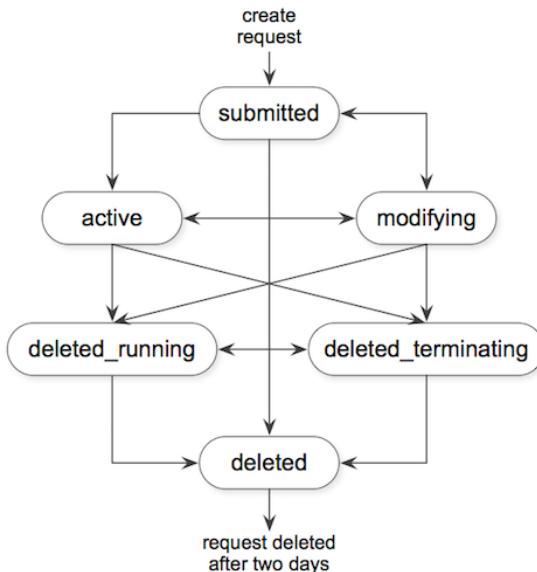
- [修改 EC2 队列 \(p. 412\)](#)
- [删除 EC2 队列 \(p. 412\)](#)
- [EC2 队列示例配置 \(p. 413\)](#)

EC2 队列请求状态

EC2 队列请求可以处于以下某种状态：

- **submitted** – 正在评估 EC2 队列请求，并且 Amazon EC2 正准备启动目标数量的实例，其中包括按需实例和/或 Spot 实例。
- **active** – 已验证 EC2 队列请求，并且 Amazon EC2 正在尝试使正在运行的实例保持目标数量。请求会保持这一状态，直到其被修改或删除。
- **modifying** – 正在修改 EC2 队列请求。请求会保持这一状态，直到修改全部完成或请求被删除。只能修改 `maintain` 请求类型。此状态不适用于其他请求类型。
- **deleted_running** – EC2 队列请求已删除且不启动其他实例。现有实例将继续运行，直至被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。
- **deleted_terminating** – EC2 队列请求已删除，且正在终止其实例。请求会保持此状态，直到所有实例都已终止。
- **deleted** – EC2 队列已删除，且没有正在运行的实例。请求将在其实例终止两天后被删除。

以下显示了 EC2 队列请求状态之间的转换。如果您超出队列限制，请求会立即被删除。



EC2 队列先决条件

要创建 EC2 队列，必须满足以下先决条件。

启动模板

启动模板包含要启动的实例的有关信息，例如，实例类型、可用区以及您愿意支付的最高价。有关更多信息，请参阅[通过启动模板启动实例 \(p. 379\)](#)。

用于 EC2 队列的服务相关角色

`AWSServiceRoleForEC2Fleet` 角色授予 EC2 队列代表您请求、启动、终止和标记实例的权限。Amazon EC2 使用此服务相关角色完成以下操作：

- `ec2:RequestSpotInstances` – 请求 Spot 实例。
- `ec2:TerminateInstances` – 终止 Spot 实例。
- `ec2:DescribeImages` – 描述 Spot 实例的 Amazon 系统映像 (AMI)。
- `ec2:DescribeInstanceStatus` – 描述 Spot 实例的状态。
- `ec2:DescribeSubnets` – 描述 Spot 实例的子网。
- `ec2:CreateTags` – 在 Spot 实例中添加系统标签。

确保此角色存在，然后才使用 AWS CLI 或 API 来创建 EC2 队列。要创建该角色，请如下使用 IAM 控制台。

为 EC2 队列创建 AWSServiceRoleForEC2Fleet 角色

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 对于 Select type of trusted entity (选择受信任实体的类型)，选择 AWS service (AWS 服务)。
4. 对于 Choose the service that will use this role (选择将使用此角色的服务)，选择 EC2 - Fleet (EC2 - 队列)，然后依次选择 Next: Permissions (下一步: 权限)、Next: Tags (下一步: 标签) 和 Next: Review (下一步: 审核)。
5. 在 Review (审核) 页面上，选择 Create role (创建角色)。

如果您不再需要使用 EC2 队列，我们建议您删除 AWSServiceRoleForEC2Fleet 角色。当此角色从您的账户中删除后，如果您创建其他队列，可再次创建此角色。

有关更多信息，请参阅 IAM 用户指南 中的 [使用服务相关角色](#)。

授予用于加密的 AMI 和 EBS 快照的 CMK 的访问权限

如果在 EC2 队列中指定[加密的 AMI \(p. 134\)](#) 或[加密的 Amazon EBS 快照 \(p. 851\)](#)，并且您使用客户托管客户主密钥 (CMK) 进行加密，则必须为 AWSServiceRoleForEC2Fleet 角色授予使用 CMK 的权限，以便 Amazon EC2 可以代表您启动实例。为此，您必须在 CMK 中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[使用授权](#)和[在 AWS KMS 中使用密钥策略](#)。

为 AWSServiceRoleForEC2Fleet 角色授予使用 CMK 的权限

- 使用 `create-grant` 命令在 CMK 中添加授权，并指定授予权限的委托人 (AWSServiceRoleForEC2Fleet 服务相关角色) 以执行授权允许的操作。CMK 是由 `key-id` 参数和 CMK 的 ARN 指定的。委托人是由 `grantee-principal` 参数和 AWSServiceRoleForEC2Fleet 服务相关角色的 ARN 指定的。

以下示例设置了相应的格式以便于阅读。

```
aws kms create-grant
--region us-east-1
--key-id arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab
--grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet
--operations "Decrypt" "Encrypt" "GenerateDataKey" "GenerateDataKeyWithoutPlaintext"
"CreateGrant" "DescribeKey" "ReEncryptFrom" "ReEncryptTo"
```

EC2 队列和 IAM 用户

如果您的 IAM 用户将创建或管理 EC2 队列，请确保为其授予所需的权限，如下所示。

向 IAM 用户授予 EC2 队列权限

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Policies。
3. 选择创建策略。
4. 在创建策略页面上，选择 JSON 选项卡，将文本替换为以下内容，并选择查看策略。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iam>ListRoles",  
                "iam:PassRole",  
                "iam>ListInstanceProfiles"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

ec2:* 为 IAM 用户授予调用所有 Amazon EC2 API 操作的权限。要将用户限制到特定 Amazon EC2 API 操作，请改为指定这些操作。

IAM 用户必须具有相应权限，可以调用 iam>ListRoles 操作以枚举现有 IAM 角色、调用 iam:PassRole 操作以指定 EC2 队列角色以及调用 iam>ListInstanceProfiles 操作以枚举现有实例配置文件。

(可选) 要使 IAM 用户能够使用 IAM 控制台创建角色或实例配置文件，您必须向该策略添加以下操作：

- iam>AddRoleToInstanceProfile
 - iam:AttachRolePolicy
 - iam>CreateInstanceProfile
 - iam>CreateRole
 - iam:GetRole
 - iam>ListPolicies
5. 在查看策略页面上，输入策略名称和描述，然后选择创建策略。
 6. 在导航窗格中，选择用户，然后选择相应用户。
 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。选择之前创建的策略，然后选择 Next: Review (下一步：查看)。
 9. 选择 Add permissions (添加权限)。

EC2 队列运行状况检查

EC2 队列每 2 分钟检查一次队列中实例的运行状况。实例的运行状况为 healthy 或 unhealthy。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 \(p. 528\)](#)。

您可以配置EC2 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。在替换运行状况不佳的实例时，队列的容量可能在几分钟内降至其目标容量之下。

要求

- 仅保持目标容量的 EC2 队列 (而非一次性队列) 支持运行状况检查替换。
- 您可以将 EC2 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。

生成 EC2 队列 JSON 配置文件

要创建 EC2 队列，只需指定启动模板、总目标容量以及默认购买选项是按需还是 Spot。如果不指定参数，队列将使用默认值。要查看队列配置参数的完整列表，可以按以下操作生成 JSON 文件。

通过命令行使用所有可能的 EC2 队列参数生成 JSON 文件

- 使用 `create-fleet` (AWS CLI) 命令和 `--generate-cli-skeleton` 参数生成 EC2 队列 JSON 文件：

```
aws ec2 create-fleet --generate-cli-skeleton
```

可用 EC2 队列参数如下：

```
{  
    "DryRun": true,  
    "ClientToken": "",  
    "SpotOptions": {  
        "AllocationStrategy": "lowest-price",  
        "InstanceInterruptionBehavior": "hibernate",  
        "InstancePoolsToUseCount": 0,  
        "SingleInstanceType": true,  
        "SingleAvailabilityZone": true,  
        "MaxTotalPrice": 0,  
        "MinTargetCapacity": 0  
    },  
    "OnDemandOptions": {  
        "AllocationStrategy": "prioritized",  
        "SingleInstanceType": true,  
        "SingleAvailabilityZone": true,  
        "MaxTotalPrice": 0,  
        "MinTargetCapacity": 0  
    },  
    "ExcessCapacityTerminationPolicy": "termination",  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "",  
                "LaunchTemplateName": "",  
                "Version": ""  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "t2.micro",  
                    "MaxPrice": "",  
                    "SubnetId": "",  
                    "AvailabilityZone": "",  
                    "WeightedCapacity": null,  
                    "Priority": null,  
                    "Placement": {  
                        "AvailabilityZone": "",  
                        "就近": null  
                    }  
                }  
            ]  
        }  
    ]  
}
```

```
        "AvailabilityZone": "",  
        "Affinity": "",  
        "GroupName": "",  
        "PartitionNumber": 0,  
        "HostId": "",  
        "Tenancy": "dedicated",  
        "SpreadDomain": ""  
    }  
}  
]  
]  
],  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 0,  
    "OnDemandTargetCapacity": 0,  
    "SpotTargetCapacity": 0,  
    "DefaultTargetCapacityType": "spot"  
},  
"TerminateInstancesWithExpiration": true,  
"Type": "maintain",  
"ValidFrom": "1970-01-01T00:00:00",  
"ValidUntil": "1970-01-01T00:00:00",  
"ReplaceUnhealthyInstances": true,  
"TagSpecifications": [  
    {  
        "ResourceType": "fleet",  
        "Tags": [  
            {  
                "Key": "",  
                "Value": ""  
            }  
        ]  
    }  
]  
}  
}
```

EC2 队列 JSON 配置文件参考

Note

请对所有参数值使用小写形式；否则，当 Amazon EC2 使用 JSON 文件启动 EC2 队列时您会收到错误消息。

AllocationStrategy (适用于 SpotOptions)

(可选) 指示如何跨由 EC2 队列指定的 Spot 实例池分配 Spot 实例目标容量。有效值为 `lowest-price` 和 `diversified`。默认为 `lowest-price`。请指定满足您的需求的分配策略。有关更多信息，请参阅 [Spot 实例的分配策略 \(p. 394\)](#)。

InstanceInterruptionBehavior

(可选) Spot 实例中断时的行为。有效值包括 `hibernate`、`stop` 和 `terminate`。默认情况下，在 Spot 实例中断时，Spot 服务终止这些实例。如果队列类型为 `maintain`，则可以指定在 Spot 实例中断时 Spot 服务休眠或停止这些实例。

InstancePoolsToUseCount

在其中分配您的目标 Spot 容量的 Spot 池数量。仅当 Spot AllocationStrategy 设置为 `lowest-price` 时有效。EC2 队列选择成本最低的 Spot 池并在您指定数量的 Spot 池之间均匀分配目标 Spot 容量。

SingleInstanceType

表示队列使用一种实例类型以启动队列中的所有 Spot 实例。

SingleAvailabilityZone

表示队列在单个可用区中启动所有 Spot 实例。

MaxTotalPrice

您愿意为 Spot 实例支付的每小时最大金额。

MinTargetCapacity

队列中的 Spot 实例的最小目标容量。如果未达到最小目标容量，则队列不会启动任何实例。

AllocationStrategy (适用于 OnDemandOptions)

在满足按需容量时使用的启动模板覆盖的顺序。如果您指定 `lowest-price`，EC2 队列将使用价格来确定顺序，价格最低的首先启动。如果您指定优先级，EC2 队列 使用您分配到各个启动模板覆盖的优先级，最高优先级的首先启动。如果您不指定值，EC2 队列默认为 `lowest-price`。

SingleInstanceType

表示队列使用一种实例类型以启动队列中的所有按需实例。

SingleAvailabilityZone

表示队列在单个可用区中启动所有按需实例。

MaxTotalPrice

您愿意为按需实例支付的每小时最大金额。

MinTargetCapacity

队列中的按需实例的最小目标容量。如果未达到最小目标容量，则队列不会启动任何实例。

ExcessCapacityTerminationPolicy

(可选) 指示当 EC2 队列的总目标容量降到 EC2 队列的当前大小以下时，是否应终止正在运行的实例。有效值为 `no-termination` 和 `termination`。

LaunchTemplateId

要使用的启动模板的 ID。您必须指定启动模板 ID 或启动模板名称。启动模板必须指定 Amazon 系统映像 (AMI)。有关创建启动模板的更多信息，请参阅[通过启动模板启动实例 \(p. 379\)](#)。

LaunchTemplateName

要使用的启动模板的名称。您必须指定启动模板 ID 或启动模板名称。启动模板必须指定 Amazon 系统映像 (AMI)。有关更多信息，请参阅[通过启动模板启动实例 \(p. 379\)](#)。

Version

启动模板的版本号。

InstanceType

(可选) 实例类型。如果输入，此值将覆盖启动模板。实例类型必须具有您所需的最低硬件规格 (vCPU、内存或存储)。

MaxPrice

(可选) 您愿意为 Spot 实例支付的每单位小时的最高价。如果输入，此值将覆盖启动模板。您可以使用默认最高价 (按需价格)，也可以指定您愿意支付的最高价。如果最高价低于指定的实例类型的 Spot 价格，则不会启动 Spot 实例。

SubnetId

(可选) 要在其中启动实例的子网的 ID。如果输入，此值将覆盖启动模板。

要创建新 VPC，请转到 Amazon VPC 控制台。完成操作后，请返回 JSON 文件并输入新子网 ID。

AvailabilityZone

(可选) 要在其中启动实例的可用区。默认由 AWS 为您的实例选择可用区。如果愿意，您可以指定特定可用区。如果输入，此值将覆盖启动模板。

指定一个或多个可用区。如果您在一个可用区中有多个子网，请指定合适的子网。要添加子网，请转至 Amazon VPC 控制台。完成操作后，请返回 JSON 文件并输入新子网 ID。

WeightedCapacity

(可选) 指定实例类型提供的单位数量。如果输入，此值将覆盖启动模板。

Priority

启动模板覆盖的优先级。如果 AllocationStrategy 设置为 prioritized，EC2 队列使用优先级来确定首先使用哪个启动模板覆盖来满足按需容量。优先级最高的首先启动。有效值为从 0 开始的整数。数字越小，优先级越高。如果未设置数字，覆盖具有最低的优先级。

TotalTargetCapacity

要启动的实例数量。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、内存或存储)。如果请求类型为 maintain，您可以指定目标容量 0 并以后添加容量。

OnDemandTargetCapacity

(可选) 要启动的按需实例的数量。此数字必须小于 TotalTargetCapacity。

SpotTargetCapacity

(可选) 要启动的 Spot 实例的数量。此数字必须小于 TotalTargetCapacity。

DefaultTargetCapacityType

如果 TotalTargetCapacity 的值高于 OnDemandTargetCapacity 和 SpotTargetCapacity 的组合值，则以此处指定的实例购买选项启动差值。有效值为 on-demand 或 spot。

TerminateInstancesWithExpiration

(可选) 默认情况下，Amazon EC2 在 EC2 队列请求过期时终止您的实例。默认值为 true。要保持这些实例在请求过期后继续运行，请不要为此参数输入值。

类型

(可选) 指示 EC2 队列通过以下三种方式之一提交请求：针对所需容量提交同步一次性请求 (instant)；针对所需容量提交异步一次性请求，但不尝试保持容量，也不会在容量不可用时向其他容量池提交请求 (request)；针对所需容量提交异步请求并通过补充中断的 Spot 实例来持续保持所需容量 (maintain)。有效值包括 instant、request 和 maintain。默认值为 maintain。有关更多信息，请参阅 [EC2 队列请求类型 \(p. 393\)](#)。

ValidFrom

(可选) 要创建仅在特定时段内有效的请求，请输入开始日期。

ValidUntil

(可选) 要创建仅在特定时段内有效的请求，请输入结束日期。

ReplaceUnhealthyInstances

(可选) 要替换配置为 maintain 队列的 EC2 队列中运行状况不佳的实例，请输入 true。否则，请将此参数留空。

TagSpecifications

(可选) 创建时标记 EC2 队列 请求的键值对。ResourceType 的值必须为 fleet，否则队列请求失败。要在启动时标记实例，请在 [启动模板 \(p. 380\)](#) 中指定标签。有关启动后标记的信息，请参阅 [标记资源 \(p. 942\)](#)。

创建 EC2 队列

在创建 EC2 队列时，您必须指定启动模板，其中包含要启动的实例的有关信息，例如，实例类型、可用区以及您愿意支付的最高价。

您可以创建一个 EC2 队列，其中包含多个覆盖启动模板的启动规范。启动规范可以有不同的实例类型、可用区、子网和最高价，并且可以包含不同的权重容量。

在创建 EC2 队列时，可以使用 JSON 文件指定要启动的实例的有关信息。有关更多信息，请参阅[EC2 队列 JSON 配置文件参考 \(p. 405\)](#)。

只能使用 AWS CLI 创建 EC2 队列。

创建 EC2 队列 (AWS CLI)

- 可以使用以下 [create-fleet](#) (AWS CLI) 命令创建 EC2 队列。

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

有关示例配置文件，请参阅[EC2 队列示例配置 \(p. 413\)](#)。

以下是 request 或 maintain 类型的队列的示例输出。

```
{  
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"  
}
```

以下是启动了目标容量的 instant 类型队列的示例输出。

```
{  
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",  
    "Errors": [],  
    "Instances": [  
        {  
            "LaunchTemplateAndOverrides": {  
                "LaunchTemplateSpecification": {  
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",  
                    "Version": "1"  
                },  
                "Overrides": {  
                    "InstanceType": "c5.large",  
                    "AvailabilityZone": "us-east-1a"  
                }  
            },  
            "Lifecycle": "on-demand",  
            "InstanceIds": [  
                "i-1234567890abcdef0",  
                "i-9876543210abcdef9"  
            ],  
            "InstanceType": "c5.large",  
            "Platform": null  
        },  
        {  
            "LaunchTemplateAndOverrides": {  
                "LaunchTemplateSpecification": {  
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",  
                    "Version": "1"  
                },  
                "Overrides": {  
                    "InstanceType": "c4.large",  
                    "AvailabilityZone": "us-east-1a"  
                }  
            },  
            "Lifecycle": "on-demand",  
            "InstanceIds": [  
                "i-5678901234abcdef0",  
                "i-5432109876abcdef9"  
            ],  
            "InstanceType": "c4.large",  
            "Platform": null  
        }  
    ]  
}
```

```
        "Platform": null
    },
]
}
```

以下是启动了部分目标容量并且出现“无法启动实例”错误的 instant 类型队列的示例输出。

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": "",
      "InstanceType": "c4.xlarge",
      "Platform": null
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
  ]
}
```

以下是未启动任何实例的 instant 类型队列的示例输出。

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {

```

```
        "InstanceType": "c4.xlarge",
        "AvailabilityZone": "us-east-1a",
    },
},
"Lifecycle": "on-demand",
"ErrorCode": "InsufficientCapacity",
"ErrorMessage": "",
"InstanceType": "c4.xlarge",
"Platform": null
},
{
"LaunchTemplateAndOverrides": {
    "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
        "Version": "1"
    },
    "Overrides": {
        "InstanceType": "c5.large",
        "AvailabilityZone": "us-east-1a",
    }
},
"Lifecycle": "on-demand",
"ErrorCode": "InsufficientCapacity",
"ErrorMessage": "",
"InstanceType": "c5.large",
"Platform": null
},
],
"Instances": []
}
```

标记 EC2 队列

要对您的 EC2 队列 请求进行分类和管理，您可使用自定义元数据为它们做标记。有关更多信息，请参阅[标记您的 Amazon EC2 资源 \(p. 940\)](#)。

您可以在创建 EC2 队列 请求时或之后为其分配标签。分配给队列请求的标签未分配给队列启动的实例。

要标记新的 EC2 队列 请求

要在创建时标记 EC2 队列 请求，请在用于创建该队列的[JSON 文件 \(p. 404\)](#)中指定键值对。`ResourceType` 的值必须为 `fleet`。如果指定其他值，队列请求失败。

要标记 EC2 队列 启动的实例

要在队列启动实例时标记这些实例，请在 EC2 队列请求中引用的[启动模板 \(p. 380\)](#)中指定标签。

标记现有 EC2 队列 请求和实例 (AWS CLI)

可以使用以下 [create-tags](#) 命令标记现有的资源。

```
aws ec2 create-tags --resources fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE i-1234567890abcdef0 --tags Key=purpose,Value=test
```

监控 EC2 队列

EC2 队列在有可用容量时启动按需实例，在最高价超过 Spot 价格并且有可用容量时启动 Spot 实例。按需实例持续运行至您将其终止，Spot 实例持续运行至遇到中断或您将其终止。

正在运行的实例的返回列表将定期刷新，或可能过时。

监控 EC2 队列 (AWS CLI)

可以使用以下 [describe-fleets](#) 命令描述 EC2 队列。

```
aws ec2 describe-fleets
```

下面是示例输出。

```
{  
    "Fleets": [  
        {  
            "Type": "maintain",  
            "FulfilledCapacity": 2.0,  
            "LaunchTemplateConfigs": [  
                {  
                    "LaunchTemplateSpecification": {  
                        "Version": "2",  
                        "LaunchTemplateId": "lt-07b3bc7625cdab851"  
                    }  
                },  
                ],  
            "TerminateInstancesWithExpiration": false,  
            "TargetCapacitySpecification": {  
                "OnDemandTargetCapacity": 0,  
                "SpotTargetCapacity": 2,  
                "TotalTargetCapacity": 2,  
                "DefaultTargetCapacityType": "spot"  
            },  
            "FulfilledOnDemandCapacity": 0.0,  
            "ActivityStatus": "fulfilled",  
            "FleetId": "fleet-76e13e99-01ef-4bd6-ba9b-9208de883e7f",  
            "ReplaceUnhealthyInstances": false,  
            "SpotOptions": {  
                "InstanceInterruptionBehavior": "terminate",  
                "InstancePoolsToUseCount": 1,  
                "AllocationStrategy": "lowest-price"  
            },  
            "FleetState": "active",  
            "ExcessCapacityTerminationPolicy": "termination",  
            "CreateTime": "2018-04-10T16:46:03.000Z"  
        }  
    ]  
}
```

可以使用以下 [describe-fleet-instances](#) 命令描述指定 EC2 队列的实例。

```
aws ec2 describe-fleet-instances --fleet-id fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE
```

```
{  
    "ActiveInstances": [  
        {  
            "InstanceId": "i-09cd595998cb3765e",  
            "InstanceHealth": "healthy",  
            "InstanceType": "m4.large",  
            "SpotInstanceRequestId": "sir-86k84j6p"  
        },  
        {  
            "InstanceId": "i-09cf95167ca219f17",  
            "InstanceHealth": "healthy",  
            "InstanceType": "m4.large",  
            "SpotInstanceRequestId": "sir-dvxi7fsm"  
        }  
    ],  
    "FleetId": "fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

可以使用以下 `describe-fleet-history` 命令描述指定 EC2 队列在指定时间内的历史记录。

```
aws ec2 describe-fleet-history --fleet-request-id fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2018-04-10T00:00:00Z
```

```
{  
    "HistoryRecords": [],  
    "FleetId": "fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE",  
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",  
    "StartTime": "2018-04-09T23:53:20.000Z"  
}
```

修改 EC2 队列

您可以修改处于 `submitted` 或 `active` 状态的 EC2 队列。当您修改队列时，它会进入 `modifying` 状态。

您可以修改 EC2 队列的以下参数：

- `target-capacity-specification` – 增加或减少 `TotalTargetCapacity`、`OnDemandTargetCapacity` 和 `SpotTargetCapacity` 的目标容量。
- `excess-capacity-termination-policy` – 当 EC2 队列的总目标容量降到队列的当前大小以下时是否应终止正在运行的实例。有效值为 `no-termination` 和 `termination`。

Note

您只能修改 `Type=maintain` 的 EC2 队列。

如果提升目标容量，EC2 队列会根据为 `DefaultTargetCapacityType` 指定的实例购买选项（按需实例或 Spot 实例）启动额外的实例。

如果 `DefaultTargetCapacityType` 为 `spot`，EC2 队列会根据其分配策略启动额外的 Spot 实例。如果分配策略为 `lowest-price`，队列将从请求中价格最低的 Spot 实例池启动实例。如果分配策略为 `diversified`，队列将在请求中的池间分配实例。

在减少目标容量时，EC2 队列会删除超过新目标容量的任何打开的请求。您可以请求队列终止实例，直到队列的大小达到新目标容量。如果分配策略是 `lowest-price`，则队列会终止每单位价格最高的实例。如果分配策略是 `diversified`，则队列会在池间终止实例。或者，您可以请求 EC2 队列保持队列当前的队列大小，而不替换已中断的 Spot 实例或者您手动终止的任何实例。

当 EC2 队列因目标容量下降而终止某个 Spot 实例时，该实例将收到一条 Spot 实例中断通知。

修改 EC2 队列 (AWS CLI)

可以使用以下 `modify-fleet` 命令更新指定 EC2 队列的目标容量。

```
aws ec2 modify-fleet --fleet-id fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity-specification TotalTargetCapacity=20
```

如果要减少目标容量，但希望保持队列的当前大小，您可以按如下方式修改上面的命令。

```
aws ec2 modify-fleet --fleet-id fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity-specification TotalTargetCapacity=10 --excess-capacity-termination-policy no-termination
```

删除 EC2 队列

如果您不再需要某一 EC2 队列，可以将其删除。在删除队列后，它不会再启动新实例。

您必须指定 EC2 队列是否必须终止其实例。如果您指定在队列删除后必须终止实例，队列会进入 deleted_terminating 状态。否则，队列会进入 deleted_running 状态，并且实例会继续运行，直到遇到中断或您手动将其终止。

删除 EC2 队列 (AWS CLI)

可以使用 `delete-fleets` 命令和 `--terminate-instances` 参数删除指定的 EC2 队列并终止实例。

```
aws ec2 delete-fleets --fleet-ids fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --terminate-instances
```

下面是示例输出。

```
{  
    "UnsuccessfulFleetDeletions": [],  
    "SuccessfulFleetDeletions": [  
        {  
            "CurrentFleetState": "deleted_terminating",  
            "PreviousFleetState": "active",  
            "FleetId": "fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE"  
        }  
    ]  
}
```

您可以使用 `--no-terminate-instances` 参数修改上面的命令，以删除指定的 EC2 队列而不终止实例。

```
aws ec2 delete-fleets --fleet-ids fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --no-terminate-instances
```

下面是示例输出。

```
{  
    "UnsuccessfulFleetDeletions": [],  
    "SuccessfulFleetDeletions": [  
        {  
            "CurrentFleetState": "deleted_running",  
            "PreviousFleetState": "active",  
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"  
        }  
    ]  
}
```

EC2 队列示例配置

下列示例显示了可与 `create-fleet` 命令结合使用以创建 EC2 队列的启动配置。有关 `create-fleet` 参数的更多信息，请参阅[EC2 队列 JSON 配置文件参考 \(p. 405\)](#)。

示例

- 示例 1：启动 Spot 实例作为默认购买选项 (p. 414)
- 示例 2：启动 按需实例作为默认购买选项 (p. 414)
- 示例 3：启动按需实例作为主容量 (p. 414)
- 示例 4：使用最低价分配策略启动 Spot 实例 (p. 415)
- 示例 5：使用容量预留和优先分配策略启动 按需实例 (p. 415)
- 示例 6：当总目标容量大于未使用的 容量预留 数时，使用 容量预留 和优先分配策略启动 按需实例 (p. 417)
- 示例 7：使用容量预留和最低价格分配策略启动 按需实例 (p. 419)

- [示例 8：当总目标容量大于未使用的 容量预留 数时，使用容量预留和最低价格分配策略启动 按需实例 \(p. 421\)](#)

示例 1：启动 Spot 实例作为默认购买选项

下面的示例指定了 EC2 队列中所需的最少参数：启动模板、目标容量和默认购买选项。启动模板由其启动模板 ID 和版本号标识。队列的目标容量为 2 个实例，默认购买选项为 spot，因此队列启动两个 Spot 实例。

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 2,  
        "DefaultTargetCapacityType": "spot"  
    }  
}
```

示例 2：启动 按需实例作为默认购买选项

下面的示例指定了 EC2 队列中所需的最少参数：启动模板、目标容量和默认购买选项。启动模板由其启动模板 ID 和版本号标识。队列的目标容量为 2 个实例，默认购买选项为 on-demand，因此队列启动两个按需实例。

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 2,  
        "DefaultTargetCapacityType": "on-demand"  
    }  
}
```

示例 3：启动按需实例作为主容量

下面的示例为队列指定两个实例的总目标容量和 1 个按需实例的目标容量。默认购买选项为 spot。队列按照指定的方式启动 1 个按需实例，但需要再启动一个实例以满足总目标容量要求。差值的购买选项是通过 `TotalTargetCapacity - OnDemandTargetCapacity = DefaultTargetCapacityType` 计算的，这使得队列启动 1 个 Spot 实例。

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
        }  
    ]
```

```
        },
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

示例 4：使用最低价分配策略启动 Spot 实例

如果未指定 Spot 实例的分配策略，则使用默认分配策略 `lowest-price`。以下示例使用 `lowest-price` 分配策略。覆盖启动模板的三个启动规范有不同的实例类型，但有相同的权重容量和子网。总目标容量为两个实例，默认购买选项为 `spot`。EC2 队列按启动规范的最低价格实例类型启动两个 Spot 实例。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
        },
        {
            "Overrides": [
                {
                    "InstanceType": "c4.large",
                    "WeightedCapacity": 1,
                    "SubnetId": "subnet-a4f6c5d3"
                },
                {
                    "InstanceType": "c3.large",
                    "WeightedCapacity": 1,
                    "SubnetId": "subnet-a4f6c5d3"
                },
                {
                    "InstanceType": "c5.large",
                    "WeightedCapacity": 1,
                    "SubnetId": "subnet-a4f6c5d3"
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

示例 5：使用容量预留和优先分配策略启动 按需实例

可以通过将 `容量预留` 的使用策略配置为 `use-capacity-reservations-first` 来将队列配置为在启动按需实例时首先使用按需容量预留。此外，如果多个实例池具有未使用的容量预留，则应用选定的按需分配策略。在该示例中，按需分配策略为 `prioritized`。

在该示例中，有 15 个可用的未使用容量预留。此数目超过了队列的 12 个按需实例的按需容量。

账户在 3 个不同的池中有以下 15 个未使用的容量预留。每个池中的容量预留数由 `AvailableInstanceCount` 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c4.large",
    "InstancePlatform": "Linux/UNIX",
```

```
        "AvailabilityZone": "us-east-1a",
        "AvailableInstanceCount": 5,
        "InstanceMatchCriteria": "open",
        "State": "active"
    }

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c3.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

以下队列配置仅显示该示例的相关配置。按需分配策略为 `prioritized`，容量预留的使用策略为 `use-capacity-reservations-first`。总目标容量为 12，而默认目标容量类型为 `on-demand`。

Note

队列类型必须为 `instant`。其他队列类型不支持容量预留。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-1234567890abcdefg",
                "Version": "1"
            }
            "Overrides": [
                {
                    "InstanceType": "c4.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 1.0
                },
                {
                    "InstanceType": "c3.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 2.0
                },
                {
                    "InstanceType": "c5.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 3.0
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

```
},
"OnDemandOptions": {
    "AllocationStrategy": "prioritized"
    "CapacityReservationOptions": {
        "UsageStrategy": "use-capacity-reservations-first"
    }
},
"Type": "instant",
}
```

在使用上述配置创建 instant 队列后，将启动下面的 12 个实例来满足目标容量：

- us-east-1a 中的 5 个 c4.large 按需实例 – us-east-1a 中的 c4.large 的优先级第一，并且有 5 个可用的未使用的容量预留
- us-east-1a 中的 5 个 c3.large 按需实例 – us-east-1a 中的 c3.large 的优先级第二，并且有 5 个可用的未使用的 c3.large 容量预留
- us-east-1a 中的 2 个 c5.large 按需实例 – us-east-1a 中的 c5.large 的优先级第三，并且有 5 个可用的未使用的 c5.large 容量预留，只需其中的 2 个即可满足目标容量

在启动队列后，您可以运行 [describe-capacity-reservations](#) 来查看保留的未使用的容量预留的数目。在此示例中，您该看到以下响应，该响应指示已使用所有 c4.large 和 c3.large 容量预留，有 3 个 c5.large 容量预留未使用。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c4.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c3.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 3
}
```

示例 6：当总目标容量大于未使用的容量预留数时，使用容量预留和优先分配策略启动按需实例

可以通过将容量预留的使用策略配置为 `use-capacity-reservations-first` 来将队列配置为在启动按需实例时首先使用按需容量预留。此外，如果未使用的容量预留数少于按需目标容量，则将根据选定的按需分配策略启动剩余的按需目标容量。在该示例中，按需分配策略为 `prioritized`。

在该示例中，有 15 个可用的未使用容量预留。此数目少于队列的 16 个按需实例的按需目标容量。

账户在 3 个不同的池中有以下 15 个未使用的容量预留。每个池中的容量预留数由 `AvailableInstanceCount` 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c4.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}

{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c3.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

以下队列配置仅显示该示例的相关配置。按需分配策略为 prioritized，容量预留的使用策略为 use-capacity-reservations-first。总目标容量为 16，而默认目标容量类型为 on-demand。

Note

队列类型必须为 instant。其他队列类型不支持容量预留。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                    "InstanceType": "c4.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 1.0
                },
                {
                    "InstanceType": "c3.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 2.0
                },
                {
                    "InstanceType": "c5.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1,
                    "Priority": 3.0
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized"
    }
}
```

```
"CapacityReservationOptions": {  
    "UsageStrategy": "use-capacity-reservations-first"  
}  
,  
"Type": "instant",  
}
```

在使用上述配置创建 instant 队列后，将启动下面的 16 个实例来满足目标容量：

- us-east-1a 中的 6 个 c4.large 按需实例 – us-east-1a 中的 c4.large 的优先级第一，并且有 5 个可用的未使用的容量预留。首先使用容量预留启动 5 个按需实例，并根据按需分配策略（此示例中为 prioritized）启动另一个按需实例。
- us-east-1a 中的 5 个 c3.large 按需实例 – us-east-1a 中的 c3.large 的优先级第二，并且有 5 个可用的未使用的 c3.large 容量预留
- us-east-1a 中的 5 个 c5.large 按需实例 – us-east-1a 中的 c5.large 的优先级第三，并且有 5 个可用的未使用的 c5.large 容量预留

在启动队列后，您可以运行 [describe-capacity-reservations](#) 来查看保留的未使用的容量预留的数目。在此示例中，您应看到以下响应，该响应指示所有池中的所有容量预留均已使用。

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "c4.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "c3.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "c5.large",  
    "AvailableInstanceCount": 0  
}
```

示例 7：使用容量预留和最低价格分配策略启动按需实例

可以通过将容量预留的使用策略配置为 `use-capacity-reservations-first` 来将队列配置为在启动按需实例时首先使用按需容量预留。此外，如果多个实例池具有未使用的容量预留，则应用选定的按需分配策略。在该示例中，按需分配策略为 `lowest-price`。

在该示例中，有 15 个可用的未使用容量预留。此数目超过了队列的 12 个按需实例的按需容量。

账户在 3 个不同的池中有以下 15 个未使用的容量预留。每个池中的容量预留数由 `AvailableInstanceCount` 指示。

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m5.large",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m5.large",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}
```

```
"InstanceType": "m4.xlarge",
"InstancePlatform": "Linux/UNIX",
"AvailabilityZone": "us-east-1a",
"AvailableInstanceCount": 5,
"InstanceMatchCriteria": "open",
"State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

以下队列配置仅显示该示例的相关配置。按需分配策略为 `lowest-price`，容量预留的使用策略为 `use-capacity-reservations-first`。总目标容量为 12，而默认目标容量类型为 `on-demand`。

在此示例中，个按需实例 价格为：

- m5.large – 每小时 0.096 美元
- m4.xlarge – 每小时 0.20 美元
- m4.2xlarge – 每小时 0.40 美元

Note

队列类型必须为 `instant`。其他队列类型不支持 容量预留。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
        },
        "Overrides": [
            {
                "InstanceType": "m5.large",
                "AvailabilityZone": "us-east-1a",
                "WeightedCapacity": 1
            },
            {
                "InstanceType": "m4.xlarge",
                "AvailabilityZone": "us-east-1a",
                "WeightedCapacity": 1
            },
            {
                "InstanceType": "m4.2xlarge",
                "AvailabilityZone": "us-east-1a",
                "WeightedCapacity": 1
            }
        ]
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    }
},
```

```
"OnDemandOptions": {  
    "AllocationStrategy": "lowest-price"  
    "CapacityReservationOptions": {  
        "UsageStrategy": "use-capacity-reservations-first"  
    }  
},  
"Type": "instant",  
}
```

在使用上述配置创建 instant 队列后，将启动下面的 12 个实例来满足目标容量：

- us-east-1a 中的 5 个 m5.large 按需实例 – us-east-1a 中的 m5.large 的价格最低，并且有 5 个可用的未使用的容量预留
- us-east-1a 中的 5 个 m4.large 按需实例 – us-east-1a 中的 m4.large 的价格第二低，并且有 5 个可用的未使用的 c3.large 容量预留
- us-east-1a 中的 2 个 m4.2xlarge 按需实例 – us-east-1a 中的 m4.2xlarge 的价格第三低，并且有 5 个可用的未使用的 c5.large 容量预留，只需其中的 2 个即可满足目标容量

在启动队列后，您可以运行 [describe-capacity-reservations](#) 来查看保留的未使用的容量预留的数目。在此示例中，您应看到以下响应，该响应指示已使用所有 m5.large 和 m4.xlarge 容量预留，有 3 个 m4.2xlarge 容量预留未使用。

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m4.xlarge",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m4.2xlarge",  
    "AvailableInstanceCount": 3  
}
```

示例 8：当总目标容量大于未使用的容量预留数时，使用容量预留和最低价格分配策略启动按需实例

可以通过将容量预留的使用策略配置为 `use-capacity-reservations-first` 来将队列配置为在启动按需实例时首先使用按需容量预留。此外，如果未使用的容量预留数少于按需目标容量，则将根据选定的按需分配策略启动剩余的按需目标容量。在该示例中，按需分配策略为 `lowest-price`。

在该示例中，有 15 个可用的未使用容量预留。此数目少于队列的 16 个按需实例的按需目标容量。

账户在 3 个不同的池中有以下 15 个未使用的容量预留。每个池中的容量预留数由 `AvailableInstanceCount` 指示。

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"
```

```
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

以下队列配置仅显示该示例的相关配置。按需分配策略为 `lowest-price`，容量预留的使用策略为 `use-capacity-reservations-first`。总目标容量为 16，而默认目标容量类型为 `on-demand`。

在此示例中，个按需实例 价格为：

- m5.large – 每小时 0.096 美元
- m4.xlarge – 每小时 0.20 美元
- m4.2xlarge – 每小时 0.40 美元

Note

队列类型必须为 `instant`。其他队列类型不支持 容量预留。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                    "InstanceType": "m5.large",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "m4.xlarge",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1
                }
            ]
        }
    ],
}
```

```
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 16,  
    "DefaultTargetCapacityType": "on-demand"  
},  
"OnDemandOptions": {  
    "AllocationStrategy": "lowest-price"  
    "CapacityReservationOptions": {  
        "UsageStrategy": "use-capacity-reservations-first"  
    }  
},  
"Type": "instant",  
}
```

在使用上述配置创建 instant 队列后，将启动下面的 16 个实例来满足目标容量：

- us-east-1a 中的 6 个 m5.large 按需实例 – us-east-1a 中的 m5.large 的价格最低，并且有 5 个可用的未使用的容量预留。首先使用容量预留启动 5 个按需实例，并根据按需分配策略（此示例中为 lowest-price）启动另一个按需实例。
- us-east-1a 中的 5 个 m4.large 按需实例 – us-east-1a 中的 m4.large 的价格第二低，并且有 5 个可用的未使用的 c3.large 容量预留
- us-east-1a 中的 5 个 m4.2xlarge 按需实例 – us-east-1a 中的 m4.2xlarge 的价格第三低，并且有 5 个可用的未使用的 c5.large 容量预留

在启动队列后，您可以运行 [describe-capacity-reservations](#) 来查看保留的未使用的容量预留的数目。在此示例中，您应看到以下响应，该响应指示所有池中的所有容量预留均已使用。

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m4.xlarge",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m4.2xlarge",  
    "AvailableInstanceCount": 0  
}
```

连接到 Linux 实例

连接到您启动的 Linux 实例，并在本地计算机和实例之间传输文件。

要连接到 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](#)。

连接方法

本地计算机的操作系统决定了用于连接到 Linux 实例的方法类型。

本地计算机	可用的连接方法
Linux 或 macOS X	SSH 客户端 (p. 426)

本地计算机	可用的连接方法
	EC2 Instance Connect (p. 428) AWS Systems Manager 会话管理器
Windows	PuTTY (p. 436) 适用于 Linux 的 Windows 子系统 (p. 441) SSH 客户端 (p. 426) AWS Systems Manager 会话管理器

Amazon EC2 控制台提供了一个选项，以使用 Java SSH 客户端直接从浏览器连接到实例。但是，许多浏览器不再支持此功能。有关更多信息，请参阅[无法使用我的浏览器进行连接 \(p. 961\)](#)。

在连接到 Linux 实例后，您可以尝试阅读我们的教程之一，例如，教程：[使用 Amazon Linux AMI 安装 LAMP Web 服务器 \(p. 37\)](#)或[教程：使用 Amazon Linux 托管 WordPress 博客 \(p. 47\)](#)。

连接到您的实例的常规先决条件

在连接到您的 Linux 实例之前，请确认以下常规先决条件：

- [获取有关您的实例的信息 \(p. 424\)](#)
- [启用您的实例的入站流量 \(p. 425\)](#)
- [查找私有密钥 \(p. 425\)](#)
- (可选) [获取实例指纹 \(p. 425\)](#)

获取有关您的实例的信息

- 获得实例的 ID.

您可以通过使用 Amazon EC2 控制台获得您的实例的 ID (位于 Instance ID (实例 ID) 列中)。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。

可使用 Amazon EC2 控制台获取实例的公有 DNS。选中 Public DNS (IPv4) (公有 DNS (IPv4)) 列。如果此列已隐藏，请选择 Show/Hide (显示/隐藏) 图标，然后选择 Public DNS (IPv4) (公有 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。可以使用 Amazon EC2 控制台获取实例的 IPv6 地址。选中 IPv6 IPs (IPv6 IP) 字段。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 \(p. 576\)](#)。

- 获取用于启动实例的 AMI 的默认用户名：

- 对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。
- 对于 CentOS AMI，用户名是 `centos`。
- 对于 Debian AMI，用户名是 `admin` 或 `root`。
- 对于 Fedora AMI，用户名为 `ec2-user` 或 `fedora`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。

- 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名是 `ubuntu`。
- 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。

启用您的实例的入站流量

- 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。默认情况下，VPC 的默认安全组不允许传入 SSH 流量。默认情况下，启动实例向导创建的安全组支持 SSH 流量。有关更多信息，请参阅 [为您的 Linux 实例授权入站流量 \(p. 757\)](#)。

查找私有密钥

- 查找私有密钥并验证权限

获取您在启动实例时指定的密钥对的 `.pem` 文件在您电脑上位置的完全限定路径。有关如何创建密钥对的更多信息，请参阅 [使用 Amazon EC2 创建密钥对](#)。

确保 `.pem` 文件具有权限 0400 而不是 0777。有关更多信息，请参阅 [错误：未保护的私钥文件 \(p. 959\)](#)。

设置私有密钥的权限

1. 在命令行 shell 中，转到在启动实例时创建的私有密钥文件的目录位置。
2. 使用以下命令设置您的私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 /path/my-key-pair.pem
```

如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅 [错误：未保护的私钥文件 \(p. 959\)](#)。

(可选) 获取实例指纹

若要防范中间人攻击，您在连接您的实例时可以验证 RSA 密钥指纹。如果您从第三方的公用 AMI 启动了实例，则验证指纹将很有用。

首先获取实例指纹。然后，当您连接实例时，将会提示您验证指纹。您可以将您已获取的指纹与显示的指纹进行比较来实施验证。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。如果二者匹配，则您可以放心地连接到您的实例。

获取实例指纹的先决条件：

- 要获取实例指纹，您必须使用 AWS CLI。有关安装 AWS CLI 的信息，请参阅 [AWS Command Line Interface 用户指南 中的安装 AWS 命令行界面](#)。
- 该实例必须处于 `running` 状态而不是 `pending` 状态。

获取实例指纹

1. 在您的本地计算机（并非实例）上，使用 `get-console-output` (AWS CLI) 命令获取指纹，如下所示：

```
$ aws ec2 get-console-output --instance-id instance_id
```

以下是怎样应查找的内容的示例：

```
-----BEGIN SSH HOST KEY FINGERPRINTS -----  
... 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f ...  
-----END SSH HOST KEY FINGERPRINTS-----
```

2. 在生成的输出中，找到 SSH HOST KEY FINGERPRINTS 部分并记录下 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）。SSH HOST KEY FINGERPRINTS 部分仅在实例首次启动之后可用。

使用 SSH 连接到 Linux 实例

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实例时收到错误，请参阅 [排查实例的连接问题 \(p. 955\)](#)。

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 页上的 Status Checks 列中查看此信息。

先决条件

在连接到 Linux 实例之前，请先完成以下先决条件：

- 验证有关连接到您的实例的常规先决条件。
[有关更多信息，请参阅 连接到您的实例的常规先决条件 \(p. 424\)](#)。
- 在您的本地计算机上安装 SSH 客户端。

您的本地计算机很可能已默认安装 SSH 客户端。您可以通过在命令行键入 ssh 来检查 SSH 客户端。如果您的本地计算机无法识别该命令，您可安装 SSH 客户端。有关在 Linux 或 macOS X 上安装 SSH 客户端的信息，请参阅 <http://www.openssh.com>。有关在 Windows 10 上安装 SSH 客户端的信息，请参阅 [Windows 中的 OpenSSH](#)。

使用 SSH 客户端连接到 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实例时收到错误，请参阅 [排查实例的连接问题 \(p. 955\)](#)。

使用 SSH 连接到您的实例

- 在终端窗口中，使用 ssh 命令连接到该实例。您可以指定私有密钥 (.pem) 文件、AMI 的用户名以及实例的公有 DNS 名称。例如，如果您使用了 Amazon Linux 2 或 Amazon Linux AMI，则用户名为 ec2-user。有关查找 AMI 的用户名和实例的 DNS 名称的更多信息，请参阅 [获取有关您的实例的信息 \(p. 424\)](#)。

```
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)?
```

2. (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、适当的用户名和 IPv6 地址。例如 , 如果您使用了 Amazon Linux 2 或 Amazon Linux AMI , 则用户名为 ec2-user。

```
ssh -i /path/my-key-pair.pem ec2-user@2001:db8:1234:1a00:9691:9503:25ad:1761
```

3. (可选) 验证安全警报中的指纹是否与您之前在 [\(可选\) 获取实例指纹 \(p. 425\)](#) 中获得的指纹相匹配。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。
4. 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协议 (SCP)。本节介绍了如何使用 SCP 传输文件。该步骤与使用 SSH 连接到实例的步骤类似。

先决条件

- 验证有关将文件传输到您的实例的常规先决条件。

将文件传输到实例的常规先决条件与连接到实例的常规先决条件相同。有关更多信息 , 请参阅 [连接到您的实例的常规先决条件 \(p. 424\)](#)。

- 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。有关更多信息 , 请参阅 <http://www.openssh.org>。

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. 使用实例的公有 DNS 名称将文件传输到您的实例。例如 , 如果私有密钥文件的名称是 my-key-pair、要传输的文件是 SampleFile.txt、用户名是 ec2-user、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:~
```

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)?
```

2. (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@
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~
```

3. (可选) 验证安全警报中的指纹是否与您之前在 [\(可选\) 获取实例指纹 \(p. 425\)](#) 中获得的指纹相匹配。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。
4. 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
```

如果您收到“bash: scp: command not found (bash: scp: 命令未找到)”错误，您必须先在 Linux 实例上安装 scp。对于某些操作系统，该命令会位于 `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
```

5. 要反方向传输文件（从 Amazon EC2 实例中传输到本地计算机），请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
```

6. （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 EC2 Instance Connect 连接到 Linux 实例

Amazon EC2 Instance Connect 提供了一种简单且安全的方法以使用安全 Shell (SSH) 连接到实例。通过使用 EC2 Instance Connect，您可以使用 AWS Identity and Access Management (IAM) 策略和委托人控制对实例的 SSH 访问，从而无需共享和管理 SSH 密钥。使用 EC2 Instance Connect 的所有连接请求将[记录到 AWS CloudTrail 中，以便您可以审核连接请求 \(p. 572\)](#)。

您可以使用 Instance Connect 通过基于浏览器的客户端、Amazon EC2 Instance Connect CLI 或您选择的 SSH 客户端连接到 Linux 实例。

在使用 EC2 Instance Connect 连接到实例时，Instance Connect API 将一次性使用的 SSH 公有密钥推送到[实例元数据 \(p. 499\)](#)，将在其中保留 60 秒。附加到 IAM 用户的 IAM 策略授权 IAM 用户将公有密钥推送到实例元数据。SSH 守护程序使用在安装 Instance Connect 时配置的 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser`，从实例元数据中查找公有密钥以进行身份验证，并将您连接到实例。

Note

如果从运行 Windows 的本地计算机中连接到 Linux 实例，请参阅以下文档：[使用 PuTTY 从 Windows 连接到 Linux 实例 \(p. 436\)](#) 和 [使用 Windows Subsystem for Linux 从 Windows 连接到 Linux 实例 \(p. 441\)](#)。

目录

- [设置 EC2 Instance Connect \(p. 429\)](#)
- [使用 EC2 Instance Connect 进行连接 \(p. 433\)](#)
- [卸载 EC2 Instance Connect \(p. 435\)](#)

设置 EC2 Instance Connect

Amazon Linux 2 2.0.20190618 或更高版本预配置了 EC2 Instance Connect。对于支持的其他 Linux 发行版，您必须为将支持使用 Instance Connect 的每个实例设置 Instance Connect。这是每个实例的一次性要求。

用于设置 Instance Connect 的任务

- [步骤 1：配置对实例的网络访问 \(p. 429\)](#)
- [步骤 1：在实例上安装 EC2 Instance Connect \(p. 430\)](#)
- [步骤 3：\(可选 \) 安装 EC2 Instance Connect CLI \(p. 432\)](#)
- [步骤 4：为 EC2 Instance Connect 配置 IAM 权限 \(p. 432\)](#)

限制

- 支持以下 Linux 发行版：
 - Amazon Linux 2 (任何版本)
 - Ubuntu 16.04 或更高版本
- 如果为 SSH 身份验证配置了 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser` 设置，则 EC2 Instance Connect 安装不会更新它们。因此，您无法使用 Instance Connect。
- EC2 Instance Connect 仅与 实例元数据服务版本 1 一起使用。如果将实例元数据服务配置为要求使用 实例元数据服务版本 2，则无法使用 EC2 Instance Connect。有关更多信息，请参阅[配置实例元数据服务 \(p. 499\)](#)。

先决条件

- 确认满足使用 SSH 连接到实例的一般先决条件。
[有关更多信息，请参阅 连接到您的实例的常规先决条件 \(p. 424\)。](#)
- 在您的本地计算机上安装 SSH 客户端。

您的本地计算机很可能已默认安装 SSH 客户端。您可以通过在命令行键入 `ssh` 来检查 SSH 客户端。如果您的本地计算机无法识别该命令，您可安装 SSH 客户端。有关在 Linux 或 macOS X 上安装 SSH 客户端的信息，请参阅 <http://www.openssh.com>。有关在 Windows 10 上安装 SSH 客户端的信息，请参阅 [Windows 中的 OpenSSH](#)。

- 在本地计算机上安装 AWS CLI。

要配置 IAM 权限，您必须使用 AWS CLI。有关安装 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南 中的[安装 AWS CLI](#)。

- [Ubuntu] 在实例上安装 AWS CLI。

要在 Ubuntu 实例上安装 EC2 Instance Connect，您必须在实例上使用 AWS CLI。有关安装 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南 中的[安装 AWS CLI](#)。

步骤 1：配置对实例的网络访问

您必须配置对实例的以下网络访问权限，以便可以安装 EC2 Instance Connect 并允许用户连接到实例：

- 确保与您实例关联的安全组[允许来自您 IP 地址端口 22 上的传入 SSH 流量 \(p. 758\)](#)。默认情况下，VPC 的默认安全组不允许传入 SSH 流量。默认情况下，由启动向导创建的安全组允许传入的 SSH 流量。有关更多信息，请参阅[为您的 Linux 实例授权入站流量 \(p. 757\)](#)。
- (基于浏览器的客户端) 我们建议实例允许来自以下位置的入站 SSH 流量：[为该服务发布的建议 IP 块](#)。在 `service` 参数中使用 `EC2_INSTANCE_CONNECT` 筛选条件以获取 EC2 Instance Connect 子集中的 IP 地址范围。有关更多信息，请参阅 Amazon Web Services 一般参考 中的[AWS IP 地址范围](#)。

步骤 1：在实例上安装 EC2 Instance Connect

安装 EC2 Instance Connect 将在实例上配置 SSH 守护程序。对于使用 Amazon Linux 2 和 Ubuntu 启动的实例，安装 EC2 Instance Connect 的过程是不同的。

Amazon Linux 2

在使用 Amazon Linux 2 启动的实例上安装 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。

可以使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名。对于 Amazon Linux 2，默认用户名是 `ec2-user`。

例如，如果实例是使用 Amazon Linux 2 启动的，实例的公有 DNS 是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

有关连接到实例的更多信息，请参阅[使用 SSH 连接到 Linux 实例 \(p. 426\)](#)。

2. 在实例上安装 EC2 Instance Connect 程序包。

对于 Amazon Linux 2，请使用 `yum install` 命令。

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

将会在 `/opt/aws/bin/` 文件夹中看到四个新文件：

```
eic_curlAuthorizedKeys  
eic_harvestHostkeys  
eic_parseAuthorizedKeys  
eic_runAuthorizedKeys
```

3. (可选) 验证是否在实例上成功安装了 Instance Connect。

可以使用 `sudo less` 命令检查是否正确更新了 `/etc/ssh/sshd_config` 文件，如下所示：

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

如果 `/etc/ssh/sshd_config` 文件中的 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser` 行包含以下值，则成功安装了 Instance Connect：

```
AuthorizedKeysCommand /opt/aws/bin/eic_runAuthorizedKeys %u %f  
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` 设置 `eic_runAuthorizedKeys` 文件以从实例元数据中查找密钥
- `AuthorizedKeysCommandUser` 将系统用户设置为 `ec2-instance-connect`

Note

如果以前配置了 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser`，则 Instance Connect 安装不会更改这些值，并且您无法使用 Instance Connect。

Ubuntu

在使用 Ubuntu 16.04 或更高版本启动的实例上安装 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。

可以使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名。对于 Ubuntu AMI，用户名是 `ubuntu`。

如果实例是使用 Ubuntu 启动的，实例的公有 DNS 是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

有关连接到实例的更多信息，请参阅[使用 SSH 连接到 Linux 实例 \(p. 426\)](#)。

2. (可选) 确保您的实例具有最新 Ubuntu AMI。

对于 Ubuntu，使用 `apt-get update` 命令更新实例上的所有程序包。

```
ubuntu:~$ sudo apt-get update
```

3. 在实例上安装 Instance Connect 程序包。

对于 Ubuntu，请使用 `sudo apt-get install` 命令安装 `.deb` 程序包。

```
ubuntu:~$ sudo apt-get install ec2-instance-connect
```

将会在 `/usr/share/ec2-instance-connect/` 文件夹中看到四个新文件：

```
eic_curlAuthorizedKeys  
eic_harvestHostkeys  
eic_parseAuthorizedKeys  
eic_runAuthorizedKeys
```

4. (可选) 验证是否在实例上成功安装了 Instance Connect。

可以使用 `sudo less` 命令检查是否正确更新了 `/lib/systemd/system/ssh.service.d/ec2-instance-connect.conf`，如下所示：

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

如果 `/lib/systemd/system/ssh.service.d/ec2-instance-connect.conf` 文件中的 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser` 行包含以下值，则成功安装了 Instance Connect：

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_runAuthorizedKeys %u %f  
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` 设置 `eic_runAuthorizedKeys` 文件以从实例元数据中查找密钥
- `AuthorizedKeysCommandUser` 将系统用户设置为 `ec2-instance-connect`

Note

如果以前配置了 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser`，则 Instance Connect 安装不会更改这些值，并且您无法使用 Instance Connect。

有关 EC2 Instance Connect 程序包的更多信息，请参阅 GitHub 网站上的 [aws/aws-ec2-instance-connect-config](#)。

步骤 3：(可选) 安装 EC2 Instance Connect CLI

EC2 Instance Connect CLI 提供与标准 SSH 调用类似的界面，包括查询 EC2 实例信息，生成和发布临时公有密钥以及通过单个命令 (`mssh instance_id`) 建立 SSH 连接。

Note

如果用户仅使用基于浏览器的客户端或 SSH 客户端连接到实例，则无需安装 EC2 Instance Connect CLI。

安装 EC2 Instance Connect CLI 程序包

使用 `pip` 安装 `ec2instanceconnectcli` 程序包。有关更多信息，请参阅 GitHub 网站上的 [aws/aws-ec2-instance-connect-cli](#)，以及 Python Package Index (PyPI) 网站上的 <https://pypi.org/project/ec2instanceconnectcli/>。

```
$ pip install ec2instanceconnectcli
```

步骤 4：为 EC2 Instance Connect 配置 IAM 权限

如果 IAM 用户将使用 EC2 Instance Connect 连接到实例，您必须为其授予将公有密钥推送到实例的权限。有关更多信息，请参阅 IAM 用户指南 中的 [Amazon EC2 Instance Connect 的操作、资源和条件键](#)。

以下说明介绍如何使用 AWS CLI 创建并附加策略。有关如何使用 AWS 管理控制台的说明，请参阅 IAM 用户指南 中的 [创建 IAM 策略 \(控制台 \)](#) 和 [将策略直接附加到用户以添加权限](#)。

限制

对于 Instance Connect，我们目前不支持基于标签的授权。

为 IAM 用户授予 EC2 Instance Connect (AWS CLI) 权限

1. 创建一个 JSON 策略文档，其中包含以下内容：

- `ec2-instance-connect:SendSSHPublicKey` 操作。此操作为 IAM 用户授予将公有密钥推送到实例的权限。使用 `ec2-instance-connect:SendSSHPublicKey`，考虑限制对特定 EC2 实例的访问。否则，具有此权限的所有 IAM 用户都可以连接到所有 EC2 实例。
- `ec2:osuser` 条件。这指定可以将公有密钥推送到实例的操作系统用户的名称。使用用于启动实例的 AMI 的默认用户名。例如，对于 Ubuntu，Amazon Linux 2 的默认用户名为 `ec2-user` 和 `ubuntu`。
- `ec2:DescribeInstances` 操作。使用 EC2 Instance Connect CLI 时此操作是必需的，因为包装程序会调用此操作。IAM 用户可能已经拥有从另一个策略调用此操作的权限。

下面是示例策略文档。如果您的用户将仅使用 SSH 客户端连接到您的实例，则可以省略 `ec2:DescribeInstances` 操作的语句。您可以替换 `Resource` 中的指定实例，以授予用户使用 EC2 Instance Connect 访问所有 EC2 实例的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2-instance-connect:SendSSHPublicKey",  
            "Resource": [  
                "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",  
                "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:osuser": "ami-username"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DescribeInstances",  
            "Resource": "*"  
        }  
    ]  
}
```

2. 使用 [create-policy](#) 命令创建新的托管策略，并指定您创建的 JSON 文档以作为新策略的内容。

```
$ aws iam create-policy --policy-name my-policy --policy-document file://JSON-file-name
```

3. 使用 [attach-user-policy](#) 命令将托管策略附加到指定的 IAM 用户。对于 [--user-name](#) 参数，请指定 IAM 用户的友好名称（而不是 ARN）。

```
$ aws iam attach-user-policy --policy-arn arn:aws:iam::account-id:policy/my-policy --  
user-name IAM-friendly-name
```

使用 EC2 Instance Connect 进行连接

以下说明介绍如何使用 EC2 Instance Connect 连接到 Linux 实例。

使用 Instance Connect 进行连接的选项

- [使用基于浏览器的客户端进行连接 \(p. 434\)](#)
- [使用 EC2 Instance Connect CLI 进行连接 \(p. 434\)](#)
- [使用您自己的密钥和 SSH 客户端进行连接 \(p. 435\)](#)

限制

- 支持以下 Linux 发行版：
 - Amazon Linux 2 (任何版本)
 - Ubuntu 16.04 或更高版本
- 要使用 Amazon EC2 控制台进行连接，实例必须具有公有 IP 地址 (IPv4 或 IPv6)。您可以使用 EC2 Instance Connect CLI 通过实例的私有 IP 地址进行连接。
- 目前不支持 Safari 浏览器。
- EC2 Instance Connect 仅与 实例元数据服务版本 1 一起使用。如果将实例元数据服务配置为要求使用实例元数据服务版本 2，则无法使用 EC2 Instance Connect。有关更多信息，请参阅[配置实例元数据服务 \(p. 499\)](#)。

先决条件

- 在实例上安装 Instance Connect。
有关更多信息，请参阅 [设置 EC2 Instance Connect \(p. 429\)](#)。
- (可选) 在本地计算机上安装 SSH 客户端。

如果用户仅使用控制台或 EC2 Instance Connect CLI 连接到实例，则无需安装 SSH 客户端。您的本地计算机很可能已默认安装 SSH 客户端。您可以通过在命令行键入 ssh 来检查 SSH 客户端。如果您的本地计算机无法识别该命令，您可安装 SSH 客户端。有关在 Linux 或 macOS X 上安装 SSH 客户端的信息，请参阅 <http://www.openssh.com>。有关在 Windows 10 上安装 SSH 客户端的信息，请参阅 [Windows 中的 OpenSSH](#)。

- (可选) 在本地计算机上安装 EC2 Instance Connect CLI。

如果用户仅使用控制台或 SSH 客户端连接到实例，则无需安装 EC2 Instance Connect CLI。有关更多信息，请参阅 [步骤 3：\(可选 \) 安装 EC2 Instance Connect CLI \(p. 432\)](#)。

使用基于浏览器的客户端进行连接

您可以通过从 Amazon EC2 控制台中选择实例，然后选择使用 EC2 Instance Connect 进行连接，以使用基于浏览器的客户端连接到实例。Instance Connect 处理权限并提供成功的连接。

从 Amazon EC2 控制台使用基于浏览器的客户端连接到您的实例

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Instances (实例)。
- 选择实例，然后选择连接。
- 选择 EC2 Instance Connect (基于浏览器的 SSH 连接)，然后选择连接。

将打开一个窗口，并且您连接到实例。

使用 EC2 Instance Connect CLI 进行连接

您可以使用 EC2 Instance Connect CLI 并仅提供实例 ID 以连接到实例，同时 Instance Connect CLI 在一次调用中执行以下三个操作：它生成一次性使用的 SSH 公有密钥，将密钥推送到实例以在其中保留 60 秒，并将用户连接到实例。您可以在 Instance Connect CLI 中使用基本 SSH/SFTP 命令。

Amazon Linux 2

使用 EC2 Instance Connect CLI 连接到实例

将 mssh 命令与实例 ID 一起使用，如下所示。您无需指定 AMI 的用户名。

```
$ mssh i-001234a4bf70dec41EXAMPLE
```

Ubuntu

使用 EC2 Instance Connect CLI 连接到实例

将 mssh 命令与实例 ID 以及 Ubuntu AMI 的默认用户名一起使用，如下所示。您必须指定 AMI 的用户名，否则会出现以下错误：身份验证失败。

```
$ mssh ubuntu@i-001234a4bf70dec41EXAMPLE
```

使用您自己的密钥和 SSH 客户端进行连接

您可以使用自己的 SSH 密钥，并在使用 EC2 Instance Connect API 时从您选择的 SSH 客户端连接到您的实例。这使您能够从将公有密钥推送到实例的 Instance Connect 功能中受益。

要求

支持的 RSA 密钥类型是 OpenSSH 和 SSH2。支持的长度为 2048 和 4096。有关更多信息，请参阅 [将您自己的公有密钥导入 Amazon EC2 \(p. 761\)](#)。

使用您自己的密钥和任何 SSH 客户端连接到实例

1. (可选) 生成新的 SSH 私有密钥和公有密钥。

您可以使用以下命令生成新的 SSH 私有密钥和公有密钥 (my_rsa_key 和 my_rsa_key.pub) :

```
$ ssh-keygen -t rsa -f my_rsa_key
```

2. 将 SSH 公有密钥推送到实例。

使用 [send-ssh-public-key](#) 命令可将 SSH 公有密钥推送到实例。如果使用 Amazon Linux 2 启动实例，则 AMI 的默认用户名是 ec2-user。如果使用 Ubuntu 启动实例，则 AMI 的默认用户名是 ubuntu。

以下示例将公有密钥推送到指定的可用区中的指定实例，以对 ec2-user 进行身份验证：

```
$ aws ec2-instance-connect send-ssh-public-key --instance-id i-001234a4bf70dec41EXAMPLE  
--availability-zone us-west-2b --instance-os-user ec2-user --ssh-public-key  
file:///my_rsa_key.pub
```

3. 使用私有密钥连接到实例。

从实例元数据中删除公有密钥之前，可以使用 ssh 命令通过私有密钥连接到实例（在 60 秒后删除）。指定与公有密钥对应的私有密钥、用于启动实例的 AMI 的默认用户名以及实例的公有 DNS。

```
$ ssh -i my_rsa_key ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com
```

卸载 EC2 Instance Connect

要禁用 EC2 Instance Connect，请连接到您的实例并卸载您在操作系统上安装的 ec2-instance-connect 程序包。如果 sshd 配置与您安装 EC2 Instance Connect 时设置的配置匹配，卸载 ec2-instance-connect 还会删除 sshd 配置。如果在安装 EC2 Instance Connect 后修改了 sshd 配置，您必须手动更新该配置。

Amazon Linux 2

您可以在 Amazon Linux 2 2.0.20190618 或更高版本上卸载 EC2 Instance Connect，其中预配置了 EC2 Instance Connect。

在使用 Amazon Linux 2 启动的实例上卸载 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。指定您在启动实例时用于实例的 SSH 密钥对以及 Amazon Linux 2 AMI 的默认用户名，即 ec2-user。

例如，以下 ssh 命令使用密钥对 my_ec2_private_key.pem 连接到具有公有 DNS 名称 ec2-a-b-c-d.us-west-2.compute.amazonaws.com 的实例。

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

2. 使用以下 yum 命令卸载 ec2-instance-connect 程序包。

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

在使用 Ubuntu AMI 启动的实例上卸载 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。指定您在启动实例时用于实例的 SSH 密钥对以及 Ubuntu AMI 的默认用户名，即 ubuntu。

例如，以下 ssh 命令使用密钥对 my_ec2_private_key.pem 连接到具有公有 DNS 名称 ec2-a-b-c-d.us-west-2.compute.amazonaws.com 的实例。

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

2. 使用以下 apt-get 命令卸载 ec2-instance-connect 程序包。

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

使用 PuTTY 从 Windows 连接到 Linux 实例

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](#)。

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 页上的 Status Checks 列中查看此信息。

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：

- 验证有关连接到您的实例的常规先决条件。
[有关更多信息，请参阅 **连接到您的实例的常规先决条件 \(p. 424\)**](#)。
- 在您的本地计算机上安装 PuTTY。

从 [PuTTY 下载页面](#)下载 PuTTY 并安装。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。

- 使用 PuTTYgen 转换您的私有密钥

找到您在启动实例时指定的密钥对的私有密钥 (.pem 文件)。将 .pem 文件转换为 .ppk 文件以用于 PuTTY。有关更多信息，请按照下一节中的步骤操作。

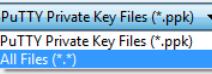
使用 PuTTYgen 转换私有密钥

PuTTY 自身并不支持由 SSH 密钥生成的私有密钥格式 (.pem)。PuTTY 提供一个名为 PuTTYgen 的工具，此工具可以将密钥转换为所需的 PuTTY 格式。您必须如下所示将私有密钥 (.pem 文件) 转换为此格式 (.ppk 文件)，以便使用 PuTTY 连接到您的实例。

转换您的私有密钥

- 从 Start (开始) 菜单中，依次选择 All Programs (所有程序)、PuTTY、PuTTYgen。
- 在 Type of key to generate 下，选择 RSA。如果您使用的是旧版本的 PuTTYgen，请选择 SSH-2 RSA。



- 选择 Load。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。
- File name: 
- 选择在启动实例时指定的密钥对的 .pem 文件，然后选择 Open (打开)。PuTTYgen 会显示一个通知，指示已成功导入 .pem 文件。选择 OK。
- 要以 PuTTY 可使用的格式保存密钥，请选择保存私有密钥。PuTTYgen 将显示有关保存没有密码的密钥的警告。选择是。

Note

私有密钥上的密码提供额外一层保护。即使发现了您的私有密钥，也不能在没有密码的情况下使用该密钥。使用密码的缺点是自动化更难实现，因为需要人工干预以登录到实例或将文件复制到实例中。

- 为密钥指定您用于密钥对的相同名称（例如 my-key-pair）并选择 Save (保存)。PuTTY 会自动添加 .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。

连接到 Linux 实例

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。有关更多信息，请参阅上一个部分中的[使用 PuTTYgen 转换私有密钥 \(p. 436\)](#)。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](#)。

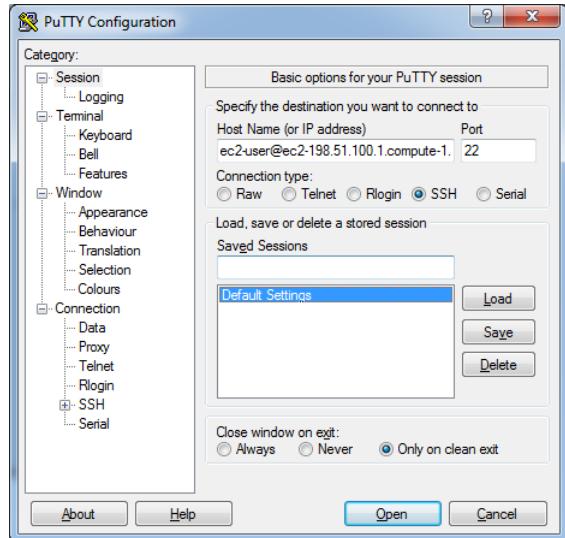
使用 PuTTY 连接到您的实例

- 启动 PuTTY (在开始菜单中，选择所有程序 > PuTTY > PuTTY)。
- 在 Category 窗格中，选择 Session 并填写以下字段：
 - 在主机名框中，输入 `user_name@public_dns_name` (有关如何获取实例的公有 DNS 名称，请参阅[获取有关实例的信息 \(p. 424\)](#))。
 - (仅限 IPv6) 要使用实例的 IPv6 地址连接，请输入 `user_name@ipv6_address`。

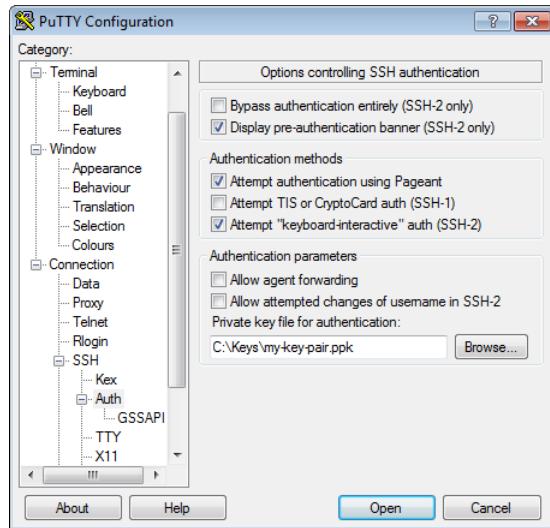
对于 `user_name`，确保为您的 AMI 指定相应的用户名。例如：

- 对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。
- 对于 CentOS AMI，用户名是 `centos`。
- 对于 Debian AMI，用户名是 `admin` 或 `root`。
- 对于 Fedora AMI，用户名为 `ec2-user` 或 `fedora`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
- 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名是 `ubuntu`。

- 另外，如果 ec2-user 和 root 无法使用，请与 AMI 供应商核实。
- b. 确保端口值为 22。
- c. 在连接类型下，选择 SSH。



3. (可选) 您可以配置 PuTTY 以定期自动发送“保持连接”数据以将会话保持活动状态。要避免由于会话处于不活动状态而与实例断开连接，这是非常有用的。在 Category 窗格中，选择 Connection，然后在 Seconds between keepalives 字段中输入所需的间隔。例如，如果您的会话在处于不活动状态 10 分钟后断开连接，请输入 180 以将 PuTTY 配置为每隔 3 分钟发送一次保持活动数据。
4. 在 Category 窗格中，展开 Connection，再展开 SSH，然后选择 Auth。完成以下操作：
 - a. 选择 Browse。
 - b. 选择为密钥对生成的 .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。在类别下面，选择会话，在保存的会话中输入会话的名称，然后选择保存。
 - d. 选择 Open。



5. 如果这是第一次连接到该实例，PuTTY 将显示安全警报对话框，以询问您是否信任要连接到的主机。

- a. (可选) 验证安全警报对话框中的指纹是否与您之前在 [\(可选\) 获取实例指纹 \(p. 425\)](#) 中获得的指纹相匹配。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。
- b. 选择是。将打开一个窗口，并且您连接到实例。

Note

如果您在将私有密钥转换成 PuTTY 格式时指定了密码，当您登录到实例时，您必须提供该密码。

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，可用于在 Windows 计算机和 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 \(p. 439\)](#)。

要使用 PSCP，您需要使用在[使用 PuTTYgen 转换私有密钥 \(p. 436\)](#)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 Sample_file.txt 文件从 Windows 计算机上的 C:\ 驱动器传输到 Amazon Linux 实例上的 ec2-user 主目录：

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt ec2-user@public_dns:/home/ec2-user/  
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。

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt ec2-user@[ipv6-address]:/home/ec2-  
user/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 转换私有密钥 \(p. 436\)](#)中生成的私有密钥。您还需要使用 Linux 实例的公有 DNS 地址。

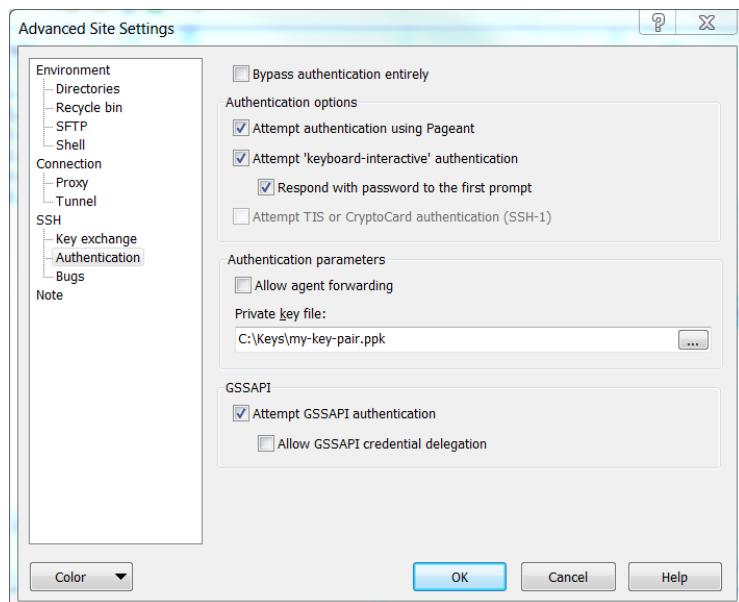
1. 从 <http://winscp.net/eng/download.php> 上下载并安装 WinSCP。对于大多数用户而言，采用默认安装选项就可以了。
2. 启动 WinSCP。
3. 在 WinSCP 登录屏幕中，对于 Host name，请输入实例的公有 DNS 主机名称或公有 IPv4 地址。

(仅限 IPv6) 要使用实例的 IPv6 地址登录，请输入实例的 IPv6 地址。

4. 对于用户名，请输入默认的 AMI 用户名。
 - 对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 ec2-user。
 - 对于 CentOS AMI，用户名是 centos。
 - 对于 Debian AMI，用户名是 admin 或 root。

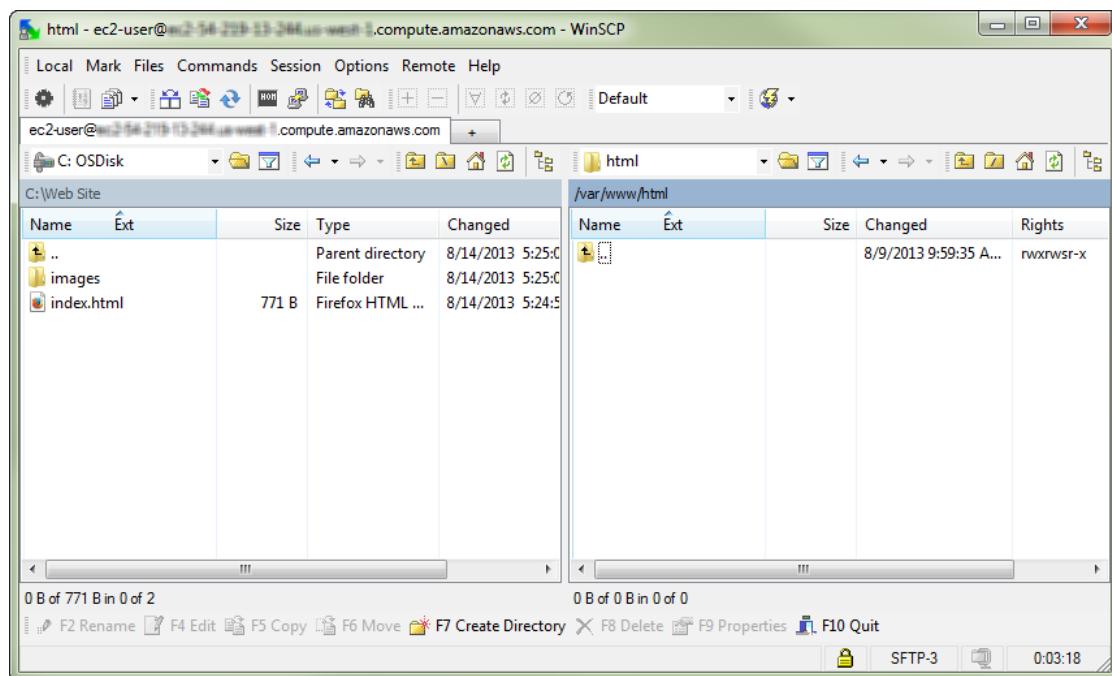
- 对于 Fedora AMI，用户名为 `ec2-user` 或 `fedora`。
 - 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
 - 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
 - 对于 Ubuntu AMI，用户名是 `ubuntu`。
 - 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。
5. 为您的实例指定私有密钥。对于私有密钥，请输入私有密钥的路径，或选择 ... 按钮以浏览文件。要打开高级站点设置，对于较高版本的 WinSCP，请选择高级。要查找私有密钥文件设置，请在 SSH 下面选择身份验证。

以下是 WinSCP 版本 5.9.4 中的屏幕截图：



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 转换私有密钥 \(p. 436\)](#)。

6. (可选) 在左侧面板中，选择目录。对于远程目录，请输入要将文件添加到的目录的路径。要打开高级站点设置，对于较高版本的 WinSCP，请选择高级。要查找远程目录设置，请在环境下面选择目录。
7. 选择登录。要将主机指纹添加到主机缓存中，请选择是。



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。

如果您收到“Cannot execute SCP to start transfer (无法执行 SCP 以开始传输)”错误，必须先在 Linux 实例上安装 scp。对于某些操作系统，该命令会位于 `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 Windows Subsystem for Linux 从 Windows 连接到 Linux 实例

以下说明介绍如何使用 Windows Subsystem for Linux (WSL) 上的 Linux 发行版来连接到您的实例。可以免去下载 WSL，可用于在 Windows 上直接将本机 Linux 命令行工具与传统 Windows 桌面一起运行，而不会产生虚拟机开销。

通过安装 WSL，您可以使用本机 Linux 环境连接到 Linux EC2 实例，而不是使用 PuTTY 或 PuTTYgen。Linux 环境让连接到 Linux 实例变得更轻松，因为它附带一个本机 SSH 客户端，可用于连接到 Linux 实例并更改 .pem 密钥文件的权限。Amazon EC2 控制台提供用于连接到 Linux 实例的 SSH 命令，并且您可以获得 SSH 命令中的详细输出以进行故障排除。有关更多信息，请参阅 [Windows Subsystem for Linux 文档](#)。

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 页上的 Status Checks 列中查看此信息。

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](#)。

目录

- [先决条件 \(p. 426\)](#)
- [使用 WSL 连接到 Linux 实例 \(p. 442\)](#)
- [使用 SCP 将文件从 Linux 传输到 Linux 实例 \(p. 443\)](#)
- [卸载 WSL \(p. 444\)](#)

Note

在安装 WSL 后，所有先决条件和步骤都相同（如使用 SSH 连接到 Linux 实例 (p. 426) 中所述），并且体验与使用本机 Linux 的体验类似。

先决条件

在连接到 Linux 实例之前，请先完成以下先决条件：

- 验证有关连接到您的实例的常规先决条件。
有关更多信息，请参阅 [连接到您的实例的常规先决条件 \(p. 424\)](#)。
- 在本地计算机上安装 Windows Subsystem for Linux (WSL) 和 Linux 发行版。

按照 [Windows 10 安装指南](#) 中的说明执行操作来安装 WSL 和 Linux 发行版。说明中的示例安装的是 Linux 的 Ubuntu 发行版，但您可以安装任意发行版。系统会提示您重新启动计算机以使更改生效。

- 将私有密钥从 Windows 复制到 WSL。

在 WSL 终端窗口中，将 .pem 文件（适用于您在启动实例时指定的密钥对）从 Windows 复制到 WSL。记下在连接到实例时要使用的 WSL 上的 .pem 文件的完全限定路径。有关如何指定 Windows 硬盘的路径的信息，请参阅[如何访问我的 C 驱动器？](#)。

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

使用 WSL 连接到 Linux 实例

通过以下过程使用 Windows Subsystem for Linux (WSL) 连接到 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. 在终端窗口中，使用 ssh 命令连接到该实例。您可以指定私有密钥 (.pem) 文件、AMI 的用户名以及实例的公有 DNS 名称。例如，如果您使用了 Amazon Linux 2 或 Amazon Linux AMI，则用户名为 ec2-user。有关查找 AMI 的用户名和实例的 DNS 名称的更多信息，请参阅[获取有关您的实例的信息 \(p. 424\)](#)。

```
sudo 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)?
```

2. (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、适当的用户名和 IPv6 地址。例如，如果您使用了 Amazon Linux 2 或 Amazon Linux AMI，则用户名为 ec2-user。

```
sudo ssh -i /path/my-key-pair.pem ec2-user@2001:db8:1234:1a00:9691:9503:25ad:1761
```

3. (可选) 验证安全警报中的指纹是否与您之前在 ([可选 \) 获取实例指纹 \(p. 425\)](#) 中获得的指纹相匹配。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。
4. 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协议 (SCP)。本节介绍了如何使用 SCP 传输文件。该步骤与使用 SSH 连接到实例的步骤类似。

先决条件

- 验证有关将文件传输到您的实例的常规先决条件。

将文件传输到实例的常规先决条件与连接到实例的常规先决条件相同。有关更多信息，请参阅 [连接到您的实例的常规先决条件 \(p. 424\)](#)。

- 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。有关更多信息，请参阅 <http://www.openssh.org>。

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. 使用实例的公有 DNS 名称将文件传输到您的实例。例如，如果私有密钥文件的名称是 my-key-pair、要传输的文件是 SampleFile.txt、用户名是 ec2-user、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:~
```

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)?
```

2. (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@
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~
```

3. (可选) 验证安全警报中的指纹是否与您之前在 [\(可选\) 获取实例指纹 \(p. 425\)](#) 中获得的指纹相匹配。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。
4. 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
```

如果您收到“bash: scp: command not found (bash: scp: 命令未找到)”错误，您必须先在 Linux 实例上安装 scp。对于某些操作系统，该命令会位于 `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
```

5. 要反方向传输文件（从 Amazon EC2 实例中传输到本地计算机），请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
```

6. （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
```

卸载 WSL

有关卸载 Windows Subsystem for Linux 的信息，请参阅[如何卸载 WSL 发行版](#)？

使用会话管理器连接到 Linux 实例

会话管理器是一项完全托管的 AWS Systems Manager 功能，可让您通过基于浏览器的交互一键式 shell 或 AWS CLI 管理 Amazon EC2 实例。您可以使用会话管理器通过您账户中的实例来启动会话。启动会话后，您可以像通过任何其他连接类型一样运行 bash 命令。有关会话管理器的更多信息，请参阅 AWS Systems Manager 用户指南中的[AWS Systems Manager 会话管理器](#)。

在尝试使用会话管理器连接到实例之前，请确保已完成必要的设置步骤。有关更多信息和说明，请参阅[会话管理器入门](#)。

使用 Amazon EC2 控制台通过会话管理器连接到 Linux 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 (实例)。
3. 选择实例，然后选择连接。
4. 对于 Connection method (连接方法)，请选择 Session Manager (会话管理器)。
5. 选择 Connect。

Note

如果您收到一个错误，该错误指示您无权执行一个或多个 Systems Manager 操作 (`ssm:command-name`)，则必须更新您的策略以允许您从 Amazon EC2 控制台启动会话。有关

更多信息，请参阅 AWS Systems Manager 用户指南 中的[会话管理器的快速入门默认 IAM 策略](#)。

停止和启动您的实例

您可以停止和启动将 Amazon EBS 卷作为其根设备的实例。该实例将保留其实例 ID，但是可以按照[概述 \(p. 445\)](#)部分中所述进行更改。

当您终止一个实例时，我们会将其关闭。我们不会对已停止的实例收费，也不会收取数据传输费，但我们会对所有 Amazon EBS 卷的存储收费。您每次启动已停止的实例时，我们将收取最低一分钟的使用费用。一分钟之后，我们仅按您使用实例的秒数收费。例如，如果您运行一个实例 20 秒后停止实例，我们将按一整分钟收取费用。如果您运行一个实例 3 分 40 秒，我们将收取 3 分 40 秒的使用费用。

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分离卷，将其附加到运行中的实例并进行修改，然后将其分离，再次附加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附加。

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 \(p. 458\)](#)。如果您愿意休眠实例，请参阅[使 Linux 实例休眠 \(p. 447\)](#)。有关更多信息，请参阅[重启、停止、休眠与终止之间的区别 \(p. 373\)](#)。

目录

- [概述 \(p. 445\)](#)
- [停止实例后会发生什么 \(API\) \(p. 446\)](#)
- [停止和启动您的实例 \(p. 446\)](#)
- [修改已停止的实例 \(p. 447\)](#)
- [故障排除 \(p. 447\)](#)

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 \(p. 85\)](#)。

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。
- 实例会在停止和启动时保留其私有 IPv4 地址以及任何 IPv6 地址。我们会释放公有 IPv4 地址并在您启动实例时为其分配新的 IPv4 地址。
- 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。借助 EC2-Classic，弹性 IP 地址会在您停止实例时取消与其的关联。有关更多信息，请参阅[EC2-Classic \(p. 672\)](#)。
- 当您停止和启动 Windows 实例时，EC2Config 服务将对该实例执行任务，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 或 Amazon EC2 用户指南（适用于 Windows 实例）中的[使用 EC2Config 服务配置 Windows 实例](#)。
- 如果您的实例处于 Auto Scaling 组中，则 Amazon EC2 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 Amazon EC2 Auto Scaling 用户指南 中的[Auto Scaling 实例的运行状况检查](#)。

- 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 \(p. 678\)](#)。

有关更多信息，请参阅 [重启、停止、休眠与终止之间的区别 \(p. 373\)](#)。

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。

停止实例后会发生什么 (API)

使用 `stop-instances` 命令停止 EC2 实例后，将在操作系统级别注册以下内容：

- API 请求将向访客发送按钮按下事件。
- 由于此按钮按下事件，将停止各种系统服务。`systemd` 处理系统的正常关闭。来自管理程序的 ACPI 关闭按钮按下事件触发正常关闭。
- 启动 ACPI 关闭。
- 当正常关闭进程退出时，实例将关闭。没有可配置的操作系统关闭时间。

停止和启动您的实例

您可以使用控制台或命令行停止和启动由 Amazon EBS 支持的实例。

默认情况下，当您通过由 Amazon EBS 支持的实例（使用 `shutdown` 或 `poweroff` 命令）启动关闭时，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 \(p. 460\)](#)。

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. 依次选择 Actions、Instance State、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。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

3. 在确认对话框中，选择 Yes, Stop。停止实例可能需要几分钟时间。
4. 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 \(p. 447\)](#)。
5. 要启动已停止的实例，请选择该实例，然后依次选择 Actions (操作)、Instance State (实例状态) 和 Start (启动)。
6. 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。

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[更改实例类型 \(p. 233\)](#)。
- 要更改您的实例的用户数据，请参阅[与实例用户数据配合使用 \(p. 510\)](#)。
- 要为您的实例启用或禁用 EBS 优化，请参阅[修改 EBS 优化 \(p. 875\)](#)。
- 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 \(p. 929\)](#)。

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

如果您停止了由 Amazon EBS 支持的实例，而该实例“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 \(p. 961\)](#)。

使 Linux 实例休眠

当您使实例休眠时，我们会向操作系统发出信号来执行休眠 (suspend-to-disk)。休眠会将实例内存 (RAM) 中的内容保存到您的 Amazon EBS 根卷。我们保留实例的 Amazon EBS 根卷以及任何附加的 Amazon EBS 数据卷。在启动实例时：

- Amazon EBS 根卷会恢复为之前的状态
- 会重新加载 RAM 内容
- 并恢复实例上之前运行的进程
- 之前附加的数据卷会重新附加，实例也会保留其实例 ID

只有当实例[已启用休眠 \(p. 451\)](#)并且满足[休眠先决条件 \(p. 449\)](#)，您才可以使该实例休眠。

如果实例或应用程序在引导和进行内存占用以开始发挥全部生产功能时所需的时间较长，您可以使用休眠来预热实例。要预热实例，您需要执行以下操作：

1. 启动实例时启用休眠。
2. 将其设置为所需的状态。
3. 使实例休眠，并根据需要随时恢复到休眠前的状态。

当实例处于 `stopped` 状态时，我们不会收取已休眠实例的使用费用。当实例处于 `stopping` 状态时，此时 RAM 的内容会转移到 Amazon EBS 根卷，我们会收取实例使用费用。（这不同于您[停止一个实例 \(p. 445\)](#)而不使其休眠。）我们不会收取数据传输的使用费用。但是，我们会收取所有 Amazon EBS 卷的存储费用，包括存储 RAM 内容的费用。

如果您不再需要某个实例，可以随时终止它，包括当实例处于 `stopped`（已休眠）状态时。有关更多信息，请参阅[终止您的实例 \(p. 458\)](#)。

Note

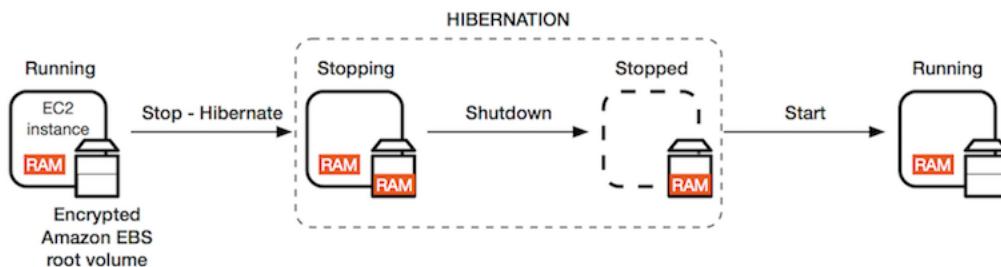
有关在 Windows 实例上使用休眠的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[使 Windows 实例休眠](#)。

目录

- [休眠概述 \(p. 448\)](#)
- [休眠先决条件 \(p. 449\)](#)
- [限制 \(p. 449\)](#)
- [配置现有 AMI 以支持休眠 \(p. 450\)](#)
- [为实例启用休眠 \(p. 451\)](#)
- [在实例上禁用 KASLR \(仅限 Ubuntu\) \(p. 452\)](#)
- [使实例休眠 \(p. 453\)](#)
- [启动已休眠的实例 \(p. 454\)](#)
- [休眠故障排除 \(p. 455\)](#)

休眠概述

下图显示了休眠过程的基本概述。



当您使正在运行的实例休眠时，将出现以下情况：

- 启动休眠时，实例将进入 `stopping` 状态。我们会向操作系统发出信号来执行休眠 (suspend-to-disk)。休眠会冻结所有进程、将 RAM 中的内容保存到 Amazon EBS 根卷，然后执行常规关闭。
- 关闭完成后，实例将进入 `stopped` 状态。
- 所有 Amazon EBS 卷保持附加到实例，而且其数据将保留下，包括已保存的 RAM 内容。
- 大多数情况下，实例会在启动时迁移到新的底层主机。当您停止并启动实例时，也会发生此类情况。
- 当您启动实例时，实例将启动，操作系统从 Amazon EBS 根卷读取 RAM 内容，然后再对进程解除冻结以恢复其状态。
- 实例在休眠和启动时会保留其私有 IPv4 地址以及任何 IPv6 地址。我们会释放公有 IPv4 地址并在您启动实例时为其分配新的 IPv4 地址。
- 实例会保留其关联的弹性 IP 地址。您需要为与已休眠实例关联的所有弹性 IP 地址付费。借助 EC2-Classic，弹性 IP 地址会在您将实例休眠时取消与它的关联。有关更多信息，请参阅 [EC2-Classic \(p. 672\)](#)。
- 当您使 ClassicLink 实例休眠时，它会与所链接的 VPC 取消链接。您必须在启动之后将实例再次链接到 VPC。有关更多信息，请参阅 [ClassicLink \(p. 678\)](#)。

有关休眠与重启、停止和终止之间的区别，请参阅[重启、停止、休眠与终止之间的区别 \(p. 373\)](#)。

休眠先决条件

要使实例休眠，必须满足以下先决条件：

- 支持的实例系列 - C3、C4、C5、M3、M4、M5、R3、R4 和 R5。
- 实例 RAM 大小 - 必须小于 150 GB。
- 实例大小 - 裸机实例不支持。
- 支持的 AMI (必须是支持休眠的 HVM AMI)：
 - Amazon Linux 2 AMI 发布了 2019.08.29 版或更高版本。
 - Amazon Linux AMI 2018.03 发布了 2018.11.16 版或更高版本。
 - Ubuntu 18.04 LTS - Bionic AMI 发布了序列号 20190722.1 或更高版本。我们建议在采用 Ubuntu 18.04 LTS - Bionic 的实例上禁用 KASLR。有关更多信息，请参阅 [在实例上禁用 KASLR \(仅限 Ubuntu \) \(p. 452\)](#)。

要配置您自己的 AMI 以支持休眠，请参阅 [配置现有 AMI 以支持休眠 \(p. 450\)](#)。

即将支持 Ubuntu 的其他版本和其他操作系统。

有关 Windows 支持的 AMI 的信息，请参阅 Amazon EC2 用户指南 (适用于 Windows 实例) 中的 [休眠先决条件](#)。

- 根卷类型 - 必须是 Amazon EBS 卷，而不是实例存储卷。
- Amazon EBS 根卷大小 - 必须足够大，以存储 RAM 内容并满足您的预期使用量，例如，操作系统或应用程序。如果您启用休眠，则启动时在根卷上分配空间以存储 RAM。
- Amazon EBS 根卷加密 - 要使用休眠，必须加密根卷以确保在休眠时保护内存中的敏感内容。将 RAM 数据移动到 Amazon EBS 根卷时，它始终加密。根卷的加密在实例启动时实施。可以使用以下三个选项之一，以确保根卷是加密的 Amazon EBS 卷：
 - EBS“单步”加密：在单个 run-instances API 调用中，您可以从未加密的 AMI 中启动 EBS 支持的加密 EC2 实例，并且还可以同时启用休眠。有关更多信息，请参阅 [将加密与 EBS 支持的 AMI 结合使用 \(p. 134\)](#)。
 - EBS 默认加密：您可以启用 EBS 默认加密，以确保加密在您的 AWS 账户中创建的所有新的 EBS 卷。这样，您就可以为实例启用休眠，而无需在实例启动时指定加密意图。有关更多信息，请参阅 [默认加密 \(p. 853\)](#)。
 - 加密的 AMI：您可以使用加密的 AMI 启动实例以启用 EBS 加密。如果 AMI 没有加密的根快照，则可以将其复制到新的 AMI 并请求加密。有关更多信息，请参阅 [在复制过程中将未加密映像加密 \(p. 137\)](#) 和 [复制 AMI \(p. 141\)](#)。
- 在启动时启用休眠 - 您不能在现有实例（正在运行或已停止）上启用休眠。有关更多信息，请参阅 [为实例启用休眠 \(p. 451\)](#)。
- 购买选项 - 此功能仅面向按需实例和预留实例提供。它不适用于Spot 实例。有关更多信息，请参阅 [休眠中断的 Spot 实例 \(p. 327\)](#)。

限制

- 休眠不支持以下操作：
 - 更改已休眠实例的实例类型或大小
 - 从启用了休眠的实例创建快照或 AMI
 - 从已休眠的实例创建快照或 AMI
- 您不能停止实例存储支持的实例，也不能使这些实例休眠*。
- 您不能将具有超过 150 GB 的 RAM 的实例休眠。
- 您不能使位于 Auto Scaling 组中或者由 Amazon ECS 使用的实例休眠。如果实例位于 Auto Scaling 组中并且您尝试使该实例休眠，则 Amazon EC2 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 Amazon EC2 Auto Scaling 用户指南 中的 [Auto Scaling 实例的运行状况检查](#)。

- 我们支持的实例持续休眠时间不超过 60 天。要保留实例超过 60 天，您必须启动已休眠的实例，停止该实例，然后启动它。
- 我们不断通过升级和安全补丁更新平台，这可能会与现有已休眠的实例冲突。我们会通知您有关需要启动已休眠实例的关键更新，这样我们才会执行关闭或重启操作以应用必需的升级和安全补丁。

*对于启用休眠的 C3 和 R3 实例，请勿使用实例存储卷。

配置现有 AMI 以支持休眠

要让使用您自己的 AMI 启动的实例休眠，必须配置 AMI 来支持休眠。有关更多信息，请参阅 [更新实例软件 \(p. 465\)](#)。

如果您使用 [支持的 AMI \(p. 449\)](#) 之一，或者基于支持的 AMI 之一创建了 AMI，则无需配置它来支持休眠。已预配置这些 AMI 来支持休眠。

Amazon Linux 2

配置 Amazon Linux 2 AMI 以支持休眠

1. 使用以下命令更新为最新内核 4.14.138-114.102 或更高版本。

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

2. 使用以下命令从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. 使用以下命令重新引导实例。

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

4. 通过使用以下命令来确认内核版本已更新为 4.14.138-114.102 或更高版本。

```
[ec2-user ~]$ uname -a
```

5. 停止实例并创建 AMI。有关更多信息，请参阅 [从实例创建 Linux AMI \(p. 103\)](#)。

Amazon Linux

配置 Amazon Linux AMI 以支持休眠

1. 使用以下命令将最新内核更新为 4.14.77-70.59 或更高版本。

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

2. 使用以下命令从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. 使用以下命令重新引导实例。

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

4. 通过使用以下命令来确认内核版本已更新为 4.14.77-70.59 或更高版本。

```
[ec2-user ~]$ uname -a
```

5. 停止实例并创建 AMI。有关更多信息，请参阅 [从实例创建 Linux AMI \(p. 103\)](#)。

Ubuntu

配置 Ubuntu 18.04 LTS AMI 以支持休眠

1. 使用以下命令将最新内核更新为 4.15.0-1044 或更高版本。

```
[ec2-user ~]$ sudo apt update  
[ec2-user ~]$ sudo apt dist-upgrade
```

2. 使用以下命令从存储库安装 ec2-hibernate-agent 程序包。

```
[ec2-user ~]$ sudo apt install ec2-hibernate-agent
```

3. 使用以下命令重新引导实例。

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

4. 通过使用以下命令来确认内核版本已更新为 4.15.0-1044 或更高版本。

```
[ec2-user ~]$ uname -a
```

为实例启用休眠

要使实例休眠，必须先为其启用休眠。要启用休眠，您必须在启动实例时启用它。

Important

启动实例后，无法为实例启用或禁用休眠。

Console

使用控制台启用休眠

1. 按照[使用启动实例向导启动实例 \(p. 375\)](#)过程操作。
2. 在选择一个 Amazon 系统映像 (AMI) 页面上，选择一个支持休眠的 AMI。有关支持的 AMI 的更多信息，请参阅[休眠先决条件 \(p. 449\)](#)。
3. 在选择一个实例类型页面上，选择一种支持的实例类型，然后选择下一步：配置实例详细信息。有关支持的实例类型的信息，请参阅[休眠先决条件 \(p. 449\)](#)。
4. 在配置实例详细信息页面上，对于 Stop - Hibernate Behavior (停止 - 休眠操作)，选中 Enable hibernation as an additional stop behavior (启用休眠作为额外的停止操作) 复选框。
5. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。

AWS CLI

使用 AWS CLI 启用休眠

使用 `run-instances` 命令启动实例。使用 `--hibernation-options Configured=true` 参数启用休眠。

```
aws ec2 run-instances --image-id ami-0abcdef1234567890 --instance-type m5.large --  
hibernation-options Configured=true --count 1 --key-name MyKeyPair
```

适用于 Windows PowerShell 的 AWS 工具

使用 适用于 Windows PowerShell 的 AWS 工具 启用休眠

使用 [New-EC2Instance](#) 命令启动实例。使用 `-HibernationOptions_Configured $true` 参数启用休眠。

```
New-EC2Instance -ImageId ami-0abcdef1234567890 -InstanceType m5.large -  
HibernationOptions_Configured $true -MinCount 1 -MaxCount 1 -KeyName MyKeyPair
```

Console

查看是否已使用控制台为实例启用休眠

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，在详细信息窗格中，检查 Stop - Hibernation behavior (停止 - 休眠操作)。已启用 表明已为实例启用休眠。

AWS CLI

查看是否已使用 AWS CLI 为实例启用休眠

使用 [describe-instances](#) 命令并指定 `--filters "Name=hibernation-options.configured,Values=true"` 参数以筛选启用了休眠的实例。

```
aws ec2 describe-instances --filters "Name=hibernation-options.configured,Values=true"
```

输出中的以下字段指示实例已启用了休眠。

```
"HibernationOptions": {  
    "Configured": true  
}
```

适用于 Windows PowerShell 的 AWS 工具

查看是否已使用 适用于 Windows PowerShell 的 AWS 工具 为实例启用休眠

使用 [Get-EC2Instance](#) 命令并指定 `-Filter @{ Name="hibernation-options.configured"; Value="true" }` 参数以筛选启用了休眠的实例。

```
Get-EC2Instance -Filter @{ Name="hibernation-options.configured"; Value="true" }
```

输出会列出已启用休眠的 EC2 实例。

在实例上禁用 KASLR (仅限 Ubuntu)

要使用 Ubuntu 18.04 LTS - Bionic (20190722.1 版本或更高版本) 在新启动的实例上运行休眠，我们建议禁用 KASLR (内核地址空间布局随机化)。在 Ubuntu 18.04 LTS 上，默认启用 KASLR。KASLR 是一项标

准 Linux 内核安全功能，它通过随机化内核的基本地址值，来帮助减少尚未发现的内存访问漏洞的风险和后果。启用 KASLR 后，实例在休眠后可能无法恢复。

要详细了解 KASLR，请参阅 [Ubuntu 功能](#)。

在使用 Ubuntu 启动的实例上禁用 KASLR

1. 使用 SSH 连接到您的实例。有关更多信息，请参阅 [使用 SSH 连接到 Linux 实例 \(p. 426\)](#)。
2. 在选定编辑器中打开 `/etc/default/grub.d/50-cloudimg-settings.cfg` 文件。编辑 `GRUB_CMDLINE_LINUX_DEFAULT` 行以将 `nokaslr` 选项追加到其末尾，如以下示例所示。

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0 nvme_core.io_timeout=4294967295
nokaslr"
```

3. 保存文件并退出您的编辑器。
4. 运行以下命令来重新构建 grub 配置。

```
[ec2-user ~]$ sudo update-grub
```

5. 重启实例。

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

6. 确认在运行以下命令时已添加 `nokaslr`。

```
[ec2-user ~]$ cat /proc/cmdline
```

命令的输出应包含 `nokaslr` 选项。

使实例休眠

当实例[已启用休眠 \(p. 451\)](#)并且满足[休眠先决条件 \(p. 449\)](#)时，您才可以使该实例休眠。如果无法成功使实例休眠，则会进行正常关闭。

Console

使用控制台使 Amazon EBS 支持的实例休眠

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择操作、实例状态和 Stop - Hibernate (停止 - 休眠)。如果 Stop - Hibernate (停止 - 休眠) 已禁用，则实例已经休眠或停止，或者无法休眠。有关更多信息，请参阅[休眠先决条件 \(p. 449\)](#)。
4. 在确认对话框中，选择 Yes, Stop - Hibernate (是，停止 - 休眠)。使实例休眠可能需要几分钟时间。当实例正在进入休眠时，实例状态更改为正在停止；在实例已休眠的情况下，实例状态将更改为已停止。

AWS CLI

使用 AWS CLI 使 Amazon EBS 支持的实例休眠

使用 `stop-instances` 命令并指定 `--hibernate` 参数。

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0 --hibernate
```

适用于 Windows PowerShell 的 AWS 工具

使用 适用于 Windows PowerShell 的 AWS 工具 使 Amazon EBS 支持的实例休眠

使用 [Stop-EC2Instance](#) 命令并指定 `-Hibernate $true` 参数。

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0 -Hibernate $true
```

Console

查看是否已使用控制台在实例上启动休眠

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，在详细信息窗格中，检查状态转换原因消息。消息 Client.UserInitiatedHibernate: User initiated hibernate (Client.UserInitiatedHibernate: 用户启动了休眠) 指明实例上启动了休眠。

AWS CLI

查看是否已使用 AWS CLI 在实例上启动休眠

使用 [describe-instances](#) 命令并指定 `state-reason-code` 筛选条件以查看已启动了休眠的实例。

```
aws ec2 describe-instances --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

输出中的以下字段指明实例上启动了休眠。

```
"StateReason": {  
    "Code": "Client.UserInitiatedHibernate"  
}
```

适用于 Windows PowerShell 的 AWS 工具

查看是否已使用 适用于 Windows PowerShell 的 AWS 工具 在实例上启动休眠

使用 [Get-EC2Instance](#) 命令并指定 `state-reason-code` 筛选条件以查看已启动休眠的实例。

```
Get-EC2Instance -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

输出会列出已启动休眠的 EC2 实例。

启动已休眠的实例

按照启动已停止实例的相同方式，启动已休眠的实例。

Console

使用控制台启动已休眠的实例

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

2. 在导航窗格中，选择 Instances (实例)。
3. 选择已休眠的实例，然后依次选择操作、实例状态和开始。实例进入 running 状态可能需要几分钟时间。在此期间，实例[状态检查 \(p. 528\)](#)显示实例处于失败状态，直至实例已启动。

AWS CLI

使用 AWS CLI 启动已休眠的实例

使用 [start-instances](#) 命令。

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

适用于 Windows PowerShell 的 AWS 工具

使用 适用于 Windows PowerShell 的 AWS 工具 启动已休眠的实例

使用 [Start-EC2Instance](#) 命令。

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

休眠故障排除

使用此信息帮助您诊断和修复在使实例休眠时可能遇到的问题。

在启动后无法立即休眠

如果您在实例启动之后过快地尝试使实例休眠，则会收到错误。

在启动之后，您必须等待大约两分钟，然后才能休眠。

从 `stopping` 转变为 `stopped` 用时太长，内存状态在启动后无法恢复

如果正在进入休眠的实例从 `stopping` 状态转变为 `stopped` 状态用时过长，并且在启动之后内存状态未恢复，则这可能表明未正确配置休眠。

检查实例系统日志，查找与休眠相关的消息。要访问系统日志，请[连接 \(p. 423\)](#)到实例或者使用 `get-console-output` 命令。从 `hibinit-agent` 中查找日志行。如果日志行指示出现故障或者缺少日志行，则很可能在启动时配置休眠失败。

例如，以下消息指明实例根卷不够大：`hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

如果 `hibinit-agent` 中的最后日志行是 `hibinit-agent: Running: swapoff /swap`，则已成功配置休眠。

如果您未看到来自这些进程的任何日志，您的 AMI 可能不支持休眠。有关支持的 AMI 的信息，请参阅[休眠先决条件 \(p. 449\)](#)。如果您使用自己的 AMI，请确保按照[配置现有 AMI 以支持休眠 \(p. 450\)](#) 的说明操作。

实例卡在 stopping 状态

如果您已使实例休眠并且实例卡在 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 \(p. 961\)](#)。

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。

与停止并启动您的实例不同，重启实例不会启动新的实例计费周期 (最低收取一分钟的费用)。

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 \(p. 532\)](#)。

我们建议您使用 Amazon EC2 控制台、命令行工具或 Amazon EC2 API 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 控制台、命令行工具或 Amazon EC2 API 重启实例，而实例在四分钟内未完全关闭，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. 选择实例，然后选择 Actions、Instance State、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 检测到托管实例的基础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。

目录

- [确认计划停用的实例 \(p. 456\)](#)
- [使用计划停用的实例 \(p. 457\)](#)

有关实例事件类型的更多信息，请参阅[实例的计划事件 \(p. 532\)](#)。

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的账户关联的地址，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 控制面板。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。

Scheduled Events

US East (N. Virginia):

1 instances have scheduled events

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 \(p. 457\)](#)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。
3. 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。请务必在实例停用日期之前执行该操作，以防止意外的停机和数据丢失。

Warning

如果实例存储支持的实例超过了停用日期，则会终止该实例，并且无法恢复该实例或其中存储的任何数据。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	从实例创建由 EBS 支持的 AMI，以便您可以有一个备份。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在停止实例时的预期情况（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. 445) 。
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. 102) 。
实例存储	从使用 AMI 工具的实例创建由实例存储提供支持的 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. 105) 。
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. 115) 。

终止您的实例

当您不再需要实例时，可将其删除。这称为终止实例。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，您将无法连接到或启动实例。但是您可以使用同一 AMI 启动其他实例。如果您愿意停止并启动您的实例，或者将其休眠，请参阅[停止和启动您的实例 \(p. 445\)](#) 或[使 Linux 实例休眠 \(p. 447\)](#)。有关更多信息，请参阅[重启、停止、休眠与终止之间的区别 \(p. 373\)](#)。

目录

- [实例终止 \(p. 458\)](#)
- [终止实例 \(API\) 后会发生什么？ \(p. 459\)](#)
- [终止实例 \(p. 459\)](#)
- [为实例启用终止保护 \(p. 459\)](#)
- [更改实例的启动关闭操作 \(p. 460\)](#)
- [在实例终止时保留 Amazon EBS 卷 \(p. 461\)](#)
- [故障排除 \(p. 463\)](#)

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，默认情况下，即使在实例终止后，您在启动时附加的所有额外 EBS 卷或您附加到现有实例的所有 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 \(p. 461\)](#)。

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 \(p. 459\)](#)。

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 \(p. 460\)](#)。

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 (API) 后会发生什么？

使用 `terminate-instances` 命令终止 EC2 实例后，将在操作系统级别注册以下内容：

- API 请求将向访客发送按钮按下事件。
- 由于此按钮按下事件，将停止各种系统服务。`systemd` 处理系统的正常关闭。来自管理程序的 ACPI 关闭按钮按下事件触发正常关闭。
- 启动 ACPI 关闭。
- 当正常关闭进程退出时，实例将关闭。没有可配置的操作系统关闭时间。

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 (实例)。
4. 选择所需实例，然后依次选择 Actions、Instance State、Terminate。
5. 当系统提示您确认时，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。要使用 Amazon EC2 防止实例意外终止，可以为实例启用终止保护。DisableApiTermination 属性可控制是否可以使用控制台、CLI 或 API 终止实例。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 `DisableApiTermination` 属性时，`InstanceInitiatedShutdownBehavior` 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 \(p. 460\)](#)。

限制

您不能为 Spot 实例启用终止保护，当 Spot 价格超过您愿意为 Spot 实例支付的金额时，Spot 实例将终止。不过，您可以准备应用程序来处理 Spot 实例中断。有关更多信息，请参阅 [Spot 实例中断 \(p. 325\)](#)。

`DisableApiTermination` 属性不会阻止 Amazon EC2 Auto Scaling 终止实例。对于 Auto Scaling 组中的实例，请使用下列 Amazon EC2 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 Amazon EC2 Auto Scaling 用户指南中的[实例保护](#)。
- 要阻止 Amazon EC2 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 Amazon EC2 Auto Scaling 用户指南中的[暂停和恢复扩展流程](#)。
- 要指定 Amazon EC2 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 Amazon EC2 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 (操作)、Instance Settings (实例设置)、Change Termination Protection (更改终止保护)。
2. 选择 Yes, Enable (是，启用)。

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 (操作)、Instance Settings (实例设置)、Change Termination Protection (更改终止保护)。
2. 选择 Yes, Disable (是，禁用)。

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)

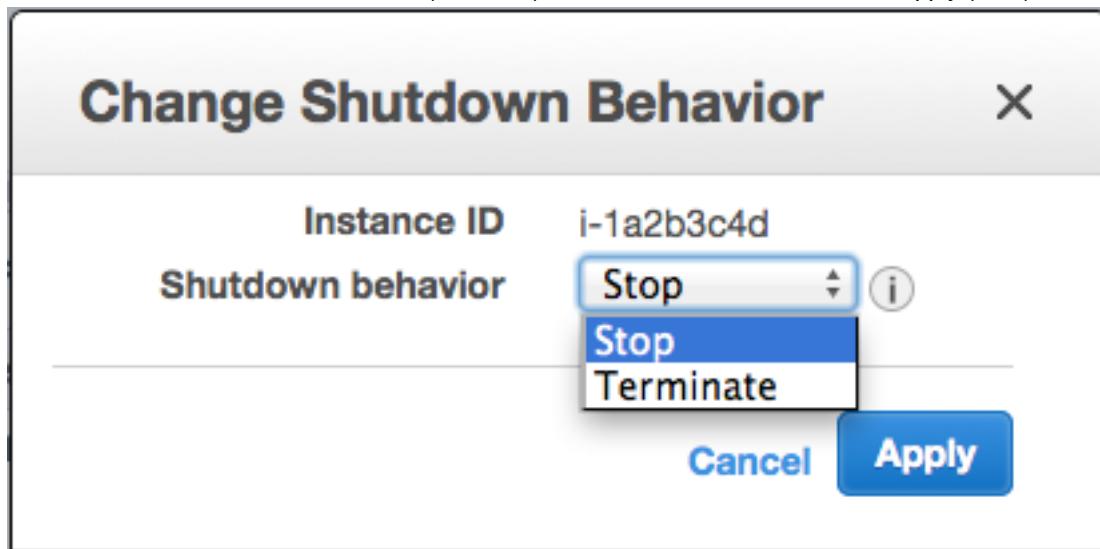
更改实例的启动关闭操作

默认情况下，从由 Amazon EBS 支持的实例启动关闭（使用 `shutdown` 或 `poweroff` 之类的命令），该实例将会停止。（请注意，`halt` 不会发出 `poweroff` 命令；如果使用 `halt` 命令，实例将不会终止；而是将 CPU 置于 HLT 状态，实例仍保持运行）。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。

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 (实例)。
3. 选择实例，然后依次选择 Actions (操作)、Instance Settings (实例设置)、Change Shutdown Behavior (更改关闭行为)。已选定当前操作。
4. 要更改行为，请从 Shutdown behavior (关闭行为) 列表中选择一个选项，然后选择 Apply (应用)。



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。根据卷是否为实例的根卷，DeleteOnTermination 属性的默认值会有所不同。

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，默認為删除该实例的根卷。DeletionOnTermination 属性可由 AMI 的创建者以及实例的启动者设置。当 AMI 的创建者或实例的启动者更改属性时，新的设置将覆盖原始 AMI 默认设置。我们建议您在使用 AMI 启动实例后验证 DeletionOnTermination 属性的默认设置。

默认情况下，当您将 EBS 卷附加到某个实例时，其 DeleteOnTermination 属性将设置为 `false`。因此，默認為保留这些卷。在该实例终止后，您可以为保留的卷拍摄快照，或将其附加到另一个实例。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 \(p. 812\)](#)。

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 \(p. 930\)](#)。

在启动该实例或在该实例正在运行时，您可以更改卷的 DeletionOnTermination 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 \(p. 462\)](#)

- 使用命令行将根卷更改为在启动时持久保留 (p. 462)
- 使用命令行更改要持久保留正在运行的实例的根卷 (p. 462)

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. 完成其余向导页面上的操作，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，可以使用以下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

您可以使用以下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 \(p. 963\)](#)。

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（由于发生基础硬件故障或需要 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。如果受损实例位于放置组中，则已恢复的实例将在放置组中运行。有关使用 Amazon CloudWatch 警报来恢复实例的更多信息，请参阅[向 Amazon CloudWatch 警报添加恢复操作 \(p. 558\)](#)。要解决实例恢复失败问题，请参阅[对实例恢复故障进行排除故障 \(p. 464\)](#)。

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
- 物理主机上影响到网络连接状态的硬件问题

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。

要求

只有具有以下特性的实例支持恢复操作：

- 使用以下其中一种实例类
型：A1、C3、C4、C5、C5n、Inf1、M3、M4、M5、M5a、M5n、P3、R3、R4、R5、R5a、R5n、T2、T3、T3a、X1 或 X1e
- 在 Virtual Private Cloud (VPC) 中运行
- 使用 default 或 dedicated 实例租赁
- 仅具有 EBS 卷（未配置实例存储卷）

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。

自动恢复过程将会尝试恢复您的实例（每天最多针对三个不同的故障）。如果实例系统状态检查故障仍然存在，建议您手动停止并启动实例。有关更多信息，请参阅[停止和启动您的实例 \(p. 445\)](#)。

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。

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。

目录

- [常见配置方案 \(p. 464\)](#)
- [在 Linux 实例上管理软件 \(p. 465\)](#)
- [在 Linux 实例上管理用户账户 \(p. 469\)](#)
- [您的 EC2 实例的处理器状态控制 \(p. 471\)](#)
- [为 Linux 实例设置时间 \(p. 476\)](#)
- [优化 CPU 选项 \(p. 480\)](#)
- [更改 Linux 实例的主机名 \(p. 490\)](#)
- [在 Linux 实例上设置动态 DNS \(p. 493\)](#)
- [启动时在 Linux 实例上运行命令 \(p. 494\)](#)
- [实例元数据和用户数据 \(p. 499\)](#)

常见配置方案

Amazon Linux 的基本发行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 \(p. 465\)](#)。

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 \(p. 469\)](#)。

Amazon Linux 实例的默认时间配置使用 Amazon Time Sync Service 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 \(p. 476\)](#)。

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 \(p. 490\)](#)。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 \(p. 493\)](#)。

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 \(p. 494\)](#)。

在 Linux 实例上管理软件

Amazon Linux 的基本发行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。

目录

- [更新实例软件 \(p. 465\)](#)
- [添加存储库 \(p. 466\)](#)
- [查找软件包 \(p. 467\)](#)
- [安装软件包 \(p. 468\)](#)
- [准备编译软件 \(p. 468\)](#)

使软件保持最新非常重要。Linux 发行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 \(p. 465\)](#)。

默认情况下，Amazon Linux 实例启动时启用以下存储库：

- Amazon Linux 2：amzn2-core 和 amzn2extra-docker
- Amazon Linux AMI：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 \(p. 466\)](#)。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 \(p. 467\)](#)。有关在 Amazon Linux 实例上安装软件的信息，请参阅[安装软件包 \(p. 468\)](#)。

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 \(p. 468\)](#)。

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 发行版（如 Ubuntu）使用 apt-get 命令和 dpkg 程序包管理器，因此，下面几部分中的 yum 示例不适用于这些发行版。

更新实例软件

使软件保持最新非常重要。Linux 发行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。

更新 Amazon Linux 实例上的所有程序包

1. (可选) 在 Shell 窗口中启动 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，不会有问题是。
 - a. 执行 screen 命令以开始会话。

```
[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 重新连接到屏幕。

```
[ec2-user ~]$ screen -r 17793
```

- d. 使用 screen 完成操作后，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
```

3. 查看所列的程序包，键入 y 并按 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。
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
```

2. 查看所列的程序包信息，键入 y 并按 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。
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。您可以手动执行此操作，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。

将 yum 存储库添加到 `/etc/yum.repos.d`

1. 查找 `.repo` 文件的位置。这随要添加的存储库而异。在本示例中，`.repo` 文件位于 `https://www.example.com/repository.repo`。
2. 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
| 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

安装存储库后，必须按照以下过程启用存储库。

在 `/etc/yum.repos.d` 中启用 yum 存储库

- 使用带 `yum-config-manager` 标志的 `--enable repository` 命令。以下命令从 Fedora 项目启用 Extra Packages for Enterprise Linux (EPEL) 存储库。默认情况下，此存储库显示在 Amazon Linux AMI 实例上的 `/etc/yum.repos.d` 中，但未启用。

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

Note

要在 Amazon Linux 2 上启用 EPEL 存储库，请使用以下命令：

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
release-latest-7.noarch.rpm
```

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该命令；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
```

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 `sudo yum install package` 命令，将 `package` 替换为要安装的软件的名称。例如，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
```

您还可使用 `sudo 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”的程序包组中包含这些工具，而这个程序包组可通过 `sudo yum groupinstall "Development Tools"` 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 `sudo yumdownloader --source` 命令下载已安装的任何程序包的源代码。

- 运行 `sudo yumdownloader --source 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 ~]$ yumdownloader --source htop
Loaded plugins: priorities, update-motd, upgrade-helper
Enabling amzn-updates-source repository
Enabling amzn-main-source repository
amzn-main-source
| 1.9 kB 00:00:00
amzn-updates-source
| 1.9 kB 00:00:00
(1/2): amzn-updates-source/latest/primary_db
| 52 kB 00:00:00
(2/2): amzn-main-source/latest/primary_db
| 734 kB 00:00:00
htop-1.0.1-2.3.amzn1.src.rpm
```

源 RPM 的位置位于您运行命令的目录中。

在 Linux 实例上管理用户账户

每个 Linux 实例均使用默认 Linux 系统用户账户启动。默认用户名由启动实例时指定的 AMI 确定。对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。对于 CentOS，用户名是 `centos`。对于 Debian，用户名是 `admin` 或 `root`。对于 Fedora，用户名是 `ec2-user` 或 `fedora`。对于 RHEL，用户名是 `ec2-user` 或 `root`。对于 SUSE，用户名是 `ec2-user` 或 `root`。对于 Ubuntu，用户名是 `ubuntu`。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](#)。

目录

- [注意事项 \(p. 469\)](#)
- [创建用户账户 \(p. 469\)](#)
- [删除用户账户 \(p. 471\)](#)

注意事项

对于许多应用程序来说，使用默认用户帐户是适当的。但是，您可以选择添加用户账户，以便个人能够拥有自己的文件和工作区。此外，为新用户创建用户账户比向多个（可能缺乏经验的）用户授予对默认用户账户的访问权限更安全，因为如果使用不当，该默认用户账户可能对系统造成严重破坏。有关更多信息，请参阅[有关保护您的 EC2 实例的提示](#)。

要使用 Linux 系统用户账户启用对 EC2 实例的用户 SSH 访问，您必须与用户分享 SSH 密钥。此外，您可以使用 EC2 实例连接来向用户提供访问权限而无需共享和管理 SSH 密钥。有关更多信息，请参阅[使用 EC2 Instance Connect 连接到 Linux 实例 \(p. 428\)](#)。

创建用户账户

首先创建用户账户，然后添加允许用户连接并登录实例的 SSH 公有密钥。

先决条件

- 为各个用户创建密钥对或使用现有密钥对

与对应用户共享 `.pem` 文件。有关更多信息，请参阅[使用 Amazon EC2 创建密钥对 \(p. 760\)](#)。

- 从各个密钥对检索公有密钥

有关更多信息，请参阅 [在 Linux 上检索密钥对的公有密钥 \(p. 762\)](#) 或 [在 Windows 上检索密钥对的公有密钥 \(p. 763\)](#)。

创建用户账户

- 使用 adduser 命令创建用户账户并将其添加到系统 (`/etc/passwd` 文件中会有一个条目) 中。该命令还可以为账户创建一个组和一个主目录。在此示例中，用户账户名为 newuser。

```
[ec2-user ~]$ sudo adduser newuser
```

[Ubuntu] 在将用户添加到 Ubuntu 系统时，请使用该命令包含 `--disabled-password` 参数，以避免向该账户添加密码。

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

- 切换到新账户，以便将创建的目录和文件具有正确的所有权。

```
[ec2-user ~]$ sudo su - newuser  
[newuser ~]$
```

请注意，在此示例中，如果提示从 ec2-user 变为 newuser，则表示您已将 Shell 会话切换到新账户。

- 将 SSH 公有密钥添加到用户账户。首先在 SSH 密钥文件的用户主目录中创建一个目录，然后创建密钥文件，最后将公有密钥粘贴到密钥文件中。
 - 在 `.ssh` 主目录中创建一个 newuser 目录，并将其权限更改为 700 (只有文件所有者能够读取、写入或打开该目录。)

```
[newuser ~]$ mkdir .ssh  
[newuser ~]$ chmod 700 .ssh
```

Important

如果没有这些确切的文件权限，用户将无法登录。

- 在 `authorized_keys` 目录中创建名为 `.ssh` 的文件并将其权限更改为 600 (只有文件所有者能够读取或写入此文件)。

```
[newuser ~]$ touch .ssh/authorized_keys  
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

Important

如果没有这些确切的文件权限，用户将无法登录。

- 使用您常用的文本编辑器 (如 vim 或 nano) 打开 `authorized_keys` 文件。

```
[newuser ~]$ nano .ssh/authorized_keys
```

将密钥对的公有密钥粘贴到该文件并保存更改。例如：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnBItnckiJ7FbtxJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQs3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb
```

BQoQzd8v7yeb7Oz1PnWoyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE

用户现在应该能够使用对应添加到 `newuser` 文件的公有密钥的私有密钥登录实例上的 `authorized_keys` 账户。

删除用户账户

如果不再需要某个用户账户，可以将其删除，使它不再可用。

使用 `userdel` 命令从系统中删除用户账户。当您指定 `-r` 参数时，用户的主目录和邮件后台打印将被删除。要保留用户的主目录和邮件后台打印，请省略 `-r` 参数。

```
[ec2-user ~]$ sudo userdel -r olduser
```

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：

- 通用 : m4.10xlarge | m4.16xlarge | m5.metal | m5d.metal
- 计算优化: c4.8xlarge | c5.metal
- 内存优化 : r4.8xlarge | r4.16xlarge | r5.metal | r5d.metal | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | x1.16xlarge | x1.32xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | z1d.metal
- 存储优化 : d2.8xlarge | i3.8xlarge | i3.16xlarge | i3.metal | i3en.metal | h1.8xlarge | h1.16xlarge
- 加速计算: f1.16xlarge | g3.16xlarge | p2.16xlarge | p3.16xlarge

以下实例类型为操作系统提供了控制处理器 C 状态的功能：

- 通用 : m5.12xlarge | m5.24xlarge | m5d.12xlarge | m5d.24xlarge
- 计算优化 : c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge
- 内存优化 : r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | r5n.24xlarge | z1d.6xlarge | z1d.12xlarge
- 存储优化 : i3en.12xlarge | i3en.24xlarge
- 加速计算 : p3dn.24xlarge

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能 (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 发行版。有关其他 Linux 发行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。

如果输出不显示 C 状态信息，请在命令中加入 --debug 选项 (sudo turbostat --debug stress <options>)。

目录

- 具有最大睿频加速频率的最高性能 (p. 472)
- 通过限制深层 C 状态实现高性能和低延迟 (p. 473)
- 变化最少的基准性能 (p. 474)

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，因为其他内核已进入 C6 睡眠状态以节省性能，并为正在工作的内核提供性能和热空间。vCPU 3 和 vCPU 10（分别与 vCPU 21 和 vCPU 28 共享一个处理器内核）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 2 上的深层睡眠状态

1. 使用所选编辑器打开 `/etc/default/grub` 文件。

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. 编辑 `GRUB_CMDLINE_LINUX_DEFAULT` 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。

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1"
GRUB_TIMEOUT=0
```

3. 保存文件并退出您的编辑器。
4. 运行以下命令重新构建启动配置。

```
[ec2-user ~]$ grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. 重启实例以启用新的内核选项。

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

限制 Amazon Linux AMI 上的深层睡眠状态

1. 使用所选编辑器打开 `/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  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  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 2 上的深层睡眠状态并禁用睿频加速

1. 使用所选编辑器打开 /etc/default/grub 文件。

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. 编辑 GRUB_CMDLINE_LINUX_DEFAULT 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。

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1"  
GRUB_TIMEOUT=0
```

3. 保存文件并退出您的编辑器。
4. 运行以下命令重新构建启动配置。

```
[ec2-user ~]$ grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. 重启实例以启用新的内核选项。

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

6. 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"
```

7. 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"
```

限制 Amazon Linux AMI 上的深层睡眠状态并禁用睿频加速

1. 使用所选编辑器打开 /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
65.33 19.02 100.00  0.00
0   0   18  0.04 2.90 2.90    0 99.96
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。

Amazon 提供 Amazon Time Sync Service，该服务可从所有 EC2 实例访问，同样由其他 AWS 服务使用。该服务在每个区域中使用一组与卫星连接的原子参考时钟，以通过网络时间协议 (NTP) 提供准确的当前协调世界时 (UTC) 全球标准时间读数。Amazon Time Sync Service 自动消除在 UTC 中添加的任何闰秒。

Amazon Time Sync Service 是通过 NTP (IP 地址为 169.254.169.123) 为 VPC 中运行的任何实例提供的。您的实例不需要访问 Internet，并且您不必配置安全组规则或网络 ACL 规则以允许进行访问。最新版本的 Amazon Linux 2 和 Amazon Linux AMIs 默认情况下与 Amazon Time Sync Service 同步。

可以使用以下步骤通过 chrony 客户端在实例上配置 Amazon Time Sync Service。或者，您也可以使用外部 NTP 源。有关 NTP 和公共时间源的更多信息，请访问 <http://www.ntp.org/>。实例需要访问 Internet，外部 NTP 时间源才能正常工作。

在 Amazon Linux AMI 上配置 Amazon Time Sync Service

Note

在 Amazon Linux 2 上，默认 chrony 配置已设置为使用 Amazon Time Sync Service IP 地址。

对于 Amazon Linux AMI，您必须编辑 chrony 配置文件以添加 Amazon Time Sync Service 的服务器条目。

配置实例以使用 Amazon Time Sync Service

1. 连接到您的实例并卸载 NTP 服务。

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. 安装 chrony 软件包。

```
[ec2-user ~]$ sudo yum install chrony
```

3. 使用任何文本编辑器 (如 vim 或 nano) 打开 /etc/chrony.conf 文件。确认该文件包含以下行：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

如果该行存在，则已配置 Amazon Time Sync Service，您可以转到下一步。如果不存在，请在该文件中已包含的任何其他 server 或 pool 语句后面添加该行，然后保存您的更改。

4. 启动 chrony 守护程序 (chronyd)。

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

```
Starting chronyd: [ OK ]
```

Note

在 RHEL 和 CentOS (最高版本为 6) 上，服务名称是 chrony 而不是 chronyd。

5. 使用 chkconfig 命令可将 chronyd 配置为在每次系统启动时启动。

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

6. 确认 chrony 使用 169.254.169.123 IP 地址同步时间。

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

.-- Source mode '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
|| | | | | | | | |
|| | | | | | | | |
|| | | | | | | | |
|| | | | | | | | |
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====

^* 169.254.169.123           3   6    17    43    -30us[ -226us] +/-  287us
^- ec2-12-34-231-12.eu-west>  2   6    17    43    -388us[ -388us] +/-   11ms
^- tshirt.heanet.ie          1   6    17    44    +178us[ +25us] +/- 1959us
^? tbag.heanet.ie            0   6     0     -      +0ns[ +0ns] +/-    0ns
^? bray.walcz.net            0   6     0     -      +0ns[ +0ns] +/-    0ns
^? 2a05:d018:c43:e312:ce77:> 0   6     0     -      +0ns[ +0ns] +/-    0ns
^? 2a05:d018:dab:2701:b70:b> 0   6     0     -      +0ns[ +0ns] +/-    0ns
```

在返回的输出中，^* 指示首选的时间源。

7. 验证 chrony 报告的时间同步指标。

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID      : A9FEA97B (169.254.169.123)
Stratum          : 4
Ref time (UTC)   : Wed Nov 22 13:18:34 2017
```

```
System time      : 0.000000626 seconds slow of NTP time
Last offset     : +0.002852759 seconds
RMS offset      : 0.002852759 seconds
Frequency       : 1.187 ppm fast
Residual freq   : +0.020 ppm
Skew            : 24.388 ppm
Root delay      : 0.000504752 seconds
Root dispersion : 0.001112565 seconds
Update interval : 64.4 seconds
Leap status     : Normal
```

在 Ubuntu 上配置 Amazon Time Sync Service

您必须编辑 chrony 配置文件以添加 Amazon Time Sync Service 的服务器条目。

配置实例以使用 Amazon Time Sync Service

1. 连接到您的实例并使用 apt 安装 chrony 软件包。

```
ubuntu:~$ sudo apt install chrony
```

Note

如有必要，请先运行 sudo apt update 以更新您的实例。

2. 使用任何文本编辑器（如 vim 或 nano）打开 /etc/chrony/chrony.conf 文件。在该文件中已包含的任何其他 server 或 pool 语句前面添加以下行，然后保存您的更改：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. 重新启动 chrony 服务。

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
[ ok ] Restarting chrony (via systemctl): chrony.service.
```

4. 确认 chrony 使用 169.254.169.123 IP 地址同步时间。

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

.-- Source mode '^' = server, '=' = peer, '#' = local clock.
/- Source state '*' = current synced, '+' = combined, '-' = not combined,
| / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||          .- xxxx [ yyyy ] +/- zzzz
||          |   xxxx = adjusted offset,
||          |   yyyy = measured offset,
||          |   zzzz = estimated error.
||          |   |
||          \   |
||          |   |
||          |   \
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
^* 169.254.169.123          3    6    17    12    +15us[ +57us] +/- 320us
^- tbag.heanet.ie          1    6    17    13   -3488us[-3446us] +/- 1779us
^- ec2-12-34-231-12.eu-west- 2    6    17    13    +893us[ +935us] +/- 7710us
^? 2a05:d018:c43:e312:ce77:6  0    6     0   10y    +0ns[ +0ns] +/-    0ns
^? 2a05:d018:d34:9000:d8c6:5  0    6     0   10y    +0ns[ +0ns] +/-    0ns
^? tshirt.heanet.ie         0    6     0   10y    +0ns[ +0ns] +/-    0ns
```

```
^? bray.walcz.net          0   6      0   10y    +0ns[  +0ns ] +/-    0ns
```

在返回的输出中，`^*` 指示首选的时间源。

- 验证 chrony 报告的时间同步指标。

```
ubuntu:~$ chronyc tracking
```

```
Reference ID      : 169.254.169.123 (169.254.169.123)
Stratum          : 4
Ref time (UTC)   : Wed Nov 29 07:41:57 2017
System time      : 0.000000011 seconds slow of NTP time
Last offset      : +0.000041659 seconds
RMS offset       : 0.000041659 seconds
Frequency        : 10.141 ppm slow
Residual freq   : +7.557 ppm
Skew             : 2.329 ppm
Root delay       : 0.000544 seconds
Root dispersion  : 0.000631 seconds
Update interval  : 2.0 seconds
Leap status      : Normal
```

在 SUSE Linux 上配置 Amazon Time Sync Service

从 <https://software.opensuse.org/package/chrony> 安装 chrony。

使用任何文本编辑器（如 vim 或 nano）打开 /etc/chrony.conf 文件。确认该文件包含以下行：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

如果此行不存在，请添加它。注释掉任何其他服务器或池行。打开 yast 并启用 chrony 服务。

在 Amazon Linux 上更改时区

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。

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。

更改实例上的时区

- 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       GMTO       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）。在此示例中，您可以使用洛杉矶的时区文件 /usr/share/zoneinfo/America/Los_Angeles。

- 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 (忽略路径的 /usr/share/zoneinfo 部分)。例如，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
```

优化 CPU 选项

Amazon EC2 实例支持多线程技术，该技术可使多个线程在一个 CPU 核心上并发运行。每个线程都表示为实例上的一个虚拟 CPU (vCPU)。实例具有默认数量的 CPU 核心，根据实例类型而异。例如，默认情况下，m5.xlarge 实例类型有两个 CPU 内核，每个内核有两个线程—，共四个 vCPU。

Note

除 T2 实例外，每个 vCPU 都是 CPU 核心的一个线程。

在大多数情况下，都有一个 Amazon EC2 实例类型，它具有适合您工作负载的内存和 vCPU 数量组合。但是，您可以指定以下 CPU 选项来针对特定工作负载或业务需求优化实例：

- CPU 核心数：您可以自定义实例的 CPU 核心数。也许可以通过这种方式让实例拥有适合内存密集型工作负载的充足内存，同时减少 CPU 核心数，从而优化您的软件的许可成本。
- 每内核线程数：您可以通过为每个 CPU 内核指定一个线程来禁用多线程技术。也许可以为特定工作负载（例如高性能计算 (HPC) 工作负载）执行该操作。

可以在实例启动期间指定上述 CPU 选项。指定 CPU 选项不会增加或减少费用。收费标准与使用默认 CPU 选项启动的实例相同。

目录

- [指定 CPU 选项的规则 \(p. 480\)](#)
- [每种实例类型的 CPU 核心数和每 CPU 核心线程数 \(p. 481\)](#)
- [指定实例的 CPU 选项 \(p. 488\)](#)
- [查看实例的 CPU 选项 \(p. 489\)](#)

指定 CPU 选项的规则

要为您的实例指定 CPU 选项，请注意以下规则：

- CPU 选项只能在实例启动期间指定，启动后无法修改。
- 启动实例时，必须在请求中指定 CPU 核心数和每核心线程数。有关示例请求，请参阅[指定实例的 CPU 选项 \(p. 488\)](#)。
- 实例的 vCPU 总数等于 CPU 内核数乘以每内核线程数。要指定自定义数量的 vCPU，必须为实例类型指定有效的 CPU 核心数和每核心线程数。不能超出实例的默认 vCPU 数量。有关更多信息，请参阅[每种实例类型的 CPU 核心数和每 CPU 核心线程数 \(p. 481\)](#)。
- 要禁用多线程技术，请为每个内核指定一个线程。
- [更改现有实例的实例类型 \(p. 233\)](#)时，CPU 选项会自动更改为新实例类型的默认 CPU 选项。
- 停止、启动或重启实例后，仍将保留指定的 CPU 选项。

每种实例类型的 CPU 核心数和每 CPU 核心线程数

下表列出了支持指定 CPU 选项的实例类型。对于每种类型，该表显示了默认的和支持的 CPU 核心数及每核心线程数。

加速计算实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
f1.2xlarge	8	4	2	1、2、3、4	1、2
f1.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
f1.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
g3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
g3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
g3.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
g3s.xlarge	4	2	2	1、2	1、2
g4dn.xlarge	4	2	2	1、2	1、2
g4dn.2xlarge	8	4	2	1、2、3、4	1、2
g4dn.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
g4dn.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
g4dn.12xlarge	48	24	2	4、6、8、10、12、14、16、18、20、22、24	
g4dn.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
p2.xlarge	4	2	2	1、2	1、2
p2.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
p2.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
p3.2xlarge	8	4	2	1、2、3、4	1、2
p3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
p3.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
p3dn.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、26	

计算优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
c4.large	2	1	2	1	1、2
c4.xlarge	4	2	2	1、2	1、2
c4.2xlarge	8	4	2	1、2、3、4	1、2
c4.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
c4.8xlarge	36	18	2	2、4、6、8、10、1122 14、16、18	
c5.large	2	1	2	1	1、2
c5.xlarge	4	2	2	2	1、2
c5.2xlarge	8	4	2	2、4	1、2
c5.4xlarge	16	8	2	2、4、6、8	1、2
c5.9xlarge	36	18	2	2、4、6、8、10、1122 14、16、18	
c5.12xlarge	48	24	2	4、6、8、10、121、122、16、18、20、22、24	
c5.18xlarge	72	36	2	4、6、8、10、121、122、16、18、20、22、24	
c5.24xlarge	96	48	2	4、6、8、10、121、122、16、18、20、22、24	
c5d.large	2	1	2	1	1、2
c5d.xlarge	4	2	2	2	1、2
c5d.2xlarge	8	4	2	2、4	1、2
c5d.4xlarge	16	8	2	2、4、6、8	1、2
c5d.9xlarge	36	18	2	2、4、6、8、10、1122 14、16、18	
c5d.12xlarge	48	24	2	4、6、8、10、121、122、16、18、20、22、24	
c5d.18xlarge	72	36	2	4、6、8、10、121、122、16、18、20、22、24	
c5d.24xlarge	96	48	2	4、6、8、10、121、122、16、18、20、22、24	
c5n.large	2	1	2	1	1、2
c5n.xlarge	4	2	2	2	1、2
c5n.2xlarge	8	4	2	2、4	1、2
c5n.4xlarge	16	8	2	2、4、6、8	1、2
c5n.9xlarge	36	18	2	2、4、6、8、10、1122 14、16、18	
c5n.18xlarge	72	36	2	4、6、8、10、121、122、16、18、20、22、24	

通用实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
m5.large	2	1	2	1	1、2
m5.xlarge	4	2	2	2	1、2
m5.2xlarge	8	4	2	2、4	1、2
m5.4xlarge	16	8	2	2、4、6、8	1、2
m5.8xlarge	32	16	2	2、4、6、8、10、1122	14、16
m5.12xlarge	48	24	2	2、4、6、8、10、1122	14、16、18、20、22、24
m5.16xlarge	64	32	2	4、6、8、10、121、12	16、18、20、22、24、26、28、30、32
m5.24xlarge	96	48	2	4、6、8、10、121、12	16、18、20、22、24
m5a.large	2	1	2	1	1、2
m5a.xlarge	4	2	2	2	1、2
m5a.2xlarge	8	4	2	2、4	1、2
m5a.4xlarge	16	8	2	2、4、6、8	1、2
m5a.8xlarge	32	16	2	2、4、6、8、10、1122	14、16
m5a.12xlarge	48	24	2	6、12、18、24	1、2
m5a.16xlarge	64	32	2	4、6、8、10、121、12	16、18、20、22、24、26、28、30、32
m5a.24xlarge	96	48	2	12、18、24、36、1482	
m5ad.large	2	1	2	1	1、2
m5ad.xlarge	4	2	2	2	1、2
m5ad.2xlarge	8	4	2	2、4	1、2
m5ad.4xlarge	16	8	2	2、4、6、8	1、2
m5ad.8xlarge	32	16	2	2、4、6、8、10、1122	14、16
m5ad.12xlarge	48	24	2	6、12、18、24	1、2
m5ad.16xlarge	64	32	2	4、6、8、10、121、12	16、18、20、22、24、26、28、30、32
m5ad.24xlarge	96	48	2	12、18、24、36、1482	
m5d.large	2	1	2	1	1、2
m5d.xlarge	4	2	2	2	1、2
m5d.2xlarge	8	4	2	2、4	1、2
m5d.4xlarge	16	8	2	2、4、6、8	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
m5d.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
m5d.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	
m5d.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	
m5d.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24	
m5dn.large	2	1	2	1	1、2
m5dn.xlarge	4	2	2	2	1、2
m5dn.2xlarge	8	4	2	2、4	1、2
m5dn.4xlarge	16	8	2	2、4、6、8	1、2
m5dn.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
m5dn.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	
m5dn.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	
m5dn.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24	
m5n.large	2	1	2	1	1、2
m5n.xlarge	4	2	2	2	1、2
m5n.2xlarge	8	4	2	2、4	1、2
m5n.4xlarge	16	8	2	2、4、6、8	1、2
m5n.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
m5n.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	
m5n.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	
m5n.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24	
t3.nano	2	1	2	1	1、2
t3.micro	2	1	2	1	1、2
t3.small	2	1	2	1	1、2
t3.medium	2	1	2	1	1、2
t3.large	2	1	2	1	1、2
t3.xlarge	4	2	2	2	1、2
t3.2xlarge	8	4	2	2、4	1、2
t3a.nano	2	1	2	1	1、2
t3a.micro	2	1	2	1	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
t3a.small	2	1	2	1	1、2
t3a.medium	2	1	2	1	1、2
t3a.large	2	1	2	1	1、2
t3a.xlarge	4	2	2	2	1、2
t3a.2xlarge	8	4	2	2、4	1、2

内存优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
r4.large	2	1	2	1	1、2
r4.xlarge	4	2	2	1、2	1、2
r4.2xlarge	8	4	2	1、2、3、4	1、2
r4.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
r4.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
r4.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
r5.large	2	1	2	1	1、2
r5.xlarge	4	2	2	2	1、2
r5.2xlarge	8	4	2	2、4	1、2
r5.4xlarge	16	8	2	2、4、6、8	1、2
r5.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	
r5.12xlarge	48	24	2	2、4、6、8、10、11、12、14、16、18、20、22、24	
r5.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	
r5.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24	
r5a.large	2	1	2	1	1、2
r5a.xlarge	4	2	2	2	1、2
r5a.2xlarge	8	4	2	2、4	1、2
r5a.4xlarge	16	8	2	2、4、6、8	1、2
r5a.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	
r5a.12xlarge	48	24	2	6、12、18、24	1、2
r5a.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
r5a.24xlarge	96	48	2	12、18、24、36、1482	
r5ad.large	2	1	2	1	1、2
r5ad.xlarge	4	2	2	2	1、2
r5ad.2xlarge	8	4	2	2、4	1、2
r5ad.4xlarge	16	8	2	2、4、6、8	1、2
r5ad.8xlarge	32	16	2	2、4、6、8、10、1122、14、16	
r5ad.12xlarge	48	24	2	6、12、18、24	1、2
r5ad.16xlarge	64	32	2	4、6、8、10、121、12、16、18、20、22、24、26、28、30、32	
r5ad.24xlarge	96	48	2	12、18、24、36、1482	
r5d.large	2	1	2	1	1、2
r5d.xlarge	4	2	2	2	1、2
r5d.2xlarge	8	4	2	2、4	1、2
r5d.4xlarge	16	8	2	2、4、6、8	1、2
r5d.8xlarge	32	16	2	2、4、6、8、10、1122、14、16	
r5d.12xlarge	48	24	2	2、4、6、8、10、1122、14、16、18、20、22、24	
r5d.16xlarge	64	32	2	4、6、8、10、121、12、16、18、20、22、24、26、28、30、32	
r5d.24xlarge	96	48	2	4、6、8、10、121、12、16、18、20、22、24	
r5dn.large	2	1	2	1	1、2
r5dn.xlarge	4	2	2	2	1、2
r5dn.2xlarge	8	4	2	2、4	1、2
r5dn.4xlarge	16	8	2	2、4、6、8	1、2
r5dn.8xlarge	32	16	2	2、4、6、8、10、1122、14、16	
r5dn.12xlarge	48	24	2	2、4、6、8、10、1122、14、16、18、20、22、24	
r5dn.16xlarge	64	32	2	4、6、8、10、121、12、16、18、20、22、24、26、28、30、32	
r5dn.24xlarge	96	48	2	4、6、8、10、121、12、16、18、20、22、24	
r5n.large	2	1	2	1	1、2
r5n.xlarge	4	2	2	2	1、2
r5n.2xlarge	8	4	2	2、4	1、2
r5n.4xlarge	16	8	2	2、4、6、8	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
r5n.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
r5n.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	
r5n.16xlarge	64	32	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	
r5n.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24	
x1.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24	
x1.32xlarge	128	64	2	4、8、12、16、20、24、28、32	36、40、44
x1e.xlarge	4	2	2	1、2	1、2
x1e.2xlarge	8	4	2	1、2、3、4	1、2
x1e.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
x1e.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
x1e.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24	
x1e.32xlarge	128	64	2	4、8、12、16、20、24、28、32	36、40、44
z1d.large	2	1	2	1	1、2
z1d.xlarge	4	2	2	2	1、2
z1d.2xlarge	8	4	2	2、4	1、2
z1d.3xlarge	12	6	2	2、4、6	1、2
z1d.6xlarge	24	12	2	2、4、6、8、10、12、14、16、18、20、22、24	
z1d.12xlarge	48	24	2	4、6、8、10、12、14、16、18、20、22、24	

存储优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
d2.xlarge	4	2	2	1、2	1、2
d2.2xlarge	8	4	2	1、2、3、4	1、2
d2.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
d2.8xlarge	36	18	2	2、4、6、8、10、12、14、16、18	
h1.2xlarge	8	4	2	1、2、3、4	1、2
h1.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
h1.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
h1.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24	

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心数	有效的每核心线程数
i3.large	2	1	2	1	1、2
i3.xlarge	4	2	2	1、2	1、2
i3.2xlarge	8	4	2	1、2、3、4	1、2
i3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2、3、4、5、6、7、8
i3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2、3、4、5、6、7、8、9、10、11、12、13
i3.16xlarge	64	32	2	2、4、6、8、10、1122	14、16、18、20、22、24
i3en.large	2	1	2	1	1、2
i3en.xlarge	4	2	2	2	1、2
i3en.2xlarge	8	4	2	2、4	1、2
i3en.3xlarge	12	6	2	2、4、6	1、2
i3en.6xlarge	24	12	2	2、4、6、8、10、1122	
i3en.12xlarge	48	24	2	2、4、6、8、10、1122	14、16、18、20、22、24
i3en.24xlarge	96	48	2	4、6、8、10、121、122、16、18、20、22、24、25	

指定实例的 CPU 选项

可以在实例启动期间指定 CPU 选项。以下示例适用于 r4.4xlarge 实例类型，该实例类型具有以下[默认值 \(p. 485\)](#)：

- 默认 CPU 核心数：8
- 默认每核心线程数：2
- 默认 vCPU：16 (8 * 2)
- 有效的 CPU 核心数：1、2、3、4、5、6、7、8
- 有效的每核心线程数：1、2

禁用多线程技术

要禁用多线程技术，请为每个内核指定一个线程。

在实例启动期间禁用多线程技术（控制台）

1. 按照[使用启动实例向导启动实例 \(p. 375\)](#)过程操作。
2. 在 Configure Instance Details (配置实例详细信息) 页面上，为 CPU options (CPU 选项) 选择 Specify CPU options (指定 CPU 选项)。
3. 对于 Core count (内核数)，选择所需的 CPU 内核数量。在此示例中，要为 r4.4xlarge 实例指定默认 CPU 内核数，请选择 8。
4. 要禁用多线程技术，请为每内核线程数选择 1。
5. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。

在实例启动期间禁用多线程技术 (AWS CLI)

使用 [run-instances](#) AWS CLI 命令，并将 --cpu-options 参数的 ThreadsPerCore 值指定为 1。对于 CoreCount，指定 CPU 内核的数量。在此示例中，要为 r4.4xlarge 实例指定默认 CPU 内核数，请指定值 8。

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options "CoreCount=8,ThreadsPerCore=1" --key-name MyKeyPair
```

指定自定义 vCPUs 数

您可以为实例自定义 CPU 内核数和每个内核的线程数。

在实例启动期间指定自定义 vCPU 数 (控制台)

以下示例启动一个具有六个 vCPU 的 r4.4xlarge 实例。

1. 按照[使用启动实例向导启动实例 \(p. 375\)](#)过程操作。
2. 在 Configure Instance Details (配置实例详细信息) 页面上，为 CPU options (CPU 选项) 选择 Specify CPU options (指定 CPU 选项)。
3. 要获得六个 vCPU，请指定三个 CPU 内核并为每个内核指定两个线程，如下所示：
 - 对于 Core count (内核数)，选择 3。
 - 对于 Threads per core (每内核线程数)，选择 2。
4. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。

在实例启动期间指定自定义 vCPU 数 (AWS CLI)

以下示例启动一个具有六个 vCPU 的 r4.4xlarge 实例。

使用 [run-instances](#) AWS CLI 命令，并在 --cpu-options 参数中指定 CPU 内核数和线程数。可以指定三个 CPU 核心并为每个核心指定两个线程，从而获得六个 vCPU。

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options "CoreCount=3,ThreadsPerCore=2" --key-name MyKeyPair
```

或者，也可以通过指定六个 CPU 核心和为每个核心指定一个线程 (禁用多线程技术) 来获得六个 vCPU：

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options "CoreCount=6,ThreadsPerCore=1" --key-name MyKeyPair
```

查看实例的 CPU 选项

您可以在 Amazon EC2 控制台中查看现有实例的 CPU 选项，也可以通过使用 AWS CLI 描述实例来查看。

查看实例的 CPU 选项 (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，然后选择实例。
3. 选择 Description (描述)，然后查看 Number of vCPUs (vCPU 数) 字段。
4. 要查看内核数和每内核线程数，请选择 Number of vCPUs (vCPU 数) 字段值。

查看实例的 CPU 选项 (AWS CLI)

可以使用 [describe-instances](#) 命令。

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
}
```

在返回的输出中，CoreCount 字段指示实例的核心数。ThreadsPerCore 字段指示每核心线程数。

或者，也可以连接实例并使用工具（例如 lscpu）查看实例的 CPU 信息。

可以使用 AWS Config 记录、评估、审计实例的配置更改，包括终止的实例。有关更多信息，请参阅 AWS Config Developer Guide 中的 [AWS Config 入门](#)。

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。

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。

- 对于 Amazon Linux 2：使用 hostnamectl 命令设置主机名以反映完全限定域名（例如 **webserver.mydomain.com**）。

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.mydomain.com
```

- 对于 Amazon Linux AMI：在您的实例上，使用常用的文本编辑器打开 /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（在实例页面上，依次选择操作、实例状态和重启）。

- 登录实例，验证主机名是否已更新。提示符应显示新主机名（直到第一个“.”），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

- 对于 Amazon Linux 2：使用 hostnamectl 命令设置主机名以反映所需的系统主机名（例如 **webserver**）。

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.localdomain
```

- 对于 Amazon Linux AMI：在您的实例上，使用常用的文本编辑器打开 /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（在实例页面上，依次选择操作、实例状态和重启）。

- 登录实例，验证主机名是否已更新。提示符应显示新主机名（直到第一个“.”），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

如果不希望修改实例的主机名，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 提示符更改为主机别名

- 在 /etc/profile.d 中创建一个文件，用于将称为 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**，请运行以下命令。

```
[ec2-user ~]$ sudo sh -c 'echo "export NICKNAME=webserver" > /etc/profile.d/prompt.sh'
```

- 使用您常用的文本编辑器（例如 vim 或 nano）打开 /etc/bashrc (Red Hat) 或 /etc/bash.bashrc (Debian/Ubuntu) 文件。您需要在编辑器命令中使用 sudo，因为 /etc/bashrc 和 /etc/bash.bashrc 归 root 所有。
- 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 或 /etc/bash.bashrc 中查找以下设置 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。

- 创建一个名为的文件 /etc/sysconfig/bash-prompt-xterm。

```
[ec2-user ~]$ sudo touch /etc/sysconfig/bash-prompt-xterm
```

- 使用以下命令使该文件可执行。

```
[ec2-user ~]$ sudo chmod +x /etc/sysconfig/bash-prompt-xterm
```

- 在您常用的文本编辑器（如 /etc/sysconfig/bash-prompt-xterm 或 vim）中打开 nano 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。
- 将以下行添加到该文件。

```
echo -ne "\033]0;${USER}@${NICKNAME}: ${PWD/#$HOME/~}\007"
```

- 注销，再重新登录，以接受新别名值。

更改其他 Linux 发行版上的主机名

此页面上的过程仅适用于 Amazon Linux。有关其他 Linux 发行版的更多信息，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？

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>。

- 对于 Amazon Linux 2：

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- 对于 Amazon Linux AMI：

```
[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. 启用 noip 服务。

- 对于 Amazon Linux 2：

```
[ec2-user ~]$ sudo systemctl enable noip.service
```

- 对于 Amazon Linux AMI :

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

4. 启动 noip 服务。

- 对于 Amazon Linux 2 :

```
[ec2-user ~]$ sudo systemctl start noip.service
```

- 对于 Amazon Linux AMI :

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

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[启动时在您的 Windows 实例上运行命令](#)和[管理 Windows 实例配置](#)。

在以下示例中，在 [Amazon Linux 2 上安装 LAMP Web 服务器 \(p. 28\)](#)中的命令转换成了 Shell 脚本和一组在实例启动时执行的 cloud-init 指令。在每个示例中，以下任务都根据用户数据执行：

- 更新发行版软件包。
- 安装必要的 Web 服务器、php 和 mariadb 程序包。
- 通过 systemctl 启动和打开 httpd 服务。
- ec2-user 将添加到 apache 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。

目录

- [先决条件 \(p. 495\)](#)
- [用户数据和 Shell 脚本 \(p. 495\)](#)
- [用户数据和控制台 \(p. 495\)](#)
- [用户数据和 cloud-init 指令 \(p. 496\)](#)
- [用户数据和 AWS CLI \(p. 497\)](#)

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 \(p. 25\)](#)。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 \(p. 18\)](#)。

此外，这些指令适用于 Amazon Linux 2，这些命令和指令可能不适用于其他 Linux 发行版。有关其他发行版的更多信息，如它们对 cloud-init 的支持，请参阅各自的具体文档。

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。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。

Important

默认情况下，用户数据脚本和 cloud-init 指令仅在您首次启动实例时在引导循环过程中运行。您可以更新配置，以确保在每次重新启动实例时都运行用户数据脚本和 cloud-init 指令。有关更多信息，请参阅 AWS 知识中心内的[如何可以在每次重新启动我的 EC2 实例时执行用户数据？](#)。

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；如果您需要非根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）。

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。

在处理用户数据脚本时，该脚本将复制到 /var/lib/cloud/instances/*instance-id*/ 目录并从该目录执行。脚本在运行后无法删除。请在从实例创建 AMI 之前务必删除 /var/lib/cloud/instances/*instance-id*/ 中的用户数据脚本。否则，该脚本将存在于从 AMI 启动的任何实例上的此目录中。

用户数据和控制台

您可在启动实例时指定实例用户数据。如果实例的根卷是 EBS 卷，您还可以停止实例并更新其用户数据。

启动时指定实例用户数据

按照[从 AMI 启动实例 \(p. 375\)](#)中介绍的实例启动过程操作，但在进行到该过程中的[Step 6 \(p. 376\)](#)时，在用户数据字段中复制 shell 脚本，然后完成启动过程。

在下面的示例脚本中，脚本将创建并配置我们的 Web 服务器。

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /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
```

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
```

您应该会看到 PHP 信息页面。如果您无法看到 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。有关更多信息，请参阅 [向安全组添加规则 \(p. 772\)](#)。

(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](#)。

查看和更新实例用户数据

修改实例用户数据

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择所需实例，然后依次选择 Actions、Instance State、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。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

4. 当系统提示您确认时，选择 Yes, Stop。停止实例可能需要几分钟时间。
5. 保持实例选定的情况下，依次选择操作、实例设置和查看/更改用户数据。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。
7. 重新启动实例。重新启动实例后，新的用户数据将在实例上可见；但不会执行用户数据脚本。

用户数据和 cloud-init 指令

cloud-init 程序包在启动时配置新 Amazon Linux 实例的特定方面；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有密钥登录。有关更多信息，请参阅 [cloud-init \(p. 149\)](#)。

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

默认情况下，用户数据脚本和 cloud-init 指令仅在您首次启动实例时在引导循环过程中运行。您可以更新配置，以确保在每次重新启动实例时都运行用户数据脚本和 cloud-init 指令。有关更多信息，请参阅 AWS 知识中心内的 [如何可以在每次重新启动我的 EC2 实例时执行用户数据？](#)。

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。

使用用户数据将 cloud-init 指令传递给实例

- 按照[从 AMI 启动实例 \(p. 375\)](#)中介绍的实例启动过程操作，但在进行到该过程中的[Step 6 \(p. 376\)](#)时，在 User data 字段中输入 cloud-init 指令文本，然后完成启动过程。

在以下示例中，这些指令在 Amazon Linux 2 上创建并配置 Web 服务器。要将命令标识为 cloud-init 指令，顶部的 #cloud-config 行是必需的。

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /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' ]
```

- 让实例有足够的空间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
```

您应该会看到 PHP 信息页面。如果您无法看到 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。有关更多信息，请参阅[向安全组添加规则 \(p. 772\)](#)。

- (可选) 如果指令没有完成预期执行的任务，或者如果您要验证指令是否正确完成，请检查 /var/log/cloud-init-output.log 上的输出日志文件，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' }
```

此指令将 runcmd 输出发送到 /var/log/cloud-init-output.log。

用户数据和 AWS CLI

您可以使用 AWS CLI 指定、修改和查看实例的用户数据。有关使用实例元数据从实例查看用户数据的信息，请参阅[检索实例用户数据 \(p. 510\)](#)。

在 Windows 上，您可以使用适用于 Windows PowerShell 的 AWS 工具而不是使用 AWS CLI。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[用户数据和 Windows PowerShell 工具](#)。

示例：启动时指定用户数据

要在启动实例时指定用户数据，请结合使用 `run-instances` 命令与 `--user-data` 参数。使用 `run-instances`，AWS CLI 将对您的用户数据执行 base64 编码。

以下示例显示如何在命令行上指定字符串形式的脚本：

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data echo user data
```

以下示例显示如何使用文本文件指定脚本。请务必使用 file:// 前缀指定该文件。

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data file://my_script.txt
```

以下是具有 Shell 脚本的示例文本文件。

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

示例：修改已停止的实例的用户数据

您可以使用 [modify-instance-attribute](#) 命令修改已停止的实例的用户数据。使用 modify-instance-attribute，AWS CLI 不会对用户数据执行 base64 编码。

在 Linux 上，使用 base64 命令对用户数据进行编码。

```
base64 my_script.txt >my_script_base64.txt
```

在 Windows 上，使用 certutil 命令可对用户数据进行编码。您必须先删除第一行 (BEGIN CERTIFICATE) 和最后一行 (END CERTIFICATE)，然后才能将此文件用于 AWS CLI。

```
certutil -encode my_script.txt my_script_base64.txt
notepad my_script_base64.txt
```

使用 --attribute 和 --value 参数可通过编码的文本文件指定用户数据。请务必使用 file:// 前缀指定该文件。

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData --
value file://my_script_base64.txt
```

示例：查看用户数据

要检索实例的用户数据，请使用 [describe-instance-attribute](#) 命令。使用 describe-instance-attribute，AWS CLI 不会对用户数据执行 base64 解码。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData
```

以下是具有已进行 base64 编码的用户数据的示例输出。

```
{
    "UserData": {
        "Value": "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAtOpzzXJ2aNlIGH0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

在 Linux 上，使用 --query 选项获取编码的用户数据和用于对该数据进行解码的 base64 命令。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData  
--output text --query "UserData.Value" | base64 --decode
```

在 Windows 上，使用 --query 选项获取编码的用户数据和用于对该数据进行解码的 certutil 命令。请注意，编码的输出存储在一个文件中，解码的输出存储在另一个文件中。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData  
--output text --query "UserData.Value" >my_output.txt  
certutil -decode my_output.txt my_output_decoded.txt  
type my_output_decoded.txt
```

下面是示例输出。

```
#!/bin/bash  
yum update -y  
service httpd start  
chkconfig httpd on
```

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。实例元数据分为几类，例如，主机名、事件和安全组。

您也可以使用实例元数据访问您启动实例时指定的用户数据。例如，您可以指定参数以配置实例，或者包含简单的脚本。您可以构建通用 AMI，并使用用户数据修改启动时提供的配置文件。例如，如果您为各种小型企业运行 Web 服务器，则这些企业可以使用相同的通用 AMI，并在启动时从您在用户数据中指定的 Amazon S3 存储桶中检索其内容。要随时添加新客户，请为客户创建一个存储桶，添加其内容，并使用在用户数据中为您的代码提供的唯一存储桶名称启动 AMI。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。属于同一保留的每个实例具有唯一的 ami-launch-index 编号，从而允许您编写代码以控制要执行的操作。例如，第一个主机可能会选择自己作为集群中的初始主节点。有关详细的 AMI 启动示例，请参阅[示例：AMI 启动索引值 \(p. 512\)](#)。

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 \(p. 519\)](#)。

Important

虽然您只能从实例本身中访问实例元数据和用户数据，但并未使用身份验证或加密方法对数据进行保护。任何可以直接访问实例的人以及可能在实例上运行的任何软件都可以查看其元数据。因此，您不应将敏感数据（例如密码或长期保存的加密密钥）存储为用户数据。

目录

- [配置实例元数据服务 \(p. 499\)](#)
- [检索实例元数据 \(p. 503\)](#)
- [与实例用户数据配合使用 \(p. 510\)](#)
- [检索动态数据 \(p. 511\)](#)
- [示例：AMI 启动索引值 \(p. 512\)](#)
- [实例元数据类别 \(p. 514\)](#)
- [实例身份文档 \(p. 519\)](#)

配置实例元数据服务

您可以使用以下其中一种方法，从正在运行的实例中访问实例元数据：

- 实例元数据服务版本 1 (IMDSv1) – 一种请求/响应方法
- 实例元数据服务版本 2 (IMDSv2) – 一种面向会话的方法

默认情况下，您可以使用 IMDSv1 和/或 IMDSv2。实例元数据服务根据以下条件区分 IMDSv1 和 IMDSv2 请求：对于任何给定请求，PUT 或 GET 标头（对于 IMDSv2 是唯一的）在该请求中是否存在。

您可以在每个实例上配置实例元数据服务，以便本地代码或用户必须使用 IMDSv2。在指定必须使用 IMDSv2 时，IMDSv1 不再起作用。有关更多信息，请参阅[配置实例元数据选项 \(p. 502\)](#)。

实例元数据服务版本 2 的工作原理

IMDSv2 使用面向会话的请求。对于面向会话的请求，您创建一个会话令牌以定义会话持续时间，该时间最少为 1 秒，最多为 6 小时。在指定的持续时间内，您可以将相同的会话令牌用于后续请求。在指定的持续时间到期后，您必须创建新的会话令牌以用于将来的请求。

以下示例使用 Linux Shell 脚本和 IMDSv2 检索顶级实例元数据项。示例命令：

- 使用 PUT 请求创建持续 6 小时 (21600 秒) 的会话令牌
- 将会话令牌存储在名为 TOKEN 的变量中
- 使用令牌请求顶级元数据项

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

在创建令牌后，您可以重复使用令牌，直到令牌过期。在以下示例命令（获取用于启动实例的 AMI 的 ID）中，将重复使用上一示例中的令牌（存储在 \$TOKEN 中）。

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
```

在使用 IMDSv2 请求实例元数据时，请求必须包含以下内容：

1. 使用 PUT 请求启动到实例元数据服务的会话。PUT 请求返回一个令牌，该令牌必须包含在对实例元数据服务的后续 GET 请求中。需要具有该令牌才能使用 IMDSv2 访问元数据。
2. 将该令牌包含在对实例元数据服务的所有 GET 请求中。如果将令牌使用设置为 required，没有有效令牌或令牌过期的请求将显示 401 – Unauthorized HTTP 错误代码。有关更改令牌使用要求的信息，请参阅 AWS CLI Command Reference 中的 [modify-instance-metadata-options](#)。
 - 令牌是实例特定的密钥。令牌在其他 EC2 实例上无效，如果尝试在生成令牌的实例外部使用，令牌将被拒绝。
 - PUT 请求必须包含一个标头，它以秒为单位指定令牌的生存时间 (TTL)，最多为 6 小时 (21600 秒)。令牌表示一个逻辑会话。TTL 指定令牌的有效时间长度，因而指定会话的持续时间。
 - 在令牌过期后，要继续访问实例元数据，您必须使用另一 PUT 创建新会话。
 - 您可以选择在每个请求中重复使用令牌或创建新的令牌。对于少量请求，在每次需要访问实例元数据服务时生成并立即使用令牌可能更方便。但为了提高效率，您可以为令牌指定更长的持续时间并重复使用令牌，而不必在每次需要请求实例元数据时都编写 PUT 请求。对并发令牌数量没有实际限制，每个令牌表示自己的会话。不过，IMDSv2 仍然受到正常实例元数据服务连接和限制的制约。有关更多信息，请参阅[限制 \(p. 509\)](#)。

允许在 IMDSv2 实例元数据请求中使用 HTTP GET 和 HEAD 方法。如果 PUT 请求包含 X-Forwarded-For 标头，则会被拒绝。

默认情况下，PUT 请求的响应在 IP 协议级别的响应跃点数限制（生存时间）为 1。如果需要增大跃点数限制，您可以使用 [modify-instance-metadata-options](#) 命令进行调整。例如，您可能需要使用更大

的跃点数限制，以便与实例上运行的容器服务保持向后兼容。有关更多信息，请参阅 AWS CLI Command Reference 中的 [modify-instance-metadata-options](#)。

转换为使用 实例元数据服务版本 2

使用 实例元数据服务版本 2 (IMDSv2) 是可选的。将继续无期限支持 实例元数据服务版本 1 (IMDSv1)。如果您选择迁移以使用 IMDSv2，我们建议您使用以下工具和转换途径。

帮助转换为 IMDSv2 的工具

如果您的软件使用 IMDSv1，请使用以下工具帮助重新配置软件，以使用 IMDSv2。

- AWS 软件：最新版本的 AWS 开发工具包和 CLI 支持 IMDSv2。要使用 IMDSv2，请确保 EC2 实例具有最新版本的 AWS 开发工具包和 CLI。有关更新 CLI 的信息，请参阅 AWS Command Line Interface 用户指南中的[升级到最新版本的 AWS CLI](#)。
- CloudWatch：IMDSv1 不使用支持令牌的会话。您可以通过 CloudWatch 指标 `MetadataNoToken` 跟踪未使用支持令牌的会话的实例元数据服务调用数。该指标跟踪使用 IMDSv1 的调用数。通过查看该指标是否为零，您可以确定是否以及何时将所有软件升级为使用 IMDSv2。有关更多信息，请参阅[实例指标 \(p. 540\)](#)。
- EC2 API 和 CLI 更新：对于现有实例，您可以使用 `modify-instance-metadata-options` CLI 命令（或 `ModifyInstanceMetadataOptions` API）以要求使用 IMDSv2。对于新实例，您可以使用 `run-instances` CLI 命令（或 `RunInstances` API）和 `metadata-options` 参数以启动要求使用 IMDSv2 的新实例。
- IAM 策略和 SCP：您可以使用条件键阻止用户启动新实例或修改正在运行的实例，除非他们指定仅使用 IMDSv2。您还可以使用另一个条件键，阻止使用通过 IMDSv1 获取的 EC2 角色凭证进行的后续 API 调用。可以在 IAM 策略或 AWS Organizations 服务控制策略 (SCP) 中使用这些条件键，如下一节中所述。有关更多信息，请参阅下一节中的将所有实例转换为 IMDSv2 时。有关示例 IAM 策略，请参阅[示例：使用实例元数据 \(p. 741\)](#)。

要求 IMDSv2 访问的建议途径

在使用上述工具时，我们建议您按照以下途径转换为 IMDSv2：

1. 在开始时

将在 EC2 实例上使用角色凭证的开发工具包、CLI 和软件更新为与 IMDSv2 兼容的版本。然后，使用 IMDSv2 请求更改直接访问实例元数据的软件（换句话说，不使用开发工具包）。有关更新 CLI 的信息，请参阅 AWS Command Line Interface 用户指南中的[升级到最新版本的 AWS CLI](#)。

2. 在转换期间

查看 CloudWatch 指标 `MetadataNoToken` 以跟踪转换进度，该指标显示对实例上的 IMDSv1 的调用次数。有关更多信息，请参阅[实例指标 \(p. 540\)](#)。

3. 在所有实例上一切准备就绪时

在 CloudWatch 指标 `MetadataNoToken` 记录使用次数为零时，说明在所有实例上一切准备就绪。在该阶段，您可以通过 `modify-instance-metadata-options` 命令要求使用 IMDSv2。您可以在正在运行的实例上进行这些更改，而无需重新启动实例。对于新启动的实例，您可以使用 `run-instances` 命令指定将仅使用 IMDSv2。只能通过 API 或 AWS CLI 指定实例元数据选项；目前，无法通过 AWS 管理控制台 指定这些选项。有关更多信息，请参阅 AWS CLI Command Reference 中的 `run-instances` 和 `modify-instance-metadata-options`。

4. 将所有实例转换为 IMDSv2 时

您可以使用 IAM 条件强制要求，除非实例使用 IMDSv2，否则，IAM 用户不能启动实例。有关更多信息，请参阅下一节中的在所有新实例上强制使用 IMDSv2。您也可以使用 IAM 条件强制要求 IAM 用户不能修改正在运行的实例以重新启用 IMDSv1，以及强制要求在实例上提供实例元数据服务。

此外，您还可以选择额外的保护层以强制从 IMDSv1 更改为 IMDSv2。在与通过 EC2 角色凭证调用的 API 相关的访问管理层上，您可以在 IAM 策略或 AWS Organizations 服务控制策略 (SCP) 中使用新的条件

键。具体来说，通过在 IAM 策略中使用值为 2.0 的策略条件键 `ec2:RoleDelivery`，使用从 IMDSv1 获取的 EC2 角色凭证进行的 API 调用将收到 `UnauthorizedOperation` 响应。通过使用 SCP 所需的该条件，可以更广泛地实现相同的效果。这会确保通过 IMDSv1 提供的凭证不能实际用于调用 API，因为任何不符合指定条件的 API 调用将会收到 `UnauthorizedOperation` 错误。有关示例 IAM 策略，请参阅 [示例：使用实例元数据 \(p. 741\)](#)。有关更多信息，请参阅 AWS Organizations 用户指南 中的 [服务控制策略](#)。

配置实例元数据选项

通过使用实例元数据选项，您可以配置新实例或现有实例以要求在请求实例元数据时使用 IMDSv2，指定 `PUT` 响应跃点数限制以及禁止访问实例元数据。您还可以在 IAM 策略或 SCP 中使用条件键以仅在实例配置为要求使用 IMDSv2 时启动实例，限制允许的跃点数或强制要求完全禁用 IMDS。要在新实例或现有实例上配置实例元数据选项，您可以使用 AWS 开发工具包或 CLI。有关更多信息，请参阅 AWS CLI Command Reference 中的 [run-instances](#) 和 [modify-instance-metadata-options](#)。

Note

在进行任何更改之前，您应谨慎执行操作并进行仔细的测试。记录以下内容：

- 如果您强制使用 IMDSv2，则使用 IMDSv1 访问实例元数据的应用程序或代理将会中断。
- 如果禁用对实例元数据的所有访问，则依赖于实例元数据访问才能正常工作的应用程序或代理将会中断。

在所有新实例上强制使用 IMDSv2

要确保 IAM 用户只能启动要求在请求实例元数据时使用 IMDSv2 的实例，您可以指定在启动实例之前要求 IMDSv2 必须满足的条件。

以下说明介绍如何使用 AWS CLI 创建并附加策略。有关如何使用 AWS 管理控制台的说明，请参阅 IAM 用户指南 中的 [创建 IAM 策略 \(控制台\)](#) 和 [将策略直接附加到用户以添加权限](#)。

- 创建一个 JSON 策略文档，其中包含以下内容：

- `ec2:RunInstances` 操作。这会为 IAM 用户授予权限以启动新的实例。
- 设置为 `required` 的 `ec2:MetadataHttpTokens` 条件。这指定了以下条件：要启动实例，必须将其配置为要求使用 IMDSv2，这会在实例元数据检索请求中使用安全令牌头。

下面是示例策略文档。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "RunInstanceWithImdsV2Only",  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:MetadataHttpTokens": "required"  
                }  
            }  
        }  
    ]  
}
```

- 使用 `create-policy` 命令创建新的托管策略，并指定您创建的 JSON 文档以作为新策略的内容。

```
$ aws iam create-policy --policy-name my-policy --policy-document file://JSON-file-name
```

3. 使用 [attach-user-policy](#) 命令将托管策略附加到指定的 IAM 用户。对于 `--user-name` 参数，请指定 IAM 用户的友好名称（而不是 ARN）。

```
$ aws iam attach-user-policy --policy-arn arn:aws:iam::account-id:policy/my-policy --user-name IAM-friendly-name
```

也可以使用 `ec2:MetadataHttpTokens`、`ec2:MetadataHttpPutResponseHopLimit` 和 `ec2:MetadataHttpEndpoint` IAM 条件键，以控制使用 [RunInstances](#) 和 [ModifyInstanceMetadataOptions](#) API 以及相应的 CLI。有关这些键的有效条件，请参阅 AWS CLI Command Reference 中的 [run-instances](#) 和 [modify-instance-metadata-options](#)。如果创建了策略，并且 API 调用中的参数与使用条件键的策略中指定的状态不匹配，API 或 CLI 调用将失败并显示 `UnauthorizedOperation` 响应。有关更多示例 IAM 策略，请参阅 [示例：使用实例元数据 \(p. 741\)](#)。

要求在现有实例上使用 IMDSv2

对于现有的实例，您可以选择要求在请求实例元数据时使用 IMDSv2。请使用 [modify-instance-metadata-options](#) CLI 命令，并将 `http-tokens` 参数设置为 `required`。请注意，在为 `http-tokens` 指定值时，还必须将 `http-endpoint` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options --instance-id i-1234567898abcdef0 --http-tokens required --http-endpoint enabled
```

要使用 IAM 策略控制 [ModifyInstanceMetadataOptions](#) API 以及 [RunInstances](#) API 的使用，请参阅 [示例：使用实例元数据 \(p. 741\)](#)。

更改现有实例上的 PUT 响应跃点数限制

对于现有的实例，您可以更改 PUT 响应跃点数限制设置。请使用 [modify-instance-metadata-options](#) CLI 命令，并将 `http-put-response-hop-limit` 参数设置为所需的跃点数。在以下示例中，跃点数限制设置为 3。请注意，在为 `http-put-response-hop-limit` 指定值时，还必须将 `http-endpoint` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options --instance-id i-1234567898abcdef0 --http-put-response-hop-limit 3 --http-endpoint enabled
```

在现有实例上禁用实例元数据访问

对于现有的实例，您可以禁用实例元数据服务的 HTTP 终端节点以禁用实例元数据访问，而无论使用的是哪种实例元数据服务版本。您可以随时启用 HTTP 终端节点以撤消该更改。请使用 [modify-instance-metadata-options](#) CLI 命令，并将 `http-endpoint` 参数设置为 `disabled`。

```
aws ec2 modify-instance-metadata-options --instance-id i-1234567898abcdef0 --http-endpoint disabled
```

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。

实例元数据可划分成不同类别。有关每个实例元数据类别的描述，请参阅 [实例元数据类别 \(p. 514\)](#)。

要从正在运行的实例中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/
```

IP 地址 169.254.169.254 是链路本地地址，仅从该实例有效。有关更多信息，请参阅 Wikipedia 上的[链路本地地址](#)。

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。

根据您使用的是 IMDSv1 还是 IMDSv2，命令格式会有所不同。默认情况下，您可以使用两种实例元数据服务。要要求使用 IMDSv2，请参阅[配置实例元数据服务 \(p. 499\)](#)。

您可以使用 cURL 等工具，如以下示例中所示。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

您也可以下载[实例元数据查询工具](#)，以通过实例元数据服务 1.0 版查询实例元数据，而不必输入完整 URI 或类别名称。

响应和错误消息

所有实例元数据以文本形式返回（HTTP 内容类型 `text/plain`）。

特定元数据资源的请求返回相应的值；如果资源不可用，则返回 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。

对于使用实例元数据服务版本 2 发出的请求，可能会返回以下 HTTP 错误代码：

- `400 - Missing or Invalid Parameters` – PUT 请求无效。
- `401 - Unauthorized` – GET 请求使用无效的令牌。建议的措施是生成新的令牌。
- `403 - Forbidden` – 不允许该请求，或禁用了实例元数据服务。

检索实例元数据的示例

示例

- [获取实例元数据的可用版本 \(p. 504\)](#)
- [获取顶级元数据项 \(p. 505\)](#)
- [获取可用的公有密钥列表 \(p. 507\)](#)
- [显示可以使用公有密钥 0 的格式 \(p. 508\)](#)
- [获取公有密钥 0 \(采用 OpenSSH 密钥格式\) \(p. 508\)](#)
- [获取实例的子网 ID \(p. 509\)](#)

获取实例元数据的可用版本

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。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v 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
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
latest
```

IMDSv1

```
[ec2-user ~]$ 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
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
latest
```

获取顶级元数据项

此示例获得顶级元数据项目。有关更多信息，请参阅 [实例元数据类别 \(p. 514\)](#)。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
```

```
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

以下示例获取在前面的示例中获取的某些顶级元数据项的值。IMDSv2 请求使用在前面的示例命令中创建和存储的令牌，并假设该令牌尚未过期。

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

获取可用的公有密钥列表

此示例获得可用公有密钥的列表。

IMDSv2

```
[ec2-user ~]$ `curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-keys/  
0=my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
```

```
0=my-public-key
```

显示可以使用公有密钥 0 的格式

此示例显示了可以使用公有密钥 0 的格式。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

获取公有密钥 0 (采用 OpenSSH 密钥格式)

此示例获得公有密钥 0 (以 OpenSSH 密钥格式)。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCACfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCVVMx
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC01BTSBdb25zb2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWE5vb251QGFTYXpbvi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSBdb25z
b2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWE5vb251QGFT
YXpbvi5jb20wgZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAaRHhd1QWIMm2nrAgMBAEwDQYJKoZIhvCNQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJ1lJ00zbhNY5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjStb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCACfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCVVMx
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC01BTSBdb25zb2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWE5vb251QGFTYXpbvi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSBdb25z
b2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWE5vb251QGFT
YXpbvi5jb20wgZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAaRHhd1QWIMm2nrAgMBAEwDQYJKoZIhvCNQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
```

```
FFBjvSfpJ1J00zbhNYS5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb  
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

获取实例的子网 ID

此示例获取实例的子网 ID。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`\&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id  
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ 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凭证，因为这可能会导致受到限制。相反，我们建议您缓存凭证，直到凭证开始接近其到期时间。

如果在访问实例元数据服务时受到限制，请使用指数回退策略重试查询。

限制实例元数据服务访问

您可以考虑使用本地防火墙规则，以禁止从某些或所有进程中访问实例元数据服务。

使用 iptables 限制访问

以下示例使用 Linux iptables 及其 owner 模块禁止 Apache Web 服务器（基于其默认安装用户 ID apache）访问 169.254.169.254。它使用拒绝规则 拒绝来自以该用户身份运行的任何进程的所有实例元数据请求（无论是 IMDSv1 还是 IMDSv2）。

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner --uid-owner apache --jump REJECT
```

或者，您可以考虑使用允许规则 以仅允许特定用户或组进行访问。从安全的角度看，允许规则可能更易于管理，因为它们要求您决定哪种软件需要访问实例元数据。如果使用允许规则，在您以后更改实例上的软件或配置时，不太可能会意外允许软件访问元数据服务（您不打算让该软件进行访问）。您还可以将组与允许规则结合使用，以便您可以在允许的组中添加和删除用户，而无需更改防火墙规则。

以下示例禁止所有进程访问实例元数据服务，但在用户账户 trustworthy-user 中运行的进程除外。

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner trustworthy-user --jump REJECT
```

Note

- 要使用本地防火墙规则，您需要修改前面的示例命令以符合您的需求。

- 默认情况下，不会在系统重新引导之间持久保留 iptables 规则。可以使用此处未介绍的操作系统功能持久保留这些规则。
- 只有在组是给定本地用户的主要组时，iptables owner 模块才会匹配组成员资格。不会匹配其他组。

使用 PF 或 IPFW 限制访问

如果使用 FreeBSD 或 OpenBSD，您也可以考虑使用 PF 或 IPFW。以下示例将实例元数据服务访问限制为仅根用户。

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

Note

PF 和 IPFW 命令的顺序至关重要。PF 默认认为最后一个匹配规则，而 IPFW 默认认为第一个匹配规则。

与实例用户数据配合使用

与实例用户数据配合使用时，请注意以下内容：

- 用户数据必须采用 base64 编码。Amazon EC2 控制台可以为您执行 base64 编码或接受 base64 编码的输入。
- 用户数据在进行 base64 编码之前的原始格式的大小限制为 16 KB。长度为 n 的字符串在进行 base64 编码之后的大小为 $\text{ceil}(n/3)*4$ 。
- 在检索用户数据时，必须对其进行 base64 解码。如果您使用实例元数据或控制台检索数据，则会自动对数据进行解码。
- 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。
- 如果您停止实例，修改用户数据，然后启动实例，则在启动实例时，不会执行更新后的用户数据。

启动时指定实例用户数据

您可在启动实例时指定用户数据。有关更多信息，请参阅 [使用启动实例向导启动实例 \(p. 375\)](#) 和 [启动时在 Linux 实例上运行命令 \(p. 494\)](#)。

修改实例用户数据

如果根卷是 EBS 卷，则可以修改处于停止状态的实例的用户数据。有关更多信息，请参阅 [查看和更新实例用户数据 \(p. 496\)](#)。

检索实例用户数据

要从正在运行的实例中检索用户数据，请使用以下 URI。

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

请求用户数据时，按原样返回数据 (内容类型 application/octet-stream)。

该示例返回以逗号分隔文本形式提供的用户数据。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

该示例返回以脚本形式提供的用户数据。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

要从您自己的计算机检索实例的用户数据，请参阅[用户数据和 AWS CLI \(p. 497\)](#)

检索动态数据

要从正在运行的实例中检索动态数据，请使用以下 URI。

```
http://169.254.169.254/latest/dynamic/
```

该示例说明了如何检索简要的实例身份类别。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/dynamic/
instance-identity/
```

```
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

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 [实例身份文档 \(p. 519\)](#)。

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 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 4 个实例，并指定用户数据。

```
aws ec2 run-instances --image-id ami-0abcdef1234567890 --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-0abcdef1234567890
- 预留 ID : r-1234567890abcabc0
- 公有密钥 : 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

元数据	值
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：

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token"  
-H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-  
data/ami-launch-index  
2
```

对于以下步骤，IMDSv2 请求使用前面的 IMDSv2 命令中存储的令牌，并假设令牌尚未过期。

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index  
2
```

2. 她将 ami-launch-index 保存为一个变量。

IMDSv2

```
[ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v  
http://169.254.169.254/latest/meta-data/ami-launch-index`
```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-  
launch-index`
```

3. 她将用户数据保存为一个变量。

IMDSv2

```
[ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v  
http://169.254.169.254/latest/user-data`
```

IMDSv1

```
[ec2-user ~]$ 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。

IMDSv2

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"replicate-every=5min
```

IMDSv1

```
[ec2-user ~]$ 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。

Important

下表中的一些类别名称是实例独有的数据的占位符。例如，*mac* 表示网络接口的 MAC 地址。您必须使用实际值替换占位符。

数据	描述	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-amis 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	与任何 Amazon EBS 卷关联的虚拟设备。仅当 Amazon EBS 卷在启动时存在或者在上一次启动该实例时存在时，这些卷才在元数据中可用。N 表示 Amazon EBS 卷的索引（例如 ebs1 或 ebs2）。	2007-12-15
block-device-mapping/eph emeral 否	任何非 NVMe 实例存储卷的虚拟设备。N 表示每个卷的索引。块储存设备映射中的实例存储卷数可能与实例的实际实例存储卷数不匹配。实例类型将决定对实例可用的实例存储卷的数量。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他实例存储卷将被忽略。	2007-12-15
block-device-mapping/root	与根设备关联的虚拟设备或分区或虚拟设备上的分区，其中根（/ 或 C:）文件系统与给定实例相关联。	2007-12-15
block-device-mapping/swap	与 swap 关联的虚拟设备。并不总是存在。	2007-12-15
elastic-gpus/ associations/ <i>elastic-gpu-id</i>	如果有 Elastic GPU 附加到实例，在有关 Elastic GPU 的信息中包含 JSON 字符串，包括其 ID 和连接信息。	2016-11-30
elastic-inference/ associations/ <i>eia-id</i>	如果有 Elastic Inference 加速器附加到实例，则在有关 Elastic Inference 加速器的信息中包含一个 JSON 字符串，包括其 ID 和类型。	2018-11-29
events/maintenance/history	如果实例存在已完成或已取消的维护事件，则包含一个 JSON 字符串，其中包含有关事件的信息。有关更多信息，请参阅 查看有关已完成或已取消的事件的事件历史记录 (p. 534) 。	2018-08-17

数据	描述	引入的版本
events/maintenance/scheduled	如果实例存在活动的维护事件，则包含一个 JSON 字符串，其中包含有关事件的信息。有关更多信息，请参阅 查看计划的事件 (p. 532) 。	2018-08-17
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 InstanceProfileId)。如果没有，则不显示。	2012-01-12
iam/security-credentials/role-name	如果存在与实例关联的 IAM 角色，则 role-name 为角色的名称，并且 role-name 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凭证 (p. 750))。如果没有，则不显示。	2012-01-12
identity-credentials/ec2/info	[仅供内部使用] AWS 用于向 Amazon EC2 基础设施的其余部分标识实例的凭据的相关信息。	2018-05-23
identity-credentials/ec2/security-credentials/ec2-instance	[仅供内部使用] AWS 用于向 Amazon EC2 基础设施的其余部分标识实例的凭据。	2018-05-23
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. 160) 。	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
metrics/vhostmd	不再可用。	2011-05-01

数据	描述	引入的版本
network/interfaces/macs/mac/device-number	与该接口关联的唯一设备号。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 AWS CLI 的 Amazon EC2 API 和 EC2 命令使用的 DeviceIndex 和 device-index 字段。	2011 年 1 月 1 日
network/interfaces/macs/mac/interface-id	网络接口的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/ipv4-associations/public-ip	与每个公用 IP 地址相关联并被分配到该接口的私有 IPv4 地址。	2011 年 1 月 1 日
network/interfaces/macs/mac/ipv6s	与接口关联的 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
network/interfaces/macs/mac/public-hostname	接口的公有 DNS (IPv4)。仅当 enableDnsHostnames 属性设置为 true 时，才返回此类别。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	与接口关联的公有 IP 地址或弹性 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。	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。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-id	接口所驻留的子网的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-ipv4-cidr-block	接口所在子网的 IPv4 CIDR 块。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-ipv6-cidr-blocks	接口所在子网的 IPv6 CIDR 块。	2016-06-30
network/interfaces/macs/mac/vpc-id	接口所驻留的 VPC 的 ID。	2011 年 1 月 1 日

数据	描述	引入的版本
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-block</code>	VPC 的主 IPv4 CIDR 块。	2011 年 1 月 1 日
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-blocks</code>	VPC 的 IPv4 CIDR 块。	2016-06-30
<code>network/interfaces/macs/mac/vpc-ipv6-cidr-blocks</code>	接口所在 VPC 的 IPv6 CIDR 块。	2016-06-30
<code>placement/availability-zone</code>	实例启动的可用区。	2008-02-01
<code>product-codes</code>	与实例关联的 AWS Marketplace 产品代码 (如果有)。	2007-03-01
<code>public-hostname</code>	实例的公有 DNS。仅当 <code>enableDnsHostnames</code> 属性设置为 <code>true</code> 时，才返回此类别。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 。	2007-01-19
<code>public-ipv4</code>	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
<code>public-keys/0/openssh-key</code>	公有密钥。仅在实例启动时提供了公有密钥的情况下可用。	1.0
<code>ramdisk-id</code>	启动时指定的 RAM 磁盘的 ID，如果适用的话。	2007-10-10
<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。 在启动后，您可以更改实例的安全组。这些更改将体现在此处和 <code>network/interfaces/macs/mac/security-groups</code> 中。	1.0
<code>services/domain</code>	区域的 AWS 资源所在的域。	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-partitionname</code> 。例如，中国 (北京) 区域中的资源的分区为 <code>aws-cn</code> 。	2015-10-20
<code>spot/instance-action</code>	操作 (休眠、停止或终止) 和操作发生的大致时间 (用 UTC 表示)。仅在已将 Spot 实例实例标记为休眠、停止或终止时才提供此项目。有关更多信息，请参阅 instance-action (p. 329) 。	2016-11-15

数据	描述	引入的版本
spot/termination-time	Spot 实例 操作系统将收到关闭信号的大致时间 (UTC)。仅当 Spot 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，2015-01-05T18:02:00Z)。如果您自己终止了 Spot 实例，那么终止时间项目不会设置为时间。有关更多信息，请参阅 termination-time (p. 330) 。	2014-11-05

动态数据类别

下表列举了动态数据的类别。

数据	描述	引入的版本
fws/instance-monitoring	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 : enabled disabled	2009-04-04
instance-identity/document	包含实例属性 (如实例 ID、私有 IP 地址等) 的 JSON。请参阅 实例身份文档 (p. 519) 。	2009-04-04
instance-identity/pkcs7	用于验证签名的文档的真实性和内容。请参阅 实例身份文档 (p. 519) 。	2009-04-04
instance-identity/signature	可被其他各方用于验证来源和真实性的数据。请参阅 实例身份文档 (p. 519) 。	2009-04-04

实例身份文档

实例身份文档是描述实例的 JSON 文件。实例身份文档带有实例身份签名和 PKCS7 签名，它们可用于验证文档中提供的信息的准确性、来源和真实性。

实例身份文档在实例启动时生成，并通过[实例元数据 \(p. 499\)](#)向实例公开。它会验证实例的属性，如实例大小、实例类型、操作系统和 AMI。

Important

由于实例身份文档和签名的动态性质，我们建议定期检索一次实例身份文档和签名。

获取实例身份文档和签名

要检索实例身份文档，请从正在运行的实例中使用以下命令。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

下面是示例输出。

```
{  
    "devpayProductCodes" : null,  
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],  
    "availabilityZone" : "us-west-2b",  
    "privateIp" : "10.158.112.84",
```

```
"version" : "2017-09-30",
"instanceId" : "i-1234567890abcdef0",
"billingProducts" : null,
"instanceType" : "t2.micro",
"accountId" : "123456789012",
"imageId" : "ami-5fb8c835",
"pendingTime" : "2016-11-19T16:32:11Z",
"architecture" : "x86_64",
"kernelId" : null,
"ramdiskId" : null,
"region" : "us-west-2"
}
```

要检索实例身份签名，请从正在运行的实例中使用以下命令。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/signature
```

下面是示例输出。

```
dExamplesjNQhhJan7pORLpLSr7lJEF4V2DhKGlyoYVBouYrY9njjyBCmhEayaGrhtS/AWY+LPx
1VSQURF5n0gwPNCuO6ICT0fNrm5IH7w9ydyaxamplejJw8XvWPxbuRkcNOTAA1p4RtCAqm4ms
x2oALjWSCBExample=
```

要检索 PKCS7 签名，请从正在运行的实例中使用以下命令。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
```

下面是示例输出。

```
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1Mq8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC01BTSDb25zb2x1MRIwEAYDVQQDEwluZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEg5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhCN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQHHEwdTZWF0dGx1Mq8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSDb25z
b2x1MRIwEAYDVQQDEwluZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEg5vb251QGft
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYAMIGJAoGBAMaK0dn+a4GmWIWJ
21uUsfwfEvyswtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSv7c7ugFFDzQGBzZswY6786m86gPE
Ibb3OhjZnzcvQAArHhd1QWIMm2nrAgMBAAwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUnteD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJ1lJ00zbhNYs5f6GuoEdmFJ10ZxBHjJnyp3780D8uTs7fLvjx79LjSTb
NYiytVbZPQU5Yaxu2jXnimvw3rrszlaEXAMPLE
```

验证 PKCS7 签名

通过用合适的 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。

AWS 账户提供的区域 AWS 公有证书如下所示。

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAg0CCQCWukjZ5V4aZzAJBgCqhkjOOAQDMFWxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIExBXYXN0aW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMqZAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0aW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIExMqZCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcs2bb1VQ4yt/5e
ih5006kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
```

```
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hv1Yt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rActXau8Qe+MBCJ1/U
hhy1KHVpCG19fueQ2s6IL0CaO/buyC1CiYQk40KNHCCfNiZbdlx1E9rpUp7bnF
1Ra2v1ntMX3caRVDbtPEWmdxSCYSYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

香港区域的 AWS 公有证书如下所示。

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC07MJe5Y3VLjAJBgCqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQOKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMqzaefw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQExdBbWF6b24gV2ViIFN1
cnZpY2VzIExMqzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfx
b1CvCoVb99570kLGn/04CowHXJ+vTBR7eyIa6AoXltsQXB0mrJswToFKKxT4gbuw
jk7s9Q0QX4CmTRwCEgO2RxtZSVjOhsUQmh+yf7Ht4OVL97LwnNfGsX2cwjcrWHYgi
71vnubNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOOG
eSNmwpW4QFu4pI1Aykm6EnTZKKHT87gdXkAkoC5AfOxxhnE2HezzHzp9Ap2tMV5
8bWNv0PHvoKCQqwfm+OUB1AxC/3vqoVkJL2mG1KgUh9+hrtptMTkwO3RREnKe7I50
x9qimJpOihrl410dYvy9xUOoz+DzFAW8+y1WVYpA4GFAKbgQDbnBAKSxWr9QHY
6Dt+EFdgz61AZLedeBKpaP53Z1DTo34J0C55YbjTwBTFGqPtOLxnUVD1Gid6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DwmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH11E2nz6pk7GbOQtLyHTAJBgcqhkjOOAQDAZAAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLttFpFJqzWHc=
-----END CERTIFICATE-----
```

巴林区域的 AWS 公有证书如下所示。

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCWVigSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQOKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMqzaefw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQExdBbWF6b24gV2ViIFN1
cnZpY2VzIExMqzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1Qli0OB
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3+oJ++q
PH1P1WGL8IZ34BUGRTtg4TVolvp0smjkMvyRu5h1dKtzjv93Ccxi5gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaScmJKxQIVAIzbIaDFRGa2qcMkW2HWASeND17bAoGBAnTz
IdhfMq+12I5iofy2oj3HI21Kj3LtZrWEg3W+4rvhL31TmOnne1rl9yGujrjQwy5
Zp9V4A/w9w2010Lx4K6hj34Eefy/aQnZwNdNhv/FQP7AzOfju+Y16L13OOHqrL0z
Q+9cf7zeosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAKEbgQCVS7m77nuNALz8
wvUqcooxXMPkxF154NxAsAul9KP9KN4svm003Zrb7t2F0tXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGwm5ED1
86ayv3c1PEDukgIAhQow38rQkN/VwHVewSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

AWS GovCloud (US-West) 区域的 AWS 公有证书如下所示。

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgCqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQOKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMqzaefw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQExdBbWF6b24gV2ViIFN1
cnZpY2VzIExMqzCCAbcwgEsBgcqhkjOOAQBMIIBHwKBgQcJkvcs2bb1VQ4yt/5e
-----END CERTIFICATE-----
```

```
ih5006kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyiQzK7wLc1nd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUp t3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgs jJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBCJ1/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
1Ra2v1ntMX3caRVDdbtPEWmdxSCYSYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mm0obpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUAMYQR7R9LINYwouHIZiqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6Rok0k9K
-----END CERTIFICATE-----
```

要获取其他区域的 AWS 公有证书，请联系 [AWS Support](#)。

验证 PKCS7 签名

- 从实例中，为 PKCS7 签名创建一个临时文件。

```
[ec2-user ~]$ PKCS7=$(mktemp)
```

- 将 -----BEGIN PKCS7----- 标头添加到临时 PKCS7 文件中。

```
[ec2-user ~]$ echo "-----BEGIN PKCS7-----" > $PKCS7
```

- 附加实例元数据中的 PKCS7 签名内容以及一个新行。

```
[ec2-user ~]$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >>
$PKCS7
[ec2-user ~]$ echo "" >> $PKCS7
```

- 附加 -----END PKCS7----- 页脚。

```
[ec2-user ~]$ echo "-----END PKCS7-----" >> $PKCS7
```

- 为实例身份文档创建一个临时文件。

```
[ec2-user ~]$ DOCUMENT=$(mktemp)
```

- 将实例元数据中的文档内容添加到临时文档文件中。

```
[ec2-user ~]$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
> $DOCUMENT
```

- 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。
- 按以下方式使用 OpenSSL 工具验证签名。

```
[ec2-user ~]$ openssl smime -verify -in $PKCS7 -inform PEM -content $DOCUMENT -certfile
AWSpubkey -noverify > /dev/null
Verification successful
```

Amazon Elastic Inference

Amazon Elastic Inference (EI) 是一种您可以附加到 Amazon EC2 CPU 实例用于加速深度学习 (DL) 推理工作负载的资源。Amazon EI 加速器提供多种大小，是一种为在 Amazon EC2 实例上运行的应用程序引入智能功能的经济高效的方法。

Amazon EI 在低成本 DL 推理加速器和实例的 CPU 之间通过 MXNet 分配由 TensorFlow、Apache MXNet 和开放神经网络交换 (ONNX) 格式定义的模型操作。

有关 Amazon Elastic Inference 的更多信息，请参阅 [Amazon EI 开发人员指南](#)。

识别 EC2 Linux 实例

您的应用程序可能需要确定是否运行在 EC2 实例上。

有关识别 Windows 实例的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Windows 实例\)](#) 中的识别 EC2 Windows 实例。

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 [实例身份文档 \(p. 519\)](#)。

检查系统 UUID

您可以获取系统 UUID 并检查 UUID 的起始 octet 中是否存在字符“ec2”或“EC2”。此确定系统是否为 EC2 实例的方法速度快，但可能不准确，因为不是 EC2 实例的系统也有很小的几率使用以这些字符开头的 UUID。此外，对于不使用 Amazon Linux 的 EC2 实例，发行版的 SMBIOS 实施可能表示 little-endian 格式的 UUID，因此“EC2”字符不显示在 UUID 的开头。

Example：从管理程序获取 UUID

如果 `/sys/hypervisor/uuid` 存在，您可以使用以下命令：

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

在以下示例输出中，UUID 以“ec2”开头，表示该系统可能是 EC2 实例。

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Example：从 DMI 获取 UUID (仅限 HVM 实例)

您仅可以在 HVM 实例中使用桌面管理接口 (DMI)。

您可以使用 `dmidecode` 工具返回 UUID。在 Amazon Linux 上，若您的实例上尚未安装 `dmidecode` 工具，请使用以下命令安装：

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

然后运行以下命令：

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

或者，使用以下命令：

```
[ec2-user ~]$ sudo cat /sys/devices/virtual/dmi/id/product_uuid
```

在以下示例输出中，UUID 以“EC2”开头，表示该系统可能是 EC2 实例。

```
EC2E1916-9099-7CAF-FD21-01234ABCDEF
```

在以下示例输出中，UUID 以 little-endian 格式表示。

```
45E12AEC-DCD1-B213-94ED-01234ABCDEF
```

在 Nitro 实例上，可以使用以下命令：

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

这将返回实例 ID，这对 EC2 实例是唯一的：

```
i-0af01c0123456789a
```

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 EC2 实例的 CPU 使用率、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	监控代理/CloudWatch Logs
CPU 使用率	CPU 利用率 (p. 539)	
网络使用率	NetworkIn (p. 539) 网络输出 (p. 539)	
磁盘性能	磁盘读取操作 (p. 539) 磁盘写入操作 (p. 539)	
磁盘读取/写入	磁盘读取字节数 (p. 539) 磁盘写入字节数 (p. 539)	
内存利用率、磁盘交换利用率、磁盘空间利用率、页面文件利用率、日志收集		[Linux 和 Windows Server 实例] 使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器收集指标和日志 [在 Windows Server 实例上从以前的 CloudWatch Logs 代理迁移] 将 Windows Server 实例日志收集迁移到 CloudWatch 代理

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 \(p. 526\)](#)
- [手动监控工具 \(p. 526\)](#)

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
- 物理主机上影响到网络连接状态的硬件问题

有关更多信息，请参阅[实例的状态检查 \(p. 528\)](#)。

- 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 \(p. 528\)](#)。

- 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。操作是向 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略发送的通知。警报仅在出现持续状态变化时才会调用操作。CloudWatch 警报将不会因为其处于特定状态而调用操作；该状态必须已改变并在指定的若干时间段内保持不变。有关更多信息，请参阅[使用 CloudWatch 监控您的实例 \(p. 538\)](#)。
- Amazon CloudWatch Events - 自动执行您的 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[Amazon CloudWatch Logs User Guide](#)。
- Amazon EC2 监控脚本 - 可以使用 Perl 脚本在您的实例中监控内存、磁盘和交换文件使用率。有关更多信息，请参阅[Amazon EC2 Linux 实例监控内存和磁盘指标](#)。
- Microsoft System Center Operations Manager 的 AWS 管理包 - 将 Amazon EC2 实例与其内部运行的 Windows 或 Linux 操作系统相关联。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，选择 Instances (实例) 以选择一个实例，然后选择 Monitoring (监控) 选项卡)
 - 卷指标详细信息 (在导航窗格中，选择 Volumes (卷) 以选择一个卷，然后选择 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。

您也可以查看为实例计划的特定事件的状态。事件状态提供了有关为实例计划的未来各项活动的信息，例如重启或停用。它们还提供了各个事件的计划开始时间和结束时间。

目录

- [实例的状态检查 \(p. 528\)](#)
- [实例的计划事件 \(p. 532\)](#)

实例的状态检查

通过实例状态监控，您可快速确定 Amazon EC2 是否检测到可能阻止您的实例运行应用程序的问题。Amazon EC2 会对每个运行的 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特定的和可检测的问题。事件状态数据扩充了 Amazon EC2 已提供的有关每个实例状态（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，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。

当状态检查失败时，状态检查的相应 CloudWatch 指标将增加。有关更多信息，请参阅[状态检查指标 \(p. 544\)](#)。您可以使用这些指标创建基于状态检查结果触发的 CloudWatch 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 \(p. 530\)](#)。

您也可以创建 Amazon CloudWatch 警报，用于监控 Amazon EC2 实例并在实例由于潜在问题而受损时自动恢复实例。有关更多信息，请参阅[恢复您的实例 \(p. 463\)](#)。

目录

- [状态检查的类型 \(p. 528\)](#)
- [查看状态检查 \(p. 529\)](#)
- [报告实例状态 \(p. 530\)](#)
- [创建和编辑状态检查警报 \(p. 530\)](#)

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

监控您的实例在其上运行的 AWS 系统。这些检查会检测出需要 AWS 参与修复的深层实例问题。如果系统状态检查失败，您可以选择等待 AWS 修复问题，也可以自行解决问题。对于由 Amazon EBS 支持的实例，您也可自行停止和启动实例，在大多数情况下，这会导致实例被迁移至新的主机。对于由实例存储支持的实例，您可以终止并替换实例。

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
- 物理主机上影响到网络连接状态的硬件问题

实例状态检查

监控您的各个实例的软件和网络配置。Amazon EC2 通过向网络接口 (NIC) 发送地址解析协议 (ARP) 请求，检查实例的运行状况。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，通常必须由您自行解决问题（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。

查看状态检查 (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 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。

The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there are tabs: Description, Status Checks (which is highlighted in orange), Monitoring, and Tags. Below the tabs, a status message says: "Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks." A "Create Status Check Alarm" button is present. The main content area is divided into two sections: "System Status Checks" and "Instance Status Checks".
System Status Checks: Describes checks monitoring AWS systems required for the instance. It shows a green status: "System reachability check passed".
Instance Status Checks: Describes checks monitoring software and network configuration. It shows a red status: "Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)".
Below these sections, there's an "Additional Resources" section with a note to submit feedback and links to developer forums and AWS Support.

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 \(p. 963\)](#)。

5. 要查看状态检查的 CloudWatch 指标，选择实例，然后选择 Monitoring (监控) 选项卡。滚动，直到您看到以下指标的图表：
 - Status Check Failed (Any) (状态检查失败(任意))
 - Status Check Failed (Instance) (状态检查失败(实例))
 - Status Check Failed (System) (状态检查失败(系统))

使用命令行查看状态

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
```

要获取实例状态为 `impaired` 的所有实例的状态，请使用以下命令。

```
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)
- [DescribeInstanceState](#) (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 \(p. 963\)](#)。

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，或者如果您想要向 AWS 发送有关您遇到的受损实例问题的更多详细信息，您可提供反馈。

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

报告实例状态（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 Instances。
3. 选择实例，选择 Status Checks (状态检查) 选项卡，然后选择 Submit feedback (提交反馈)。
4. 填写 Report Instance Status 表单，然后选择 Submit。

使用命令行报告状态反馈

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

您可以使用[状态检查指标 \(p. 544\)](#)创建 CloudWatch 警报，以在实例的状态检查失败时向您发送通知。

使用控制台创建状态检查警报

使用以下过程配置一个警报，当实例的状态检查失败时，该警报将通过电子邮件向您发送通知，或者停止、终止或恢复实例。

创建状态检查警报（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 Instances。
3. 选择实例，选择 Status Checks (状态检查) 选项卡，然后选择 Create Status Check Alarm (创建状态检查警报)。

4. 选择 Send a notification to。选择一个现有 SNS 主题，或选择 create topic (创建主题) 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。
5. (可选) 选择 Take the action (请执行以下操作)，然后选择要采取的操作。
6. 在 Whenever 中，选择想要获得通知的状态检查。

如果您在上一步中选择的是 Recover this instance，则请选择 Status Check Failed (System)。

7. 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。
8. (可选) 在 Name of alarm 中，将警报的默认名称替换为其他名称。
9. 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选择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。

使用控制台编辑状态检查警报

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions (操作)、CloudWatch Monitoring (CloudWatch 监控) 和 Add/Edit Alarms (添加/编辑警报)。
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。使用的 CloudWatch 指标为 StatusCheckFailed。

使用 AWS 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 AWS CLI 与 Amazon SNS 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:mysns-topic
```

周期为收集 Amazon CloudWatch 指标所需的时间范围（以秒为单位）。此示例使用 300，这是 60 秒乘以 5 分钟得到的结果。评估期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。警报操作是要在此警报触发时执行的操作。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。该电子邮件将提供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。

目录

- [计划事件的类型 \(p. 532\)](#)
- [查看计划的事件 \(p. 532\)](#)
- [使用计划停止或停用的实例 \(p. 535\)](#)
- [使用计划为重启的实例 \(p. 535\)](#)
- [使用计划为维护的实例 \(p. 537\)](#)

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**：实例在计划的时间停止。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**：在计划的时间，由 Amazon EBS 支持的实例将停止；由实例存储支持的实例将终止。
- **实例重启**：在计划的时间实例重启。
- **系统重启**：在计划的时间实例的主机重启。
- **系统维护**：在计划的时间，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，您还可使用以下方法之一查看计划的事件。

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，选择 Events。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。

Scheduled Events

US West (Oregon):

1 instances have scheduled events

4. 还将显示受影响资源的一些事件。例如，在导航窗格中，选择 Instances (实例)，然后选择一个实例。如果所选实例具有关联的实例停止或实例停用事件，则该事件将显示在底部窗格中。

 Retiring: This instance is scheduled for retirement after May 22, 2015 at 5:00:00 PM UTC-7. [\(i\)](#)

使用 AWS CLI 查看实例的计划事件

- 使用以下 `describe-instance-status` 命令：

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0 --query "InstanceStatuses[].[Events]"
```

以下示例输出显示重启事件：

```
[{"Events": [{"InstanceEventId": "instance-event-0d59937288b749b32", "Code": "system-reboot", "Description": "The instance is scheduled for a reboot", "NotAfter": "2019-03-15T22:00:00.000Z", "NotBefore": "2019-03-14T20:00:00.000Z", "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"}]}
```

以下示例输出显示实例停用事件。

```
[{"Events": [{"InstanceEventId": "instance-event-0e439355b779n26", "Code": "instance-stop", "Description": "The instance is running on degraded hardware", "NotBefore": "2015-05-23T00:00:00.000Z"}]}
```

使用适用于 Windows PowerShell 的 AWS 工具 查看实例的计划事件

- 使用以下 `Get-EC2InstanceState` 命令。

```
PS C:\> (Get-EC2InstanceState -InstanceId i-1234567890abcdef0).Events
```

以下示例输出显示实例停用事件。

```
Code      : instance-stop
Description : The instance is running on degraded hardware
NotBefore : 5/23/2015 12:00:00 AM
```

使用实例元数据查看实例的计划事件

- 您可以从[实例元数据 \(p. 499\)](#)中检索有关实例的活动维护事件的信息，如下所示。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

以下是 JSON 格式的计划系统重启事件信息的示例输出。

```
[  
 {  
     "NotBefore" : "21 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "21 Jan 2019 09:17:23 GMT",  
     "State" : "active"  
 },  
 ]
```

使用实例元数据查看有关实例的已完成或已取消事件的事件历史记录

- 您可以从[实例元数据 \(p. 499\)](#)中检索有关实例的已完成或已取消事件的信息，如下所示。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

以下是 JSON 格式的已取消和已完成系统重启事件相关信息的示例输出。

```
[  
 {  
     "NotBefore" : "21 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "[Canceled] scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "21 Jan 2019 09:17:23 GMT",  
     "State" : "canceled"  
 },  
 {  
     "NotBefore" : "29 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "[Completed] scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "29 Jan 2019 09:17:23 GMT",  
     "State" : "completed"  
 }  
 ]
```

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 \(p. 456\)](#)。

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。这包括附加到使用 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可能需要的数据。

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 \(p. 445\)](#)。

您可以自动化立即停止并启动以响应计划的实例停止事件。有关更多信息，请参阅 AWS Health 用户指南 中的 [自动化 EC2 实例的操作](#)。

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 必须执行安装更新或维护基础主机等任务时，它可计划实例或基础主机进行重启。您可以[重新计划大部分重启事件 \(p. 536\)](#)，以便您的实例在适合您的特定日期和时间重启。

如果您停止链接的 [EC2-Classic 实例 \(p. 681\)](#)，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。

查看重启事件类型

您可以使用 AWS 管理控制台、AWS CLI, 或 Amazon EC2 API 来查看某个重启事件是实例重启还是系统重启。

查看计划的重启事件的类型 (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 Events。
3. 从筛选器列表中选择 Instance resources (实例资源)。
4. 对于每个实例，查看 Event Type (事件类型) 列中的值。该值为 system-reboot 或 instance-reboot。

查看计划的重启事件的类型 (AWS CLI)

- 使用以下 `describe-instance-status` 命令：

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

对于计划的重启事件，Code 的值是 system-reboot 或 instance-reboot。以下示例输出显示 system-reboot 事件。

```
[  
  "Events": [
```

```
{  
    "InstanceEventId": "instance-event-0d59937288b749b32",  
    "Code": "system-reboot",  
    "Description": "The instance is scheduled for a reboot",  
    "NotAfter": "2019-03-14T22:00:00.000Z",  
    "NotBefore": "2019-03-14T20:00:00.000Z",  
    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
}  
]  
]
```

针对实例重启的操作

您可以等待实例重启在计划的维护时段进行，或者[重新计划 \(p. 536\)](#)实例重启在适合您的日期和时间进行，或者在您方便的时间自行[重新启动 \(p. 456\)](#)实例。

在实例重启之后，将清除计划的事件并更新事件说明。底层主机上的所有挂起维护都会完成，并且在实例完全启动后，即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。您可以等待系统重启在计划的维护时段进行，或者您可以[重新计划 \(p. 536\)](#)系统重启在适合您的日期和时间进行。系统重启通常在几分钟内完成。在系统重启之后，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会得到保留。在系统重启完成之后，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，如果有必要在其他时间维护实例，并且您无法重新计划系统重启，则您可以停止并启动 Amazon 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。您也可以自动化立即停止并启动实例以响应计划的系统重启事件。有关更多信息，请参阅 AWS Health 用户指南中的[自动化 EC2 实例的操作](#)。对于由实例存储支持的实例，如果您无法重新计划系统重启，可在计划的维护时段之前从最新的 AMI 启动替代实例，并将所有必需数据迁移至替代实例，然后终止原始实例。

重新计划重启事件

您可以重新计划大部分重启事件，以便您的实例在适合您的特定日期和时间重启。

重新计划重启事件（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 Events。
3. 从筛选器列表中选择 Instance resources (实例资源)。
4. 选择一个或多个实例，然后选择 Actions (操作) 和 Schedule Event (计划事件)。

只有具有事件截止日期（由 Event Deadline (事件截止期限) 的值指示）的事件才可以重新计划。

5. 对于 Event start time (事件开始时间)，输入新的重启日期和时间。新的日期和时间必须早于 Event Deadline (事件截止期限)。
6. 选择 Schedule Event (计划事件)。

更新的事件开始时间可能需要 1-2 分钟才会反映在控制台中。

重新计划重启事件（AWS CLI）

1. 只有具有事件截止日期（由 NotBeforeDeadline 的值指示）才可以重新计划。使用以下 `describe-instance-status` 命令查看 NotBeforeDeadline 参数值。

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

以下示例输出显示因 NotBeforeDeadline 包含值而可以重新计划的 system-reboot 事件。

```
[  
  "Events": [  
    {  
      "InstanceEventId": "instance-event-0d59937288b749b32",  
      "Code": "system-reboot",  
      "Description": "The instance is scheduled for a reboot",  
      "NotAfter": "2019-03-14T22:00:00.000Z",  
      "NotBefore": "2019-03-14T20:00:00.000Z",  
      "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
    }  
  ]  
]
```

2. 若要重新计划事件，应使用 [modify-instance-event-start-time](#) 命令。使用 not-before 参数指定新的事件开始时间。新的事件开始时间必须早于 NotBeforeDeadline。

```
aws ec2 modify-instance-event-start-time --instance-id i-1234567890abcdef0 --instance-event-id instance-event-0d59937288b749b32 --not-before 2019-03-25T10:00:00.000
```

在 [describe-instance-status](#) 命令返回更新的 not-before 参数值之前可能需要 1-2 分钟。

对重启事件的限制

- 只有具有事件截止日期的重启事件才可以重新计划。可以将事件重新计划到事件截止日期之前的日期。控制台中的 Event Deadline (事件截止期限) 列和 AWS CLI 中的 NotBeforeDeadline 字段指示了事件是否有截止日期。
- 只有尚未开始的重启事件才可以重新计划。控制台中的 Start Time (开始时间) 列和 AWS CLI 中的 NotBefore 字段指示了事件的开始时间。还有 5 分钟便要按计划开始的重启事件无法重新计划。
- 新的事件开始时间离当前时间必须至少有 60 分钟。
- 如果您使用控制台重新计划多个事件，则事件截止日期由具有最早的事件截止日期的事件决定。

使用计划为维护的实例

当 AWS 必须维护实例的基础主机时，它将计划实例的维护。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。实例状态说明的刷新有时需要长达 1 个小时。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 \(p. 445\)](#)。

您可以自动化立即停止并启动以响应计划维护事件。有关更多信息，请参阅 AWS Health 用户指南 中的 [自动化 EC2 实例的操作](#)。

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间段内保持正常操作，可在计划的维护时间段之前从最新的 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 \(p. 538\)](#)。

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](#)。

目录

- [对您的实例启用或禁用详细监控 \(p. 538\)](#)
- [列出实例的可用 CloudWatch 指标 \(p. 539\)](#)
- [获取实例指标的统计数据 \(p. 547\)](#)
- [绘制实例的指标图形 \(p. 554\)](#)
- [为实例创建 CloudWatch 警报 \(p. 554\)](#)
- [创建停止、终止、重启或恢复实例的警报 \(p. 555\)](#)

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。

监控类型	描述
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。在实例上启用详细监控不会影响对附加到实例的 EBS 卷的监控。有关更多信息，请参阅[Amazon EBS 的 Amazon CloudWatch 指标 \(p. 889\)](#)。

对现有实例启用详细监控（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 Instances。
3. 选择所需实例，然后依次选择 Actions (操作)、CloudWatch Monitoring (CloudWatch 监控) 和 Enable Detailed Monitoring (启用详细监控)。
4. 在 Enable Detailed Monitoring 对话框中，选择 Yes, Enable。

5. 选择 Close。

启动实例时启用详细监控 (控制台)

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。

对现有实例启用详细监控 (AWS CLI)

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
```

在启动实例时启用详细监控 (AWS CLI)

结合使用 `run-instances` 命令和 `--monitoring Enabled=true` 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。

禁用详细监控 (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 Instances。
3. 选择所需实例，然后依次选择 Actions (操作)、CloudWatch Monitoring (CloudWatch 监控) 和 Disable Detailed Monitoring (禁用详细监控)。
4. 在 Disable Detailed Monitoring 对话框中，选择 Yes, Disable。
5. 选择 Close。

禁用详细监控 (AWS CLI)

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自启动后的 5 分钟内的活动。如果您启用了详细监控，则每个数据点包含自启动后的 1 分钟内的活动。

有关获取这些指标的统计数据的信息，请参阅 [获取实例指标的统计数据 \(p. 547\)](#)。

目录

- [实例指标 \(p. 540\)](#)
- [CPU 积分指标 \(p. 541\)](#)
- [基于 Nitro 的实例的 Amazon EBS 指标 \(p. 542\)](#)
- [状态检查指标 \(p. 544\)](#)
- [Amazon EC2 指标维度 \(p. 544\)](#)
- [使用控制台列出指标 \(p. 545\)](#)

- 使用 AWS CLI 列出指标 (p. 546)

实例指标

AWS/EC2 命名空间包括以下实例指标。

指标	说明
CPUUtilization	<p>当前正在实例上使用的已分配 EC2 计算单位的百分率。此指标确定在选定实例上运行应用程序所需的处理能力。</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>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>如果没有实例存储卷，则值为 0 或不报告指标。</p> <p>单位：计数</p>
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>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>如果没有实例存储卷，则值为 0 或不报告指标。</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>报告的数量是该期间内接收的字节数。如果您使用的是基本 (5 分钟) 监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。</p> <p>如果没有实例存储卷，则值为 0 或不报告指标。</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>报告的数量是该期间内接收的字节数。如果您使用的是基本 (5 分钟) 监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。</p> <p>如果没有实例存储卷，则值为 0 或不报告指标。</p>

指标	说明
	单位 : 字节
NetworkIn	<p>实例在所有网络接口上收到的字节数。此指标用于确定流向单个实例的传入网络流量。</p> <p>报告的数量是该期间内接收的字节数。如果您使用的是基本 (5 分钟) 监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。</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。此指标用于确定来自单个实例的传出网络流量。</p> <p>报告的数字是该时间段内发送的字节数。如果您使用的是基本 (5 分钟) 监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。</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>
MetadataNoToken	<p>利用不使用令牌的方法访问实例元数据服务的次数。</p> <p>该指标用于确定是否有任何进程正在使用 实例元数据服务版本 1 访问实例元数据，但未使用令牌。如果所有请求都使用支持令牌的会话（即 实例元数据服务版本 2），则该值为 0。有关更多信息，请参阅转换为使用 实例元数据服务版本 2 (p. 501)。</p> <p>单位 : 计数</p>

CPU 积分指标

AWS/EC2 命名空间包括 [可突增性能实例 \(p. 175\)](#) 的以下 CPU 积分指标。

指标	说明
CPUCreditUsage	<p>实例为保持 CPU 使用率而花费的 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 积分指标仅每 5 分钟提供一次。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>

指标	说明
	单位 : 积分 (vCPU 分钟)
CPUCreditBalance	<p>实例自启动后已累积获得的 CPU 积分数。对于 T2 标准 , CPUCreditBalance 还包含已累积的启动积分数。</p> <p>在获得积分后 , 积分将在积分余额中累积 ; 在花费积分后 , 将从积分余额中扣除积分。积分余额具有最大值限制 , 这是由实例大小决定的。在达到限制后 , 将丢弃获得的任何新积分。对于 T2 标准 , 启动积分不计入限制。</p> <p>实例可以花费 CPUCreditBalance 中的积分 , 以便突增到基准 CPU 使用率以上。</p> <p>在实例运行过程中 , CPUCreditBalance 中的积分不会过期。在 T3 或 T3a 实例停止时 , CPUCreditBalance 值将保留七天。之后 , 所有累积的积分都将丢失。在 T2 实例停止时 , CPUCreditBalance 值不会保留 , 并且所有累积的积分都将丢失。</p> <p>CPU 积分指标仅每 5 分钟提供一次。</p> <p>单位 : 积分 (vCPU 分钟)</p>
CPUSurplusCreditBalance	<p>在 CPUCreditBalance 值为零时 , unlimited 实例花费的超额积分数。</p> <p>CPUSurplusCreditBalance 值由获得的 CPU 积分支付。如果超额积分数超出实例可在 24 小时周期内获得的最大积分数 , 则超出最大积分数的已花费超额积分将产生额外费用。</p> <p>CPU 积分指标仅每 5 分钟提供一次。</p> <p>单位 : 积分 (vCPU 分钟)</p>
CPUSurplusCreditsCharged	<p>未由获得的 CPU 积分支付并且会产生额外费用的已花费超额积分数。</p> <p>在出现以下任一情况时 , 将对花费的超额积分收费 :</p> <ul style="list-style-type: none"> • 花费的超额积分超出实例可在 24 小时周期内获得的最大积分数。对于超出最大积分数的所花费超额积分 , 将在该小时结束时向您收费。 • 实例已停止或终止。 • 实例从 unlimited 切换为 standard。 <p>CPU 积分指标仅每 5 分钟提供一次。</p> <p>单位 : 积分 (vCPU 分钟)</p>

基于 Nitro 的实例的 Amazon EBS 指标

AWS / EC2 命名空间包括基于 Nitro 的实例 (非裸机实例) 的以下 Amazon EBS 指标。有关基于 Nitro 的实例类型的列表 , 请参阅 [基于 Nitro 的实例 \(p. 163\)](#) 。

基于 Nitro 的实例的指标值将始终为整数 , 而基于 Xen 的实例的值支持小数。因此 , 基于 Nitro 的实例上的低实例 CPU 利用率可能看起来被向下舍入为 0 。

指标	说明
EBSReadOps	<p>在指定时间段内挂载到实例的所有 Amazon EBS 卷中完成的读取操作数。</p> <p>要计算该时间段的平均每秒读取 I/O 操作数 (读取 IOPS) , 请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控 , 您可以将该数字除以 300 以计算读取 IOPS。如果您使用的是详细 (1 分钟) 监控 , 请将其除以 60。</p> <p>单位 : 计数</p>
EBSWriteOps	<p>在指定时间段内附加到实例的所有 EBS 卷中完成的写入操作数。</p> <p>要计算该时间段的平均每秒写入 I/O 操作数 (写入 IOPS) , 请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控 , 您可以将该数字除以 300 以计算写入 IOPS。如果您使用的是详细 (1 分钟) 监控 , 请将其除以 60。</p> <p>单位 : 计数</p>
EBSReadBytes	<p>在指定时间段内从附加到实例的所有 EBS 卷中读取的字节数。</p> <p>报告的数字是在该时间段内读取的字节数。如果使用基本 (5 分钟) 监控 , 您可以将该数字除以 300 以计算每秒读取的字节数。如果您使用的是详细 (1 分钟) 监控 , 请将其除以 60。</p> <p>单位 : 字节</p>
EBSWriteBytes	<p>在指定时间段内写入附加到实例的所有 EBS 卷的字节数。</p> <p>报告的数字是在该时间段内写入的字节数。如果使用基本 (5 分钟) 监控 , 您可以将该数字除以 300 以计算每秒写入的字节数。如果您使用的是详细 (1 分钟) 监控 , 请将其除以 60。</p> <p>单位 : 字节</p>
EBSIOBalance%	<p>仅适用于小型实例大小。提供有关突增存储桶中剩余的 I/O 积分百分比的信息。此指标仅对基本监控可用。</p> <p>Sum 统计数据不适用于该指标。</p> <p>单位 : 百分比</p>
EBSByteBalance%	<p>仅适用于小型实例大小。提供有关突增存储桶中剩余的吞吐量积分百分比的信息。此指标仅对基本监控可用。</p> <p>Sum 统计数据不适用于该指标。</p> <p>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 \(p. 889\)](#)。有关为 Spot 队列提供的指标的信息 , 请参阅 [Spot 队列的 CloudWatch 指标 \(p. 313\)](#)。

状态检查指标

AWS/EC2 命名空间包括以下状态检查指标。默认情况下，状态检查指标可在 1 分钟的频率下免费提供。对于新启动的实例，状态检查指标数据仅在实例完成初始化状态之后 (实例进入运行状态的几分钟之内) 提供。有关 EC2 状态检查的更多信息，请参阅[实例的状态检查](#)。

指标	说明
StatusCheckFailed	<p>报告实例在上一分钟是否通过了实例状态检查和系统状态检查。</p> <p>此指标可以是 0 (通过) 或 1 (失败)。</p> <p>默认情况下，此指标可在 1 分钟的频率下免费提供。</p> <p>单位：计数</p>
StatusCheckFailed_Instance	<p>报告实例在上个 1 分钟内是否通过了 实例状况检查。</p> <p>此指标可以是 0 (通过) 或 1 (失败)。</p> <p>默认情况下，此指标可在 1 分钟的频率下免费提供。</p> <p>单位：计数</p>
StatusCheckFailed_System	<p>报告实例在上一分钟内是否通过了 系统状况检查。</p> <p>此指标可以是 0 (通过) 或 1 (失败)。</p> <p>默认情况下，此指标可在 1 分钟的频率下免费提供。</p> <p>单位：计数</p>

Amazon EC2 指标维度

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（控制台）

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。

The screenshot shows the CloudWatch Metrics console interface. At the top, there are three tabs: 'All metrics' (selected), 'Graphed metrics', and 'Graph options'. Below the tabs is a search bar with placeholder text 'Search for any metric, dimension or resource id'. The main area displays '722 Metrics' categorized by service. Each category box contains the service name, the number of metrics, and a small preview of the metrics. The categories shown are EBS (117 Metrics), EC2 (316 Metrics), EFS (7 Metrics), ELB (210 Metrics), ElasticBeanstalk (8 Metrics), RDS (60 Metrics), and S3 (4 Metrics).

4. 选择指标维度（例如 Per-Instance Metrics（每个实例的指标））。

The screenshot shows the CloudWatch Metrics console interface, filtered for the EC2 namespace. At the top, it shows 'All > EC2' and a search bar. The main area displays '103 Metrics' categorized by dimension. The categories shown are 'By Auto Scaling Group' (28 Metrics), 'By Image (AMI) Id' (7 Metrics), 'Per-Instance Metrics' (54 Metrics), 'Aggregated by Instance Type' (7 Metrics), and 'Across All Instances' (7 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。

Instance Name (192)	InstanceId	Metric Name
my-instance	i-abbc12a7	CPUUtilization
my-instance		DiskReadBytes
my-instance		DiskReadOps
my-instance		DiskWriteBytes
my-instance		DiskWriteOps
my-instance		NetworkIn
my-instance		NetworkOut
my-instance	i-abbc12a7	NetworkPacketsIn
my-instance	i-abbc12a7	NetworkPacketsOut

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 (AWS CLI)

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": "DiskReadBytes"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "DiskReadOps"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "DiskWriteBytes"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "DiskWriteOps"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "NetworkIn"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "NetworkOut"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "NetworkPacketsIn"  
        },  
        {  
            "Namespace": "AWS/EC2",  
            "Dimensions": [  
                {  
                    "Name": "InstanceId",  
                    "Value": "i-1234567890abcdef0"  
                }  
            ],  
            "MetricName": "NetworkPacketsOut"  
        }  
    ]  
}
```

```
        "Value": "i-1234567890abcdef0"
    },
    ],
    "MetricName": "NetworkIn"
},
...
}
```

列出实例的所有可用指标 (AWS CLI)

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
```

列出所有实例的指标 (AWS CLI)

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
```

获取实例指标的统计数据

您可以获取有关实例的 CloudWatch 指标的统计信息。

目录

- 统计数据概述 (p. 547)
- 获取指定实例的统计数据 (p. 548)
- 聚合多实例统计数据 (p. 550)
- 通过 Auto Scaling 组聚合统计数据 (p. 552)
- 按 AMI 聚合统计数据 (p. 553)

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	描述
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

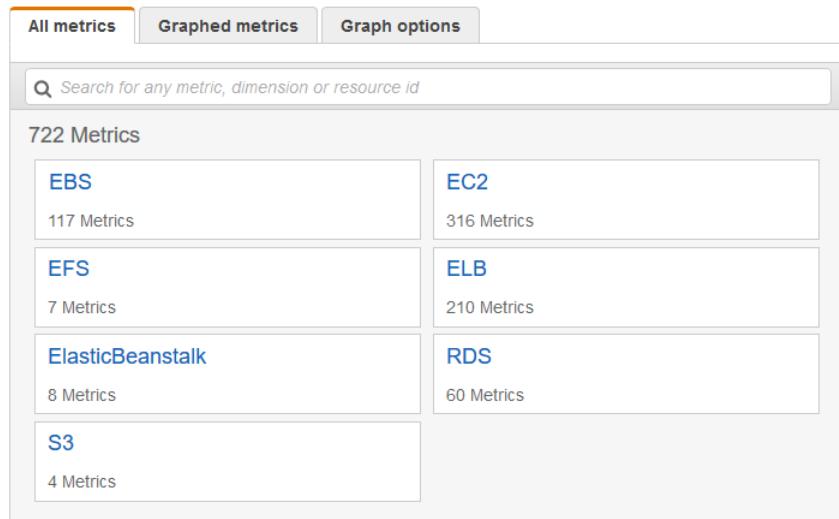
以下示例显示了如何使用 AWS 管理控制台 或 AWS CLI 来确定特定 EC2 实例的最大 CPU 利用率。

要求

- 您必须拥有实例的 ID。可使用 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 \(p. 538\)](#)。

显示指定实例的 CPU 利用率 (控制台)

- 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。

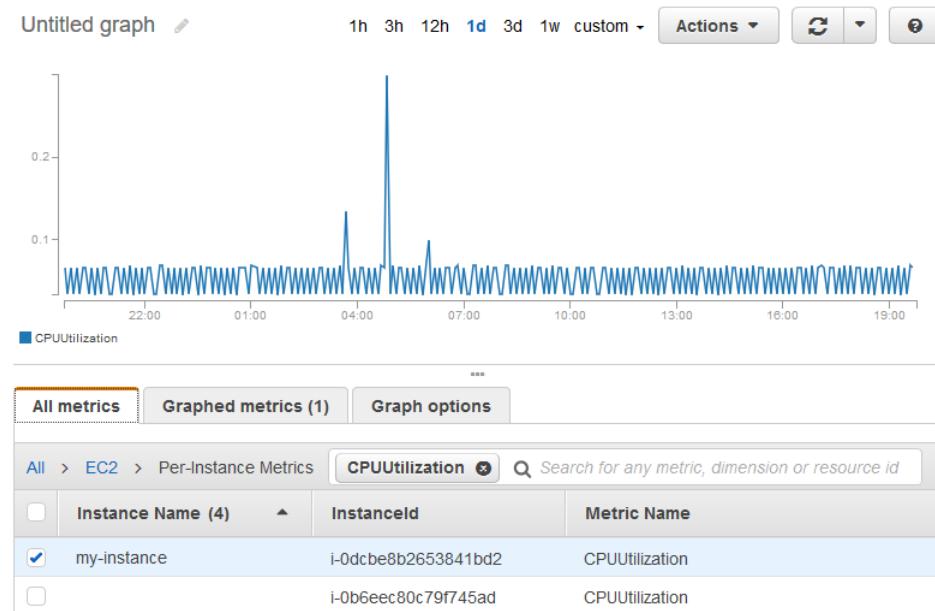


- 选择 Per-Instance Metrics (每个实例的指标) 维度。

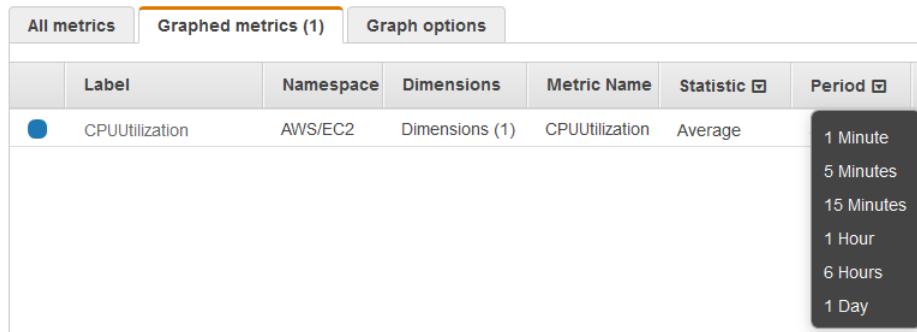
The screenshot shows the AWS CloudWatch Metrics console with the following interface elements:

- Top navigation bar: All metrics, Graphed metrics, Graph options.
- Breadcrumbs: All > EC2.
- Search bar: Search for any metric, dimension or resource id.
- Main content area: 103 Metrics. It lists five categories:
 - By Auto Scaling Group: 28 Metrics
 - By Image (AMI) Id: 7 Metrics
 - Per-Instance Metrics: 54 Metrics
 - Aggregated by Instance Type: 7 Metrics
 - Across All Instances: 7 Metrics

5. 在搜索字段中，输入 **CPUUtilization** 并按 Enter。选择特定实例所在的行，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。



6. 要更改指标的统计数据或时间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。



获取特定实例的 CPU 利用率 (AWS CLI)

使用以下 `get-metric-statistics` 命令获取指定实例的 CPUUtilization 指标（使用指定周期和时间间隔）：

```
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 使用率百分比。

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-10-19T00:18:00Z",
            "Maximum": 0.3300000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2016-10-19T03:18:00Z",
            "Maximum": 99.67000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2016-10-19T07:18:00Z",
            "Maximum": 0.3400000000000002,
            "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。

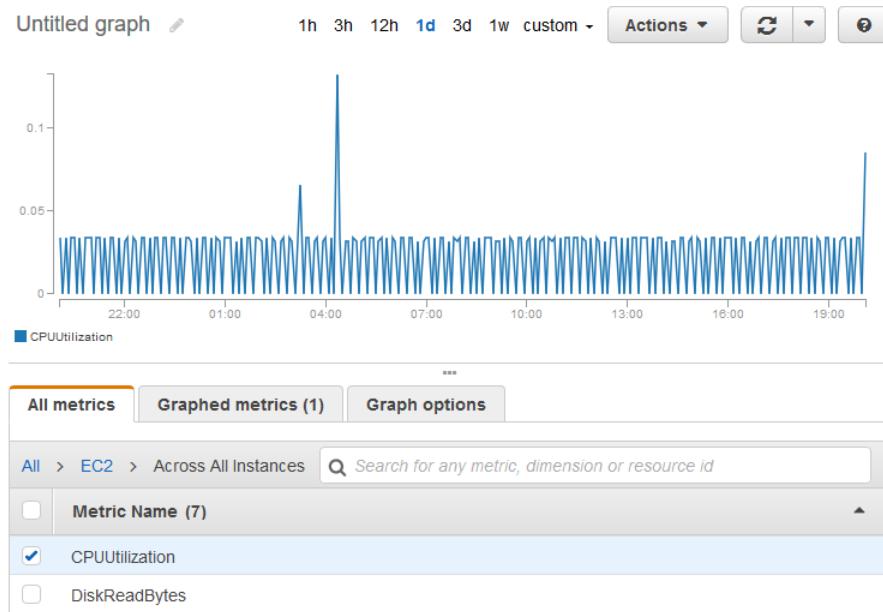
此示例显示了如何使用详细监控来获取 EC2 实例的平均 CPU 使用率。因为未指定任何维度，所以 CloudWatch 会返回 AWS/EC2 命名空间中所有维度的统计数据。

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 (控制台)

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 (跨所有实例)。
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间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

获取实例的平均 CPU 利用率 (AWS CLI)

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": 238.0,  
            "Timestamp": "2016-10-12T07:18:00Z",  
            "Average": 0.038235294117647062,  
            "Unit": "Percent"  
        }  
    ]  
}
```

```
{  
    "SampleCount": 240.0,  
    "Timestamp": "2016-10-12T09:18:00Z",  
    "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。

显示一个 Auto Scaling 组中的实例的 DiskWriteBytes (控制台)

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 组所在的行，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间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

显示一个 Auto Scaling 组中的实例的 DiskWriteBytes (AWS CLI)

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"  
        }  
    ]  
}
```

```
        "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 \(p. 538\)](#)。

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 使用率。平均值以 60 秒为时间间隔 1 天为周期。

按 AMI 显示平均 CPU 利用率（控制台）

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 所在的行，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间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

获取某个映像 ID 的平均 CPU 利用率 (AWS CLI)

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 使用率百分比。

```
{
  "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 (监控) 选项卡上查看实例的监控图表。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 平均使用率 (%)
- 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 \(p. 539\)](#)。

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 [绘制指标图表](#)。

为实例创建 CloudWatch 警报

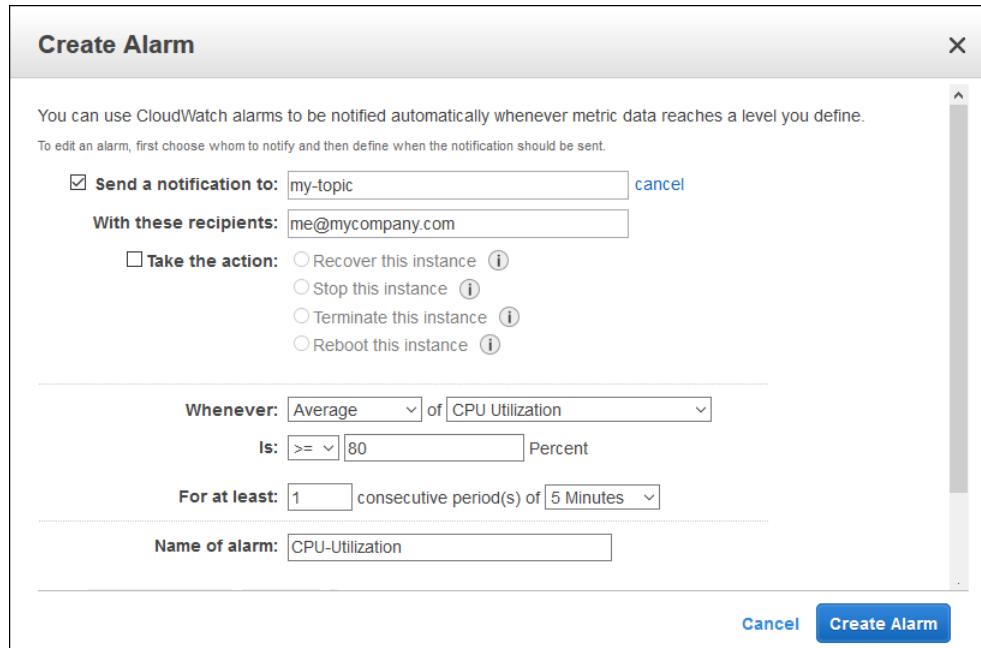
您可以创建 CloudWatch 警报来监控您的任一实例的 CloudWatch 指标。当该指标达到指定阈值时，CloudWatch 自动向您发送通知。您可以使用 Amazon EC2 控制台创建 CloudWatch 警报，或者使用 CloudWatch 控制台提供的更多高级选项。

使用 CloudWatch 控制台创建警报

有关示例，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 (创建警报) 对话框中，执行以下操作：
 - a. 选择 create topic。对于 Send a notification to (发送通知到)，输入 SNS 主题的名称。对于 With these recipients (收件人如下)，输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 并输入 80%。对于 For at least (至少)，输入 1 个 5 Minutes 的连续周期。
 - 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。

AWSServiceRoleForCloudWatchEvents 服务相关角色使 AWS 能够代表您执行警报操作。当您首次在 AWS 管理控制台、IAM CLI 或 IAM API 中创建警报时，CloudWatch 会为您创建服务相关角色。

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：

- `iam:CreateServiceLinkedRole`、`iam:GetPolicy`、`iam:GetPolicyVersion` 和 `iam:GetRole`
 - 针对包含 Amazon EC2 操作的所有警报
- `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
- 包含恢复操作的警报不需要任何特定权限。

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关联 Amazon EC2 API 的权限，将执行您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](#)。

目录

- 向 Amazon CloudWatch 警报添加停止操作 (p. 556)
- 向 Amazon CloudWatch 警报添加终止操作 (p. 557)
- 向 Amazon CloudWatch 警报添加重启操作 (p. 557)
- 向 Amazon CloudWatch 警报添加恢复操作 (p. 558)
- 使用 Amazon CloudWatch 控制台查看警报和操作历史记录 (p. 559)
- Amazon CloudWatch 警报操作场景 (p. 560)

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 使用率低于 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、持续时间和周期，还可以添加 Amazon Simple Notification Service (Amazon SNS) 通知，以便在触发警报后，您能够收到电子邮件。

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。

创建停止空闲实例的警报 (Amazon EC2 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 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Create Alarm (创建警报) 对话框中，执行以下操作：
 - a. 要在触发警报时收到电子邮件，请为 Send a notification to (发送通知到) 选择一个现有 Amazon SNS 主题，或者选择 create topic (创建主题) 创建一个新主题。
要创建新主题，请对 Send a notification to (发送通知到) 输入主题的名称，然后对 With these recipients (收件人如下) 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。
 - b. 选择 Take the action (请执行以下操作)、Stop this instance (停止此实例)。
 - c. 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 (平均值) 和 CPU Utilization (CPU 利用率)。
 - d. 对于 Is (是)，指定指标阈值。在此示例中，输入 10%。
 - e. 对于 For at least (至少)，指定警报的评估周期。在此示例中，输入 24 个 1 Hour (1 小时) 的连续周期。
 - f. 要更改警报的名称，可对 Name of alarm (警报名称) 输入新名称。警报名称必须仅包含 ASCII 字符。

如果您未输入警报名称，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。

- g. 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](#)。

创建终止空闲实例的警报（Amazon EC2 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 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Create Alarm (创建警报) 对话框中，执行以下操作：
 - a. 要在触发警报时收到电子邮件，请为 Send a notification to (发送通知到) 选择一个现有 Amazon SNS 主题，或者选择 create topic (创建主题) 创建一个新主题。

要创建新主题，请对 Send a notification to (发送通知到) 输入主题的名称，然后对 With these recipients (收件人如下) 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。

- b. 选择 Take the action (请执行以下操作)、Terminate this instance (终止此实例)。
- c. 对于 Whenever，选择统计数据，然后选择指标。在此示例中，选择 Average (平均值) 和 CPU Utilization (CPU 利用率)。
- d. 对于 Is (是)，指定指标阈值。在此示例中，输入 10%。
- e. 对于 For at least (至少)，指定警报的评估周期。在此示例中，输入 24 个 1 Hour (1 小时) 的连续周期。
- f. 要更改警报的名称，可对 Name of alarm (警报名称) 输入新名称。警报名称必须仅包含 ASCII 字符。

如果您未输入警报名称，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。

- g. 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。

与停止并重新启动您的实例不同，重启实例不会启动新的实例计费周期（最低收取一分钟的费用）。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

为了避免重启操作与恢复操作之间的竞争情况，请避免为重启警报和恢复警报设置相同的评估周期数。我们建议您将重启警报设置为 3 个 1 分钟的评估期。有关更多信息，请参阅Amazon CloudWatch 用户指南中的[评估警报](#)。

创建重启实例的警报 (Amazon EC2 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 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Create Alarm (创建警报) 对话框中，执行以下操作：
 - a. 要在触发警报时收到电子邮件，请为 Send a notification to (发送通知到) 选择一个现有 Amazon SNS 主题，或者选择 create topic (创建主题) 创建一个新主题。

要创建新主题，请对 Send a notification to (发送通知到) 输入主题的名称，然后对 With these recipients (收件人如下) 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。

- b. 选择 Take the action (请执行以下操作)、Reboot this instance (重启此实例)。
- c. 对于 Whenever (每当)，选择 Status Check Failed (Instance) (状态检查失败(实例))
- d. 对于 For at least (至少)，指定警报的评估周期。在此示例中，输入 3 个 1 Minute (1 分钟) 的连续周期。
- e. 要更改警报的名称，可对 Name of alarm (警报名称) 输入新名称。警报名称必须仅包含 ASCII 字符。

如果您未输入警报名称，Amazon CloudWatch 会自动为您创建一个。

- f. 选择 Create Alarm。

向 Amazon CloudWatch 警报添加恢复操作

您可以创建 Amazon CloudWatch 警报来监控 Amazon EC2 实例。如果实例因需要 AWS 参与才能修复的基础硬件故障或问题而受损，您可自动恢复实例。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。

CloudWatch 会阻止您将恢复操作添加到位于不支持恢复操作的实例上的警报。

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。您将注意到，实例会在已恢复的实例上重启。

恢复操作仅适用于 StatusCheckFailed_System，而不能用于 StatusCheckFailed_Instance。

下列问题可能导致系统状态检查失败：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上影响到网络连接状态的硬件问题

只有具有以下特性的实例支持恢复操作：

- 使用以下实例类型之一：
— A1、C3、C4、C5、C5n、Inf1、M3、M4、M5、M5a、M5n、P3、R3、R4、R5、R5a、R5n、T2、T3、T3a、X1e 或 X1e
- 使用 default 或 dedicated 实例租赁
- 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

为了避免重启操作与恢复操作之间的竞争情况，请避免为重启警报和恢复警报设置相同的评估周期数。我们建议您将恢复警报设置为 2 个 1 分钟的评估期。有关更多信息，请参阅Amazon CloudWatch 用户指南中的[评估警报](#)。

创建恢复实例的警报 (Amazon EC2 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 Instances。
3. 选择实例。在 Monitoring 选项卡上，选择 Create Alarm。
4. 在 Create Alarm (创建警报) 对话框中，执行以下操作：
 - a. 要在触发警报时收到电子邮件，请为 Send a notification to (发送通知到) 选择一个现有 Amazon SNS 主题，或者选择 create topic (创建主题) 创建一个新主题。

要创建新主题，请对 Send a notification to (发送通知到) 输入主题的名称，然后对 With these recipients (收件人如下) 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。

Note

- 用户必须订阅指定的 SNS 主题才能在触发警报时收到电子邮件通知。
 - 当自动实例恢复操作执行时，AWS 账户根用户始终会收到电子邮件通知，即使未指定 SNS 主题也是如此。
 - 当自动实例恢复操作执行时，AWS 账户根用户始终会收到电子邮件通知，即使未订阅指定的 SNS 主题也是如此。
- b. 选择 Take the action (请执行以下操作)、Recover this instance (恢复此实例)。
 - c. 对于 Whenever (每当)，选择 Status Check Failed (System) (状态检查失败(系统))。
 - d. 对于 For at least (至少)，指定警报的评估周期。在此示例中，输入 2 个 1 Minute (1 分钟) 的连续周期。
 - e. 要更改警报的名称，可对 Name of alarm (警报名称) 输入新名称。警报名称必须仅包含 ASCII 字符。

如果您未输入警报名称，Amazon CloudWatch 会自动为您创建一个。

- f. 选择 Create Alarm。

使用 Amazon CloudWatch 控制台查看警报和操作历史记录

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。

查看已触发的警报和操作的历史记录 (CloudWatch 控制台)

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。

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: [create topic](#)

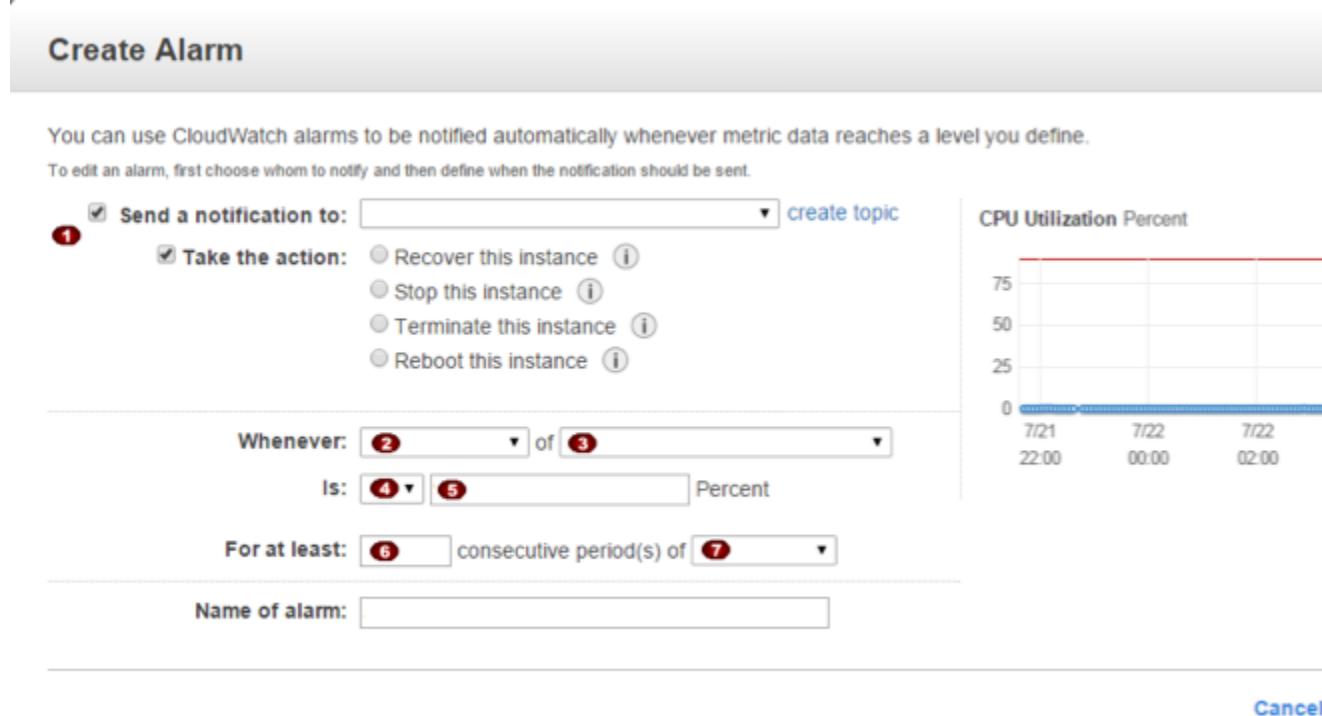
Take the action: Recover this instance [i](#)
 Stop this instance [i](#)
 Terminate this instance [i](#)
 Reboot this instance [i](#)

Whenever: of
Is: Percent

For at least: consecutive period(s) of

Name of alarm:

CPU Utilization Percent



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
1	Stop
2	最高
3	CPUUtilization
4	<=
5	10%
6	60 分钟
7	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
1	Stop and email
2	平均值
3	CPUUtilization
4	<=
5	5%
6	60 分钟
7	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
1	电子邮件
2	总计
3	网络输出
4	>
5	10GB
6	1 天
7	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
1	Stop and send SMS
2	总计
3	网络输出
4	>
5	1GB
6	1 小时
7	1

场景 5：停止出现内存泄漏的实例

创建当内存使用率达到或超过 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[为 Amazon EC2 Linux 实例监控内存和磁盘指标](#)。

设置	值
1	Stop
2	最高
3	MemoryUtilization
4	\geq
5	90%
6	1 minute
7	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
1	Stop
2	平均值
3	系统状态检查失败
4	\geq
5	1
6	15 分钟
7	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
1	终止
2	最高
3	网络输出
4	\leq

设置	值
5	100000 字节
6	5 分钟
7	1

使用 CloudWatch Events 实现 Amazon EC2 的自动化

您可以使用 Amazon CloudWatch Events 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。可自动触发的操作包括：

- 调用 AWS Lambda 函数
- 调用 Amazon EC2 Run Command
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 AWS Step Functions 状态机
- 通知 Amazon SNS 主题或 Amazon SQS 队列

一些将 CloudWatch Events 与 Amazon EC2 结合使用的示例包括：

- 在每次新的 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

您可以使用 Amazon CloudWatch 从操作系统中收集 EC2 实例的指标和日志。

CloudWatch 代理

您可以使用 CloudWatch 代理收集来自 Amazon EC2 实例和本地服务器的系统指标与日志文件。代理支持 Windows Server 和 Linux，并使您能够选择要收集的指标，包括子资源指标（如每 CPU 内核）。建议您使用代理（而不是监控脚本）收集指标和日志。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器中收集指标](#)。

CloudWatch 监控脚本

Important

建议您使用 CloudWatch 代理收集指标和日志。有关监控脚本的信息是为仍在使用旧监控脚本从其 Linux 实例收集信息的客户提供提供的。

监控脚本演示如何为 Amazon CloudWatch 生成和使用自定义指标。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使用率指标。

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](#)。

目录

- [支持的系统 \(p. 564\)](#)
- [所需权限 \(p. 564\)](#)
- [安装所需的程序包 \(p. 564\)](#)
- [安装监控脚本 \(p. 566\)](#)
- [mon-put-instance-data.pl \(p. 566\)](#)
- [mon-get-instance-stats.pl \(p. 569\)](#)
- [在控制台中查看自定义指标 \(p. 570\)](#)
- [故障排除 \(p. 570\)](#)

支持的系统

已使用以下系统在实例上测试监控脚本：

- Amazon Linux 2
- Amazon Linux AMI 2014.09.2 和更高版本
- Red Hat Enterprise Linux 6.9 和 7.4
- SUSE Linux Enterprise Server 12
- Ubuntu Server 14.04 和 16.04

所需权限

确保脚本具有通过将 IAM 角色与您的实例关联来调用以下操作的权限：

- `cloudwatch:PutMetricData`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch>ListMetrics`
- `ec2:DescribeTags`

有关更多信息，请参阅 [使用 IAM 角色 \(p. 752\)](#)。

安装所需的程序包

对于 Linux 的某些版本，您必须先安装额外的 Perl 模块，然后才能使用监控脚本。

在 Amazon Linux 2 和 Amazon Linux AMI 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 Linux 实例 \(p. 423\)](#)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install -y perl-Switch perl-Datetime perl-Sys-Syslog perl-LWP-Protocol-https  
perl-Digest-SHA.x86_64
```

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 Linux 实例 \(p. 423\)](#)。

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 libdatetime-perl
```

在 Red Hat Enterprise Linux 7 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 Linux 实例 \(p. 423\)](#)。
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 --enablerepo="rhui-REGION-rhel-server-optional" -y
sudo yum install zip unzip
```

在 Red Hat Enterprise Linux 6.9 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 Linux 实例 \(p. 423\)](#)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install perl-Datetime perl-CPAN perl-Net-SSLeay perl-IO-Socket-SSL perl-
Digest-SHA gcc -y
sudo yum install zip unzip
```

3. 以权限经过提升的用户身份运行 CPAN：

```
sudo cpan
```

出现提示时始终按 Enter，直到您看到以下提示：

```
cpan[1]>
```

4. 在 CPAN 提示下，运行以下的每个命令：运行一个命令，该命令将进行安装，然后在您返回到 CPAN 提示时运行下一个命令。在系统提示继续完成该过程时像之前一样按 Enter：

```
cpan[1]> install YAML
cpan[2]> install LWP::Protocol::https
cpan[3]> install Sys::Syslog
cpan[4]> install Switch
```

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 Linux 实例 \(p. 423\)](#)。
2. 在运行 SUSE Linux Enterprise Server 12 的服务器上，您可能需要下载 perl-Switch 程序包。您可以使用以下命令来下载并安装此程序包：

```
wget http://download.opensuse.org/repositories/devel:/languages:/perl/SLE_12_SP3/
noarch/perl-Switch-2.17-32.1.noarch.rpm
sudo rpm -i perl-Switch-2.17-32.1.noarch.rpm
```

3. 安装所需的程序包，如下所示：

```
sudo zypper install perl-Switch perl-Datetime
```

```
sudo zypper install -y "perl(LWP::Protocol::https)"
```

安装监控脚本

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 https://aws-cloudwatch.s3.amazonaws.com/downloads/  
CloudWatchMonitoringScripts-1.2.2.zip -O
```

2. 运行以下命令安装您下载的监控脚本：

```
unzip CloudWatchMonitoringScripts-1.2.2.zip && \  
rm CloudWatchMonitoringScripts-1.2.2.zip && \  
cd aws-scripts-mon
```

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 和私有访问密钥。
- LICENSE.txt – 包含 Apache 2.0 许可证的文本文件。
- NOTICE.txt – 版权声明。

mon-put-instance-data.pl

此脚本会收集当前系统的内存、交换和磁盘空间使用率数据。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	描述
--mem-util	以百分比收集和发送 MemoryUtilization 指标。此指标计算应用程序分配和操作系统使用的内存，如果您指定 --mem-used-incl-cache-buff 选项，则还将缓存和缓冲区内存包括在已用内存中。
--mem-used	收集和发送 MemoryUsed 指标（以兆字节报告）。此指标计算应用程序分配和操作系统使用的内存，如果您指定 --mem-used-incl-cache-buff 选项，则还将缓存和缓冲区内存包括在已用内存中。
--mem-used-incl-cache-buff	如果包括此选项，则在报告 --mem-util、--mem-used 和 --mem-avail 的指标时，当前用于缓存和缓冲区的内存将计为“已用”。
--mem-avail	收集和发送 MemoryAvailable 指标（以兆字节报告）。此指标计算应用程序分配和操作系统使用的内存，如果您指定 --mem-used-incl-cache-buff 选项，则还将缓存和缓冲区内存包括在已用内存中。

名称	描述
--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 / 和 /home 位置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。
--aws-credential-file=PATH	<p>提供包含 AWS 凭证的文件的位置。</p> <p>此参数不能与 --aws-access-key-id 和 --aws-secret-key 参数一起使用。</p>
--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。不要将该选项与 --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。不要将该选项与 --aws-credential-file 参数一起使用。

名称	描述
--aws-iam-role=VALUE	指定用于提供 AWS 凭证的 IAM 角色。必须提供 =VALUE 值。如果不指定凭证，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。 请勿将该选项与 --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 值是可选的，如果指定，则脚本只报告聚合指标。
--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 必须有权调用 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。该选项还会检查是否已提供凭证。在详细模式中运行时，该选项输出的指标会发送到 CloudWatch。
--from-cron	从 cron 调用脚本时，请使用该选项。使用该选项时，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证。

以下示例执行简单的测试运行而不将数据发布到 CloudWatch。

```
./mon-put-instance-data.pl --mem-util --verify --verbose
```

以下示例收集所有可用内存指标并将其发送到 CloudWatch，将缓存和缓冲区内存计为“已用”

```
./mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --mem-used --mem-avail
```

以下示例收集 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
```

以下示例收集实例类型、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
```

要为向 CloudWatch 报告的指标制定 cron 计划，请使用 `crontab -e` 命令开始编辑 `crontab`。添加下列命令，每五分钟将内存和磁盘空间使用率报告到 CloudWatch：

```
* /5 * * * * ~/aws-scripts-mon/mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --disk-space-util --disk-path=/ --from-cron
```

如果脚本遇到错误，它会在系统日志中写下错误消息。

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	描述
--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 凭证的文件的位置。
--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。不要将该选项与 --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。不要将该选项与 --aws-credential-file 选项一起使用。
--aws-iam-role=VALUE	指定用于提供 AWS 凭证的 IAM 角色。必须提供 =VALUE 值。如果不指定凭证，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。 请勿将该选项与 --aws-credential-file、--aws-access-key-id 或 --aws-secret-key 参数一起使用。
--verify	执行脚本的测试运行。该选项还会检查是否已提供凭证。
--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

要获得最近 12 小时的使用率统计数据，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
```

使用 AWS CloudTrail 记录 Amazon EC2 和 Amazon EBS API 调用

Amazon EC2 和 Amazon EBS 与 AWS CloudTrail 服务集成在一起，该服务提供用户、角色或 AWS 服务在 Amazon EC2 和 Amazon EBS 中所执行的操作的记录。CloudTrail 将对 Amazon EC2 和 Amazon EBS 的所有 API 调用均作为事件捕获，包括来自控制台的调用和对 API 的代码调用。如果您创建了跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Amazon EC2 和 Amazon EBS 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 Amazon EC2 和 Amazon EBS 发出的请求、从中发出请求的 IP 地址、发出请求的用户、发出请求的时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 [AWS CloudTrail User Guide](#)。

CloudTrail 中的 Amazon EC2 和 Amazon EBS 信息

在您创建 CloudTrail 账户时，即针对该账户启用了 AWS。当 Amazon EC2 和 Amazon EBS 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 [使用 CloudTrail 事件历史记录查看事件](#)。

要持续记录 AWS 账户中的事件（包括 Amazon EC2 和 Amazon EBS 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有区域。此跟踪在 AWS 分区中记录来自所有区域的事件，并将日志文件传送至您指定的 Amazon S3 存

储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅：

- [创建跟踪概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)
- [接收来自多个区域的 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件](#)

所有 Amazon EC2 和 Amazon EBS 操作均由 CloudTrail 记录下来并记载到 [Amazon EC2 API Reference](#) 中。举例来说，对 [RunInstances](#)、[DescribeInstances](#) 或 [CreateImage](#) 操作的调用会在 CloudTrail 日志文件中生成相应条目。

每个事件或日志条目都包含有关生成请求的人员的信息。身份信息帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

了解 Amazon EC2 和 Amazon EBS 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

下面的日志文件记录显示，用户终止了一个实例。

```
{  
    "Records": [  
        {  
            "eventVersion": "1.03",  
            "userIdentity": {  
                "type": "Root",  
                "principalId": "123456789012",  
                "arn": "arn:aws:iam::123456789012:root",  
                "accountId": "123456789012",  
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
                "userName": "user"  
            },  
            "eventTime": "2016-05-20T08:27:45Z",  
            "eventSource": "ec2.amazonaws.com",  
            "eventName": "TerminateInstances",  
            "awsRegion": "us-west-2",  
            "sourceIPAddress": "198.51.100.1",  
            "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",  
            "requestParameters": {  
                "instancesSet": {  
                    "items": [ {  
                        "instanceId": "i-1a2b3c4d"  
                    } ]  
                }  
            },  
            "responseElements": {  
                "instancesSet": {  
                    "items": [ {  
                        "instanceId": "i-1a2b3c4d",  
                        "state": "terminated"  
                    } ]  
                }  
            }  
        }  
    ]  
}
```

```
"currentState":{  
    "code":32,  
    "name":"shutting-down"  
},  
"previousState":{  
    "code":16,  
    "name":"running"  
}  
}  
}  
},  
"requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",  
"eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",  
"eventType":"AwsApiCall",  
"recipientAccountId":"123456789012"  
}  
]  
}
```

使用 AWS CloudTrail 审核通过 EC2 Instance Connect 连接的用户

可以使用 AWS CloudTrail 审核通过 EC2 Instance Connect 连接到实例的用户。

使用 AWS CloudTrail 控制台审核通过 EC2 Instance Connect 的 SSH 活动

1. 打开 AWS CloudTrail 控制台 (<https://console.aws.amazon.com/cloudtrail/>)。
2. 验证您是否位于正确的区域中。
3. 在导航窗格中，选择事件历史记录。
4. 对于筛选条件，请选择事件源，然后选择 ec2-instance-connect.amazonaws.com。
5. (可选) 对于时间范围，请选择一个时间范围。
6. 选择刷新事件图标。
7. 该页面显示与 `SendSSHPublicKey` API 调用对应的事件。使用箭头展开一个事件以查看其他详细信息，例如，用于建立 SSH 连接的用户名和 AWS 访问密钥以及源 IP 地址。
8. 要以 JSON 格式显示完整事件信息，请选择查看事件。`requestParameters` 字段包含用于建立 SSH 连接的目标实例 ID、操作系统用户名和公有密钥。

```
{  
    "eventVersion": "1.05",  
    "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",  
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",  
        "accountId": "123456789012",  
        "accessKeyId": "ABCDEFGUZHNAAW4OSN2AEXAMPLE",  
        "userName": "IAM-friendly-name",  
        "sessionContext": {  
            "attributes": {  
                "mfaAuthenticated": "false",  
                "creationDate": "2018-09-21T21:37:58Z"  
            }  
        },  
        "eventTime": "2018-09-21T21:38:00Z",  
        "eventSource": "ec2-instance-connect.amazonaws.com",  
        "eventName": "SendSSHPublicKey",  
        "awsRegion": "us-west-2",  
        "sourceIPAddress": "123.456.789.012",  
        "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",  
    }  
}
```

```
"requestParameters": {  
    "instanceId": "i-0123456789EXAMPLE",  
    "osUser": "ec2-user",  
    "SSHKey": {  
        "publicKey": "ssh-rsa ABCDEFGHIJKLMNOP01234567890EXAMPLE"  
    }  
    "responseElements": null,  
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",  
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",  
    "eventType": "AwsApiCall",  
    "recipientAccountId": "0987654321"  
}
```

如果已将 AWS 账户配置为在 S3 存储桶中收集 CloudTrail 事件，您可以按编程方式下载和审核该信息。有关更多信息，请参阅 AWS CloudTrail User Guide 中的[获取和查看 CloudTrail 日志文件](#)。

Amazon EC2 中的联网功能

Amazon EC2 提供以下联网功能。

功能

- [Amazon EC2 实例 IP 寻址 \(p. 574\)](#)
- [自带 IP 地址 \(BYOIP\) \(p. 587\)](#)
- [弹性 IP 地址 \(p. 590\)](#)
- [弹性网络接口 \(p. 595\)](#)
- [Linux 上的增强联网 \(p. 616\)](#)
- [Elastic Fabric Adapter \(p. 638\)](#)
- [置放群组 \(p. 662\)](#)
- [EC2 实例的网络最大传输单位 \(MTU\) \(p. 669\)](#)
- [Virtual Private Cloud \(p. 671\)](#)
- [EC2-Classic \(p. 672\)](#)

Amazon EC2 实例 IP 寻址

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 寻址](#)。

目录

- [私有 IPv4 地址和内部 DNS 主机名 \(p. 574\)](#)
- [公有 IPv4 地址和外部 DNS 主机名 \(p. 575\)](#)
- [弹性 IP 地址 \(IPv4\) \(p. 576\)](#)
- [Amazon DNS 服务器 \(p. 576\)](#)
- [IPv6 地址 \(p. 576\)](#)
- [使用实例的 IP 地址 \(p. 576\)](#)
- [多个 IP 地址 \(p. 580\)](#)

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 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](#)。我们会使用 DHCP 将私有 IPv4 地址分配到实例。

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，我们会为实例分配主要私有 IPv4 地址。另外，还为每个实例指定了一个可解析为主要私有 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 VPC 中实现实例之间的通信，但我们无法解析 VPC 之外的内部 DNS 主机名。

实例会收到一个来自子网 IPv4 地址范围的主要私有 IP 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的 [VPC 和子网大小调整](#)。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。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 \(p. 580\)](#)。

私有 IPv4 地址（无论是主地址还是辅助地址）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。

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 主机名解析为其 VPC 外的实例的公有 IP 地址，以及其 VPC 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。有关更多信息，请参阅[RFC 1631：IP 网络地址转换器 \(NAT\)](#)。

在默认 VPC 中启动实例时，默认情况下，我们会为实例分配公有 IP 地址。当您在非默认 VPC 中启动实例时，子网的一个属性会确定在该子网中启动的实例是否从公有 IPv4 地址池接收公有 IP 地址。默认情况下，我们不会将公有 IP 地址分配到非默认子网中启动的实例。

您可以按如下所示控制实例是否接收公有 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 \(p. 578\)](#)。

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，我们会释放它的公有 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。
- 当您将弹性 IP 地址与您实例的公有 IP 地址关联时，我们会释放该公有 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，则在多个网络接口附加到实例的情况下，该实例不会接收新地址。
- 如果您实例的公有 IP 地址在其辅助私有 IP 地址与弹性 IP 地址关联时被释放，则该实例不会接收新的公有 IP 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。

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，可能需要 24 小时，以便 IP 地址可以传递到整个 Internet。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 \(p. 590\)](#)。

如果实例分配有弹性 IP 地址，则在启用 DNS 主机名后，该实例会收到一个 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 \(p. 590\)](#)。

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。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](#)
- [向 VPC 关联 IPv6 CIDR 块](#)
- [向子网关联 IPv6 CIDR 块](#)

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，则您的实例会收到 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。
- 您向同一子网中的某个网络接口分配 IPv6 地址，并在启动后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 \(p. 596\)](#)。

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。

目录

- [确定您的公有、私有和弹性 IP 地址 \(p. 577\)](#)

- 确定 IPv6 地址 (p. 578)
- 在实例启动期间分配公有 IPv4 地址 (p. 578)
- 向实例分配 IPv6 地址 (p. 579)
- 取消分配给实例的 IPv6 地址 (p. 580)

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 \(p. 499\)](#)。

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. 如果您为与实例连接的网络接口分配了一个或多个辅助私有 IPv4 地址，那么可从 Secondary private IPs (辅助私有 IP) 字段中获取这些 IP 地址。
5. 或者，在导航窗格中，选择 Network Interfaces (网络接口)，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. 如果一个或多个弹性 IP 地址已与实例相关联，请从弹性 IP 字段中获取弹性 IP 地址。

Note

如果您的实例没有公有 IPv4 地址，但已将一个弹性 IP 地址与该实例的网络接口相关联，IPv4 公有 IP 字段将显示该弹性 IP 地址。

5. 或者，在导航窗格中，选择 Network Interfaces (网络接口)，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 IPv4 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：

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

3. 使用以下命令访问公有 IP 地址：

```
[ec2-user ~]$ curl 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

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 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)：

```
[ec2-user ~]$ curl 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

所有子网都有一个属性可确定在子网中启动的实例是否分配了公有 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 \(p. 575\)](#)。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 \(p. 590\)](#)。

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[使用启动实例向导启动实例 \(p. 375\)](#)。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 \(p. 590\)](#)。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。

所有当前生成实例类型以及 C3、R3 和 I2 以前生成实例类型都支持 IPv6。

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. 选择支持 IPv6 的 AMI 和实例类型，然后选择 Next: Configure Instance Details (下一步: 配置实例详细信息)。
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 Auto-assign IPv6 IP，选择 Enable。
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 (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
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。如果您从旧版 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 (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
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

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 \(p. 596\)](#)。

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。

目录

- [多个 IP 地址如何工作 \(p. 580\)](#)
- [使用多个 IPv4 地址 \(p. 581\)](#)
- [使用多个 IPv6 地址 \(p. 584\)](#)

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。网络接口需要附加到实例。
- 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 地址。
- 您必须从子网的 IPv6 CIDR 块范围内为网络接口选择辅助 IPv6。
- 将安全组与网络接口关联，而不是与各 IP 地址关联。因此，网络接口中指定的每个 IP 地址均受其网络接口的安全组约束。
- 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。
- 当网络接口与实例分离或附加到实例时，主要私有 IPv4 地址、辅助私有 IPv4 地址、弹性 IP 地址以及 IPv6 地址将仍然属于此辅助网络接口。
- 尽管您无法从实例分离主要网络接口，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。

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。

目录

- [分配辅助私有 IPv4 地址 \(p. 581\)](#)
- [在您的实例上配置操作系统以识别辅助私有 IPv4 地址 \(p. 583\)](#)
- [将弹性 IP 地址与辅助私有 IPv4 地址关联 \(p. 583\)](#)
- [查看您的辅助私有 IPv4 地址 \(p. 583\)](#)
- [取消分配辅助私有 IPv4 地址 \(p. 584\)](#)

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。

- [启动实例时分配辅助私有 IPv4 地址 \(p. 581\)](#)
- [使用命令行在启动期间分配辅助 IPv4 地址 \(p. 582\)](#)
- [为网络接口分配辅助私有 IPv4 地址 \(p. 582\)](#)
- [使用命令行为现有实例分配辅助私有 IPv4 \(p. 582\)](#)

启动实例时分配辅助私有 IPv4 地址

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 选择 Launch Instance。
- 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。您可以附加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 \(p. 596\)](#)。

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 \(p. 591\)](#)。

- 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 \(p. 583\)](#)。

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) 的 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，或者将该字段保留空白，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 \(p. 607\)](#)。
- 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

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

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 IPv4 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。

目录

- [分配多个 IPv6 地址 \(p. 584\)](#)
- [查看您的 IPv6 地址 \(p. 586\)](#)
- [取消分配 IPv6 地址 \(p. 586\)](#)

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 \(p. 160\)](#)。
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。
 - 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。您可以附加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 \(p. 596\)](#)。
6. 按照向导中的后续步骤附加卷并标记您的实例。
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 \(p. 775\)](#)。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 Amazon EC2 控制台的 Instances (实例) 屏幕将多个 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 (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
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 (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)。

自带 IP 地址 (BYOIP)

您可将自己的全部或部分公有 IPv4 地址从本地网络引入到 AWS 账户中。您将继续拥有地址范围，但 AWS 会将其公布在 Internet 上。在将地址范围引入 AWS 中之后，它会在您的账户中显示为地址池。您可从地址池创建弹性 IP 地址，并将其用于您的 AWS 资源，如 EC2 实例、NAT 网关和 Network Load Balancer。

Important

BYOIP 并非在所有区域中都可用。有关受支持区域的列表，请参阅[自带 IP 常见问题](#)。

要求

- 必须在区域 Internet 注册表 (RIR) 中注册地址范围，例如 American Registry for Internet Numbers (ARIN)、Réseaux IP Européens Network Coordination Centre (RIPE) 或 Asia-Pacific Network Information Centre (APNIC)。它必须由企业或机构实体注册，而不能由个人注册。
- 您可指定的最具体的地址范围为 /24。
- 您可以将每个地址范围一次添加到一个区域中。
- 您可以将每个区域的 5 个地址范围添加到您的 AWS 账户中。
- IP 地址范围中的地址必须具有干净的历史记录。我们可能会调查 IP 地址范围的声誉，并保留在其中包含的 IP 地址具有不良声誉或与恶意行为关联的情况下拒绝此 IP 地址范围的权利。
- 支持以下：
 - ARIN – “Direct Allocation”和“Direct Allocation”网络类型。
 - RIPE – “ALLOCATED PA”、“LEGACY”和“ASSIGNED PI”分配状态
 - APNIC -“ALLOCATED PORTABLE”和“ASSIGNED PORTABLE”分配状态

准备将您的地址范围引入您的 AWS 账户

要确保仅您可以将地址范围添加到您的 AWS 账户，您必须授权 Amazon 公布该地址范围。您还必须通过签名的授权消息提供您拥有该地址范围的证据。

路由来源授权 (ROA) 是有关可通过 RIR 创建的路由通告的加密声明。它包含地址范围、允许公布地址范围的自治系统编号 (ASN) 及到期日期。ROA 授权 Amazon 以特定的 AS 编号公布地址范围。但是，它不会授权您的 AWS 账户将地址范围引入 AWS。要授权您的 AWS 账户将地址范围引入 AWS，您必须在该地址范围的注册数据访问协议 (RDAP) 备注中发布自签名 X509 证书。该证书包含一个公有密钥，AWS 使用该密钥验证您所提供的授权上下文签名。您应确保您的私有密钥的安全，并使用该密钥来对授权上下文消息进行签名。

这些任务中的命令在 Linux 上受支持。在 Windows 上，您可以使用[适用于 Linux 的 Windows 子系统](#)运行 Linux 命令。

任务

- [创建一个 ROA 对象。 \(p. 588\)](#)
- [创建自签名 X509 证书 \(p. 588\)](#)
- [创建签名授权消息 \(p. 588\)](#)

创建一个 ROA 对象。

创建 ROA 对象以授权 ASN 16509 和 14618 来公布您的地址范围，以及当前授权的 ASN 来公布该地址范围。您必须将最大长度设置为要引入的最小前缀的大小（例如 /24）。若要 ROA 可用于 Amazon，可能需要多达 24 小时的时间。有关更多信息，请参阅下列内容：

- ARIN — [ROA 请求](#)
- RIPE — [管理 ROA](#)
- APNIC - [路由管理](#)

创建自签名 X509 证书

使用以下过程创建自签名 X509 证书，并将其添加到您的 RIR 的 RDAP 记录。openssl 命令需要 OpenSSL 版本 1.0.2 或更高版本。

创建自签名 X509 证书并将其添加到 RDAP 记录

1. 生成 RSA 2048 位密钥对，如下所示。

```
openssl genrsa -out private.key 2048
```

2. 使用以下命令从该密钥对创建一个公有 X509 证书。在此示例中，该证书在 365 天后过期，在此日期后它将不能是受信任的。因此，请务必相应地设置到期时间。当系统提示您提供信息时，输入默认值。

```
openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
```

3. 使用 X509 证书更新 RIR 的 RDAP 记录。请务必复制证书中的 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE-----。请务必事先在上述步骤中使用 tr -d "\n" 命令删除换行符（如果尚未这样做的话）。要查看证书，请运行以下命令。

```
cat publickey.cer
```

对于 ARIN，在地址范围的“Public Comments (公共注释)”部分中添加证书。

对于 RIPE，将证书添加为地址范围的“描述”字段。

对于 APNIC，通过电子邮件将公有密钥发送到 helpdesk@apnic.net，以将其手动添加到“remarks (备注)”字段中。请以 IP 地址的 APNIC 授权联系人身份发送电子邮件。

创建签名授权消息

签名的授权消息的格式如下所示，其中，日期是消息的到期日期。

```
1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
```

首先，创建纯文本授权消息，并将其存储在名为 text_message 的变量中，如下所示。使用您自己的值替换示例账号、地址范围和失效日期。

```
text_message="1|aws|123456789012|198.51.100.0/24|20191201|SHA256|RSAPSS"
```

接下来，使用您创建的密钥对在 `text_message` 中对授权消息进行签名，然后将其存储在名为 `signed_message` 的变量中，如下所示。

```
signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform PEM | openssl base64 | tr -- '+=' '-'_-' | tr -d "\n")
```

预配置地址范围以用于 AWS

在预置一个地址范围以用于 AWS 时，您需要确认您拥有该地址范围，并授权 Amazon 公布该地址范围。我们还会通过签名授权消息验证您拥有该地址范围。该消息是使用在通过 X509 证书更新 RDAP 记录时使用的自签名 X509 密钥对签名的。

要预配置地址范围，请使用以下 `provision-byoip-cidr` 命令。使用您自己的地址范围替换示例地址范围。`--cidr-authorization-context` 选项使用您以前创建的变量，而不是 ROA 消息。

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

预配置地址范围是一项异步操作，因此该调用会立即返回，但地址范围未准备就绪，直到其状态从 `pending-provision` 更改为 `provisioned` 才可供使用。完成预置过程最多可能需要三周时间。要监控您预置的地址范围的状态，请使用以下 `describe-byoip-cidrs` 命令。

```
aws ec2 describe-byoip-cidrs --max-results 5
```

要从您的地址池创建弹性 IP 地址，请使用 `allocate-address` 命令。您可以使用 `--public-ipv4-pool` 选项指定 `describe-byoip-cidrs` 返回的地址池的 ID。或者，您可以使用 `--address` 选项从您预置的地址范围中指定一个地址。

通过 AWS 公布地址范围

预配置地址范围后，即可对其进行公布。您必须公布预配置的确切地址范围。您不能只公布预配置的地址范围的一部分。

在通过 AWS 对地址范围进行发布之前，我们建议您停止从其他位置公布它。如果您一直从其他位置公布 IP 地址范围，我们将无法可靠地为其提供支持或解决问题。具体来说，我们无法保证到地址范围的流量将进入我们的网络。

为最大限度地减少停机时间，您可以在公布之前将 AWS 资源配置为使用地址池中的某一地址，然后停止从当前位置公布该地址并同时开始通过 AWS 公布该地址。有关从地址池分配弹性 IP 地址的更多信息，请参阅[分配弹性 IP 地址 \(p. 591\)](#)。

要公布地址范围，请使用以下 `advertise-byoip-cidr` 命令。

```
aws ec2 advertise-byoip-cidr --cidr address-range
```

Important

您最多只能每 10 秒运行一次 `advertise-byoip-cidr` 命令，即使每次指定不同的地址范围也是如此。

要停止公布地址范围，请使用以下 `withdraw-byoip-cidr` 命令。

```
aws ec2 withdraw-byoip-cidr --cidr address-range
```

Important

您最多只能每 10 秒运行一次 withdraw-byoip-cidr 命令，即使每次指定不同的地址范围也是如此。

取消预配置地址范围

要停止将地址范围用于 AWS，您可以释放仍从地址池中分配的任何弹性 IP 地址，停止公布该地址范围，然后取消预置该地址范围。

要释放每个弹性 IP 地址，请使用以下 [release-address](#) 命令。

```
aws ec2 release-address --allocation-id eipalloc-12345678
```

要停止公布地址范围，请使用以下 [withdraw-byoip-cidr](#) 命令。

```
aws ec2 withdraw-byoip-cidr --cidr address-range
```

要取消预置地址范围，请使用以下 [deprovision-byoip-cidr](#) 命令。

```
aws ec2 deprovision-byoip-cidr --cidr address-range
```

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。

目录

- [弹性 IP 地址基础信息 \(p. 590\)](#)
- [使用弹性 IP 地址 \(p. 591\)](#)
- [将反向 DNS 用于电子邮件应用程序 \(p. 595\)](#)
- [弹性 IP 地址限额 \(p. 595\)](#)

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。您不能重用公有 IPv4 地址，并且不能将公有 IPv4 地址转换为弹性 IP 地址。有关更多信息，请参阅[公有 IPv4 地址和外部 DNS 主机名 \(p. 575\)](#)。
- 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。即使您取消关联实例的弹性 IP 地址并将其与另一个实例重新关联，与实例的任何开放连接仍会在一段时间内有效。我们建议您使用重新关联的弹性 IP 地址重新建立这些连接。

- 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附加的网络接口关联，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。
- 从已引入到您 AWS 账户的 IP 地址池分配弹性 IP 地址时，该地址不会计入弹性 IP 地址限制。

使用弹性 IP 地址

以下部分介绍如何使用弹性 IP 地址。

任务

- [分配弹性 IP 地址 \(p. 591\)](#)
- [描述您的弹性 IP 地址 \(p. 592\)](#)
- [标记弹性 IP 地址 \(p. 592\)](#)
- [将弹性 IP 地址与正在运行的实例关联起来 \(p. 593\)](#)
- [取消关联弹性 IP 地址，并将它与其他实例重新关联 \(p. 593\)](#)
- [释放弹性 IP 地址 \(p. 594\)](#)
- [恢复弹性 IP 地址 \(p. 594\)](#)

分配弹性 IP 地址

您可以从 Amazon 的公有 IPv4 地址池分配弹性 IP 地址，也可以从已引入到您 AWS 账户的自定义 IP 地址池分配该地址。有关将您自己的 IP 地址范围引入到您 AWS 账户的更多信息，请参阅 [自带 IP 地址 \(BYOIP\) \(p. 587\)](#)。

您可以使用 Amazon EC2 控制台或命令行分配弹性 IP 地址。

使用控制台从 Amazon 的公有 IPv4 地址池分配弹性 IP 地址

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Elastic IPs。
- 选择 Allocate new address。
- 对于 IPv4 address pool (IPv4 地址池)，选择 Amazon pool (Amazon 池)。
- 选择 Allocate (分配)，然后关闭确认屏幕。

使用控制台从您自己的 IP 地址池分配弹性 IP 地址

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Elastic IPs。
- 选择 Allocate new address。
- 对于 IPv4 address pool (IPv4 地址池)，选择 Owned by me (我拥有的)，然后选择 IP 地址池。

要查看所选地址池的 IP 地址范围及已从该地址池分配的 IP 地址的数量，请查看 [Address ranges \(地址范围\)](#)。

5. 对于 IPv4 address (IPv4 地址)，执行以下操作之一：
 - 要让 Amazon EC2 从地址池选择 IP 地址，请选择 No preference (无首选项)。
 - 要从地址池中选择特定的 IP 地址，请选择 Select an address (选择一个地址)，然后键入该 IP 地址。
6. 选择 Allocate (分配)，然后关闭确认屏幕。

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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

标记弹性 IP 地址

可以为您的弹性 IP 地址分配自定义标签，以不同的方式对它们分类，例如按用途、所有者或环境。这有助于您根据所分配的自定义标签快速查找特定弹性 IP 地址。

Note

不支持使用弹性 IP 地址标签跟踪成本分配。

使用控制台标记弹性 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. 选择要标记的弹性 IP 地址，然后选择标签。
4. 选择 Add/Edit Tags。
5. 在添加/编辑标签对话框中，选择创建标签，然后指定该标签的键和值。
6. (可选) 选择创建标签，为弹性 IP 地址添加额外的标签。
7. 选择 Save。

使用命令行标记弹性 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 \(p. 3\)](#)。

- [create-tags](#) (AWS CLI)

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

- [New-EC2Tag](#) (适用于 Windows PowerShell 的 AWS 工具)

New-EC2Tag 命令需要 Tag 参数，来指定弹性 IP 地址标签要使用的键值对。以下命令创建 Tag 参数：

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

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。

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. 选择弹性 IP 地址，然后选择 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)

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)。

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)

恢复弹性 IP 地址

如果您已释放您的弹性 IP 地址，则可能能够恢复它。以下规则适用：

- 如果弹性 IP 地址已分配至其他 AWS 账户，或者该地址将导致您超出弹性 IP 地址限制，则您无法恢复该地址。
- 您不能恢复与弹性 IP 地址关联的标签。
- 您只能使用 Amazon EC2 API 或命令行工具恢复弹性 IP 地址。

使用命令行恢复弹性 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) — 使用 --address 参数按如下方式指定 IP 地址。

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

- [New-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具) — 使用 -Address 参数按如下方式指定 IP 地址。

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

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 Internet 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几率。

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

默认情况下，所有 AWS 账户在每个区域最多可拥有五 (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，则可请求提高限制。要请求提高限制，请完成 [Amazon VPC 限制申请表](#)（选择 VPC Elastic IP Address Limit (VPC 弹性 IP 地址限制)）。描述您的使用案例，让我们能够了解您的需求。要请求 EC2-Classic 的弹性 IP 地址，请完成 [Amazon EC2 的弹性 IP 地址](#)限制申请表。

弹性网络接口

弹性网络接口（在本文档中称为网络接口）是 VPC 中的一个逻辑网络组件，代表虚拟网卡。

网络接口可以包含以下属性：

- 您的 VPC 的 IPv4 地址范围内的一个主要私有 IPv4 地址
- 您的 VPC 的 IPv4 地址范围内的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

您可以在自己的账户中创建并配置网络接口，并将其连接到您的 VPC 中的实例。您的账户也可能具有请求者托管的网络接口，这些网络接口是由 AWS 服务创建和管理的，让您可以使用其他资源和服务。您自己无法管理这些网络接口。有关更多信息，请参阅[请求者托管的网络接口 \(p. 615\)](#)。

所有网络接口都具有以 eni- 开头的资源标识符。

Important

术语“弹性网络接口”有时简写为“ENI”。这不同于弹性网络适配器 (ENA)，后者是在某些实例类型上优化网络性能的自定义接口。有关更多信息，请参阅[Linux 上的增强联网 \(p. 616\)](#)。

目录

- 网络接口基本知识 (p. 596)
- 每个实例类型的每个网络接口的 IP 地址 (p. 596)
- 网络接口的使用场景 (p. 605)
- 网络接口最佳配置实践 (p. 606)
- 使用网络接口 (p. 608)
- 请求者托管的网络接口 (p. 615)

网络接口基本知识

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。

您也可以修改网络接口的属性，包括更改其安全组和管理其 IP 地址。

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。您可以创建并附加额外的网络接口。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 \(p. 596\)](#)。

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 \(p. 575\)](#)。

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 \(p. 576\)](#)。

监控 IP 流量

您可以在网络接口上启用 VPC 流日志以捕获有关出入该网络接口的 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](#)。

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 \(p. 580\)](#)。有关 VPC 中的 IPv6 的更多信息，请参阅Amazon VPC 用户指南中的[您的 VPC 中的 IP 寻址](#)。

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
a1.medium	2	4	4
a1.large	3	10	10
a1.xlarge	4	15	15
a1.2xlarge	4	15	15
a1.4xlarge	8	30	30
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
c5.large	3	10	10
c5.xlarge	4	15	15
c5.2xlarge	4	15	15
c5.4xlarge	8	30	30
c5.9xlarge	8	30	30
c5.12xlarge	8	30	30
c5.18xlarge	15	50	50
c5.24xlarge	15	50	50
c5.metal	15	50	50
c5d.large	3	10	10
c5d.xlarge	4	15	15
c5d.2xlarge	4	15	15
c5d.4xlarge	8	30	30
c5d.9xlarge	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
c5d.12xlarge	8	30	30
c5d.18xlarge	15	50	50
c5d.24xlarge	15	50	50
c5d.metal	15	50	50
c5n.large	3	10	10
c5n.xlarge	4	15	15
c5n.2xlarge	4	15	15
c5n.4xlarge	8	30	30
c5n.9xlarge	8	30	30
c5n.18xlarge	15	50	50
c5n.metal	15	50	50
cc2.8xlarge	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
f1.2xlarge	4	15	15
f1.4xlarge	8	30	30
f1.16xlarge	8	50	50
g2.2xlarge	4	15	不支持 IPv6
g2.8xlarge	8	30	不支持 IPv6
g3s.xlarge	4	15	15
g3.4xlarge	8	30	30
g3.8xlarge	8	30	30
g3.16xlarge	15	50	50
g4dn.xlarge	3	10	10
g4dn.2xlarge	3	10	10
g4dn.4xlarge	3	10	10
g4dn.8xlarge	4	15	15
g4dn.12xlarge	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
g4dn.16xlarge	15	50	50
h1.2xlarge	4	15	15
h1.4xlarge	8	30	30
h1.8xlarge	8	30	30
h1.16xlarge	15	50	50
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
i3.16xlarge	15	50	50
i3.metal	15	50	50
i3en.large	3	10	10
i3en.xlarge	4	15	15
i3en.2xlarge	4	15	15
i3en.3xlarge	4	15	15
i3en.6xlarge	8	30	30
i3en.12xlarge	8	30	30
i3en.24xlarge	15	50	50
i3en.metal	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

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
m2.4xlarge	8	30	不支持 IPv6
m3.medium	2	6	不支持 IPv6
m3.large	3	10	不支持 IPv6
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
m5.large	3	10	10
m5.xlarge	4	15	15
m5.2xlarge	4	15	15
m5.4xlarge	8	30	30
m5.8xlarge	8	30	30
m5.12xlarge	8	30	30
m5.16xlarge	15	50	50
m5.24xlarge	15	50	50
m5.metal	15	50	50
m5a.large	3	10	10
m5a.xlarge	4	15	15
m5a.2xlarge	4	15	15
m5a.4xlarge	8	30	30
m5a.8xlarge	8	30	30
m5a.12xlarge	8	30	30
m5a.16xlarge	15	50	50
m5a.24xlarge	15	50	50
m5ad.large	3	10	10
m5ad.xlarge	4	15	15
m5ad.2xlarge	4	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
m5ad.4xlarge	8	30	30
m5ad.8xlarge	8	30	30
m5ad.12xlarge	8	30	30
m5ad.16xlarge	15	50	50
m5ad.24xlarge	15	50	50
m5d.large	3	10	10
m5d.xlarge	4	15	15
m5d.2xlarge	4	15	15
m5d.4xlarge	8	30	30
m5d.8xlarge	8	30	30
m5d.12xlarge	8	30	30
m5d.16xlarge	15	50	50
m5d.24xlarge	15	50	50
m5d.metal	15	50	50
m5dn.large	3	10	10
m5dn.xlarge	4	15	15
m5dn.2xlarge	4	15	15
m5dn.4xlarge	8	30	30
m5dn.8xlarge	8	30	30
m5dn.12xlarge	8	30	30
m5dn.16xlarge	15	50	50
m5dn.24xlarge	15	50	50
m5n.large	3	10	10
m5n.xlarge	4	15	15
m5n.2xlarge	4	15	15
m5n.4xlarge	8	30	30
m5n.8xlarge	8	30	30
m5n.12xlarge	8	30	30
m5n.16xlarge	15	50	50
m5n.24xlarge	15	50	50
p2.xlarge	4	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
p2.8xlarge	8	30	30
p2.16xlarge	8	30	30
p3.2xlarge	4	15	15
p3.8xlarge	8	30	30
p3.16xlarge	8	30	30
p3dn.24xlarge	15	50	50
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
r5.large	3	10	10
r5.xlarge	4	15	15
r5.2xlarge	4	15	15
r5.4xlarge	8	30	30
r5.8xlarge	8	30	30
r5.12xlarge	8	30	30
r5.16xlarge	15	50	50
r5.24xlarge	15	50	50
r5.metal	15	50	50
r5a.large	3	10	10
r5a.xlarge	4	15	15
r5a.2xlarge	4	15	15
r5a.4xlarge	8	30	30
r5a.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
r5a.12xlarge	8	30	30
r5a.16xlarge	15	50	50
r5a.24xlarge	15	50	50
r5ad.large	3	10	10
r5ad.xlarge	4	15	15
r5ad.2xlarge	4	15	15
r5ad.4xlarge	8	30	30
r5ad.8xlarge	8	30	30
r5ad.12xlarge	8	30	30
r5ad.16xlarge	15	50	50
r5ad.24xlarge	15	50	50
r5d.large	3	10	10
r5d.xlarge	4	15	15
r5d.2xlarge	4	15	15
r5d.4xlarge	8	30	30
r5d.8xlarge	8	30	30
r5d.12xlarge	8	30	30
r5d.16xlarge	15	50	50
r5d.24xlarge	15	50	50
r5d.metal	15	50	50
r5dn.large	3	10	10
r5dn.xlarge	4	15	15
r5dn.2xlarge	4	15	15
r5dn.4xlarge	8	30	30
r5dn.8xlarge	8	30	30
r5dn.12xlarge	8	30	30
r5dn.16xlarge	15	50	50
r5dn.24xlarge	15	50	50
r5n.large	3	10	10
r5n.xlarge	4	15	15
r5n.2xlarge	4	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
r5n.4xlarge	8	30	30
r5n.8xlarge	8	30	30
r5n.12xlarge	8	30	30
r5n.16xlarge	15	50	50
r5n.24xlarge	15	50	50
t1.micro	2	2	不支持 IPv6
t2.nano	2	2	2
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
t2.large	3	12	12
t2.xlarge	3	15	15
t2.2xlarge	3	15	15
t3.nano	2	2	2
t3.micro	2	2	2
t3.small	3	4	4
t3.medium	3	6	6
t3.large	3	12	12
t3.xlarge	4	15	15
t3.2xlarge	4	15	15
t3a.nano	2	2	2
t3a.micro	2	2	2
t3a.small	2	4	4
t3a.medium	3	6	6
t3a.large	3	12	12
t3a.xlarge	4	15	15
t3a.2xlarge	4	15	15
u-6tb1.metal	5	30	30
u-9tb1.metal	5	30	30
u-12tb1.metal	5	30	30
u-18tb1.metal	15	50	50

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
u-24tb1.metal	15	50	50
x1.16xlarge	8	30	30
x1.32xlarge	8	30	30
x1e.xlarge	3	10	10
x1e.2xlarge	4	15	15
x1e.4xlarge	4	15	15
x1e.8xlarge	4	15	15
x1e.16xlarge	8	30	30
x1e.32xlarge	8	30	30
z1d.large	3	10	10
z1d.xlarge	4	15	15
z1d.2xlarge	4	15	15
z1d.3xlarge	8	30	30
z1d.6xlarge	8	30	30
z1d.12xlarge	15	50	50
z1d.metal	15	50	50

网络接口的使用场景

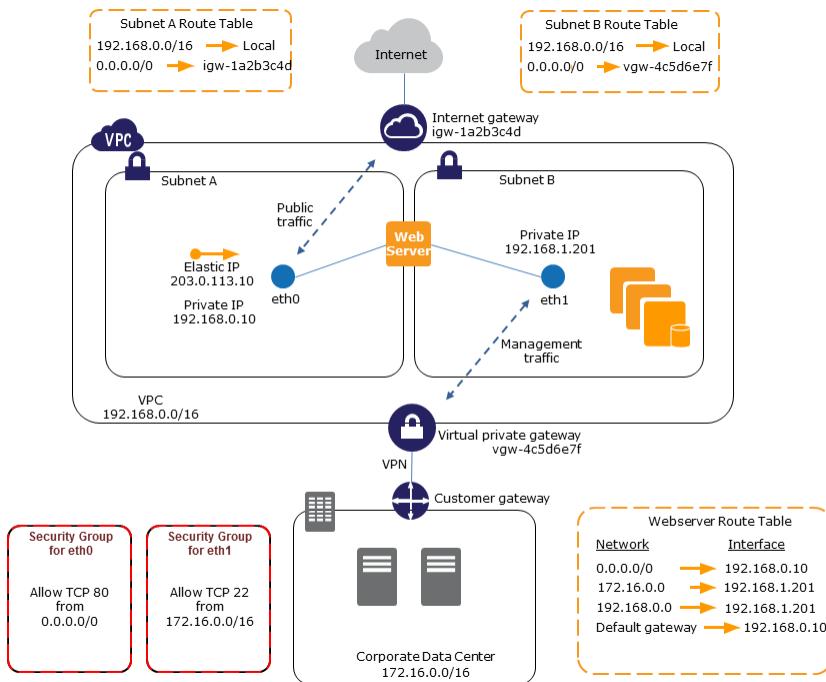
当您想执行以下操作时，将多个网络接口附加到一个实例很有帮助：

- 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。
- 创建一个低成本、高可用性解决方案。

创建一个管理网络

您可以使用网络接口创建管理网络。在此场景中，实例上的主网络接口 (eth0) 处理公有流量，辅助网络接口 (eth1) 处理后端管理流量，并连接到您的 VPC 中有较多限制性访问控制的单独子网。公有接口（无论是否处于负载均衡器之后）有一个关联的安全组来控制从 Internet 对服务器的访问（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），而私有接口的关联安全组只能控制来自 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。



在您的 VPC 中使用网络和安全性设备

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。您可以创建并附加辅助网络接口至 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/目标检查设置其他接口。

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，则其网络接口可附加到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（热附加）、实例停止时（暖附加）或实例启动时（冷附加）将网络接口连接到实例。
- 您可以在实例运行时或停止时分离次要网络接口。但是，您不能分离主网络接口（eth0）。
- 如果实例位于相同可用区和 VPC 但位于不同子网，您可以将网络接口从一个实例移动到另一个实例。
- 使用 CLI、API 或开发工具包启动实例时，您可以指定主网络接口（eth0）和附加网络接口。
- 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连接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附加或热附加，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附加到一个实例，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 \(p. 581\)](#)。

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*)

在网络接口附加、分离或重新附加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 *75-persistent-net-generator.rules* 的 *70-persistent-net.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 地址作为辅助地址添加至网络接口。

ec2ifup ethN

扩展标准 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

扩展标准 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。

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
```

要彻底禁用自动化，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 控制台或命令行使用网络接口。

目录

- [创建网络接口 \(p. 608\)](#)
- [删除网络接口 \(p. 609\)](#)
- [查看有关网络接口的详细信息 \(p. 609\)](#)
- [在启动实例时附加网络接口 \(p. 609\)](#)
- [将网络接口附加到已停止的实例或正在运行的实例 \(p. 610\)](#)
- [将网络接口与实例分离 \(p. 611\)](#)
- [更改安全组 \(p. 612\)](#)
- [更改源或目标检查 \(p. 612\)](#)
- [关联弹性 IP 地址 \(IPv4\) \(p. 612\)](#)
- [取消关联弹性 IP 地址 \(IPv4\) \(p. 613\)](#)
- [分配 IPv6 地址 \(p. 613\)](#)
- [取消分配 IPv6 地址 \(p. 614\)](#)
- [更改终止行为 \(p. 614\)](#)
- [添加或编辑描述 \(p. 614\)](#)
- [添加或编辑标签 \(p. 615\)](#)

创建网络接口

您可以在子网中创建一个网络接口。在创建网络接口之后，您不能将其移动至另一子网，而且您只能将该网络接口连接到同一可用区中的实例。

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。
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私有 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

要删除实例，您必须先分离网络接口。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。

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

您可以查看您账户中的所有网络接口。

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. 要查看详细信息，请选择详细信息。

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)

在启动实例时附加网络接口

启动实例时，您可以指定一个现有的网络接口或附加其他网络接口。

Note

如果在将网络接口附加到实例时发生错误，则会导致实例启动失效。

使用控制台在启动实例时附加网络接口

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。您可以附加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 \(p. 596\)](#)。

Note

如果您指定了多个网络接口，则无法给您的实例自动分配公有 IPv4 地址。

6. (仅限 IPv6) 如果您正在拥有关联的 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，无论您在此步骤中选择哪个选项，实例都将与该网络接口的安全组关联。

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附加网络接口

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)

将网络接口附加到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) 或 Network Interfaces (网络接口) 页面，将网络接口连接至您的 VPC 中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 \(p. 575\)](#)。

使用实例页面将网络接口附加到实例

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附加到实例

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附加到实例

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 Instances (实例) 或 Network Interfaces (网络接口) 页面来分离辅助网络接口。

使用实例页面将网络接口与实例分离

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分离

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。

Note

- 仅将强制分离选项用作从失败的实例分离网络接口的最后手段。
- 如果使用强制分离选项分离网络接口，则可能无法在未先停止并启动实例的情况下将其他网络接口附加到实例上的同一索引。
- 如果强制分离网络接口，则[实例元数据 \(p. 499\)](#)可能不会得到更新。这意味着与分离的网络接口关联的属性可能仍然可见。当您停止并启动实例时，实例元数据将得到更新。
- 您无法强制从 EC2-Classic 实例分离网络接口。

使用命令行分离网络接口

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 作为网络接口的子网。

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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

更改源或目标检查

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。

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。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 IPv6 地址。要让 AWS 为您选择一个地址，请保留自动分配值。

5. 选择是，请更新。

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. 选择是，请更新。

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

您可以设置附加到实例的网络接口的终止行为。您可以指定在终止网络接口附加到的实例时是否自动删除该接口。

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 [标记您的 Amazon EC2 资源 \(p. 940\)](#)。

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)

请求者托管的网络接口

请求者托管的网络接口是 AWS 服务在您的 VPC 中创建的网络接口。此网络接口可代表其他服务的实例（例如 Amazon RDS 实例），或者它可让您访问其他服务或资源（例如 AWS PrivateLink 服务）或 Amazon ECS 任务。

您无法修改或分离请求者托管的网络接口。如果您删除该网络接口代表的资源，AWS 服务会为您分离并删除该网络接口。要更改请求者托管的网络接口的安全组，您可能需要使用该服务的控制台或命令行工具。想要了解更多有关信息，请参阅 [服务文档](#)。

您可以为请求者托管的网络接口加标签。有关更多信息，请参阅 [添加或编辑标签 \(p. 615\)](#)。

您可以查看自己账户中的请求者托管的网络接口。

使用控制台查看请求者托管的网络接口

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. 选择网络接口并在详细信息窗格中查看以下信息：

- Attachment owner (连接所有者)：如果该网络接口是您创建的，该字段会显示您的 AWS 账户 ID。否则，它会显示创建该网络接口的委托人或服务的别名或 ID。
- 描述：提供有关网络接口的用途的信息，例如“VPC 终端节点接口”。

使用命令行查看请求者托管的网络接口

1. 使用 [describe-network-interfaces](#) AWS CLI 命令可以描述您的账户中的网络接口。

```
aws ec2 describe-network-interfaces
```

2. 如果该网络接口由其他 AWS 服务托管，则在输出中，RequesterManaged 字段会显示 true。

```
{
    "Status": "in-use",
    ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    "NetworkInterfaceId": "eni-c8fbc27e",
    "VpcId": "vpc-1a2b3c4d",
    "PrivateIpAddresses": [
        {
            "PrivateDnsName": "ip-10-0-2-227.ec2.internal",
            "Primary": true,
            "PrivateIpAddress": "10.0.2.227"
        }
    ],
    "RequesterManaged": true,
    ...
}
```

或者，使用 [Get-EC2NetworkInterface](#) Windows PowerShell 工具 命令。

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 \(p. 616\)](#)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 使用率。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。

目录

- [增强联网类型 \(p. 616\)](#)
- [在实例上启用增强联网 \(p. 617\)](#)
- [在 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 617\)](#)
- [在 Linux 实例上启用 Intel 82599 VF 接口增强联网 \(p. 628\)](#)
- [对 Elastic Network Adapter \(ENA\) 进行故障排除 \(p. 633\)](#)

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：

Elastic Network Adapter (ENA)

对于支持的实例类型，Elastic Network Adapter (ENA) 最多支持 100 Gbps 的网络速度。

A1, C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d 实例使用 Elastic Network Adapter 实现增强联网。

Intel 82599 虚拟功能 (VF) 接口

对于受支持的实例类型，Intel 82599 虚拟功能接口最多支持 10 Gbps 的网络速度。

C3、C4、D2、I2、M4 (m4.16xlarge 除外) 和 R3 实例使用 Intel 82599 VF 接口实现增强联网。

有关每个实例类型支持的网络速度的信息，请参阅 [Amazon EC2 实例类型](#)。

在实例上启用增强联网

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 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 617\)](#)中的步骤。

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 Linux 实例上启用 Intel 82599 VF 接口增强联网 \(p. 628\)](#)中的步骤。

在 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网

Amazon EC2 通过 Elastic Network Adapter (ENA) 提供增强联网功能。

目录

- [要求 \(p. 617\)](#)
- [测试是否启用了增强联网功能 \(p. 618\)](#)
- [在 Amazon Linux AMI 上启用增强联网 \(p. 619\)](#)
- [在 Ubuntu 上启用增强联网 \(p. 620\)](#)
- [在 Linux 上启用增强联网 \(p. 621\)](#)
- [利用 DKMS 在 Ubuntu 上启用增强联网 \(p. 623\)](#)
- [故障排除 \(p. 625\)](#)
- [操作系统优化 \(p. 625\)](#)

要求

要使用 ENA 准备增强联网，请按如下方式设置您的实例：

- 从以下支持的实例类型中选择：A1, C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d。
- 使用支持的 Linux 内核版本及支持的发行版启动实例，以便为实例自动启用 ENA 增强联网。有关更多信息，请参阅 [ENA Linux 内核驱动程序发行说明](#)。
- 确保实例具有 Internet 连接。
- 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无法访问操作系统。如果您有最新备份，则发生此情况时仍将保留数据。

测试是否启用了增强联网功能

若要测试是否已启用了增强联网，请确认实例上已安装 ena 模块且设置了 enaSupport 属性。如果实例满足这两个条件，则 ethtool -i eth_n 命令应显示该模块已在网络接口上使用。

内核模块 (ena)

要确认已安装 ena 模块，请使用 modinfo 命令，如以下示例中所示。

```
[ec2-user ~]$ modinfo ena
filename:      /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:       1.5.0g
license:        GPL
description:   Elastic Network Adapter (ENA)
author:         Amazon.com, Inc. or its affiliates
srcversion:    692C7C68B8A9001CB3F31D0
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:
retpoline:     Y
intree:         Y
name:          ena
...
```

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 上启用增强联网 \(p. 620\)](#)。

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-ids 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

使用以下命令验证是否在特定接口上使用了 ena 模块 (替代要检查的接口名称)。如果您使用单个接口 (默认设置)，则它是 eth0。如果操作系统支持[可预测的网络名称 \(p. 622\)](#)，这可以是 ens5 等名称。

在以下示例中，ena 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0
driver: 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
```

在此示例中，ena 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。

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

在 Amazon Linux AMI 上启用增强联网

Amazon Linux 2 和最新版本的 Amazon Linux AMI 安装有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 HVM 版本的 Amazon Linux 在支持的实例类型上启动实例，则已为您的实例启用增强联网。有关更多信息，请参阅 [测试是否启用了增强联网功能 \(p. 618\)](#)。

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。

在 Amazon Linux AMI 上启用增强联网

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启实例：[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[测试是否启用了增强联网功能 \(p. 618\)](#)中的 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. [由 EBS 支持的实例] 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。

[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：[在 Amazon Linux AMI 上启用增强联网 \(实例存储支持的实例\) \(p. 620\)](#)。

6. 使用以下任一命令从本地计算机启用增强联网属性：

- [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 \(p. 102\)](#)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。
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[测试是否启用了增强联网功能 \(p. 618\)](#)中的 `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 \(p. 633\)](#)。

在 Amazon Linux AMI 上启用增强联网 (实例存储支持的实例)

按照上述过程操作，直到您停止实例的步骤。按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- [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 上启用增强联网

最新的 Ubuntu 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 Ubuntu HVM AMI 在支持的实例类型上启动实例，则已为您的实例启用增强联网。有关更多信息，请参阅[测试是否启用了增强联网功能 \(p. 618\)](#)。

如果您使用较旧的 AMI 启动了实例，并且实例尚未启用增强联网，则可以安装 `linux-aws` 内核程序包以获取最新的增强联网功能驱动程序并更新所需的属性。

安装 `linux-aws` 内核程序包 (Ubuntu 16.04 或更高版本)

Ubuntu 16.04 和 18.04 随附 Ubuntu 自定义内核 (`linux-aws` 内核程序包)。要使用不同的内核，请联系 [AWS Support](#)。

安装 linux-aws 内核程序包 (Ubuntu Trusty 14.04)

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 linux-aws
```

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. [由 EBS 支持的实例] 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。
[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：[在 Ubuntu 上启用增强联网 \(由实例存储支持的实例\) \(p. 621\)](#)。
4. 使用以下任一命令从本地计算机启用增强联网属性：
 - [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
```

5. (可选) 从实例创建 AMI，如[创建 Amazon EBS 支持的 Linux AMI \(p. 102\)](#)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。
6. 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。

在 Ubuntu 上启用增强联网 (由实例存储支持的实例)

按照上述过程操作，直到您停止实例的步骤。按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- [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 Linux 上启用增强联网

下面的过程提供了在 Amazon Linux AMI 或 Ubuntu 之外的 Linux 发行版（如 SUSE Linux Enterprise Server (SLES)、Red Hat Enterprise Linux 或 CentOS）上启用增强联网的一般步骤。在开始之前，请参阅[测试是否启用了增强联网功能 \(p. 618\)](#)以检查是否已对您的实例启用增强联网。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 发行版的特定文档。

对 Linux 启用增强联网

1. 连接到您的实例。
2. 从位于以下网址的 GitHub 克隆您实例上的 ena 模块的源代码：<https://github.com/amzn/amzn-drivers>。（SUSE SLES 12 SP2 及更高版本默认情况下包括 ENA 2.02，因此，您无需下载和编译 ENA 驱动程序。对于 SLES 12 SP2 及更高版本，您应提出请求以将希望的驱动程序版本添加到备用内核）。

```
git clone https://github.com/amzn/amzn-drivers
```

3. 在实例上编译并安装 ena 模块。
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。例如，如果您的发行版支持 dracut，则可使用以下命令。

```
dracut -f -v
```

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。

```
rpm -qa | grep -e '^systemd-[0-9]\+\| ^udev-[0-9]\+'  
systemd-208-11.el7_0.2.x86_64
```

在以上 Red Hat Enterprise Linux 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 中的 /etc/default/grub 行，可禁用可预测的网络接口名称。

```
sudo sed -i '/^GRUB_CMDLINE_LINUX/s/$/\ net.ifnames=0/' /etc/default/grub
```

- c. 重新构建 grub 配置文件。

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [由 EBS 支持的实例] 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。

[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：[在 Linux 上启用增强联网（-由实例存储支持的实例）\(p. 623\)](#)。

8. 使用以下任一命令从本地计算机启用增强联网 enaSupport 属性：

- [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 \(p. 102\)](#) 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，则必须在创建 AMI 之前将其删除。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 \(p. 633\)](#)。

在 Linux 上启用增强联网 (-由实例存储支持的实例)

按照上述过程操作，直到您停止实例的步骤。按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Register-EC2Image -EnaSupport ...
```

利用 DKMS 在 Ubuntu 上启用增强联网

此方法仅用于测试和反馈目的。它不供生产部署使用。有关生产部署，请参阅[在 Ubuntu 上启用增强联网 \(p. 620\)](#)。

Important

使用 DKMS 可避免您的订阅的支持协议。使用 kmod 配置是运行最新可用的内核模块的可接受替代方案。

在 Ubuntu 上启用 ENA 增强联网 (EBS 支持的实例)

1. 按照[在 Ubuntu 上启用增强联网 \(p. 620\)](#)中的步骤 1 和 2 操作。
2. 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
```

3. 从位于以下网址的 GitHub 克隆您实例上的 `ena` 模块的源代码：<https://github.com/amzn/amzn-drivers>。

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

4. 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
```

5. 使用以下值创建 DKMS 配置文件 (替代您的 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"
```

6. 使用 DKMS 在实例上添加、构建和安装 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 命令构建该模块。

```
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
```

7. 重新构建 initramfs , 以便在启动时加载正确的模块。

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. 使用 [测试是否启用了增强联网功能 \(p. 618\)](#) 中的 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:    9693C876C54CA64AE48FOCA
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)
```

- 继续执行在 [Ubuntu 上启用增强联网 \(p. 620\)](#) 中的步骤 3。

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 \(p. 633\)](#)。

操作系统优化

若要在具有增强联网的实例上实现最高网络性能，您可能需要修改默认操作系统配置。对于需要高网络性能的应用程序，我们建议进行以下配置更改。

除了这些操作系统优化之外，您还应考虑网络流量的最大传输单位 (MTU)，并根据您的工作负载和网络架构相应调整。有关更多信息，请参阅 [EC2 实例的网络最大传输单位 \(MTU\) \(p. 669\)](#)。

AWS 定期测量在集群置放群组中启动的实例之间的平均往返延迟，在 99.9% 的情况下该值为 50us，尾延迟为 200us。如果您的应用程序需要稳定的低延迟，建议在基于 Nitro 的固定性能实例上，使用最新版本的 ENA 驱动程序。

这些过程针对 Amazon Linux 2 和 Amazon Linux AMI 编写。不过，它们也适用于搭载内核版本 3.9 及更高版本的其他 Linux 发行版。有关更多信息，请参阅系统特定的文档。

针对增强联网优化 Amazon Linux 实例

- 检查实例的时钟源：

```
cat /sys/devices/system/clocksource/clocksource0/current_clocksource
```

- 如果时钟源为 xen，请完成以下子步骤。否则，请跳至 [Step 3 \(p. 626\)](#)。

- 编辑 GRUB 配置并将 xen_nopvspin=1 和 clocksource=tsc 添加到内核引导选项。

- 对于 Amazon Linux 2，编辑 /etc/default/grub 文件并将这些选项添加到 GRUB_CMDLINE_LINUX_DEFAULT 行，如下所示：

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
biosdevname=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1 clocksource=tsc"
GRUB_TIMEOUT=0
```

- 对于 Amazon Linux AMI，编辑 /boot/grub/grub.conf 文件并将这些选项添加到 kernel 行，如下所示：

```
kernel /boot/vmlinuz-4.14.62-65.117.amzn1.x86_64 root=LABEL=/ console=tty1
console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1
clocksource=tsc
```

- (仅限 Amazon Linux 2) 重新生成 GRUB 配置文件以应用这些更改：

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

3. 如果 [您的 EC2 实例的处理器状态控制 \(p. 471\)](#) 上将您的实例类型列出为支持的实例类型，请防止系统使用深层 C 状态，以确保低延迟的系统性能。有关更多信息，请参阅[通过限制深层 C 状态实现高性能和低延迟 \(p. 473\)](#)。

- a. 编辑 GRUB 配置并将 `intel_idle.max_cstate=1` 添加到内核引导选项。

- 对于 Amazon Linux 2，编辑 `/etc/default/grub` 文件并将此选项添加到 `GRUB_CMDLINE_LINUX_DEFAULT` 行，如下所示：

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1
clocksource=tsc intel_idle.max_cstate=1
GRUB_TIMEOUT=0
```

- 对于 Amazon Linux AMI，编辑 `/boot/grub/grub.conf` 文件并将此选项添加到 `kernel` 行，如下所示：

```
kernel /boot/vmlinuz-4.14.62-65.117.amzn1.x86_64 root=LABEL=/ console=tty1
console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1
clocksource=tsc intel_idle.max_cstate=1
```

- b. (仅限 Amazon Linux 2) 重新生成 GRUB 配置文件以应用这些更改：

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. 确保您预留的内核内存充足，可以保持高速率的数据包缓冲区分配（默认值可能会太小）。

- 使用您选择的编辑器（以 `root` 身份或者使用 `sudo`）打开 `/etc/sysctl.conf` 文件。
- 将具有适合您实例类型的预留内核内存值（以 KB 为单位）的 `vm.min_free_kbytes` 行添加到文件。根据经验，您应将此值设置为可用系统内存的 1-3% 之间，并上调或下调此值以满足应用程序需求。

```
vm.min_free_kbytes = 1048576
```

- c. 使用下面的命令应用此配置：

```
sudo sysctl -p
```

- d. 通过以下命令验证设置已应用：

```
sudo sysctl -a 2>&1 | grep min_free_kbytes
```

5. 重启实例以加载新配置：

```
sudo reboot
```

6. (可选) 手动分发数据包接收中断，使其与属于相同 NUMA 节点的不同 CPU 关联。但是，请谨慎使用此项，因为全局禁用了 irqbalancer。

Note

此步骤中的配置更改在重启之后不保留。

- a. 创建一个名为 `smp_affinity.sh` 的文件，并将以下代码块粘贴到该文件中：

```
#!/bin/sh
service irqbalance stop
affinity_values=(00000001 00000002 00000004 00000008 00000010 00000020 00000040
00000080)
```

```
irqs=$(grep eth /proc/interrupts|awk '{print $1}'|cut -d : -f 1))
irqLen=${#irqs[@]}
for (( i=0; i<${irqLen}; i++ )); do
    echo $(printf "0000,0000000,0000000,0000000,${affinity_values[$i]}") > /proc/
irq/${irqs[$i]}/smp_affinity;
    echo "IRQ ${irqs[$i]} =" $(cat /proc/irq/${irqs[$i]}/smp_affinity);
done
```

- b. 使用以下命令运行脚本：

```
sudo bash ./smp_affinity.sh
```

7. (可选) 如果处理接收 IRQ 的 vCPU 过载，或者您的应用程序网络处理需要较高的 CPU 能力，您可以通过接收数据包转向 (RPS)，将部分网络处理分载到其他核心。确保用于 RPS 的核心属于同一个 NUMA 节点，以避免 NUMA 节点间锁定。例如，要将核心 8-15 用于数据包处理，请使用以下命令。

Note

此步骤中的配置更改在重启之后不保留。

```
for i in `seq 0 7`; do echo $(printf "0000,0000000,0000000,0000000,0000ff00") | sudo
tee /sys/class/net/eth0/queues/rx-$i/rps_cpus; done
```

8. (可选) 如果可能，请在相同 NUMA 节点上执行所有处理。

- a. 安装 numactl：

```
sudo yum install -y numactl
```

- b. 当您运行网络处理程序时，请将其绑定到单个 NUMA 节点。例如，以下命令将 shell 脚本 run.sh 绑定到 NUMA 节点 0：

```
numactl --cpunodebind=0 --membind=0 run.sh
```

- c. 如果您启用了超线程，则可以配置应用程序在每个 CPU 核心中仅使用单个硬件线程。

- 使用 lscpu 命令可以查看映射到 NUMA 节点的 CPU 核心：

```
lscpu | grep NUMA
```

输出：

```
NUMA node(s):      2
NUMA node0 CPU(s): 0-15,32-47
NUMA node1 CPU(s): 16-31,48-63
```

- 您可以使用以下命令，查看哪些硬件线程属于某个物理 CPU：

```
cat /sys/devices/system/cpu/cpu0/topology/thread_siblings_list
```

输出：

```
0,32
```

在此示例中，线程 0 和 32 映射到 CPU 0。

- 若要避免在线程 32-47 (实际上是与线程 0-15 在同一个 CPU 上的硬件线程) 上运行，请使用以下命令：

```
numactl --physcpubind=+0-15 --membind=0 ./run.sh
```

- 为不同流量类使用多个弹性网络接口。例如，如果您运行使用后端数据库的 Web 服务器，请为 Web 服务器前端使用一个弹性网络接口，为数据库连接使用另一个弹性网络接口。

在 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 接口提供增强联网功能。

目录

- [要求 \(p. 628\)](#)
- [测试是否启用了增强联网功能 \(p. 628\)](#)
- [在 Amazon Linux 上启用增强联网 \(p. 630\)](#)
- [在 Ubuntu 上启用增强联网 \(p. 631\)](#)
- [在其他 Linux 发行版上启用增强联网 \(p. 631\)](#)
- [排除连接问题 \(p. 633\)](#)

要求

要使用 Intel 82599 VF 接口准备增强联网，请按如下方式设置您的实例：

- 从以下支持的实例类型中选择：C3、C4、D2、I2、M4（不包括 m4.16xlarge）和 R3。
- 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 Amazon EBSHVM AMI 启动由 – 提供支持且支持增强联网的实例—Amazon Linux，则已为您的实例启用增强联网。

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。

- 确保实例具有 Internet 连接。
- 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无法访问操作系统。如果您有最新备份，则发生此情况时仍将保留数据。

测试是否启用了增强联网功能

如果已在您的实例上安装 ixgbevf 模块且设置了 sriovNetSupport 属性，请启用 Intel 82599 VF 接口增强联网。

实例属性 (sriovNetSupport)

要检查实例是否设置了增强联网 sriovNetSupport 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 sriovNetSupport
```

- [Get-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

如果未设置此属性，则 SriovNetSupport 为空。如果设置了此属性，则值很简单，如以下示例输出所示。

```
"SriovNetSupport": {  
    "Value": "simple"  
},
```

映像属性 (sriovNetSupport)

要检查 AMI 是否设置了增强联网 sriovNetSupport 属性，请使用以下任一命令：

- [describe-images](#) (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

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

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

如果未设置此属性，则 SriovNetSupport 为空。如果设置了此属性，则值很简单。

网络接口驱动程序

使用以下命令验证是否在特定接口上使用了该模块（替代要检查的接口名称）。如果您使用单个接口（默认设置），则为 eth0。如果操作系统支持[可预测的网络名称 \(p. 632\)](#)，这可以是 ens5 等名称。

在以下示例中，ixgbevf 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0  
driver: 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
```

在此示例中，已加载 ixgbevf 模块。此实例正确配置了增强联网。

```
[ec2-user ~]$ ethtool -i eth0  
driver: ixgbevf  
version: 4.0.3  
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 Amazon Linux 上启用增强联网

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，如果使用最新的 Amazon Linux HVM AMI 启动实例类型，则已为您的实例启用增强联网。有关更多信息，请参阅 [测试是否启用了增强联网功能 \(p. 628\)](#)。

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。

Warning

增强联网属性启用之后将无法禁用。

启用增强联网

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启实例：[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[测试是否启用了增强联网功能 \(p. 628\)](#)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. [由 EBS 支持的实例] 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。

[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：[启用增强联网 \(由实例存储支持的实例\) \(p. 631\)](#)。

6. 使用以下任一命令从本地计算机启用增强联网属性：
 - [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 \(p. 102\)](#) 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[测试是否启用了增强联网功能 \(p. 628\)](#)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 (由实例存储支持的实例)

按照上述过程操作，直到您停止实例的步骤。按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --srivnet-support simple ...
```

- [Register-EC2Image \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

在 Ubuntu 上启用增强联网

在开始之前，在您的实例上[检查是否已启用增强联网 \(p. 628\)](#)。

Quick Start Ubuntu HVM AMI 包含实现增强联网所需的驱动程序。如果您的 ixgbevf 版本早于 2.16.4，则可以安装 linux-aws 内核程序包以获取最新增强的联网功能驱动程序。

以下过程提供了在 Ubuntu 实例上编译 ixgbevf 模块的一般步骤。

安装 linux-aws 内核程序包

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 linux-aws
```

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。

在其他 Linux 发行版上启用增强联网

在开始之前，在您的实例上[检查是否已启用增强联网 \(p. 628\)](#)。最新 Quick Start HVM AMI 包含实现增强联网所需的驱动程序，因此您无需执行其他步骤。

下面的过程提供了在 Amazon Linux 或 Ubuntu 之外的 Linux 发行版上启用 Intel 82599 VF 接口增强联网所需的一般步骤。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 发行版的特定文档。

对 Linux 启用增强联网

1. 连接到您的实例。
2. 从 Sourceforge 上的 [ixgbevf](https://sourceforge.net/projects/e1000/files/%20stable/) 源代码。
[位置在实例上下载 ixgbevf 模块的源代码。](#)
3. 在实例上编译并安装 ixgbevf 模块。

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新构建驱动程序，则系统会在下次重新启动时恢复为特定于发行版的 ixgbevf 模块。这可能会在特定于发行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 Enterprise Linux 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 中的 /etc/default/grub 行，可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. [由 EBS 支持的实例] 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。

[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：[启用增强联网 \(由实例存储支持的实例-\)](#) (p. 633)。

8. 使用以下任一命令从本地计算机启用增强联网属性：

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --srivnet-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 \(p. 102\)](#) 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，则必须在创建 AMI 之前将其删除。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 (由实例存储支持的实例-)

按照上述过程操作，直到您停止实例的步骤。按照[创建由实例存储支持的 Linux AMI \(p. 105\)](#)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --srivnet-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。请尝试安装用于您的实例的 Linux 发行版所附带的 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。

有关更多信息，请参阅我如何在我的 EC2 实例上启用和配置增强联网功能？。

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 \(p. 633\)](#)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。

目录

- [排除连接问题 \(p. 633\)](#)
- [保持活动机制 \(p. 634\)](#)
- [注册表读取超时 \(p. 635\)](#)
- [统计数据 \(p. 635\)](#)
- [syslog 中的驱动程序错误日志 \(p. 637\)](#)

排除连接问题

如果您在启用增强联网时丢失连接，则 ena 模块可能与您的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 \(p. 634\)](#))。

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[ena 中的步骤尝试重新安装具有当前内核版本的在 Linux 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 617\)](#) 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 \(p. 105\)](#) 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

ENA 设备按固定速度 (通常每秒一次) 发布保持活动事件。ENA 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，ENA 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: code*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_refill_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

ENAs 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 ENAs 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。
- **27**：Elastic Network Adapter 驱动程序不支持从 snmpd 轮询以太网功能。

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。

Elastic Fabric Adapter

Elastic Fabric Adapter (EFA) 是一种网络设备，可以将其附加到 Amazon EC2 实例以加速高性能计算 (HPC) 和机器学习应用程序。通过使用 EFA，您可以实现本地 HPC 集群的应用程序性能，并具有 AWS 云提供的可扩展性、灵活性和弹性。

与以前在基于云的 HPC 系统中使用的 TCP 传输相比，EFA 提供更低且更一致的延迟和更高的吞吐量。它提高了实例间通信的性能，这对于扩展 HPC 和机器学习应用程序至关重要。它经过优化以在现有的 AWS 网络基础设施上使用，并且可以根据应用程序要求进行扩展。

EFA 与 Libfabric 1.8.1 集成在一起，并支持适用于 HPC 应用程序的 Open MPI 4.0.2 和 Intel MPI 2019 Update 6 以及适用于机器学习应用程序的 Nvidia Collective Communications Library (NCCL)。

Note

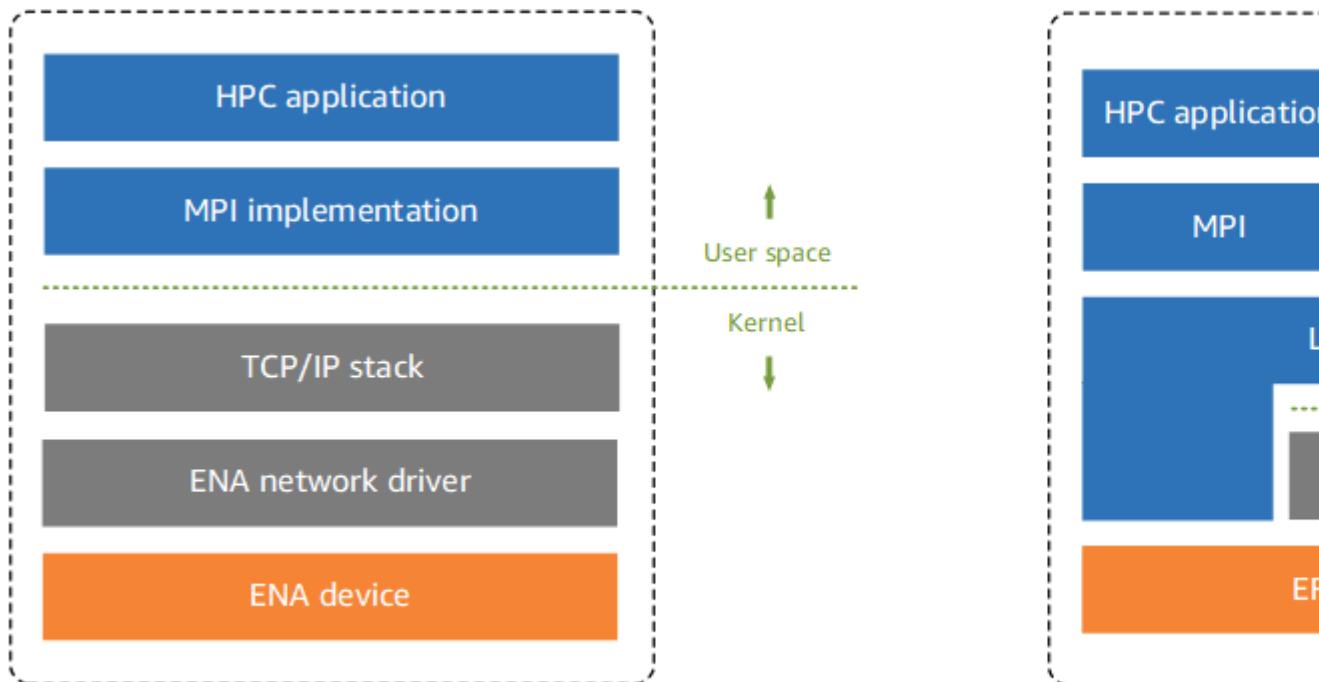
在 Windows 实例上不支持 EFAs 的操作系统绕过功能。如果将 EFA 附加到一个 Windows 实例，该实例将作为 Elastic Network Adapter，而没有添加的 EFA 功能。

目录

- [EFA 基础知识 \(p. 639\)](#)
- [支持的接口和库 \(p. 640\)](#)
- [支持的实例类型 \(p. 640\)](#)
- [支持 AMI \(p. 640\)](#)
- [EFA 限制 \(p. 640\)](#)
- [EFA 和 MPI 入门 \(p. 640\)](#)
- [EFA 和 NCCL 入门 \(p. 645\)](#)
- [使用 EFA \(p. 658\)](#)
- [监控 EFA \(p. 661\)](#)

EFA 基础知识

EFA 是具有添加的功能的 Elastic Network Adapter (ENA)。它提供了 ENA 的所有功能，并具有额外的操作系统绕过功能。操作系统绕过是一种访问模式，它允许 HPC 和机器学习应用程序直接与网络接口硬件通信以提供低延迟且可靠的传输功能。



Traditional HPC software stack in EC2

HPC software

以前，HPC 应用程序使用消息传递接口 (MPI) 与系统的网络传输进行交互。在 AWS 云中，这意味着应用程序与 MPI 进行交互，然后 MPI 使用操作系统的 TCP/IP 堆栈和 ENA 设备驱动程序以启用实例之间的网络通信。

通过使用 EFA，HPC 应用程序使用 MPI 或 NCCL 与 Libfabric API 进行交互。Libfabric API 绕过操作系统内核，并直接与 EFA 设备通信以将数据包放在网络上。这减少了开销，并且可以更有效地运行 HPC 应用程序。

Note

libfabric 是 OpenFabrics 接口 (OFI) 框架的核心组件，它定义并导出 OFI 的 user-space API。有关更多信息，请参阅 [libfabric OpenFabrics](#) 网站。

EFAs 和 ENA 之间的差异

Elastic Network Adapter (ENA) 提供支持 VPC 网络所需的传统 IP 网络功能。EFAs 提供与 ENA 相同的所有传统 IP 网络功能，并且它们还支持操作系统绕过功能。操作系统绕过允许 HPC 和机器学习应用程序绕过操作系统内核，并直接与 EFA 设备进行通信。

支持的接口和库

EFA 支持以下接口和库：

- Open MPI 4.0.2
- Intel MPI 2019 Update 6
- NVIDIA Collective Communications Library (NCCL) 2.4.2 及更高版本

支持的实例类型

以下实例类型支持 EFAs：c5n.18xlarge, c5n.metal, i3en.24xlarge, inf1.24xlarge, m5dn.24xlarge, m5n.24xlarge, r5dn.24xlarge, r5n.24xlarge, and p3dn.24xlarge。

支持 AMI

以下 AMI 支持 EFAs：Amazon Linux, Amazon Linux 2, RHEL 7.6, RHEL 7.7, CentOS 7, Ubuntu 16.04, and Ubuntu 18.04。

EFA 限制

EFA 具有以下限制：

- 您只能为每个实例附加一个 EFA。
- EFA 操作系统绕过流量限制为单个子网。换句话说，无法将 EFA 流量从一个子网发送到另一个子网。可以将来自 EFA 的普通 IP 流量从一个子网发送到另一个子网。
- 无法路由 EFA 操作系统绕过流量。仍然可以路由来自 EFA 的普通 IP 流量。
- EFA 必须是一个安全组的成员，以允许进出安全组本身的所有入站和出站流量。

EFA 和 MPI 入门

本教程可帮助您为 HPC 工作负载启动启用了 EFA 和 MPI 的实例集群。在本教程中，您将执行以下步骤：

目录

- 步骤 1：准备启用 EFA 的安全组 (p. 641)
- 步骤 2：启动临时实例 (p. 641)
- 步骤 3：安装 Libfabric 和 Open MPI (p. 642)
- 步骤 4：(可选) 安装 Intel MPI (p. 643)
- 步骤 5：安装 HPC 应用程序 (p. 644)
- 步骤 6：创建启用 EFA 的 AMI (p. 644)
- 步骤 7：在集群置放群组中启动启用 EFA 的实例 (p. 644)
- 步骤 8：终止临时实例 (p. 645)

步骤 1：准备启用 EFA 的安全组

EFA 需要使用一个安全组，以允许传入和传出安全组本身的所有入站和出站流量。

创建启用了 EFA 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 Security Groups (安全组)，然后选择 Create Security Group (创建安全组)。
3. 在 Create Security Group (创建安全组) 窗口中，执行以下操作：
 - a. 对于 Security group name (安全组名称)，请输入一个描述性的安全组名称，例如 EFA-enabled security group。
 - b. (可选) 对于 Description (描述)，请输入安全组的简要描述。
 - c. 对于 VPC，请选择要在其中启动启用了 EFA 的实例的 VPC。
 - d. 选择 Create。
4. 选择您创建的安全组，然后在 Description (描述) 选项卡上复制 Group ID (组 ID)。
5. 在 Inbound (入站) 和 Outbound (出站) 选项卡上，执行以下操作：
 - a. 选择 Edit。
 - b. 对于 Type (类型)，请选择 All traffic (所有流量)。
 - c. 对于 Source，选择 Custom。
 - d. 将您复制的安全组 ID 粘贴到该字段中。
 - e. 选择 Save。

步骤 2：启动临时实例

启动一个临时实例，可用于安装和配置 EFA 软件组件。您使用该实例创建一个启用了 EFA 的 AMI，您可以从中启动启用了 EFA 的实例。

启动临时实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在 Choose an AMI (选择 AMI) 页面上，针对以下支持的 AMIs 之一选择选择：Amazon Linux, Amazon Linux 2, RHEL 7.6, RHEL 7.7, CentOS 7, Ubuntu 16.04, and Ubuntu 18.04。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择以下支持的实例类型之一，然后选择下一步：配置实例详细信息：c5n.18xlarge, c5n.metal, i3en.24xlarge, inf1.24xlarge, m5dn.24xlarge, m5n.24xlarge, r5dn.24xlarge, r5n.24xlarge, and p3dn.24xlarge。
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 Elastic Fabric Adapter，请选择启用。

- b. 在 Network Interfaces (网络接口) 部分中，为设备 eth0 选择 New network interface (新网络接口)。
- c. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上，除了 AMI 指定的卷 (如根设备卷) 以外，还要指定要附加到实例的卷，然后选择 Next: Add Tags (下一步：添加标签)。
7. 在 Add Tags (添加标签) 页面上，指定一个可用于标识临时实例的标签，然后选择 Next: Configure Security Group (下一步：配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上，为 Assign a security group (分配安全组) 选择 Select an existing security group (选择一个现有的安全组)，然后选择在步骤 1 中创建的安全组。
9. 在 Review Instance Launch (核查实例启动) 页面上，检查这些设置，然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 3：安装 Libfabric 和 Open MPI

在临时实例上安装支持 EFA 所需的启用了 EFA 的内核、EFA 驱动程序、libfabric 和 Open MPI 堆栈。

在临时实例上安装 libfabric 和 Open MPI

1. 连接到您在步骤 2 中启动的实例。有关更多信息，请参阅[连接到 Linux 实例 \(p. 423\)](#)。
2. 下载 EFA 软件安装文件。要下载最新的稳定版本，请使用以下命令。

```
$ curl -O https://s3-us-west-2.amazonaws.com/aws-efa-installer/aws-efa-installer-1.7.1.tar.gz
```

您也可以通过将上面命令中的版本号替换为 latest 来获取最新版本。

3. 软件安装文件将打包为压缩的 .tar.gz 文件。从压缩的 .tar.gz 文件中提取文件，并导航到提取的目录。

```
$ tar -xf aws-efa-installer-1.7.1.tar.gz
```

```
$ cd aws-efa-installer
```

4. 运行 EFA 软件安装脚本。

```
$ sudo ./efa_installer.sh -y
```

Libfabric 安装在 /opt/amazon/efa 目录中，而 Open MPI 安装在 /opt/amazon/openmpi 目录中。

5. 注销实例，然后重新登录。
6. 确认已成功安装 EFA 软件组件。

```
$ fi_info -p efa
```

该命令应返回有关 libfabric EFA 接口的信息。以下示例显示了命令输出。

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-dgrm
```

```
version: 2.0
type: FI_EP_DGRAM
protocol: FI_PROTO_EFA
provider: efa;ofi_rxn
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-dgram
version: 1.0
type: FI_EP_RDM
protocol: FI_PROTO_RXD
```

步骤 4：(可选) 安装 Intel MPI

Note

如果您打算使用 Open MPI，请跳过此步骤。仅在您打算使用 Intel MPI 时执行此步骤。

Intel MPI 需要使用额外的安装和环境变量配置。

先决条件

确保执行以下步骤的用户具有 sudo 权限。

安装 Intel MPI

1. 要下载 Intel MPI 安装文件，请访问 [Intel 开发人员专区网站](#)。

您必须先进行注册，然后才能下载安装文件。在注册后，请执行以下操作：

- a. 对于 Product (产品)，选择 Intel MPI Library for Linux (适用于 Linux 的 Intel MPI 库)。
 - b. 对于 Version (版本)，请选择 2019 Update 6。
 - c. 选择具有 .tar.gz 文件名的按钮。例如，l_mpi_2019.6.154.tgz。
2. 安装文件将打包为压缩的 .tar.gz 文件。从压缩的 .tar.gz 文件中提取文件，并导航到提取的目录。

```
$ tar -xf file_name.tgz
```

```
$ cd directory_name
```

3. 使用所需的文本编辑器打开 silent.cfg。在第 10 行，将 ACCEPT_EULA=decline 更改为

ACCEPT_EULA=accept。保存更改并关闭该文件。

4. 运行安装脚本。

```
$ sudo ./install.sh -s silent.cfg
```

默认情况下，Intel MPI 安装到 /opt/intel/impi/ 目录中。

5. 将 Intel MPI 环境变量添加到相应的 shell 启动脚本，以确保每次实例启动时都设置它们。根据您的 shell 执行下列操作之一。

- 对于 bash，将以下环境变量添加到 /home/*username*/.bashrc 和 /home/*username*/.bash_profile。

```
source /opt/intel/impi/2019.6.154/intel64/bin/mpivars.sh
```

- 对于 csh 和 tcsh，将以下环境变量添加到 /home/*username*/.cshrc。

```
source /opt/intel/impi/2019.6.154/intel64/bin/mpivarsh.csh
```

6. 注销实例，然后重新登录。
7. 运行以下命令以确认是否已成功安装 Intel MPI。

```
$ which mpicc
```

以下示例显示了命令输出。

```
/opt/intel/compilers_and_libraries_2020.0.154/linux/mpi/intel64/bin/mpicc
```

Note

如果您不再需要使用 Intel MPI，请从 shell 启动脚本中删除环境变量。

步骤 5：安装 HPC 应用程序

在临时实例上安装 HPC 应用程序。安装过程因特定的 HPC 应用程序而异。有关在 Linux 实例上安装软件的更多信息，请参阅在 [Linux 实例上管理软件](#)。

Note

您可能需要参阅 HPC 应用程序文档以了解安装说明。

步骤 6：创建启用 EFA 的 AMI

在安装所需的软件组件后，您创建一个 EFA 和启用了 NCCL 的 AMI，可以将其重复使用以启动 EFA 和启用了 NCCL 的实例。

从临时实例中创建 AMI

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. 选择您在步骤 1 中创建的实例，然后选择 Actions (操作)、Image (映像) 和 Create Image (创建映像)。
4. 在 Create Image (创建映像) 窗口中，执行以下操作：
 - a. 对于 Image name (映像名称)，请为 AMI 输入一个描述性名称。
 - b. (可选) 对于 Image description (映像描述)，请输入 AMI 的简要描述。
 - c. 选择 Create Image (创建映像)，然后选择 Close (关闭)。
5. 在导航窗格中，选择 AMI。
6. 在列表中找到您创建的 AMI。等待状态从 pending 转变为 available，然后再继续执行下一步。

步骤 7：在集群置放群组中启动启用 EFA 的实例

使用在步骤 6 中创建的启用了 EFA 的 AMI 以及在步骤 1 中创建的启用了 EFA 的安全组，在集群置放群组中启动启用了 EFA 的实例。

Note

在集群置放群组中启动启用了 EFA 的实例并不是一个绝对要求。不过，我们建议在集群置放群组中运行启用了 EFA 的实例，因为它在单个可用区的低延迟组中启动实例。

在集群置放群组中启动启用了 EFA 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 AMI (选择 AMI) 页面上，选择 My AMIs (我的 AMI)，找到您在步骤 6 中创建的 AMI，然后选择 Select (选择)。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择以下支持的实例类型之一，然后选择下一步：配置实例详细信息：c5n.18xlarge, c5n.metal, i3en.24xlarge, inf1.24xlarge, m5dn.24xlarge, m5n.24xlarge, r5dn.24xlarge, r5n.24xlarge, and p3dn.24xlarge。
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 (实例的数量)，请输入要启动的启用了 EFA 的实例数量。
 - b. 对于 Network (网络) 和 Subnet (子网)，请选择要在其中启动实例的 VPC 和子网。
 - c. 对于 Placement group (置放群组)，请选择 Add instance to placement group (将实例添加到置放群组)。
 - d. 对于 Placement group name (置放群组名称)，请选择 Add to a new placement group (添加到新的置放群组)，输入一个描述性的置放群组名称，然后为 Placement group strategy (置放群组策略) 选择 cluster (集群)。
 - e. 对于 EFA，请选择 Enable (启用)。
 - f. 在 Network Interfaces (网络接口) 部分中，为设备 eth0 选择 New network interface (新网络接口)。您可以选择指定主 IPv4 地址以及一个或多个辅助 IPv4 地址。如果在具有关联的 IPv6 CIDR 块的子网中启动实例，您可以选择指定主 IPv6 地址以及一个或多个辅助 IPv6 地址。
 - g. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上，除了 AMI 指定的卷 (如根设备卷) 以外，还要指定要附加到实例的卷，然后选择 Next: Add Tags (下一步：添加标签)。
7. 在 Add Tags (添加标签) 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 (下一步：配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上，为 Assign a security group (分配安全组) 选择 Select an existing security group (选择一个现有的安全组)，然后选择在步骤 1 中创建的安全组。
9. 选择 Review and Launch。
10. 在 Review Instance Launch (核查实例启动) 页面上，检查这些设置，然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 8：终止临时实例

此时，您不再需要使用在步骤 1 中启动的临时实例。您可以终止该实例以停止产生费用。

终止临时实例

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. 选择您在步骤 1 中创建的临时实例，然后选择操作、实例状态、终止和是，请终止。

EFA 和 NCCL 入门

Nvidia Collective Communications Library (NCCL) 是一个标准集体通信例程库，它适用于跨单个节点或多个节点的多个 GPU。可将 NCCL 与 EFA、libfabric 和 MPI 结合使用来支持各种机器学习工作负载。有关更多信息，请参阅 [NCCL 网站](#)。

Note

- 仅 p3dn.24xlarge 实例支持将 NCCL 与 EFA 结合使用。
- 仅支持将 NCCL 2.4.2 及更高版本与 EFA 结合使用。

以下教程可帮助您为机器学习工作负载启动启用了 EFA 和 NCCL 的实例集群。

- [使用基础 AMI \(p. 646\)](#)
- [使用 AWS 深度学习 AMI \(p. 654\)](#)

使用基础 AMI

以下步骤将帮助您开始使用下列基础 AMI：Amazon Linux, Amazon Linux 2, RHEL 7.6, RHEL 7.7, CentOS 7, Ubuntu 16.04, and Ubuntu 18.04。

目录

- [步骤 1：准备启用 EFA 的安全组 \(p. 646\)](#)
- [步骤 2：启动临时实例 \(p. 647\)](#)
- [步骤 3：安装 Libfabric 和 Open MPI \(p. 647\)](#)
- [步骤 4：安装 Nvidia GPU 驱动程序和 Nvidia CUDA 工具包 \(p. 648\)](#)
- [步骤 5：安装 NCCL \(p. 649\)](#)
- [步骤 6：安装 aws-ofi-nccl 插件 \(p. 650\)](#)
- [步骤 7：安装 NCCL 测试 \(p. 651\)](#)
- [步骤 8：测试 EFA 和 NCCL 配置 \(p. 651\)](#)
- [步骤 9：安装机器学习应用程序 \(p. 652\)](#)
- [步骤 10：创建启用了 EFA 和 NCCL 的 AMI \(p. 652\)](#)
- [步骤 11：终止临时实例 \(p. 653\)](#)
- [步骤 12：在集群置放群组中启动启用了 EFA 和 NCCL 的实例 \(p. 653\)](#)
- [步骤 13：启用无密码 SSH \(p. 653\)](#)

步骤 1：准备启用 EFA 的安全组

EFA 需要使用一个安全组，以允许传入和传出安全组本身的所有入站和出站流量。

创建启用了 EFA 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 Security Groups (安全组)，然后选择 Create Security Group (创建安全组)。
3. 在 Create Security Group (创建安全组) 窗口中，执行以下操作：
 - a. 对于 Security group name (安全组名称)，请输入一个描述性的安全组名称，例如 EFA-enabled security group。
 - b. (可选) 对于 Description (描述)，请输入安全组的简要描述。
 - c. 对于 VPC，请选择要在其中启动启用了 EFA 的实例的 VPC。
 - d. 选择 Create。
4. 选择您创建的安全组，然后在 Description (描述) 选项卡上复制 Group ID (组 ID)。
5. 在 Inbound (入站) 和 Outbound (出站) 选项卡上，执行以下操作：
 - a. 选择 Edit。
 - b. 对于 Type (类型)，请选择 All traffic (所有流量)。
 - c. 对于 Source，选择 Custom。
 - d. 将您复制的安全组 ID 粘贴到该字段中。
 - e. 选择 Save。

步骤 2：启动临时实例

启动一个临时实例，可用于安装和配置 EFA 软件组件。您使用该实例创建一个启用了 EFA 的 AMI，您可以从中启动启用了 EFA 的实例。

启动临时实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在 Choose an AMI (选择 AMI) 页面上，从下列 AMI 中进行选择：Amazon Linux, Amazon Linux 2, RHEL 7.6, RHEL 7.7, CentOS 7, Ubuntu 16.04, and Ubuntu 18.04。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择 p3dn.24xlarge，然后选择 Next: Configure Instance Details (下一步: 配置实例详细信息)。
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 Elastic Fabric Adapter，请选择启用。
 - b. 在 Network Interfaces (网络接口) 部分中，为设备 eth0 选择 New network interface (新网络接口)。
 - c. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上，除了 AMI 指定的卷 (如根设备卷) 以外，还要指定要附加到实例的卷。然后，选择 Next: Add Tags (下一步: 添加标签)。
7. 在 Add Tags (添加标签) 页面上，指定一个可用于标识临时实例的标签，然后选择 Next: Configure Security Group (下一步: 配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上，对于 Assign a security group (分配安全组)，选择 Select an existing security group (选择现有安全组)。然后，选择您在步骤 1 中创建的安全组。
9. 在 Review Instance Launch (核查实例启动) 页面上，检查这些设置，然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 3：安装 Libfabric 和 Open MPI

在临时实例上安装支持 EFA 所需的启用了 EFA 的内核、EFA 驱动程序、libfabric 和 Open MPI 堆栈。

在临时实例上安装 libfabric 和 Open MPI

1. 连接到您在步骤 2 中启动的实例。有关更多信息，请参阅[连接到 Linux 实例 \(p. 423\)](#)。
2. 下载 EFA 软件安装文件。要下载最新的稳定版本，请使用以下命令。

```
$ curl -O https://s3-us-west-2.amazonaws.com/aws-efa-installer/aws-efa-installer-1.7.1.tar.gz
```

您也可以通过将上面命令中的版本号替换为 latest 来获取最新版本。

3. 软件安装文件将打包为压缩的 .tar.gz 文件。从压缩的 .tar.gz 文件中提取文件，并导航到提取的目录。

```
$ tar -xf aws-efa-installer-1.7.1.tar.gz
```

```
$ cd aws-efa-installer
```

4. 运行 EFA 软件安装脚本。

```
$ sudo ./efa_installer.sh -y
```

Libfabric 安装在 /opt/amazon/efa 目录中，而 Open MPI 安装在 /opt/amazon/openmpi 目录中。

5. 注销实例，然后重新登录。
6. 确认已成功安装 EFA 软件组件。

```
$ fi_info -p efa
```

该命令应返回有关 libfabric EFA 接口的信息。以下示例显示了命令输出。

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-dgram
    version: 2.0
    type: FI_EP_DGRAM
    protocol: FI_PROTO_EFA
provider: efa;ofi_rxd
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-dgram
    version: 1.0
    type: FI_EP_RDM
    protocol: FI_PROTO_RXD
```

步骤 4：安装 Nvidia GPU 驱动程序和 Nvidia CUDA 工具包

安装 Nvidia GPU 驱动程序和 Nvidia CUDA 工具包

1. 安装在安装 Nvidia GPU 驱动程序和 Nvidia CUDA 工具包时需要的实用程序。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ sudo yum groupinstall 'Development Tools' -y
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ sudo apt-get install build-essential -y
```

2. 要使用 Nvidia GPU 驱动程序，您必须先禁用 nouveau 开源驱动程序。

- a. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

- b. 将 nouveau 添加到 /etc/modprobe.d/blacklist.conf 黑名单文件。

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
```

```
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. 使用首选文本编辑器打开 `/etc/default/grub`，并添加以下内容。

```
$ GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. 重新生成 Grub 配置。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ sudo update-grub
```

3. 重启实例并重新连接到它。

4. 下载 Nvidia CUDA 工具包安装程序。

```
$ wget http://developer.download.nvidia.com/compute/cuda/10.1/Prod/local_installers/
cuda_10.1.243_418.87.00_linux.run
```

5. 运行 Nvidia CUDA 工具包安装程序。

```
$ sudo sh cuda_10.1.243_418.87.00_linux.run
```

当系统提示您接受许可协议时，输入 `accept` 并按 Enter 键。

6. 在 CUDA 安装程序菜单上，确保所有项目已选定，突出显示 `Install`，然后按 Enter 键。

7. 将以下语句添加到 shell 启动脚本，以确保实例每次启动时都设置 CUDA 路径。

```
export PATH=/usr/local/cuda-10.1/bin:/usr/local/cuda-10.1/NsightCompute-2019.1${PATH:+:
${PATH}}
export LD_LIBRARY_PATH=/usr/local/cuda-10.1/lib64${LD_LIBRARY_PATH:+:
${LD_LIBRARY_PATH}}
```

- 对于 bash shell，将语句添加到 `/home/username/.bashrc` 和 `/home/username/.bash_profile`。

- 对于 tcsh shell，将语句添加到 `/home/username/.cshrc`。

8. 要验证 Nvidia GPU 驱动程序是否正常运行，请运行以下命令。

```
$ nvidia-smi -q | head
```

此命令应返回有关 Nvidia GPU、Nvidia GPU 驱动程序和 Nvidia CUDA 工具包的信息。

步骤 5：安装 NCCL

安装 NCCL。有关 NCCL 的更多信息，请参阅 [NCCL 存储库](#)。

先决条件

- NCCL 需要 Nvidia CUDA 7.0 或更高版本。有关安装最新版本的更多信息，请参阅 Nvidia 网站上的 [CUDA Toolkit 10.1 Update 2 下载](#)。

安装 NCCL

- 导航到您的主目录。

```
$ cd $HOME
```

- 将官方 NCCL 存储库克隆到实例，然后导航到本地克隆的存储库。

```
$ git clone https://github.com/NVIDIA/nccl.git
```

```
$ cd nccl
```

- 生成并安装 NCCL，然后指定 CUDA 安装目录。以下命令假定将 CUDA 安装到默认目录中。

```
$ make -j src.build
```

步骤 6：安装 aws-ofi-nccl 插件

aws-ofi-nccl 插件将 NCCL 的面向连接的传输 API 映射到 libfabric 的无连接可靠接口。这使您能够在运行基于 NCCL 的应用程序时将 libfabric 用作网络提供程序。有关 aws-ofi-nccl 插件的更多信息，请参阅 [aws-ofi-nccl 存储库](#)。

安装 aws-ofi-nccl 插件

- 导航到您的主目录。

```
$ cd $HOME
```

- 安装在安装 aws-ofi-nccl 插件时所需的实用程序。要安装所需的实用程序，请运行以下命令。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ sudo yum install libudev-devel -y
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ sudo apt-get install libudev-dev libtool autoconf -y
```

- 将官方 AWS aws-ofi-nccl 存储库的 aws 分支克隆到实例，然后导航到本地克隆的存储库。

```
$ git clone https://github.com/aws/aws-ofi-nccl.git -b aws
```

```
$ cd aws-ofi-nccl
```

- 要生成 configure 脚本，请运行 autogen.sh 脚本。

```
$ ./autogen.sh
```

- 要生成 make 文件，请运行 configure 脚本并指定 MPI、libfabric、NCCL 和 CUDA 安装目录。

```
$ ./configure --with-mpi=/opt/amazon/openmpi --with-libfabric=/opt/amazon/efa --with-nccl=$HOME/nccl/build --with-cuda=/usr/local/cuda-10.1
```

6. 安装 aws-ofi-nccl 插件。

```
$ sudo make
```

```
$ sudo make install
```

步骤 7：安装 NCCL 测试

安装 NCCL 测试。NCCL 测试使您能够确认是否已正确安装 NCCL 以及它是否正在按预期运行。有关 NCCL 测试的更多信息，请参阅 [nccl-tests 存储库](#)。

安装 NCCL 测试

1. 导航到您的主目录。

```
$ cd $HOME
```

2. 将官方 nccl-tests 存储库克隆到实例，然后导航到本地克隆的存储库。

```
$ git clone https://github.com/NVIDIA/nccl-tests.git
```

```
$ cd nccl-tests
```

3. 将 libfabric 目录添加到 LD_LIBRARY_PATH 变量。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. (仅限 Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7) 默认情况下，make 文件会在 *mpi_home*/lib 目录中查找所需的库。不过，如果 Open MPI 已随 EFA 一起安装，则库位于 *mpi_home*/lib64 中。要在 make 文件中更新路径，请运行以下命令。

```
$ sed -i s/'NVLDFLAGS += -L$(MPI_HOME)\lib -lmpi'/'NVLDFLAGS += -L$(MPI_HOME)\lib64 -lmpi' / src/Makefile
```

5. 安装 NCCL 测试并指定 MPI、NCCL 和 CUDA 安装目录。

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=$HOME/nccl/build CUDA_HOME=/usr/local/cuda-10.1
```

步骤 8：测试 EFA 和 NCCL 配置

运行测试以确保为 EFA 和 NCCL 正确配置临时实例。

测试 EFA 和 NCCL 配置

- 创建一个主机文件来指定要在其上运行测试的主机。以下命令创建一个名为 my-hosts 的主机文件，该文件包含对实例本身的引用。

```
$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

- 运行测试并指定主机文件 (--hostfile) 和要使用的 GPU 数 (-n)。以下命令在实例本身的 8 个 GPU 上运行 all_reduce_perf 测试，并指定以下环境变量。

- FI_PROVIDER="efa" – 指定 fabric 接口提供程序。此项必须设置为 "efa"。
- FI_EFA_TX_MIN_CREDITS=64 – 指定发送方从接收方请求的最小发送积分数。对于使用 EFA 的 NCCL 作业，建议的值为 64。只应为大于 256 MB 的邮件传输增大此值。
- NCCL_DEBUG=INFO – 启用详细调试输出。您也可以指定 VERSION 以在测试开始时仅输出 NCCL 版本，或指定 WARN 以仅接收错误消息。
- NCCL_TREE_THRESHOLD=0 – 为测试禁用树算法。

有关 NCCL 测试参数的更多信息，请参阅官方 nccl-tests 存储库中的 [NCCL 测试自述文件](#)。

- Amazon Linux、Amazon Linux 2、RHEL 7.6/7.7、CentOS 7

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_PROVIDER="efa" \
-x FI_EFA_TX_MIN_CREDITS=64 \
-x LD_LIBRARY_PATH=$HOME/nccl/build/lib:/usr/local/cuda-10.1/lib64:/opt/amazon/efa/
lib64:/opt/amazon/openmpi/lib64:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
-x NCCL_TREE_THRESHOLD=0 \
--hostfile my-hosts -n 8 -N 8 \
--mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- Ubuntu 16.04 和 Ubuntu 18.04

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_PROVIDER="efa" \
-x FI_EFA_TX_MIN_CREDITS=64 \
-x LD_LIBRARY_PATH=$HOME/nccl/build/lib:/usr/local/cuda-10.1/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
-x NCCL_TREE_THRESHOLD=0 \
--hostfile my-hosts -n 8 -N 8 \
--mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

步骤 9：安装机器学习应用程序

在临时实例中安装机器学习应用程序。安装过程因特定的机器学习应用程序而异。有关在 Linux 实例上安装软件的更多信息，请参阅[在 Linux 实例上管理软件](#)。

Note

您可能需要参阅机器学习应用程序文档以了解安装说明。

步骤 10：创建启用了 EFA 和 NCCL 的 AMI

在安装所需的软件组件后，您创建一个 EFA 和启用了 NCCL 的 AMI，可以将其重复使用以启动 EFA 和启用了 NCCL 的实例。

从临时实例中创建 AMI

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. 选择您在步骤 1 中创建的实例，然后选择 Actions (操作)、Image (映像) 和 Create Image (创建映像)。
4. 在 Create Image (创建映像) 窗口中，执行以下操作：
 - a. 对于 Image name (映像名称)，请为 AMI 输入一个描述性名称。
 - b. (可选) 对于 Image description (映像描述)，请输入 AMI 的简要描述。
 - c. 选择 Create Image (创建映像)，然后选择 Close (关闭)。
5. 在导航窗格中，选择 AMI。
6. 在列表中找到您创建的 AMI。等待状态从 pending 转变为 available，然后再继续执行下一步。

步骤 11：终止临时实例

此时，您不再需要使用在步骤 1 中启动的临时实例。您可以终止该实例以停止产生费用。

终止临时实例

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. 选择您在步骤 1 中创建的临时实例，然后选择操作、实例状态、终止和是，请终止。

步骤 12：在集群置放群组中启动启用了 EFA 和 NCCL 的实例

使用之前创建的启用了 EFA 的 AMI 和启用了 EFA 的安全组，在集群置放群组中启动 EFA 和启用了 NCCL 的实例。

在集群置放群组中启动 EFA 和启用了 NCCL 的实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在选择 AMI 页面上，选择我的 AMI，找到您之前创建的 AMI，然后选择选择。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择 p3dn.24xlarge，然后选择 Next: Configure Instance Details (下一步: 配置实例详细信息)。
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 (实例数)，请输入要启动的 EFA 和启用了 NCCL 的实例的数量。
 - b. 对于 Network (网络) 和 Subnet (子网)，请选择要在其中启动实例的 VPC 和子网。
 - c. 对于 Placement group (置放群组)，请选择 Add instance to placement group (将实例添加到置放群组)。
 - d. 对于 Placement group name (置放群组名称)，请选择 Add to a new placement group (添加到新的置放群组)，然后为置放群组输入一个描述性名称。对于 Placement group strategy (置放群组策略)，选择 cluster (集群)。
 - e. 对于 EFA，请选择 Enable (启用)。
 - f. 在 Network Interfaces (网络接口) 部分中，为设备 eth0 选择 New network interface (新网络接口)。您可以选择指定主 IPv4 地址以及一个或多个辅助 IPv4 地址。如果在具有关联的 IPv6 CIDR 块的子网中启动实例，您可以选择指定主 IPv6 地址以及一个或多个辅助 IPv6 地址。
 - g. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上，除了 AMI 指定的卷 (如根设备卷) 以外，还要指定要附加到实例的卷。然后，选择 Next: Add Tags (下一步: 添加标签)。

7. 在 Add Tags (添加标签) 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 (下一步：配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上，为 Assign a security group (分配安全组) 选择 Select an existing security group (选择一个现有安全组)，然后选择之前创建的安全组。
9. 选择 Review and Launch。
10. 在 Review Instance Launch (核查实例启动) 页面上，检查这些设置，然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 13：启用无密码 SSH

要在集群中的所有实例中运行机器学习应用程序，您必须从领导节点到成员节点都启用无密码 SSH 访问。领导节点是在其中运行应用程序的实例。集群中的其余实例都是成员节点。

在集群中的实例间启用无密码 SSH

1. 选择集群中的一个实例作为领导节点，并连接到该节点。
2. 禁用 `strictHostKeyChecking` 并启用领导节点上的 `ForwardAgent`。使用首选文本编辑器打开 `~/.ssh/config`，并添加以下内容。

```
$ Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. 生成 RSA 密钥对。

```
$ ssh-keygen -t rsa -N "" -f /home/ubuntu/.ssh/id_rsa
```

将在 `$HOME/.ssh/` 目录中创建密钥对。

4. 更改领导节点上私有密钥的权限。

```
$ chmod 600 ~/.ssh/id_rsa
```

5. 使用首选文本编辑器打开 `~/.ssh/id_rsa.pub`，并复制密钥。

6. 对于集群中的每个成员节点，请执行以下操作：

- a. 连接到实例。
- b. 使用首选文本编辑器打开 `~/.ssh/authorized_keys` 并添加之前复制的公用密钥。

7. 要测试无密码 SSH 能否正常工作，请连接到领导节点并运行以下命令。

```
$ ssh member_node_private_ip
```

您应该能够在不提示密钥或密码的情况下连接到成员节点。

使用 AWS 深度学习 AMI

以下步骤将帮助您开始使用下列 AWS 深度学习 AMI：

- 深度学习 AMI (Amazon Linux 2) 版本 25.0 及更高版本
- 深度学习 AMI (Amazon Linux) 版本 25.0 及更高版本
- 深度学习 AMI (Ubuntu 18.04) 版本 25.0 及更高版本
- 深度学习 AMI (Ubuntu 16.04) 版本 25.0 及更高版本

有关更多信息，请参阅 [AWS Deep Learning AMI 用户指南](#)。

目录

- [步骤 1：准备启用 EFA 的安全组 \(p. 655\)](#)
- [步骤 2：启动临时实例 \(p. 655\)](#)
- [步骤 3：测试 EFA 和 NCCL 配置 \(p. 656\)](#)
- [步骤 4：安装机器学习应用程序 \(p. 656\)](#)
- [步骤 5：创建启用了 EFA 和 NCCL 的 AMI \(p. 657\)](#)
- [步骤 6：终止临时实例 \(p. 657\)](#)
- [步骤 7：在集群置放群组中启动启用了 EFA 和 NCCL 的实例 \(p. 657\)](#)
- [步骤 8：启用无密码 SSH \(p. 657\)](#)

步骤 1：准备启用 EFA 的安全组

EFA 需要使用一个安全组，以允许传入和传出安全组本身的所有入站和出站流量。

创建启用了 EFA 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 Security Groups (安全组)，然后选择 Create Security Group (创建安全组)。
3. 在 Create Security Group (创建安全组) 窗口中，执行以下操作：
 - a. 对于 Security group name (安全组名称)，请输入一个描述性的安全组名称，例如 EFA-enabled security group。
 - b. (可选) 对于 Description (描述)，请输入安全组的简要描述。
 - c. 对于 VPC，请选择要在其中启动启用了 EFA 的实例的 VPC。
 - d. 选择 Create。
4. 选择您创建的安全组，然后在 Description (描述) 选项卡上复制 Group ID (组 ID)。
5. 在 Inbound (入站) 和 Outbound (出站) 选项卡上，执行以下操作：
 - a. 选择 Edit。
 - b. 对于 Type (类型)，请选择 All traffic (所有流量)。
 - c. 对于 Source，选择 Custom。
 - d. 将您复制的安全组 ID 粘贴到该字段中。
 - e. 选择 Save。

步骤 2：启动临时实例

启动一个临时实例，可用于安装和配置 EFA 软件组件。您使用该实例创建一个启用了 EFA 的 AMI，您可以从中启动启用了 EFA 的实例。

启动临时实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在 Choose an AMI (选择 AMI) 页面上，选择受支持的 AWS 深度学习 AMI 版本 25.0 或更高版本。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择 p3dn.24xlarge，然后选择 Next: Configure Instance Details (下一步: 配置实例详细信息)。
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 Elastic Fabric Adapter , 请选择启用。
- b. 在 Network Interfaces (网络接口) 部分中 , 为设备 eth0 选择 New network interface (新网络接口)。
- c. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上 , 除了 AMI 指定的卷 (如根设备卷) 以外 , 还要指定要附加到实例的卷。然后 , 选择 Next: Add Tags (下一步: 添加标签)。
7. 在 Add Tags (添加标签) 页面上 , 指定一个可用于标识临时实例的标签 , 然后选择 Next: Configure Security Group (下一步 : 配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上 , 对于 Assign a security group (分配安全组) , 选择 Select an existing security group (选择现有安全组)。然后 , 选择您在步骤 1 中创建的安全组。
9. 在 Review Instance Launch (核查实例启动) 页面上 , 检查这些设置 , 然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 3：测试 EFA 和 NCCL 配置

运行测试以确保为 EFA 和 NCCL 正确配置临时实例。

测试 EFA 和 NCCL 配置

1. 创建一个主机文件来指定要在其上运行测试的主机。以下命令创建一个名为 my-hosts 的主机文件 , 该文件包含对实例本身的引用。

```
$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

2. 运行测试并指定主机文件 (--hostfile) 和要使用的 GPU 数 (-n)。以下命令在实例本身的 8 个 GPU 上运行 all_reduce_perf 测试 , 并指定以下环境变量。
 - FI_PROVIDER="efa" – 指定 fabric 接口提供程序。此项必须设置为 "efa"。
 - FI_EFA_TX_MIN_CREDITS=64 – 指定发送方从接收方请求的最小发送积分数。对于使用 EFA 的 NCCL 作业 , 建议的值为 64。只应为大于 256 MB 的邮件传输增大此值。
 - NCCL_DEBUG=INFO – 启用详细调试输出。您也可以指定 VERSION 以在测试开始时仅输出 NCCL 版本 , 或指定 WARN 以仅接收错误消息。
 - NCCL_TREE_THRESHOLD=0 – 为测试禁用树算法。

有关 NCCL 测试参数的更多信息 , 请参阅官方 nccl-tests 存储库中的 [NCCL 测试自述文件](#)。

```
/opt/amazon/openmpi/bin/mpirun \
-x FI_PROVIDER="efa" \
-x FI_EFA_TX_MIN_CREDITS=64 \
-x NCCL_DEBUG=INFO \
-x NCCL_TREE_THRESHOLD=0 \
--hostfile my-hosts -n 8 -N 8 \
--mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none \
$HOME/src/bin/efa-tests/efa-cuda-10.0/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

步骤 4：安装机器学习应用程序

在临时实例中安装机器学习应用程序。安装过程因特定的机器学习应用程序而异。有关在 Linux 实例上安装软件的更多信息 , 请参阅[在 Linux 实例上管理软件](#)。

Note

您可能需要参阅机器学习应用程序文档以了解安装说明。

步骤 5：创建启用了 EFA 和 NCCL 的 AMI

在安装所需的软件组件后，您创建一个 EFA 和启用了 NCCL 的 AMI，可以将其重复使用以启动 EFA 和启用了 NCCL 的实例。

从临时实例中创建 AMI

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. 选择您在步骤 1 中创建的实例，然后选择 Actions (操作)、Image (映像) 和 Create Image (创建映像)。
4. 在 Create Image (创建映像) 窗口中，执行以下操作：
 - a. 对于 Image name (映像名称)，请为 AMI 输入一个描述性名称。
 - b. (可选) 对于 Image description (映像描述)，请输入 AMI 的简要描述。
 - c. 选择 Create Image (创建映像)，然后选择 Close (关闭)。
5. 在导航窗格中，选择 AMI。
6. 在列表中找到您创建的 AMI。等待状态从 pending 转变为 available，然后再继续执行下一步。

步骤 6：终止临时实例

此时，您不再需要使用在步骤 1 中启动的临时实例。您可以终止该实例以停止产生费用。

终止临时实例

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. 选择您在步骤 1 中创建的临时实例，然后选择操作、实例状态、终止和是，请终止。

步骤 7：在集群置放群组中启动启用了 EFA 和 NCCL 的实例

使用之前创建的启用了 EFA 的 AMI 和启用了 EFA 的安全组，在集群置放群组中启动 EFA 和启用了 NCCL 的实例。

在集群置放群组中启动 EFA 和启用了 NCCL 的实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在选择 AMI 页面上，选择我的 AMI，找到您之前创建的 AMI，然后选择选择。
4. 在 Choose an Instance Type (选择实例类型) 页面上，选择 p3dn.24xlarge，然后选择 Next: Configure Instance Details (下一步: 配置实例详细信息)。
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 (实例数)，请输入要启动的 EFA 和启用了 NCCL 的实例的数量。
 - b. 对于 Network (网络) 和 Subnet (子网)，请选择要在其中启动实例的 VPC 和子网。
 - c. 对于 Placement group (置放群组)，请选择 Add instance to placement group (将实例添加到置放群组)。
 - d. 对于 Placement group name (置放群组名称)，请选择 Add to a new placement group (添加到新的置放群组)，然后为置放群组输入一个描述性名称。对于 Placement group strategy (置放群组策略)，选择 cluster (集群)。
 - e. 对于 EFA，请选择 Enable (启用)。
 - f. 在 Network Interfaces (网络接口) 部分中，为设备 eth0 选择 New network interface (新网络接口)。您可以选择指定主 IPv4 地址以及一个或多个辅助 IPv4 地址。如果在具有关联的 IPv6 CIDR 块的子网中启动实例，您可以选择指定主 IPv6 地址以及一个或多个辅助 IPv6 地址。

- g. 选择 Next: Add Storage。
6. 在 Add Storage (添加存储) 页面上，除了 AMI 指定的卷 (如根设备卷) 以外，还要指定要附加到实例的卷。然后，选择 Next: Add Tags (下一步: 添加标签)。
7. 在 Add Tags (添加标签) 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 (下一步：配置安全组)。
8. 在 Configure Security Group (配置安全组) 页面上，为 Assign a security group (分配安全组) 选择 Select an existing security group (选择一个现有安全组)，然后选择之前创建的安全组。
9. 选择 Review and Launch。
10. 在 Review Instance Launch (核查实例启动) 页面上，检查这些设置，然后选择 Launch (启动) 以选择一个密钥对并启动您的实例。

步骤 8：启用无密码 SSH

要在集群中的所有实例中运行机器学习应用程序，您必须从领导节点到成员节点都启用无密码 SSH 访问。领导节点是在其中运行应用程序的实例。集群中的其余实例都是成员节点。

在集群中的实例间启用无密码 SSH

1. 选择集群中的一个实例作为领导节点，并连接到该节点。
2. 禁用 `strictHostKeyChecking` 并启用领导节点上的 `ForwardAgent`。使用首选文本编辑器打开 `~/.ssh/config`，并添加以下内容。

```
$ Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. 生成 RSA 密钥对。

```
$ ssh-keygen -t rsa -N "" -f /home/ubuntu/.ssh/id_rsa
```

将在 `$HOME/.ssh/` 目录中创建密钥对。

4. 更改领导节点上私有密钥的权限。

```
$ chmod 600 ~/.ssh/id_rsa
```

5. 使用首选文本编辑器打开 `~/.ssh/id_rsa.pub`，并复制密钥。

6. 对于集群中的每个成员节点，请执行以下操作：

- a. 连接到实例。
 - b. 使用首选文本编辑器打开 `~/.ssh/authorized_keys` 并添加之前复制的公用密钥。
7. 要测试无密码 SSH 能否正常工作，请连接到领导节点并运行以下命令。

```
$ ssh member_node_private_ip
```

您应该能够在不提示密钥或密码的情况下连接到成员节点。

使用 EFA

您可以在 Amazon EC2 中创建、使用和管理 EFA，就像任何其他弹性网络接口一样。不过，与弹性网络接口不同，无法将 EFAs 附加到处于运行状态的实例，也无法将其从处于运行状态的实例中分离。

EFA 要求

要使用 EFA，您必须执行以下操作：

- 使用以下支持的实例类型之一：c5n.18xlarge, c5n.metal, i3en.24xlarge, inf1.24xlarge, m5dn.24xlarge, m5n.24xlarge, r5dn.24xlarge, r5n.24xlarge, and p3dn.24xlarge。
- 使用以下支持的 AMIs 之一：Amazon Linux, Amazon Linux 2, RHEL 7.6, RHEL 7.7, CentOS 7, Ubuntu 16.04, and Ubuntu 18.04。
- 安装 EFA 软件组件。有关更多信息，请参阅 [步骤 3：安装 Libfabric 和 Open MPI \(p. 642\)](#) 和 [步骤 4：\(可选\) 安装 Intel MPI \(p. 643\)](#)。
- 使用一个安全组，以允许进出安全组本身的所有入站和出站流量。有关更多信息，请参阅 [步骤 1：准备启用 EFA 的安全组 \(p. 641\)](#)。

目录

- [创建 EFA \(p. 659\)](#)
- [将 EFA 附加到停止的实例 \(p. 660\)](#)
- [在启动实例时附加 EFA \(p. 660\)](#)
- [将 EFA 添加到启动模板 \(p. 660\)](#)
- [将 IP 地址分配给 EFA \(p. 660\)](#)
- [从 EFA 中取消分配 IP 地址 \(p. 660\)](#)
- [更改安全组 \(p. 661\)](#)
- [分离 EFA \(p. 661\)](#)
- [查看 EFAs \(p. 661\)](#)
- [删除 EFA \(p. 661\)](#)

创建 EFA

您可以在 VPC 上的子网中创建 EFA。在创建 EFA 后，您无法将其移动到另一个子网，并且只能将其附加到同一可用区中的已停止实例。

使用控制台创建新的 EFA

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 (描述)，请输入一个描述性的 EFA 名称。
5. 对于 Subnet (子网)，请选择要在其中创建 EFA 的子网。
6. 对于 Private IP (私有 IP)，请输入主私有 IPv4 地址。如果未指定 IPv4 地址，我们将从选定的子网中选择一个可用的私有 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. 对于 EFA，请选择已启用。
10. 选择 Yes, Create。

使用 AWS CLI 创建新的 EFA

使用 `create-network-interface` 命令，并为 `interface-type` 指定 `efa`，如以下示例中所示。

```
$ aws ec2 create-network-interface --subnet-id subnet-01234567890 --description example_efa  
--interface-type efa
```

将 EFA 附加到停止的实例

您可以将 EFA 附加到处于 `stopped` 状态的任何支持的实例。您无法将 EFA 附加到处于 `running` 状态的实例。有关支持的实例类型的更多信息，请参阅[支持的实例类型 \(p. 640\)](#)。

您可以使用将弹性网络接口附加到实例的相同方式将 EFA 附加到实例。有关更多信息，请参阅[将网络接口附加到已停止的实例或正在运行的实例 \(p. 610\)](#)。

在启动实例时附加 EFA

在启动实例时附加现有的 EFA (AWS CLI)

使用 `run-instances` 命令，并为 `NetworkInterfaceId` 指定 EFA 的 ID，如以下示例中所示。

```
$ aws ec2 run-instances --image-id ami_id --count 1 --instance-type c5n.18xlarge --key-name my_key_pair --network-interfaces DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

在启动实例时附加新的 EFA (AWS CLI)

使用 `run-instances` 命令，并为 `InterfaceType` 指定 `efa` 的 ID，如以下示例中所示。

```
$ aws ec2 run-instances --image-id ami_id --count 1 --instance-type c5n.18xlarge --key-name my_key_pair --network-interfaces DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

将 EFA 添加到启动模板

您可以创建一个启动模板，其中包含启动启用了 EFA 的实例所需的配置信息。要创建启用了 EFA 的启动模板，请创建新的启动模板并指定支持的实例类型、启用了 EFA 的 AMI 以及启用了 EFA 的安全组。有关更多信息，请参阅[EFA 和 MPI 入门 \(p. 640\)](#)。

您可以利用启动模板通过其他 AWS 服务（如 AWS Batch）启动启用了 EFA 的实例。

有关创建启动模板的更多信息，请参阅[创建启动模板 \(p. 380\)](#)。

将 IP 地址分配给 EFA

如果具有弹性 IP (IPv4) 地址，您可以将其与 EFA 相关联。如果在具有关联的 IPv6 CIDR 块的子网中预置了 EFA，您可以将一个或多个 IPv6 地址分配给 EFA。

您可以使用将 IP 地址分配给弹性网络接口的相同方式将弹性 IP (IPv4) 和 IPv6 地址分配给 EFA。有关更多信息，请参阅：

- [关联弹性 IP 地址 \(IPv4\) \(p. 612\)](#)
- [分配 IPv6 地址 \(p. 613\)](#)

从 EFA 中取消分配 IP 地址

您可以使用从弹性网络接口中取消分配 IP 地址的相同方式从 EFA 中取消分配弹性 IP (IPv4) 和 IPv6 地址。有关更多信息，请参阅：

- [取消关联弹性 IP 地址 \(IPv4\) \(p. 613\)](#)

- 取消分配 IPv6 地址 (p. 614)

更改安全组

您可以更改与 EFA 关联的安全组。要启用操作系统绕过功能，EFA 必须是一个安全组的成员，以允许进出安全组本身的所有入站和出站流量。

您可以使用更改与弹性网络接口关联的安全组的相同方式更改与 EFA 关联的安全组。有关更多信息，请参阅[更改安全组 \(p. 612\)](#)。

分离 EFA

要从实例中分离 EFA，您必须先停止该实例。您无法从处于运行状态的实例中分离 EFA。

您可以使用从实例中分离弹性网络接口的相同方式从实例中分离 EFA。有关更多信息，请参阅[将网络接口与实例分离 \(p. 611\)](#)。

查看 EFAs

您可以查看您的账户中的所有 EFAs。

您可以使用查看弹性网络接口的方式查看 EFAs。有关更多信息，请参阅[查看有关网络接口的详细信息 \(p. 609\)](#)。

删除 EFA

要删除 EFA，您必须先将其从实例中分离。在附加到实例时，您无法删除 EFA。

您可以使用删除弹性网络接口的相同方式删除 EFAs。有关更多信息，请参阅[删除网络接口 \(p. 609\)](#)。

监控 EFA

您可以使用以下功能监控 Elastic Fabric Adapters 的性能。

Amazon VPC 流日志

您可以创建 Amazon VPC 流日志以捕获有关进出 EFA 的流量的信息。流日志数据可以发布到 Amazon CloudWatch Logs 和 Amazon S3。在创建流日志后，您可以在所选的目标中检索和查看其数据。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [VPC Flow Logs](#)。

您可以使用为弹性网络接口创建流日志的相同方式为 EFA 创建流日志。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [创建流日志](#)。

在流日志条目中，EFA 流量由 `srcAddress` 和 `destAddress` 标识，二者都格式化为 MAC 地址，如以下示例中所示。

```
version accountId eniId      srcAddress      destAddress      sourcePort destPort
protocol packets bytes start      end      action log-status
2          3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -           -
9          5689     1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Amazon CloudWatch 提供可用于实时监控 EFAs 的指标。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。有关更多信息，请参阅[使用 CloudWatch 监控您的实例 \(p. 538\)](#)。

置放群组

在您启动新的 EC2 实例时，EC2 服务会尝试以某种方式放置实例，以便将所有实例分布在基础硬件上以最大限度减少相关的故障。您可以使用置放群组影响如何放置一组相互依赖的实例，从而满足您的工作负载需求。根据工作负载类型，您可以使用以下置放策略之一创建置放群组：

- 集群 – 将一个可用区中靠近的实例打包在一起。通过使用该策略，工作负载可以实现所需的低延迟网络性能，以满足 HPC 应用程序通常使用的紧密耦合的节点到节点通信的要求。
- 分区 – 将实例分布在不同的逻辑分区上，以便一个分区中的实例组不会与不同分区中的实例组使用相同的基础硬件。该策略通常为大型分布式和重复的工作负载所使用，例如，Hadoop、Cassandra 和 Kafka。
- 分布 – 将一小组实例严格放置在不同的基础硬件上以减少相关的故障。

创建置放群组无需支付费用。

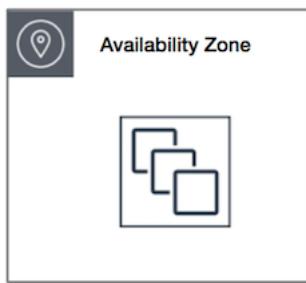
目录

- [集群置放群组 \(p. 662\)](#)
- [分区置放群组 \(p. 663\)](#)
- [分布置放群组 \(p. 663\)](#)
- [置放群组规则和限制 \(p. 664\)](#)
- [创建置放群组 \(p. 665\)](#)
- [在置放群组中启动实例 \(p. 665\)](#)
- [描述置放群组中的实例 \(p. 666\)](#)
- [更改实例的置放群组 \(p. 667\)](#)
- [删除置放群组 \(p. 668\)](#)

集群置放群组

集群置放群组是单个可用区中的实例的逻辑分组。置放群组可跨越同一区域中的对等 VPC。除了 10 Gbps 流限制之外，集群置放群组的主要优点还包括连接的非阻塞、非超额订阅、完全双截面特性。也就是说，置放群组内的所有节点都可以以 10 Gpbs 流和 100 Gbps 聚合的全线速率与该置放群组内的所有其他节点进行通信，而不会由于超额订阅而发生任何减速。

下图显示放入集群置放群组中的实例。



对于从低网络延迟和/或高网络吞吐量中受益的应用程序，以及在大部分网络流量处于该组中的实例之间的情况下，建议使用集群置放群组。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 \(p. 616\)](#)。

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。

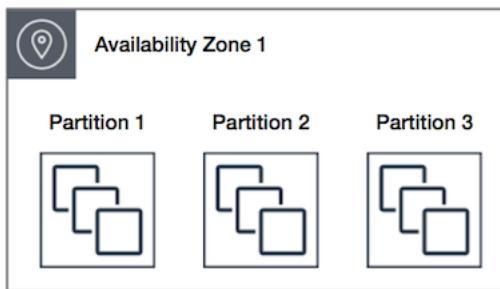
如果您停止置放群组中的某个实例，然后重启该实例，则其仍将在该置放群组中运行。但是，如果没有足够容量可用于该实例，则启动将会失败。

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。

分区置放群组

分区置放群组可帮助您的应用程序减少相关硬件故障的可能性。在使用分区置放群组时，Amazon EC2 将每个群组划分为多个逻辑段（称为“分区”）。Amazon EC2 确保置放群组中的每个分区具有自己的一组机架。每个机架具有自己的网络和电源。置放群组中的任何两个分区将不会分享相同的机架，从而让您可以在您的应用程序中隔离硬件故障的影响。

下图是单个可用区中的分区置放群组简单的直观表示。它显示了放入到一个分区置放群组的实例，该置放群组具有三个分区—分区 1、分区 2 和 分区 3。每个分区均包含多个实例。一个分区中的实例不与其他分区中的实例共享机架，这使您可以将单一硬件故障的影响限定在相关的分区内。



可使用分区置放群跨不同机架部署大型分布式和重复的工作负载，例如 HDFS、HBase 和 Cassandra。当您在分区置放群组中启动实例时，Amazon EC2 将尝试跨您指定数量的分区均匀分发实例。您还可以在特定分区中启动实例，以更好地控制实例的放置位置。

分区置放群组可以在同一区域的多个可用区中具有分区。对于每个可用区，一个分区置放群组最多可具有 7 个分区。可在分区置放群组启动的实例的数量仅受账户限制的限制。

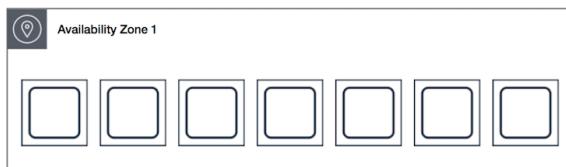
此外，分区置放群组提供对分区的可见性 — 您可以查看哪些实例位于哪些分区中。您可以与具有感知技术能力的应用程序共享此信息，例如 HDFS、HBase 和 Cassandra。这些应用程序使用此信息做出智能数据复制决策，用于提升数据的可用性和持久性。

如果在一个分区置放群组中启动一个实例，而没有足够的独特硬件来满足请求，则请求将失败。Amazon EC2 会随着时间的推移提供更多不同的硬件，因此，您稍后可以重试请求。

分布置放群组

分布置放群组是一组具有以下特点的实例：每个实例放置在不同的机架上，并且每个机架具有各自的网络和电源。

下图显示单个可用区中的 7 个实例，这些实例已放入一个分布置放群组。7 个实例放置在 7 个不同的机架上。



建议在具有少量应单独放置的重要实例的应用程序中使用分布置放群组。通过在分布置放群组中启动实例，可以降低在实例具有相同机架时同时发生故障的风险。分布置放群组可以访问不同的机架，因而适合混用不同类型的实例或随着时间的推移启动实例。

分布置放群组可以跨越同一区域中的多个可用区。每个群组在每个可用区中最多有 7 个正在运行的实例。

如果在分布置放群组中启动实例，并且没有足够的独特硬件来满足请求，请求将失败。Amazon EC2 随着时间的推移会提供更多不同的硬件，因此，您以后可以重试请求。

置放群组规则和限制

一般规则和限制

在使用置放群组之前，请注意以下规则：

- 您为置放群组指定的名称在您的区域 AWS 账户中必须是唯一的。
- 不能合并置放群组。
- 一次可在一个置放群组中启动一个实例；实例不能跨多个置放群组。
- [按需容量预留 \(p. 361\)](#) 和 [zonal 预留实例 \(p. 246\)](#) 为特定的可用区中的 EC2 实例提供容量预留。置放群组中的实例可以使用容量预留。但是，您无法为置放群组显式预留容量。
- 无法在置放群组中启动租赁为 host 的实例。

集群置放群组规则和限制

以下规则适用于集群置放群组：

- 将实例启动到集群置放群组中时，只能使用以下实例类型：
 - 通用型：A1、M4、M5、M5a、M5ad、M5d、M5dn 和 M5n
 - 计算优化型：C3、C4、C5、C5d、C5n 和 cc2.8xlarge
 - 内存优化：cr1.8xlarge、R3、R4、R5、R5a、R5ad、R5d、R5dn、R5n、X1、X1e 和 z1d
 - 存储优化型：D2、H1、hs1.8xlarge、I2、I3 和 I3en
 - 加速计算：F1、G2、G3、G4dn、P2、P3 和 P3dn
- 一个集群置放群组不能跨过多个可用区。
- 集群置放群组中的两个实例之间的最大网络吞吐量流量速度受两个实例中的较慢实例限制。对于具有高吞吐量要求的应用程序，请选择其网络连接满足您要求的实例类型。
- 对于启用了增强联网的实例，以下规则适用：
 - 对于单个流的流量，集群置放群组中的实例最多可以使用 10 Gbps。对于单个流的流量，不在集群置放群组中的实例最多可以使用 5 Gbps。
 - 在同一个区域中，通过公有 IP 地址空间或者通过 VPC 终端节点往返于 Amazon S3 存储桶之间的流量可以使用所有可用的实例聚合带宽。
- 您可以将多种类型的实例启动到集群置放群组中。不过，这会降低提供所需容量以成功完成启动的可能性。我们建议集群置放群组中的所有实例使用相同的实例类型。
- 指向 Internet 的网络流量以及通过 AWS Direct Connect 连接指向本地资源的流量限制为 5 Gbps。

分区置放群组规则和限制

以下规则适用于分区置放群组：

- 对于每个可用区，一个分区置放群组最多支持 7 个分区。您可在分区置放群组中启动的实例的数量仅受账户限制的限制。

- 在一个分区置放群组中启动实例时，Amazon EC2 将尝试跨所有分区均匀分发实例。Amazon EC2 不保证跨所有分区均匀分发实例。
- 具有 专用实例 的分区置放群组最多可具有 2 个分区。
- 专用主机 不支持分区置放群组。

分布置放群组规则和限制

以下规则适用于分布置放群组：

- 分布置放群组最多支持为每个可用区运行 7 个实例。例如，在具有三个可用区的区域中，您可以在组中总共运行 21 个实例（每个区域 7 个）。如果您尝试在同一可用区和同一个分布置放群组中启动第八个实例，则该实例将无法启动。如果您需要在可用区中拥有七个以上的实例，则建议使用多个分布置放群组。这并不能保证实例在组之间分布，但可确保每个组的分布以限制某些故障类别的影响。
- 专用实例 或 专用主机 不支持分布置放群组。

创建置放群组

您可以使用 Amazon EC2 控制台或命令行创建置放群组。

创建置放群组（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 Placement Groups (置放群组)，然后选择 Create Placement Group (创建置放群组)。
3. 指定群组的名称。
4. 选择适用于群组的策略。如果选择 Partition (分区)，则指定群组中的分区数。
5. 选择 Create。

创建置放群组（命令行）

- [create-placement-group](#) (AWS CLI)
- [New-EC2PlacementGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

创建分区置放群组 (AWS CLI)

- 使用 [create-placement-group](#) 命令并指定具有 partition 值的 --strategy 参数和 --partition-count 参数。在此示例中，分区置放群组名为 HDFS-Group-A，并包含 5 个分区。

```
aws ec2 create-placement-group --group-name HDFS-Group-A --strategy partition --partition-count 5
```

在置放群组中启动实例

您可以专门创建一个 AMI 以在置放群组中启动实例。为此，请启动一个实例，并在该实例上安装所需的软件和应用程序。然后，从该实例中创建一个 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Linux AMI \(p. 102\)](#)。

在置放群组中启动实例（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 Instances (实例)。
3. 选择 Launch Instance。按指示完成向导，注意执行以下操作：
 - 在选择一个 Amazon 系统映像 (AMI) 页上，选择一个 AMI。要选择您创建的 AMI，请选择我的 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 (配置实例详细信息) 页面上，以下字段适用于置放群组：
 - 在 Number of instances (实例数) 中，输入您在该置放群组中所需的实例总数，因为您以后可能无法向其中添加实例。
 - 对于 Placement group (置放群组)，选择 Add instance to placement group (向置放群组添加实例) 复选框。如果您在此页面上没有看到 Placement group (置放群组) 列表，请确认您选择了可启动到置放群组的实例类型，否则此选项不可用。
 - 对于 Placement group name (置放群组名称)，您可以选择将实例添加到现有置放群组，或者添加到您创建的新置放群组。
 - 对于 Placement group strategy (置放群组策略)，选择适当的策略。如果您选择 partition (分区)，则对于 Target partition (目标分区)，选择 Auto distribution (自动分配) 以让 Amazon EC2 尽力在群组的所有分区中平均地分配实例；或者指定要在其中启动实例的分区。

在置放群组中启动实例（命令行）

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. 使用以下选项之一将实例启动到置放群组：
 - --placement 与 [run-instances](#) (AWS CLI)
 - 带 [New-EC2Instance](#) 的 -PlacementGroup (适用于 Windows PowerShell 的 AWS 工具)

在分区置放群组的特定部分中启动实例 (AWS CLI)

- 使用 [run-instances](#) 命令，并使用 --placement "GroupName = **HDFS-Group-A**, PartitionNumber = **3**" 参数指定置放群组名称和分区。在此示例中，置放群组名为 HDFS-Group-A，分区编号为 3。

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

描述置放群组中的实例

您可以使用 Amazon EC2 控制台或命令行查看实例的置放信息。可使用控制台查看置放群组。当前只能使用 API 或 AWS CLI 查看分区置放群组中实例的分区编号。

查看实例的置放群组（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 Instances (实例)。
3. 选择实例，在详细信息窗格中，检查 Placement group (置放群组)。如果实例未在置放群组中，则此字段为空。否则，将显示置放群组名称。如果置放群组是分区置放群组，则检查 Partition number (分区编号) 以查看实例的分区编号。

查看分区置放群组中实例的分区编号 (AWS CLI)

- 使用 `describe-instances` 命令并指定 `--instance-id` 参数。

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

响应包含置放信息，其中包含实例的置放群组名称和分区编号。

```
"Placement": {  
    "AvailabilityZone": "us-east-1c",  
    "GroupName": "HDFS-Group-A",  
    "PartitionNumber": 3,  
    "Tenancy": "default"  
}
```

筛选特定分区置放群组和分区编号的实例 (AWS CLI)

- 使用 `describe-instances` 命令并指定具有 `placement-group-name` 和 `placement-partition-number` 筛选条件的 `--filters` 参数。在此示例中，置放群组名为 HDFS-Group-A，分区编号为 7。

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-Group-A" "Name = placement-partition-number, Values = 7"
```

响应列出了位于指定置放群组的指定分区中的所有实例。以下示例输出仅显示所返回实例的实例 ID、实例类型和置放信息。

```
"Instances": [  
    {  
        "InstanceId": "i-0a1bc23d4567e8f90",  
        "InstanceType": "r4.large",  
    },  
  
    {  
        "Placement": {  
            "AvailabilityZone": "us-east-1c",  
            "GroupName": "HDFS-Group-A",  
            "PartitionNumber": 7,  
            "Tenancy": "default"  
        }  
    },  
  
    {  
        "InstanceId": "i-0a9b876cd5d4ef321",  
        "InstanceType": "r4.large",  
    },  
  
    {  
        "Placement": {  
            "AvailabilityZone": "us-east-1c",  
            "GroupName": "HDFS-Group-A",  
            "PartitionNumber": 7,  
            "Tenancy": "default"  
        }  
    },  
]
```

更改实例的置放群组

您可以将现有实例移动到置放群组，将一个置放群组中的实例移动到另一个置放群组或从置放群组中删除实例。在开始之前，实例必须处于 `stopped` 状态。

您可以使用命令行或 AWS 开发工具包来更改实例的置放群组。

将实例移至置放群组 (命令行)

1. 使用以下命令之一停止实例：

- [stop-instances \(AWS CLI\)](#)
- [Stop-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

2. 使用 [modify-instance-placement](#) 命令 (AWS CLI) , 并指定要将实例移到的置放群组的名称。

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name MySpreadGroup
```

或者 , 使用 [Edit-EC2InstancePlacement](#) 命令 (适用于 Windows PowerShell 的 AWS 工具)。

3. 使用以下命令之一重新启动实例：

- [start-instances \(AWS CLI\)](#)
- [Start-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

删除置放群组中的实例 (命令行)

1. 使用以下命令之一停止实例：

- [stop-instances \(AWS CLI\)](#)
- [Stop-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

2. 使用 [modify-instance-placement](#) 命令 (AWS CLI) , 并为群组名称指定一个空字符串。

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name ""
```

或者 , 使用 [Edit-EC2InstancePlacement](#) 命令 (适用于 Windows PowerShell 的 AWS 工具)。

3. 使用以下命令之一重新启动实例：

- [start-instances \(AWS CLI\)](#)
- [Start-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某个置放群组 , 您可以将其删除。您必须先终止在您的置放群组中启动的所有实例或将这些实例移动到另一个置放群组 , 然后才能删除您的置放群组。

终止或移动实例并删除置放群组 (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 Instances (实例)。
3. 选择并终止置放群组中的所有实例。在终止实例之前 , 您可以在详细信息窗格中检查置放组值以确认该实例位于某个置放组中。

或者 , 执行 [更改实例的置放群组 \(p. 667\)](#) 中的步骤以将实例移动到其他置放群组。

4. 在导航窗格中 , 选择 Placement Groups。
5. 选择该置放群组 , 然后选择删除置放群组。
6. 当系统提示进行确认时 , 选择 Delete。

终止实例并删除置放群组 (命令行)

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 \(AWS CLI\)](#)
- [Remove-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 或巨型帧。

目录

- [巨型帧 \(9001 MTU\) \(p. 669\)](#)
- [路径 MTU 发现 \(p. 669\)](#)
- [查看两个主机之间的路径 MTU \(p. 670\)](#)
- [在您的 Linux 实例上检查并设置 MTU \(p. 670\)](#)
- [故障排除 \(p. 671\)](#)

巨型帧 (9001 MTU)

巨型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。但是，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，则对数据包进行分段；如果在 IP 标头中设置了 *Don't Fragment* 标记，则丢弃数据包。

不应将巨型帧用于 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段，从而减缓此流量。要使用 VPC 中的巨型帧而不减慢 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。

对于在集群置放群组中并置的实例，巨型帧有助于实现可能的最大网络吞吐量，建议在这种情况下使用这些帧。有关更多信息，请参阅 [置放群组 \(p. 662\)](#)。

您可以通过 AWS Direct Connect 使用巨型帧在 VPC 与本地网络之间进行通信。有关更多信息以及如何验证巨型帧功能，请参阅 AWS Direct Connect 用户指南 中的 [设置网络 MTU](#)。

[当前一代的所有实例 \(p. 165\)](#)都支持巨型帧。以下前一代实例支持巨型帧：C3、G2、I2、M3 和 R3。

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 规则添加到您的实例的入站安全组规则。有关更多信息，请参阅 [用于路径 MTU 发现的规则 \(p. 777\)](#)。

Important

将您的实例的安全组修改为允许路径 MTU 发现不能保证巨型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。

查看两个主机之间的路径 MTU

您可使用 `tracepath` 命令查看两个主机之间的路径 MTU，此命令是很多 Linux 发行版默认情况下提供的 `iputils` 程序包的一部分，包括 Amazon Linux)。

使用 `tracepath` 检查路径 MTU

使用以下命令检查您的 EC2 实例与另一个主机之间的路径 MTU。可以使用 DNS 名称或 IP 地址作为目的地。如果目的地是另一个 EC2 实例，则验证安全组是否允许入站 UDP 流量。本例检查 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。

在您的 Linux 实例上检查并设置 MTU

一些实例配置为使用巨型帧，另一些则配置为使用标准帧大小。您可能希望将巨型帧用于您的 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

您可使用以下 `ip` 命令检查当前 MTU 值。请注意，在示例输出中，`mtu 9001` 指示此实例使用了巨型帧。

```
[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 Linux 实例上设置 MTU 值

1. 可以使用 `ip` 命令设置 MTU 值。以下命令将预期 MTU 值设置为 1500，但是您可以使用 9001 代替。

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (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。

- 对于 Amazon Linux 2，将以下一行添加到 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件：

```
MTU=1500
```

将以下行添加到 `/etc/dhcp/dhclient.conf` 文件：

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name, domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-servers;
```

- 对于 Amazon Linux，将以下几行添加到 `/etc/dhcp/dhclient-eth0.conf` 文件。

```
interface "eth0" {
    supersede interface-mtu 1500;
}
```

- 对于其他 Linux 发行版，请参阅其具体文档。

- (可选) 重启实例并验证 MTU 设置是否正确。

故障排除

如果在使用巨型帧时您的 EC2 实例和 Amazon Redshift 集群之间出现连接问题，请参阅 Amazon Redshift Cluster Management Guide 中的 [查询挂起](#)

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 Amazon EC2 资源（如实例）启动到 VPC 的子网中。您的 VPC 与您在自己的数据中心中运行的传统网络可能极为相似，同时享有使用来自 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 或您自己的数据中心。

在您创建 AWS 账户时，我们会为您在每个 AWS 区域中创建一个默认 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。或者，您也可以创建自己的非默认 VPC 并根据需要对其进行配置。

如果您的 AWS 账户是在 2013 年 12 月 4 日之前创建的，您可能在某些区域中具有 EC2-Classic 平台支持。如果您的 AWS 账户是在 2013 年 12 月 4 日之后创建的，它不支持 EC2-Classic，因此您必须在 VPC 中启动您的资源。有关更多信息，请参阅[EC2-Classic \(p. 672\)](#)。

Amazon VPC 文档

有关 Amazon VPC 的更多信息，请参阅以下文档。

指南	描述
Amazon VPC 用户指南	介绍了主要概念并提供了有关使用 Amazon VPC 功能的说明。
Amazon VPC Peering Guide	介绍了 VPC 对等连接并提供了有关使用这些连接的说明。

指南	描述
AWS 站点到站点 VPN 网络管理员指南	帮助网络管理员配置客户网关。

EC2-Classic

通过使用 EC2-Classic，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。通过使用 Amazon VPC，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。

EC2-Classic 平台是在 Amazon EC2 的初始版本中引入的。如果您的 AWS 账户是在 2013 年 12 月 4 日之后创建的，它不支持 EC2-Classic，因此您必须在 VPC 中启动您的 Amazon EC2 实例。

如果您的账户不支持 EC2-Classic，我们会为您创建一个默认 VPC。默认情况下，当您启动某个实例时，我们会在您的默认 VPC 中启动它。或者，您也可以创建一个非默认 VPC，然后在启动实例时指定它。

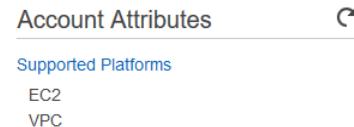
检测受支持的平台

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)。

支持 EC2-Classic 的账户

控制面板在 Account Attributes (账户属性) 下方显示以下内容，表示账户在此区域中支持 EC2-Classic 平台和 VPC，但该区域没有默认 VPC。



`describe-account-attributes` 命令的输出包含 `supported-platforms` 属性的 EC2 和 VPC 值。

```
aws ec2 describe-account-attributes --attribute-names supported-platforms
{
    "AccountAttributes": [
        {
            "AttributeName": "supported-platforms",
            "AttributeValues": [
                {
                    "AttributeValue": "EC2"
                },
                {
                    "AttributeValue": "VPC"
                }
            ]
        }
    ]
}
```

需要 VPC 的账户

控制面板在 Account Attributes (账户属性) 下方显示以下内容，表示账户在此区域中需要 VPC 来启动实例，在此区域中不支持 EC2-Classic 平台，该区域具有标识符为 `vpc-1a2b3c4d` 的默认 VPC。

Account Attributes

C

Supported Platforms

VPC

Default VPC

vpc-1a2b3c4d

`describe-account-attributes` 命令的输出仅包含 `supported-platforms` 属性的 VPC 值。

```
aws ec2 describe-account-attributes --attribute-names supported-platforms
{
    "AccountAttributes": [
        {
            "AttributeValues": [
                {
                    "AttributeValue": "VPC"
                }
            ],
            "AttributeName": "supported-platforms",
        }
    ]
}
```

EC2-Classic 中可用的实例类型

多数较新的实例类型都需要 VPC。以下是 EC2-Classic 中支持的唯一实例类型：

- 通用 : M1、M3 和 T1
- 计算优化 : C1、C3 和 CC2
- 内存优化 : CR1、M2 和 R3
- 存储优化 : D2、HS1 和 I2
- 加速计算 : G2

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需要 VPC 的实例：

- 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 软件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 \(VPC\) \(p. 21\)](#)。
- 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 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 \(p. 689\)](#)。

EC2-Classic 和 VPC 中的实例之间的区别

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。

特征	EC2-Classic	默认 VPC	非默认 VPC
公有 IPv4 地址 (来自 Amazon 的公有 IP 地址池)	您的实例从 EC2-Classic 公有 IPv4 地址池接收公有 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。
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。	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。
取消关联弹性 IP 地址	如果弹性 IP 地址已经与其他实例关联，该地址会自动与新实例关联。	如果弹性 IP 地址已经与其他实例关联，该地址会自动与新实例关联。	如果弹性 IP 地址已经与其他实例关联，则只有您允许重新关联时该操作才会成功。
标记弹性 IP 地址	您不能将标签应用于弹性 IP 地址。	您可以将标签应用于弹性 IP 地址。	您可以将标签应用于弹性 IP 地址。
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。	安全组可以引用您的 VPC 的安全组，或者引用 VPC 对等连接中的对等 VPC 的安全组。	安全组只能引用您的 VPC 的安全组。
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其与新实例关联起来，然后终止原有实例）。	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。
安全组规则	您只能为入站流量添加规则。	您可以为入站和出站流量添加规则。	您可以为入站和出站流量添加规则。

特征	EC2-Classic	默认 VPC	非默认 VPC
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 网关附加到您的默认 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。

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。不过，您可以向安全组添加或从中删除规则，并且这些更改会在经过一小段时间之后自动应用于与该安全组关联的所有实例。

您的 AWS 账户在每个区域都自动拥有一个 EC2-Classic 默认安全组。如果您尝试删除默认安全组，会显示以下错误：Client.InvalidGroup.Reserved: The security group 'default' is reserved (Client.InvalidGroup.Reserved: 保留“默认”安全组)。

您可以创建自定义安全组。安全组名称在您的区域账户中必须是唯一的。要创建在 EC2-Classic 中使用的安全组，请对 VPC 选择 No VPC (无 VPC)。

您可以对默认和自定义安全组添加入站规则。您无法更改 EC2-Classic 安全组的出站规则。创建安全组规则时，您可以在与源或目标相同的区域中使用其他 EC2-Classic 安全组。要为其他 AWS 账户指定安全组，请添加 AWS 账户 ID 作为前缀；例如 111122223333/sg-edcd9784。

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。

IP 寻址和 DNS

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。

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：

```
grep nameserver /etc/resolv.conf
```

弹性 IP 地址

如果您的账户支持 EC2-Classic，则其中一个弹性 IP 地址池可用于 EC2-Classic 平台，而另一个可用于 VPC。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，

您可迁移已分配为在 EC2-Classic 平台中使用的弹性 IP 地址以便用于 VPC。您不能将弹性 IP 地址迁移到另一个区域。

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。

从 EC2-Classic 迁移弹性 IP 地址

如果您的账户支持 EC2-Classic，则可迁移已分配为用于 EC2-Classic 平台的弹性 IP 地址以便用于同一区域内的 VPC。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 地址迁移到 VPC 后，不能将其用于 EC2-Classic。但是，如果需要，您可以将其还原到 EC2-Classic。您无法将本来分配为用于 VPC 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 \(p. 593\)](#)。

您可以迁移您的账户中拥有的数量的 EC2-Classic 弹性 IP 地址。但是，在迁移弹性 IP 地址时，该地址会计入 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 \(p. 595\)](#)。

您不能迁移在 24 小时之前分配给您的账户弹性 IP 地址。

您可使用 Amazon EC2 控制台或 Amazon VPC 控制台从 EC2-Classic 迁移弹性 IP 地址。该选项仅在您的账户支持 EC2-Classic 时可用。

使用 Amazon EC2 控制台移动弹性 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 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。

在将弹性 IP 地址移走后，您可以在 Elastic IPs (弹性 IP) 页面上的 Allocation ID (分配 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 [Premium Support](#)。

使用命令行移动弹性 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)
- [Move-EC2AddressToVpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行将弹性 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)
- [Restore-EC2AddressToClassic](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行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)
- [Get-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

在 EC2-Classic 与 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 VPC 平台之间共享或访问 (例如 , 通过 ClassicLink) 。有关更多信息 , 请参阅 [ClassicLink \(p. 678\)](#)。

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 \(p. 689\)](#)。

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 VPC 。您无法将本来分配为在 VPC 中使用的弹性 IP 地址迁移至 EC2-Classic 。有关更多信息 , 请参阅 从 EC2-Classic 迁移弹性 IP 地址 (p. 676) 。
实例	EC2-Classic 实例可以使用公有 IPv4 地址与 VPC 中的实例通信 , 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 中的实例迁移至 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. 689) 。

资源	备注
	Classic 中的 Linux 实例迁移到 VPC 中的 Linux 实例 (p. 689) 。
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。您无法在 EC2-Classic 的负载均衡器中注册 VPC 中的实例。
置放群组	
Reserved Instance	可以将 预留实例 的网络平台从 EC2-Classic 更改为 VPC。有关更多信息，请参阅 修改预留实例 (p. 265) 。
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 安全组复制到 VPC 安全组。有关更多信息，请参阅 正在创建安全组 (p. 771) 。
快照	

以下资源不能在 EC2-Classic 与 VPC 之间共享或移动：

- Spot 实例

ClassicLink

ClassicLink 允许您将 EC2-Classic 实例链接到账户中位于同一区域内的 VPC。如果您将 VPC 安全组与 EC2-Classic 实例关联，这会允许 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。

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。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 \(p. 689\)](#)。

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计费方式。

目录

- [ClassicLink 基础知识 \(p. 679\)](#)
- [ClassicLink 限制 \(p. 681\)](#)
- [使用 ClassicLink \(p. 681\)](#)
- [ClassicLink 的 IAM 策略示例 \(p. 684\)](#)
- [示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 \(p. 687\)](#)

ClassicLink 基础知识

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，您的账户中的所有 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 (实例) 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 和链接的实例 \(p. 683\)](#)。

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 \(p. 683\)](#)。

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。

如果使用 Elastic Load Balancing，您可以向负载均衡器注册链接的 EC2-Classic 实例。您必须在启用了 ClassicLink 的 VPC 中创建负载均衡器，并启用在其中运行实例的可用区。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。

如果您使用 Amazon EC2 Auto Scaling，则可以创建一个 Amazon EC2 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 [Amazon EC2 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 集群，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 集群，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 \(p. 704\)](#)。

有关使用 ClassicLink 的策略的更多信息，请参阅以下示例：[ClassicLink 的 IAM 策略示例 \(p. 684\)](#)。

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 中实例的传入和传出流量，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 \(p. 687\)](#)。

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-Classical 实例一次只能链接到一个 VPC。
- 如果您停止链接的 EC2-Classical 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-Classical 实例链接到不同区域或不同 AWS 账户中的 VPC。
- 您不能使用 ClassicLink 将一个 VPC 实例链接到另一个 VPC 或 EC2-Classical 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](#)。
- 您不能将 VPC 弹性 IP 地址与链接的 EC2-Classical 实例关联。
- 您不能允许 EC2-Classical 实例进行 IPv6 通信。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。
- 路由与 EC2-Classical 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 \(p. 680\)](#)。
- 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-Classical 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-Classical 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。如果您需要为专用 VPC 启用 ClassicLink，请在 AWS Support 请求中提供这么做的详细原因。

- 如果您将 EC2-Classical 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-Classical 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。
- ClassicLink 不支持 VPC 外的传递关系。链接的 EC2-Classical 实例不能访问与 VPC 关联的任何 VPN 连接、VPC 网关终端节点、NAT 网关或 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-Classical 实例。

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-Classical 实例链接到 VPC 或取消其链接。

Note

ClassicLink 功能仅显示在支持 EC2-Classical 的账户和区域的控制台中。

任务

- 为 VPC 启用 ClassicLink (p. 682)
- 创建启用了 ClassicLink 的 VPC (p. 682)
- 将实例链接到 VPC (p. 682)
- 在启动时将实例链接到 VPC (p. 682)
- 查看启用了 ClassicLink 的 VPC 和链接的实例 (p. 683)
- 启用 ClassicLink DNS 支持 (p. 683)
- 禁用 ClassicLink DNS 支持 (p. 684)
- 从 VPC 取消与实例的链接 (p. 684)
- 对 VPC 禁用 ClassicLink (p. 684)

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 \(p. 680\)](#)。

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。
5. (可选) 如果您希望公有 DNS 主机名解析为私有 IP 地址，请在链接任何实例之前先对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅[启用 ClassicLink DNS 支持 \(p. 683\)](#)。

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 仪表板上，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](#)。
5. (可选) 如果您希望公有 DNS 主机名解析为私有 IP 地址，请在链接任何实例之前先对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅[启用 ClassicLink DNS 支持 \(p. 683\)](#)。

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。

(可选) 如果您希望公有 DNS 主机名解析为私有 IP 地址，请在链接实例之前先对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅[启用 ClassicLink DNS 支持 \(p. 683\)](#)。

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。

在启动时将实例链接到 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 仪表板中，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 \(p. 375\)](#)。

查看启用了 ClassicLink 的 VPC 和链接的实例

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 实例与 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，则链接的 EC2-Classic 实例可以访问与 VPC 关联的所有私有托管区。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-Classical 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 取消与实例的链接

如果您不再需要 EC2-Classical 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-Classical 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-Classical 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。

ClassicLink 的 IAM 策略示例

您可以为 VPC 启用 ClassicLink，然后将 EC2-Classical 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-Classical 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。

示例

- [使用 ClassicLink 的完全权限 \(p. 685\)](#)
- [为 VPC 启用和禁用 ClassicLink \(p. 685\)](#)
- [链接实例 \(p. 685\)](#)
- [取消链接实例 \(p. 686\)](#)

使用 ClassicLink 的完全权限

以下策略授予用户如下权限：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

以下策略为用户授予将实例链接到 VPC 的权限，但前提是实例具有 m3.large 实例类型。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:vpc/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/purpose": "classiclink"  
                }  
            }  
        }  
    ]  
}
```

```
"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/*"
    ]
}
]
```

以下策略为用户授予权限：仅将实例链接到特定 VPC (vpc-1a2b3c4d) 以及仅将 VPC 中的特定安全组 (sg-1122aabb 和 sg-aabb2233) 与实例相关联。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"
            ]
        }
    ]
}
```

取消链接实例

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。第二条语句为用户授予使用 VPC 资源的权限，需要具有该权限才能从 VPC 中取消链接实例。

```
{
    "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/*"
            ]
        }
    ]
}
```

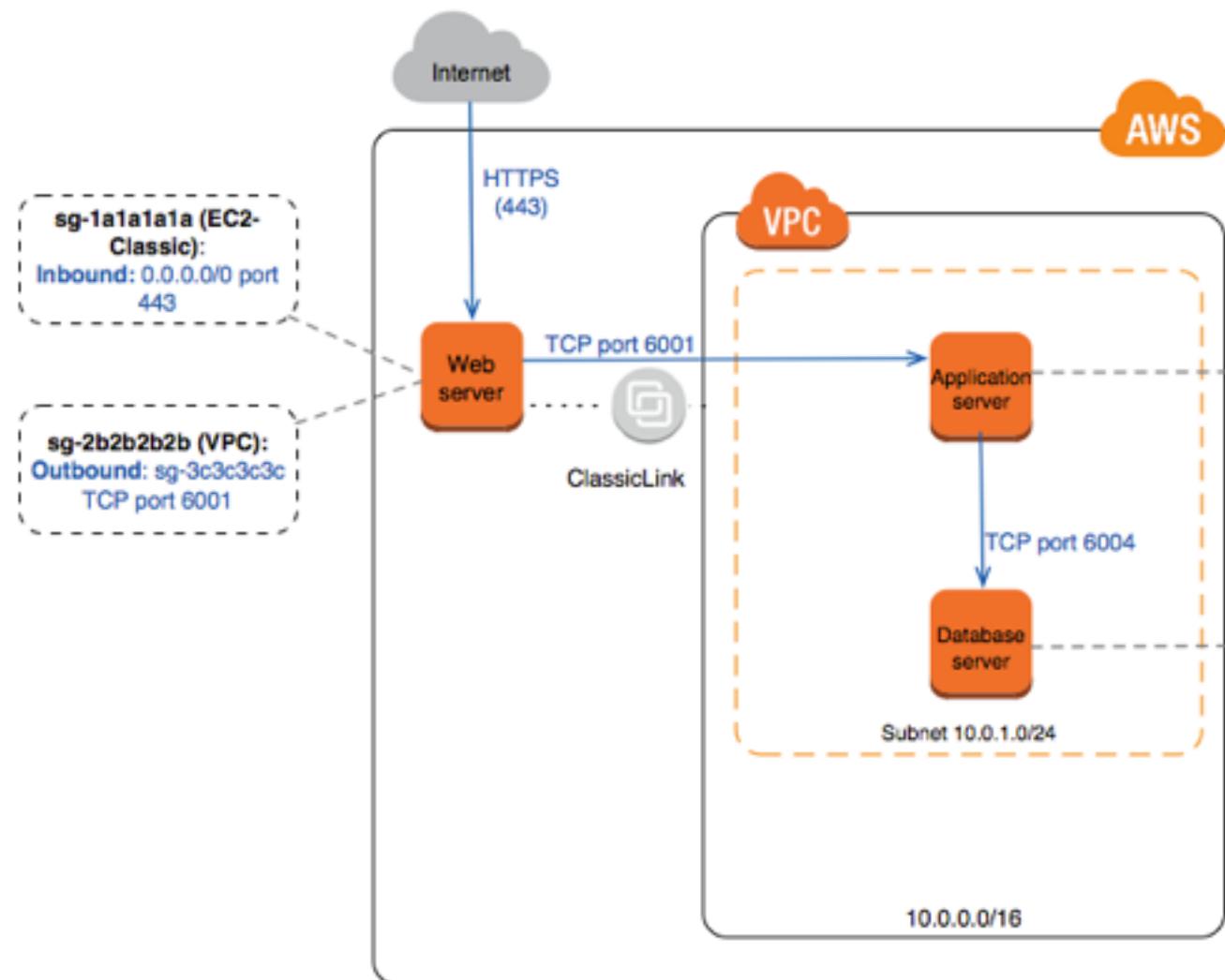
```
        "arn:aws:ec2:region:account:vpc/*"
    ]
}
}
```

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)。

Inbound			
Source	Type	Port Range	Comments
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)。

Outbound			
Destination	Type	Port Range	Comments
sg-3c3c3c3c	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 sg-3c3c3c3c 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。

Inbound			
Source	Type	Port Range	Comments
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。
Outbound			
Destination	Type	Port Range	Comments
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。

Inbound			
Source	Type	Port Range	Comments

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

如果您的 AWS 账户是在 2013 年 12 月 4 日之前创建的，您可能在某些区域中具有 EC2-Classic 支持。一些 Amazon EC2 资源和功能（如增强联网和较新的实例类型）需要 Virtual Private Cloud (VPC)。有些资源可在 EC2-Classic 和 VPC 之间共享，而有些则不能。有关更多信息，请参阅[在 EC2-Classic 与 VPC 之间共享和访问资源 \(p. 677\)](#)。

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次应用程序，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](#)。

目录

- [完整迁移到 VPC \(p. 689\)](#)
- [使用 ClassicLink 增量迁移到 VPC \(p. 695\)](#)

完整迁移到 VPC

完成以下任务可将应用程序从 EC2-Classic 完全迁移到 VPC。

任务

- [步骤 1：创建 VPC \(p. 689\)](#)
- [步骤 2：配置安全组 \(p. 690\)](#)
- [步骤 3：从您的 EC2-Classic 实例创建 AMI \(p. 690\)](#)
- [步骤 4：在 VPC 中启动实例 \(p. 691\)](#)
- [示例：迁移简单的 Web 应用程序 \(p. 692\)](#)

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：

- AWS 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，请使用该选项。
- 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，请使用该选项。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），请使用该选项。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 安全组 \(p. 768\)](#)。

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 安全组 \(p. 768\)](#)。

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 (描述) 选项卡上的 Root device type (根设备类型) 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 \(p. 87\)](#)。

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. 102) 。

实例根设备类型	操作
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. 105) 。
实例存储	将由实例存储支持的实例转换为由 EBS 支持的实例。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. 115) 。

(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 — 如同使用物理硬盘一样。Amazon EBS 卷可以与同一可用区中的任何实例附加和分离。您可以将卷与 EC2-Classic 中实例分离，并将它附加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 \(p. 783\)](#)
- [创建 Amazon EBS 卷 \(p. 798\)](#)
- [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)

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 \(p. 812\)](#)
- [创建 Amazon EBS 快照 \(p. 815\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 799\)](#)

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[使用启动实例向导启动实例 \(p. 375\)](#)。

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。

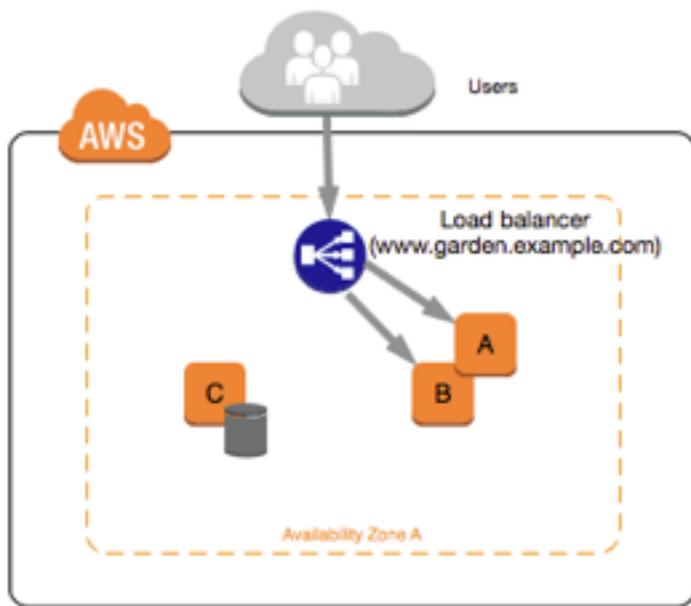
在您的默认 VPC 内启动 实例

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。

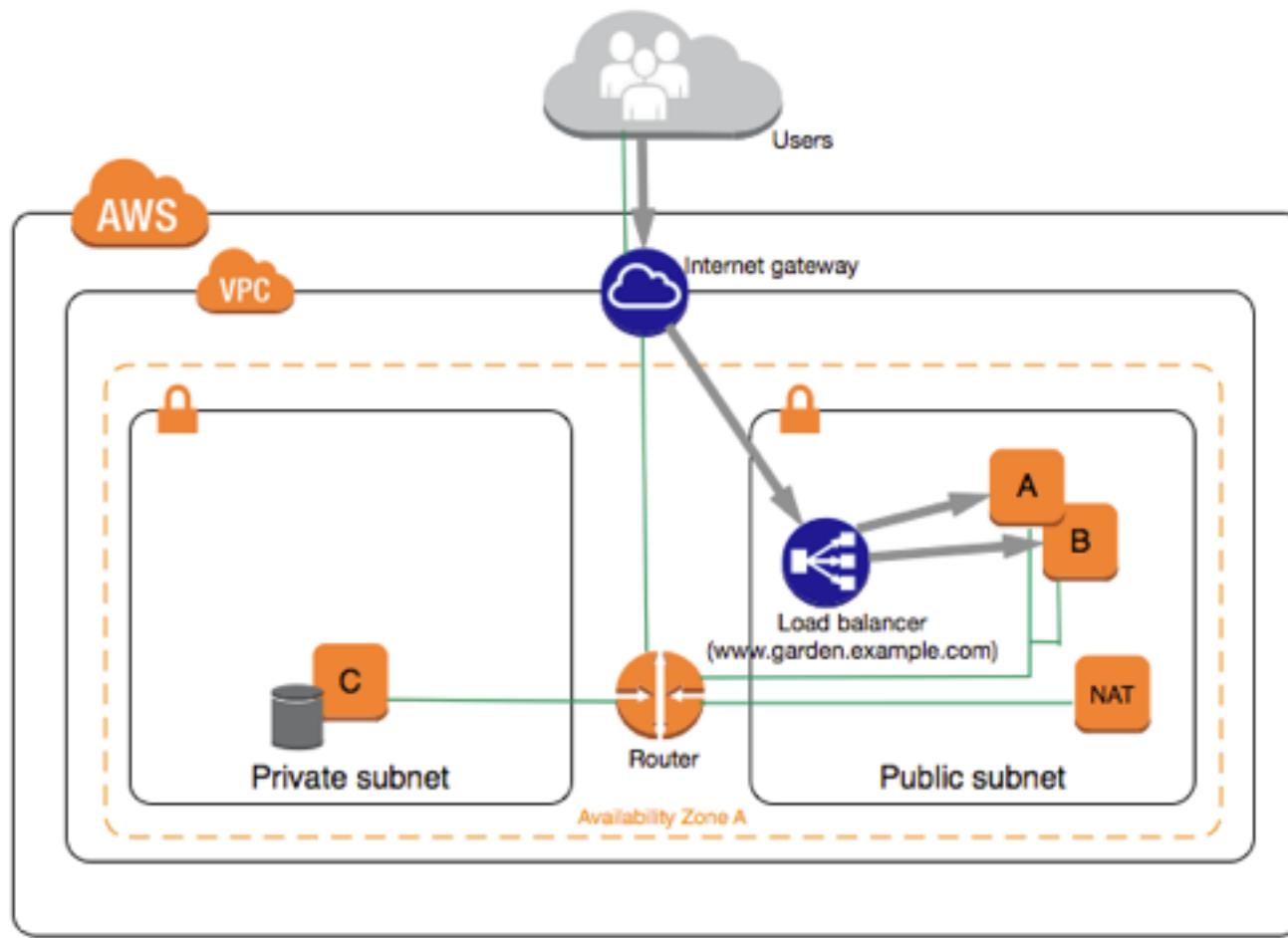
有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#)。

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，Elastic Load Balancing 用于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 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。在此情况下，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。将弹性 IP 地址迁移到 VPC，并在公有子网中创建负载均衡器来对 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 \(p. 690\)](#)。
- 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 \(p. 690\)](#)。

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 \(p. 691\)](#)。
- 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 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[从 EC2-Classic 迁移弹性 IP 地址 \(p. 676\)](#)。
- **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 Route 53 中的别名记录集。有关使用 Route 53 的更多信息，请参阅[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，从而允许您的新 VPC 资源使用私有 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 \(p. 678\)](#)。

主题

- [步骤 1：准备迁移序列 \(p. 695\)](#)
- [步骤 2：创建 VPC \(p. 695\)](#)
- [步骤 3：为 VPC 启用 ClassicLink \(p. 696\)](#)
- [步骤 4：从您的 EC2-Classic 实例创建 AMI \(p. 696\)](#)
- [步骤 5：在 VPC 中启动实例 \(p. 697\)](#)
- [步骤 6：将 EC2-Classic 实例链接到 VPC \(p. 697\)](#)
- [步骤 7：完成 VPC 迁移 \(p. 698\)](#)

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，请使用该选项。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)，请使用该选项。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 \(p. 678\)](#)。

为 VPC 启用 ClassicLink

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Your VPCs。
- 选择您的 VPC，然后从 Actions 列表中选择 Enable ClassicLink。
- 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 (描述) 选项卡上的 Root device type (根设备类型) 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 \(p. 87\)](#)。

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. 102) 。
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. 105) 。
实例存储	将由实例存储支持的实例转换为由 EBS 支持的实例。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. 115) 。

(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 — 如同使用物理硬盘一样。Amazon EBS 卷可以与同一可用区中的任何实例附加和分离。您可以将卷与 EC2-Classic 中实例分离，并将它附加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 \(p. 783\)](#)
- [创建 Amazon EBS 卷 \(p. 798\)](#)
- [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)

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 \(p. 812\)](#)
- [创建 Amazon EBS 快照 \(p. 815\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 799\)](#)

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[使用启动实例向导启动实例 \(p. 375\)](#)。

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 VPC。有关更多信息，请参阅[从 EC2-Classic 迁移弹性 IP 地址 \(p. 676\)](#)。

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 中的安全性

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 [AWS 合规性计划](#) 的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 Amazon EC2 的合规性计划，请参阅[合规性计划范围内的 AWS 服务](#)。
- 云中的安全性 – 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon EC2 时应用责任共担模式。它说明了如何配置 Amazon EC2 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Amazon EC2 资源。

目录

- [Amazon EC2 中的基础设施安全性 \(p. 699\)](#)
- [Amazon EC2 中的恢复功能 \(p. 700\)](#)
- [Amazon EC2 中的数据保护 \(p. 701\)](#)
- [适用于 Amazon EC2 的 Identity and Access Management \(p. 701\)](#)
- [Amazon EC2 密钥对 \(p. 759\)](#)
- [Linux 实例的 Amazon EC2 安全组 \(p. 768\)](#)
- [Amazon EC2 中的更新管理 \(p. 780\)](#)
- [Amazon EC2 的合规性验证 \(p. 780\)](#)

Amazon EC2 中的基础设施安全性

作为一项托管服务，Amazon EC2 由 [Amazon Web Services：安全流程概述](#) 白皮书中所述的 AWS 全球网络安全流程提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Amazon EC2。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

网络隔离

Virtual Private Cloud (VPC) 是 AWS 云上您自己的逻辑隔离区域中的虚拟网络。可以使用单独的 VPC 按工作负载或组织实体隔离基础设施。

子网是 VPC 中的 IP 地址范围。在启动实例时，您可以在 VPC 上的子网中启动该实例。可以使用子网隔离单个 VPC 中的应用程序层（例如，Web、应用程序和数据库）。如果不应直接从 Internet 访问实例，请使用私有子网访问。

要从 VPC 中调用 Amazon EC2 API 而不通过公有 Internet 发送流量，请使用 AWS PrivateLink。

物理主机上的隔离

同一物理主机上的不同 EC2 实例彼此隔离，就好像它们位于不同的物理主机上一样。管理程序隔离 CPU 和内存，并为实例提供虚拟化磁盘，而不是访问原始磁盘设备。

在停止或终止实例时，管理程序将清理分配给实例的内存（设置为零），然后再将内存分配给新实例并重置每个存储块。这会确保不会意外向另一个实例泄露数据。

网络 MAC 地址由 AWS 网络基础设施动态分配给实例。IP 地址由 AWS 网络基础设施动态分配给实例，或者由 EC2 管理员通过经过身份验证的 API 请求进行分配。AWS 网络允许实例仅从分配给它们的 MAC 和 IP 地址发送流量。否则，将会丢弃流量。

默认情况下，实例无法接收未明确将其指定为目标地址的流量。如果需要在实例上运行网络地址转换 (NAT)、路由或防火墙服务，您可以为网络接口禁用源/目标检查。

控制网络流量

请考虑使用以下方法来控制到 EC2 实例的网络流量：

- 使用[安全组 \(p. 768\)](#)限制实例访问。例如，您可以仅允许来自公司网络地址范围的流量。
- 如果不应直接从 Internet 访问实例，请使用私有子网访问。使用堡垒主机或 NAT 网关从私有子网中的实例进行 Internet 访问。
- 使用 AWS Virtual Private Network 或 AWS Direct Connect 建立从远程网络到 VPC 的私有连接。有关更多信息，请参阅[网络到 Amazon VPC 的连接选项](#)。
- 使用[VPC Flow Logs](#) 监控到达实例的流量。
- 使用[AWS Security Hub](#) 检查来自实例的意外网络访问。
- 使用[EC2 Instance Connect \(p. 428\)](#) 通过安全 Shell (SSH) 连接到实例，而无需共享和管理 SSH 密钥。
- 使用[AWS Systems Manager 会话管理器](#)远程访问实例，而不是打开入站 SSH 端口和管理 SSH 密钥。
- 使用[AWS Systems Manager Run Command](#) 自动执行常见的管理任务，而不是打开入站 SSH 端口和管理 SSH 密钥。

除了限制对每个 Amazon EC2 实例的网络访问之外，Amazon VPC 还支持实施额外的网络安全控制，如内联网关、代理服务器和各种网络监控选项。

有关更多信息，请参阅[保护 Amazon EC2 实例](#)。

Amazon EC2 中的恢复功能

AWS 全球基础设施围绕 AWS 区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

除了 AWS 全球基础设施以外，Amazon EC2 还提供以下功能以支持数据恢复：

- 跨区域复制 AMI
- 跨区域复制 EBS 快照
- 使用 Amazon 数据生命周期管理器 自动处理 EBS 快照
- 使用 Amazon EC2 Auto Scaling 保持队列的运行状况和可用性

- 使用 Elastic Load Balancing 在一个或多个可用区中的多个实例之间分配传入流量

Amazon EC2 中的数据保护

Amazon Elastic Compute Cloud (Amazon EC2) 符合 AWS [责任共担模式](#)，该模型包含适用于数据保护的法规和准则。AWS 负责保护运行所有 AWS 服务的全球基础设施。AWS 保持对该基础设施上托管的数据的控制，包括用于处理客户内容和个人数据的安全配置控制。作为数据控制者或数据处理者，AWS 客户和 APN 合作伙伴对他们放在 AWS 云中的任何个人数据承担责任。

出于数据保护的目的，我们建议您保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置单个用户账户，以便仅向每个用户提供履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 TLS 与 AWS 资源进行通信。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段或元数据（例如函数名称和标签）。可能会选取您输入到元数据的任何数据以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

有关数据保护的更多信息，请参阅 AWS 安全性博客上的 [AWS 责任共担模式和 GDPR 博客文章](#)。

静态加密

Amazon EBS 加密是适用于 EBS 卷和快照的加密解决方案。它使用 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK)。有关更多信息，请参阅[Amazon EBS Encryption \(p. 851\)](#)。

NVMe 实例存储卷上的数据是使用实例上的硬件模块中实施的 XTS-AES-256 密码加密的。加密密钥是使用硬件模块生成的，并且对每台 NVMe 实例存储设备都是唯一的。当实例停止或终止并且无法恢复时，将销毁所有加密密钥。无法禁用此加密，并且无法提供自己的加密密钥。

传输中加密

AWS 在 EC2 实例之间提供安全的私有连接。此外，我们会将 AEAD 算法与 256 位加密技术一起使用，以便自动对同一 VPC 或对等 VPC 中支持实例之间的传输中流量进行加密。此加密功能将使用基础硬件的分载功能，对网络性能不会造成影响。支持的实例包括：C5n、G4、I3en、M5dn、M5n、P3dn、R5dn 和 R5n。

SSH 提供了用于远程访问 Linux 实例的安全通信通道。使用 AWS Systems Manager 会话管理器和 Run Command 对实例的远程访问是使用 TLS 1.2 加密的，创建连接的请求是使用 SigV4 签名的。

可以使用传输层安全性 (TLS) 等加密协议加密在客户端和实例之间传输的敏感数据。

适用于 Amazon EC2 的 Identity and Access Management

您的安全凭证使 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。

目录

- [网络访问您的实例 \(p. 702\)](#)
- [Amazon EC2 权限属性 \(p. 702\)](#)
- [IAM 和 Amazon EC2 \(p. 702\)](#)
- [Amazon EC2 的 IAM 策略 \(p. 704\)](#)
- [适用于 Amazon EC2 的 IAM 角色 \(p. 749\)](#)
- [为您的 Linux 实例授权入站流量 \(p. 757\)](#)

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 \(p. 757\)](#)。

Amazon EC2 权限属性

您的组织可能有多个 AWS 账户。借助 Amazon EC2，您可以指定能够使用您的 Amazon 系统映像 (AMI) 和 Amazon EBS 快照的其他 AWS 账户。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 \(p. 92\)](#)。

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 \(p. 822\)](#)。

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凭证
- 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. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
3. 对于 Group Name (组名称)，为您的组键入一个名称，然后选择 Next Step (下一步)。
4. 在 Attach Policy (附加策略) 页面上，选择 AWS 托管策略，然后选择 Next Step (下一步)。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 Create Group。

您的新组列在 Group Name 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. 对于 User name (用户名)，请输入用户名。
3. 对于 Access type (访问类型)，选择 Programmatic access (编程访问) 和 AWS 管理控制台 access (控制台访问)。
4. 对于 Console password (控制台密码)，选择下列选项之一：
 - 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输入的密码。
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。选中您之前创建的组旁边的复选框，然后选择 Next: Review。
7. 选择 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。

Important

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 \(p. 704\)](#)
- [适用于 Amazon EC2 的 IAM 角色 \(p. 749\)](#)
- [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。

在将策略附加到一个用户或一组用户时，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，您无法指定用户可用于该操作的资源。相反，您必须允许用户将所有资源用于该操作。

任务	主题
了解策略的基本结构	策略语法 (p. 704)
在策略中定义操作	Amazon EC2 操作 (p. 705)
在策略中定义特定资源	适用于 Amazon EC2 的 Amazon 资源名称 (p. 705)
将条件应用于资源的使用	Amazon EC2 的条件键 (p. 708)
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. 712)
测试策略	检查用户是否具有所需权限 (p. 712)
针对 CLI 或软件开发工具包的策略示例	使用 AWS CLI 或 AWS SDK 的策略示例 (p. 714)
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. 742)

策略结构

以下主题说明 IAM 策略的结构。

目录

- [策略语法 \(p. 704\)](#)
- [Amazon EC2 操作 \(p. 705\)](#)
- [适用于 Amazon EC2 的 Amazon 资源名称 \(p. 705\)](#)
- [Amazon EC2 的条件键 \(p. 708\)](#)
- [检查用户是否具有所需权限 \(p. 712\)](#)

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": "Resource"  
    }  
  ]  
}
```

```
"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 \(p. 705\)](#)。
- Resource：受操作影响的资源。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 \(p. 705\)](#)。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 \(p. 712\)](#)。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 的条件键 \(p. 708\)](#)。

有关 Amazon EC2 的示例 IAM 策略语句的更多信息，请参阅 [使用 AWS CLI 或 AWS SDK 的策略示例 \(p. 714\)](#)。

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，并非所有 API 操作都支持各个 ARN。我们将在以后添加对其他 API 操作的支持和其他 Amazon EC2 资源的 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 \(p. 712\)](#)。

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)。

account

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>
指定账户在指定区域拥有的所有 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 cgw-id 是 cgw-xxxxxxxx
DHCP 选项集	<code>arn:aws:ec2:region:account:dhcp-options/dhcp-options-id</code> 其中 dhcp-options-id 是 dopt-xxxxxxxx
Elastic GPU	<code>arn:aws:ec2:region:account:elastic-gpu/*</code>
映像	<code>arn:aws:ec2:region::image/image-id</code> 其中 image-id 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，instance-id 是 i-xxxxxxxx 或 i-xxxxxxxxxxxxxxxxxxxx

资源类型	ARN
实例配置文件	arn:aws:iam::account:instance-profile/instance-profile-name 其中 instance-profile-name 是实例配置文件的名称，而不使用 region
Internet 网关	arn:aws:ec2:region:account:internet-gateway/igw-id 其中 igw-id 是 igw-xxxxxxxx
密钥对	arn:aws:ec2:region:account:key-pair/key-pair-name 其中 key-pair-name 是密钥对名称（例如，gsg-keypair）
启动模板	arn:aws:ec2:region:account:launch-template/launch-template-id 其中 launch-template-id 是 lt-xxxxxxxxxxxxxxxxxx
NAT 网关	arn:aws:ec2:region:account:natgateway/natgateway-id 其中 natgateway-id 是 nat-xxxxxxxxxxxxxxxxxx
网络 ACL	arn:aws:ec2:region:account:network-acl/nacl-id 其中 nacl-id 是 acl-xxxxxxxx
网络接口	arn:aws:ec2:region:account:network-interface/eni-id 其中 eni-id 是 eni-xxxxxxxx
置放群组	arn:aws:ec2:region:account:placement-group/placement-group-name 其中 placement-group-name 是置放群组名称（例如，my-cluster）
Reserved Instance	arn:aws:ec2:region:account:reserved-instances/reservation-id 其中，reservation-id 为 xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
路由表	arn:aws:ec2:region:account:route-table/route-table-id 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
Spot 实例请求	arn:aws:ec2:region:account:spot-instances-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

资源类型	ARN
Volume	arn:aws:ec2:region:account:volume/volume-id 其中，volume-id 是 vol-xxxxxxxx 或 vol-xxxxxxxxxxxxxxxxxxxx
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 卷附加到一个实例，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个资源，请使用逗号分隔其 ARN，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](#)。

Amazon EC2 的条件键

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键值对。条件键不区分大小写。我们已经定义了 AWS 范围内的条件键以及其他特定于服务的条件键。

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。必须满足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

许多条件键是特定于某个资源的，而某些 API 操作会使用多个资源。如果您使用条件键编写策略，请使用语句的 `Resource` 元素指定要应用该条件键的资源。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键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键的资源忽略条件键。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。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 \(p. 712\)](#)。

条件键	键值对	评估类型
ec2:AccepterVpc	"ec2:AccepterVpc":"vpc-arn" 其中，vpc-arn 是 VPC 对等连接中接受方 VPC 的 VPC ARN	ARN , Null
ec2:AuthorizedService	"ec2:AuthorizedService":"service-principal" 其中 service-principal 为服务委托方 (例如，ecs.amazonaws.com)	字符串 , Null
ec2:AuthorizedUser	"ec2:AuthorizedUser":"principal-arn" 其中 principal-arn 是委托人的 ARN (例如，arn:aws:iam::123456789012:root)	ARN , Null
ec2:AvailabilityZone	"ec2:AvailabilityZone":"az-api-name" 其中 az-api-name 是可用区的名称 (例如，us-east-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:ElasticGpuType	"ec2:ElasticGpuType":"elastic-gpu-type" 其中，elastic-gpu-type 是 Elastic GPU 类型的名称	字符串 , Null
ec2:Encrypted	"ec2:Encrypted":"encrypted-flag" 其中 encrypted-flag 是 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 machine aki ari	字符串 , Null
ec2:InstanceMarketType	"ec2:InstanceMarketType":"market-type" 其中 market-type 为 spot on-demand	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:IsLaunchTemplateResource	"ec2:IsLaunchTemplateResource":"launch-template-resource-flag" 其中 launch-template-resource-flag 是 true false	布尔值 , Null
ec2:LaunchTemplate	"ec2:LaunchTemplate":"launch-template-arn"	ARN , Null

条件键	键值对	评估类型
	其中 launch-template-arn 是启动模板 ARN	
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
ec2:ParentVolume	"ec2:ParentVolume":"volume-arn" 其中 volume-arn 是卷 ARN	ARN , Null
ec2:Permission	"ec2:Permission":"permission" 其中 permission 是 INSTANCE-ATTACH EIP-ASSOCIATE	字符串 , 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 spread	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-east-2)。要列出您的区域, 请使用 describe-regions 。此条件键可用于所有 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:ReservedInstancesOfferingType	"ec2:ReservedInstancesOfferingType":"offering-type" 其中 offering-type 是 No Upfront Partial Upfront All Upfront	字符串 , Null
ec2:ResourceTag	"/"ec2:ResourceTag/tag-key":"tag-value" 其中 tag-key 和 tag-value 是标签密钥对	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

条件键	键值对	评估类型
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)。有关更多信息 , 请参阅 Amazon EBS 卷类型 (p. 785) 。	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
ec2:VolumeType	"ec2:VolumeType":"volume-type-name" 其中 , volume-type-name 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。	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 范围的条件键。有关更多信息 , 请参阅IAM 用户指南中的[在所有请求中可用的信息](#)。

所有 Amazon EC2 操作都支持 aws:RequestedRegion 和 ec2:Region 条件键。有关更多信息 , 请参阅[示例 : 限制对特定区域的访问 \(p. 715\)](#)。

ec2:SourceInstanceARN 键可用于指定作为请求源的实例的 ARN 的条件。此条件键在 AWS 范围内可用 , 并不特定于服务。有关策略示例 , 请参阅[允许 EC2 实例附加或分离卷](#)和[示例 : 允许特定实例查看其他 AWS 服务中的资源 \(p. 739\)](#)。ec2:SourceInstanceARN 键不能用作变量来填充语句中 Resource 元素的 ARN。

以下 AWS 条件键是针对 Amazon EC2 引入的 , 只有有限数量的额外服务支持它们。

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

有关适用于 Amazon EC2 的策略语句示例，请参阅 [使用 AWS CLI 或 AWS SDK 的策略示例 \(p. 714\)](#)。

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 CLI Command Reference 中的 `decode-authorization-message`。

Amazon EC2 API 操作支持的资源级权限

资源级权限是指指定允许用户对哪些资源执行操作的能力。Amazon EC2 对资源级权限提供部分支持。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。

如果 Amazon EC2 API 操作不支持资源级权限，那么，您可以为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 Amazon EC2 操作创建或修改的资源以及可以在 IAM 策略语句中使用的 ARN 和 Amazon EC2 条件键的更多信息，请参阅 IAM 用户指南中的 [Amazon EC2 的操作、资源和条件键](#)。

有关更多信息和示例策略，请参阅 Amazon EC2 用户指南中的 [Amazon EC2 的 IAM 策略](#)。

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 [标记资源 \(p. 942\)](#)。

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": {  
            "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。

如果在启动模板中提供了标签，并在 ec2:CreateTags 操作中指定了启动模板，则还会评估 ec2:RunInstances 操作。有关策略示例，请参阅[启动模板中的标签 \(p. 733\)](#)。

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键和值组合，例如强制实施标签 `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 条件键或 aws:TagKeys 条件键，并在资源创建操作中使用修饰符 ForAnyValue。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。

对于条件，条件键不区分大小写，条件值区分大小写。因此，要强制标签键区分大小写，请使用 aws:TagKeys 条件键，其中标签键指定为条件中的值。

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[使用 AWS CLI 或 AWS SDK 的策略示例 \(p. 714\)](#)。

使用 AWS CLI 或 AWS SDK 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 \(p. 742\)](#)。有关特定于 Amazon VPC 的 IAM 策略，请参阅[控制对 Amazon VPC 资源的访问](#)。

示例

- [示例：只读访问权限 \(p. 715\)](#)
- [示例：限制对特定区域的访问 \(p. 715\)](#)
- [使用实例 \(p. 716\)](#)
- [使用卷 \(p. 717\)](#)
- [使用快照 \(p. 719\)](#)
- [启动实例 \(RunInstances\) \(p. 726\)](#)
- [示例：使用预留实例 \(p. 736\)](#)
- [示例：标记资源 \(p. 736\)](#)
- [示例：使用 IAM 角色 \(p. 738\)](#)
- [示例：使用路由表 \(p. 739\)](#)
- [示例：允许特定实例查看其他 AWS 服务中的资源 \(p. 739\)](#)
- [示例：使用启动模板 \(p. 740\)](#)
- [示例：使用实例元数据 \(p. 741\)](#)

示例：只读访问权限

以下策略为用户授予使用名称以 `Describe` 开头的所有 Amazon EC2 API 操作的权限。`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 \(p. 712\)](#)。

用户无权对资源执行任何操作（除非其他语句为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": "*"  
        }  
    ]  
}
```

示例：限制对特定区域的访问

以下策略拒绝用户使用所有 Amazon EC2 API 操作的权限，除非区域为欧洲（法兰克福）。该区域使用全局条件键 `aws:RequestedRegion`，所有 Amazon EC2 API 操作均支持此条件键。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "aws:RequestedRegion": "eu-central-1"  
                }  
            }  
        }  
    ]  
}
```

或者，您也可以使用条件键 `ec2:Region`，此条件键是 Amazon EC2 特定的，所有 Amazon EC2 API 操作均支持它。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "ec2:Region": "eu-central-1"  
                }  
            }  
        }  
    ]  
}
```

使用实例

示例

- [示例：描述、启动、停止和终止所有实例 \(p. 716\)](#)
- [示例：描述所有实例，以及仅停止、启动和终止特定实例 \(p. 716\)](#)

示例：描述、启动、停止和终止所有实例

以下策略为用户授予使用 Action 元素中指定的 API 操作的权限。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 \(p. 712\)](#)。

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": "*"  
        }  
    ]  
}
```

示例：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在操作中指定所有资源；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 \(p. 712\)](#)。

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-1:1234567890123456:instance/i-0598c7d356eba48d7"  
        }  
    ]  
}
```

```
    "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"
        }
    }
}
]
```

使用卷

示例

- [示例：附加和分离卷 \(p. 717\)](#)
- [示例：创建卷 \(p. 718\)](#)
- [示例：创建具有标签的卷 \(p. 718\)](#)

示例：附加和分离卷

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": "iam-user-name"
                }
            }
        }
    ]
}
```

```
        "StringEquals": {
            "ec2:ResourceTag/volume_user": "${aws:username}"
        }
    }
}
]
```

示例：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"
                }
            }
        ]
    ]
}
```

示例：创建具有标签的卷

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，用户还必须具有使用 `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[用于标记的资源级权限 \(p. 712\)](#)。

```
{
    "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"]
                }
            }
        },
        {
            "Sid": "AllowCreateTags",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*"
        }
    ]
}
```

```
"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 CreateTags 请求中指定了标签时，系统才会评估 CreateVolume 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"
                }
            }
        }
    ]
}
```

使用快照

以下是 CreateSnapshot (EBS 卷的时间点快照) 和 CreateSnapshots (多卷快照) 的示例策略。

示例

- [示例：创建快照 \(p. 719\)](#)
- [示例：创建快照 \(p. 720\)](#)
- [示例：创建具有标签的快照 \(p. 720\)](#)
- [示例：创建具有标签的快照 \(p. 721\)](#)
- [示例：修改快照的权限设置 \(p. 726\)](#)

示例：创建快照

以下策略允许客户使用 CreateSnapshot API 操作。仅当卷已加密并且卷大小不超过 20 GiB 时，客户才能创建快照。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "NumericLessThan": {  
                    "ec2:VolumeSize": "20"  
                },  
                "Bool": {  
                    "ec2:Encrypted": "true"  
                }  
            }  
        }  
    ]  
}
```

示例：创建快照

以下策略允许客户使用 [CreateSnapshots](#) API 操作。仅当实例上的所有卷均为类型 GP2 时，客户才能创建快照。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshots",  
            "Resource": [  
                "arn:aws:ec2:us-east-1::snapshot/*",  
                "arn:aws:ec2:/*:*:instance/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshots",  
            "Resource": "arn:aws:ec2:us-east-1:/*:volume/*",  
            "Condition": {  
                "StringLikeIfExists": {  
                    "ec2:VolumeType": "gp2"  
                }  
            }  
        }  
    ]  
}
```

示例：创建具有标签的快照

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求客户将标签 `costcenter=115` 和 `stack=prod` 应用于任何新快照。`aws:TagKeys` 条件键使用 `ForAllValues` 修饰符指示只能在请求中指定键 `costcenter` 和 `stack`。如果不满足其中任一条件，则请求将失败。

对于应用标签的资源创建操作，客户还必须具有使用 `CreateTags` 操作的权限。第三个语句使用 `ec2:CreateAction` 条件键使客户只能在 `CreateSnapshot` 上下文中创建标签。客户无法标记现有卷或任何其他资源。有关更多信息，请参阅[用于标记的资源级权限](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*"  
        },  
        {  
            "Sid": "AllowCreateTaggedSnapshots",  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "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::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction": "CreateSnapshot"  
                }  
            }  
        }  
    ]  
}
```

示例：创建具有标签的快照

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求客户将标签 `costcenter=115` 和 `stack=prod` 应用于任何新快照。`aws:TagKeys` 条件键使用 `ForAllValues` 修饰符指示只能在请求中指定键 `costcenter` 和 `stack`。如果不满足其中任一条件，则请求将失败。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSchedules",  
            "Resource": [  
                "arn:aws:ec2:us-east-1::snapshot/*",  
                "arn:aws:ec2:/*:instance/*",  
                "arn:aws:ec2:/*:volume/*"  
            ]  
        },  
        {  
            "Sid": "AllowCreateTaggedSnapshots",  
            "Effect": "Allow",  
            "Action": "ec2:CreateSchedules",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/costcenter": "115",  
                    "aws:RequestTag/stack": "prod"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": [  
                        "costcenter",  
                        "stack"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```
"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::snapshot/*",  
    "Condition": {  
        "StringEquals": {  
            "ec2:CreateAction": "CreateSnapshot"  
        }  
    }  
}  
]  
}
```

下面的策略允许客户创建快照而无需指定标签。仅在 CreateSnapshot 或 CreateSnapshots 请求中指定标签的情况下，系统才会评估 CreateTags 操作。如果指定一个标签，则该标签必须是 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:CreateSnapshot",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/purpose": "test",  
                    "ec2:CreateAction": "CreateSnapshot"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": "purpose"  
                }  
            }  
        }  
    ]  
}
```

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshots",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "*"  
        }  
    ]  
}
```

```
"Effect": "Allow",
"Action": "ec2:CreateTags",
"Resource": "arn:aws:ec2:us-east-1::snapshot/*",
"Condition": {
    "StringEquals": {
        "aws:RequestTag/purpose": "test",
        "ec2:CreateAction": "CreateSnapshots"
    },
    "ForAllValues:StringEquals": {
        "aws:TagKeys": "purpose"
    }
}
]
```

以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。客户可向快照添加其他标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/User": "${aws:username}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Environment": "Dev",
                    "aws:RequestTag/User": "${aws:username}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
        }
    ]
}
```

CreateSnapshots 的以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1:/*:instance/*",
        }
    ]
}
```

```
"Effect": "Allow",
"Action": "ec2:CreateSnapshots",
"Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
"Condition": {
    "StringEquals": {
        "ec2:ResourceTag/User": "${aws:username}"
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshots",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Environment": "Dev",
            "aws:RequestTag/User": "${aws:username}"
        }
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
}
]
```

以下策略仅允许在以下情况下删除快照：快照已使用客户的 User:username 进行标记。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2>DeleteSnapshot",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/User": "${aws:username}"
                }
            }
        }
    ]
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2>CreateSnapshot",
                "ec2>CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2>CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Value": "stack"
                }
            }
        }
    ]
}
```

```
        "Condition":{  
            "ForAnyValue:StringEquals":{  
                "aws:TagKeys":"stack"  
            }  
        }  
    }  
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 `value=stack` 时拒绝操作。

```
{  
    "Version":"2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateSnapshots",  
                "ec2:CreateTags"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "ec2:CreateSnapshots",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition":{  
                "ForAnyValue:StringEquals":{  
                    "aws:TagKeys":"stack"  
                }  
            }  
        }  
    ]  
}
```

以下策略允许您将多个操作整合到单个策略中。您只能在快照在区域 `us-east-1` 中创建快照（在 `CreateSnapshots` 的上下文稿中）。您只能在快照正在区域 `us-east-1` 中创建时且实例类型为 `t2*` 时创建快照（在 `CreateSnapshots` 的上下文中）。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateSnapshots",  
                "ec2:CreateSnapshot",  
                "ec2:CreateTags"  
            ],  
            "Resource": [  
                "arn:aws:ec2:*:*:instance/*",  
                "arn:aws:ec2:*:*:snapshot/*",  
                "arn:aws:ec2:*:*:volume/*"  
            ],  
            "Condition":{  
                "StringEqualsIgnoreCase": {  
                    "ec2:Region": "us-east-1"  
                },  
                "StringLikeIfExists": {  
                    "ec2:InstanceType": [  
                        "t2.*"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

示例：修改快照的权限设置

以下策略仅允许在以下情况下修改快照：快照已使用 User:`username` 标记，其中 `username` 是客户的 AWS 账户用户名。如果未满足此条件，则请求将失败。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2: ModifySnapshotAttribute",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/user-name": "${aws:username}"
                }
            }
        }
    ]
}
```

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 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，用户必须具有使用这些 Amazon EC2 资源的权限。您可以创建要求用户对 RunInstances 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。

有关启动实例所需的资源级权限的更多信息，请参阅 IAM 用户指南 中的 [Amazon EC2 的操作、资源和条件键](#)。

默认情况下，用户没有描述、启动、停止或终止生成的实例的权限。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 [使用实例 \(p. 716\)](#)。

资源

- [AMI \(p. 726\)](#)
- [实例类型 \(p. 727\)](#)
- [子网 \(p. 728\)](#)
- [EBS 卷 \(p. 729\)](#)
- [标签 \(p. 730\)](#)
- [启动模板中的标签 \(p. 733\)](#)
- [Elastic GPUs \(p. 733\)](#)
- [启动模板 \(p. 734\)](#)

AMI

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（除非其他语句允许用户执行此操作）。

```
{
```

```
"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/*",
            "arn:aws:ec2:region:account:subnet/*",
            "arn:aws:ec2:region:account:network-interface/*"
        ]
    }
]
```

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)。

```
{
    "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，您也可以创建一个策略，以拒绝用户启动 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)。

```
{
  "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::image/ami-*",
    "arn:aws:ec2:region:account:key-pair/*",
    "arn:aws:ec2:region:account:security-group/*"
]
}
]
```

或者，您也可以创建一个策略，以拒绝用户将实例启动到任何其他子网的权限。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。

```
{
    "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，用户在启动期间附加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::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/*"
    ]
}
}
```

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，用户必须具有使用 `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 \(p. 712\)](#)。

```
{
    "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 `RunInstances` 和 `environment=production` 通过 `purpose=webserver` 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 `ForAnyValue` 条件使用了 `aws:TagKeys` 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:network-interface/*",  
                "arn:aws:ec2:region:account:security-group/*",  
                "arn:aws:ec2:region:account:key-pair/*"  
            ]  
        }  
    ]  
}
```

```
        "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"
                }
            }
        }
    ]
}
```

启动模板中的标签

在以下示例中，用户可以启动实例，但前提是他们使用特定的启动模板 (lt-09477bcd97b0d310e)。ec2:IsLaunchTemplateResource 条件键禁止用户覆盖在启动模板中指定的任何资源。语句的第二部分允许用户在创建时标记实例 — 如果在启动模板中为实例指定了标签，则该语句部分是必需的。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": "*",  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/  
lt-09477bcd97b0d310e"  
                },  
                "Bool": {  
                    "ec2:IsLaunchTemplateResource": "true"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:region:account:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2>CreateAction" : "RunInstances"  
                }  
            }  
        }  
    ]  
}
```

Elastic GPUs

在以下策略中，用户可以启动实例并指定要附加到实例的 Elastic GPU。用户可以在任何区域中启动实例，但他们只能在 us-east-2 区域中启动期间附加 Elastic GPU。

ec2:ElasticGpuType 条件键使用 ForAnyValue 修饰符指示只允许在请求中使用 Elastic GPU 类型 eg1.medium 和 eg1.large。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:*:account:elastic-gpu/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-2"  
                },  
                "ForAnyValue:StringLike": {  
                    "ec2:ElasticGpuType": "eg1.medium",  
                    "ec2:ElasticGpuType": "eg1.large"  
                }  
            }  
        }  
    ]  
}
```

```
"ec2:ElasticGpuType": [
    "eg1.medium",
    "eg1.large"
]
}
},
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2::::image/ami-*",
        "arn:aws:ec2::::account:network-interface/*",
        "arn:aws:ec2::::account:instance/*",
        "arn:aws:ec2::::account:subnet/*",
        "arn:aws:ec2::::account:volume/*",
        "arn:aws:ec2::::account:key-pair/*",
        "arn:aws:ec2::::account:security-group/*"
    ]
}
]
```

启动模板

在以下示例中，用户可以启动实例，但前提是他们使用特定的启动模板 (lt-09477bcd97b0d310e)。用户可以在 RunInstances 操作中指定参数以覆盖启动模板中的任何参数。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/
lt-09477bcd97b0d310e"
                }
            }
        }
    ]
}
```

在该示例中，只有在用户使用启动模板时，他们才能启动实例。该策略使用 `ec2:IsLaunchTemplateResource` 条件键禁止用户覆盖 RunInstances 请求中的任何启动模板资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"
                },
                "Bool": {
                    "ec2:IsLaunchTemplateResource": "true"
                }
            }
        }
    ]
}
```

```
        }
    ]  
}
```

以下示例策略允许用户启动实例，但前提是他们使用启动模板。用户无法覆盖请求中的子网和网络接口参数；只能在启动模板中指定这些参数。语句的第一部分使用 [NotResource](#) 元素允许子网和网络接口以外的所有其他资源。语句的第二部分允许子网和网络接口资源，但前提是它们来自于启动模板。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": [ "arn:aws:ec2:region:account:subnet/*",
                      "arn:aws:ec2:region:account:network-interface/*" ],
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [ "arn:aws:ec2:region:account:subnet/*",
                    "arn:aws:ec2:region:account:network-interface/*" ],
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    }
  ]
}
```

以下示例允许用户启动实例，但前提是他们使用启动模板，并且启动模板具有标签 [Purpose=Webservers](#)。用户无法覆盖 RunInstances 操作中的任何启动模板参数。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account:launch-template/*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account:launch-template/*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    }
  ]
}
```

```
        "StringEquals": {
            "ec2:ResourceTag/Purpose": "Webservers"
        }
    }
}
```

示例：使用 预留实例

下面的策略向用户授予在账户中查看、修改和购买预留实例的权限。

无法为个别的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 * 通配符指示用户可以在操作中指定所有资源；在本例中，他们可以列出并修改账户中的所有 预留实例。他们还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": "*"
        }
    ]
}
```

要允许用户查看和修改账户中的 预留实例，但不允许购买新的 预留实例，请使用以下命令：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        }
    ]
}
```

示例：标记资源

仅当标签包含键 CreateTags 和值 environment 时，下面的策略才允许用户使用 production 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": {
            "aws:RequestTag/environment": "production"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "environment"
            ]
        }
    }
}
]
```

以下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 environment、值为 test 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。用户不需要使用 ec2:DeleteTags 操作删除具有标签的资源的权限，他们仅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": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": ["environment", "cost-center"]
                }
            }
        }
    ]
}
```

}

该策略仅允许用户删除任何资源上的 environment=prod 标签，但前提是已使用键为 owner、值为 IAM 用户名的标签标记该资源。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"]  
                }  
            }  
        }  
    ]  
}
```

示例：使用 IAM 角色

以下策略允许用户将 IAM 角色附加、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，因此该策略还授予用户使用 ec2:DescribeIamInstanceProfileAssociations 操作的权限。

IAM 用户必须具有使用 iam:PassRole 操作的权限，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附加或替换 IAM 角色。用户只能附加或替换名称以 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 \(p. 750\)](#)。

```
{  
    "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-*"  
        }  
    ]  
}
```

示例：使用路由表

以下策略允许用户添加、删除和替换仅与 VPC vpc-ec43eb89 关联的路由表的路由。要为 ec2:vpc 条件键指定 VPC，必须指定 VPC 的完整 ARN。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DeleteRoute",  
                "ec2>CreateRoute",  
                "ec2:ReplaceRoute"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region:account:route-table/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-ec43eb89"  
                }  
            }  
        }  
    ]  
}
```

示例：允许特定实例查看其他 AWS 服务中的资源

下面是您可能附加到 IAM 角色的策略的示例。该策略允许实例查看不同 AWS 服务中的资源。它使用 ec2:SourceInstanceARN 条件键指定从中发出请求的实例必须是实例 i-093452212644b0dd6。如果同一个 IAM 角色还与另一个实例关联，则另一个实例无法执行任何这些操作。

ec2:SourceInstanceARN 键是一个 AWS 范围的条件键，因此可用于其他服务操作，而不仅仅是 Amazon EC2。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeVolumes",  
                "s3>ListAllMyBuckets",  
                "dynamodb>ListTables",  
                "rds:DescribeDBInstances"  
            ],  
            "Resource": [  
                "*"  
            ],  
            "Condition": {  
                "ArnEquals": {  
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account:instance/  
i-093452212644b0dd6"  
                }  
            }  
        }  
    ]  
}
```

示例：使用启动模板

以下策略允许用户创建启动模板版本和修改启动模板，但仅适用于特定的启动模板 (lt-09477bcd97b0d3abc)。用户无法使用其他启动模板。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ec2>CreateLaunchTemplateVersion",  
                "ec2:ModifyLaunchTemplate"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:ec2:region:account:launch-template/lt-09477bcd97b0d3abc"  
        }  
    ]  
}
```

以下策略允许用户删除任何启动模板和启动模板版本，但前提是启动模板具有标签 Purpose=Testing。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ec2>DeleteLaunchTemplate",  
                "ec2>DeleteLaunchTemplateVersions"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:ec2:region:account:launch-template/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/Purpose": "Testing"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

示例：使用实例元数据

以下策略确保用户只能使用 实例元数据服务版本 2 (IMDSv2) 检索[实例元数据 \(p. 499\)](#)。您可以将以下四个策略合并为一个具有四个语句的策略。当合并为一个策略时，您可以将该策略用作服务控制策略 (SCP)。它可很好地用作应用于现有 IAM 策略的拒绝策略（取消和限制现有权限），也可以很好地用作在账户、OU 或整个组织中全局应用的服务控制策略。

Note

以下 RunInstances 元数据选项策略必须与授予委托人使用 RunInstances 启动实例的权限的策略结合使用。如果委托人没有同时具有 RunInstances 权限，则无法启动实例。有关更多信息，请参阅[使用实例 \(p. 716\)](#)和[启动实例 \(RunInstances\) \(p. 726\)](#) 中的策略。

以下策略指定您不能调用 RunInstances API，除非该实例也选择需要使用 IMDSv2（由 "ec2:MetadataHttpTokens": "required" 指示）。如果您未指定实例需要 IMDSv2，则在调用 RunInstances API 时会收到 UnauthorizedOperation 错误。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

以下策略指定您不能调用 RunInstances API，除非您还指定了跃点限制，且跃点限制不能超过 3。如果您无法执行此操作，则在调用 RunInstances API 时会收到 UnauthorizedOperation 错误。

Note

当以下策略和前一个策略通过 SCP 应用于账户时，您无法使用 EC2 控制台启动实例，因为控制台尚不支持 MetadataHttpTokens 和 MetadataHttpPutResponseHopLimit 参数。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

```
        }
    ]
}
```

以下策略删除了一般管理员修改实例元数据选项的能力，并且仅允许具有 ec2-imds-admins 角色的用户进行更改。如果除 ec2-imds-admins 角色以外的任何委托人尝试调用 ModifyInstanceMetadataOptions API，则会收到 UnauthorizedOperation 错误。此语句可用于控制 ModifyInstanceMetadataOptions API 的使用；目前对于 ModifyInstanceMetadataOptions API 没有精细访问控制（条件）。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

以下策略指定如果将此策略应用于某个角色，并且该角色由 EC2 服务代入且生成的凭证用于对请求进行签名，则必须由从 IMDSv2 中检索的 EC2 角色凭证对该请求进行签名。否则，它的所有 API 调用都会收到 UnauthorizedOperation 错误。此语句/策略可广泛应用，因为如果请求未由 EC2 角色证书签名，则其为无效。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

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。

Tip

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。

示例

- [示例：只读访问权限 \(p. 743\)](#)
- [示例：使用 EC2 启动向导 \(p. 744\)](#)
- [示例：使用卷 \(p. 746\)](#)
- [示例：使用安全组 \(p. 747\)](#)
- [示例：使用弹性 IP 地址 \(p. 748\)](#)
- [示例：使用预留实例 \(p. 749\)](#)

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。](#)

示例：只读访问权限

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：[示例：只读访问权限 \(p. 715\)](#) 用户无法对这些资源执行任何操作或创建新资源（除非其他语句为用户授予执行此操作的权限）。

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

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哪些单个资源。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 \(p. 712\)](#)。

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": [  
            "cloudwatch:DescribeAlarms",  
            "cloudwatch:GetMetricStatistics"  
        ],  
        "Resource": "*"  
    }  
}]
```

```
    "Action": [
        "ec2:DescribeInstances",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics"
    ],
    "Resource": "*"
}
]
```

示例：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。

基本启动向导访问

要成功完成启动，必须为用户授予使用 `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。
- `ec2:DescribeSubnets`：查看所选 VPC 的所有可用子网。
- `ec2:DescribeSecurityGroups` 或 `ec2>CreateSecurityGroup`：查看并选择现有安全组或创建新的安全组。
- `ec2:DescribeKeyPairs` 或 `ec2:CreateKeyPair`：选择现有密钥对或创建新密钥对。
- `ec2:AuthorizeSecurityGroupIngress`：添加入站规则。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "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`：查看并选择特定可用区。
- `ec2:DescribeNetworkInterfaces`：查看并选择所选子网的现有网络接口。

- 要向 VPC 安全组添加出站规则，必须为用户授予使用 `ec2:AuthorizeSecurityGroupEgress` API 操作的权限。要修改或删除现有规则，必须为用户授予使用相关 `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[用于标记的资源级权限 \(p. 712\)](#)。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

为用户授予使用 `ec2:CreateTags` 操作的权限时请小心谨慎。这会限制您使用 `ec2:ResourceTag` 条件键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。

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 `t2.micro` 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。

第一条语句为用户授予权限以查看启动向导中的选项或创建新选项，如上例所示。第二条语句为用户授予权限以将网络接口、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[启动实例 \(RunInstances\) \(p. 726\)](#)。第三和第四条语句分别为用户授予权限以使用实例（仅当实例是 `t2.micro` 实例）和 AMI 资源（仅当 AMI 由 Amazon 所有时）。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances", "ec2:DescribeImages",  
                "ec2:DescribeKeyPairs", "ec2>CreateKeyPair", "ec2:DescribeVpcs",  
                "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups", "ec2>CreateSecurityGroup",  
                "ec2AuthorizeSecurityGroupIngress"  
            ],  
            "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": "t2.micro"  
                }  
            }  
        }  
    ]  
}
```

```
},
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:sa-east-1::image/ami-*"
    ],
    "Condition": {
        "StringEquals": {
            "ec2:Owner": "amazon"
        }
    }
}
]
```

示例：使用卷

以下策略为用户授予查看和创建卷以及将卷与特定实例附加和分离的权限。

用户可以将任何卷附加到具有标签“purpose=test”的实例，也可以从这些实例分离卷。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:DescribeAvailabilityZones 操作以确保用户可以在创建卷时选择可用区。

用户无法标记其创建的卷 (卷创建期间或之后)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "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/*"
        }
    ]
}
```

```
    ]  
}
```

示例：使用安全组

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 的现有安全组添加和删除入站和出站规则。

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"  
                }  
            }  
        }  
    ]  
}
```

使用“Create Security Group (创建安全组)”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，必须为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。

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允许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。此策略还为用户授予删除与 VPC `vpc-1a2b3c4d` 关联的安全组的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2: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"  
                }  
            }  
        }  
    ]  
}
```

示例：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**：分配弹性 IP 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。
- **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": "*"  
        }  
    ]  
}
```

示例：使用预留实例

以下策略可以附加到 IAM 用户。它可让用户查看和修改您的账户中的预留实例，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权限。

```
{  
    "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，例如删除 `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 凭证签署 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凭证。例如，您可以安全地将您的 AWS 凭证分配至实例，从而允许这些实例上运行的应用程序使用您的凭证签署请求，并保护您的凭证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 Spot 实例或 Auto Scaling 组中的实例。当您更换 AWS 凭证时，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凭证。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 凭证，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. 在您启动实例时指定角色，或者将角色附加到现有实例。
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 中的存储桶所需的权限。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。如果您更改了某个角色，系统会将此更改传播到所有实例。

在创建 IAM 角色时，请关联最小权限 IAM 策略，这些策略将限制对应用程序所需的特定 API 调用的访问权限。

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 \(p. 712\)](#) 以及以下示例：[示例：使用 IAM 角色 \(p. 738\)](#)。

主题

- [实例配置文件 \(p. 750\)](#)
- [通过实例元数据检索安全凭证 \(p. 750\)](#)
- [允许 IAM 用户将 IAM 角色传递给实例 \(p. 751\)](#)
- [使用 IAM 角色 \(p. 752\)](#)

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名称列表选择角色。

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，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凭证

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凭证为其定义的操作和资源的权限。这些安全凭证是临时的，我们会自动更换它们。我们在旧凭证过期前至少五分钟提供可用的新凭证。

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凭证。可能泄露您的凭证的服务类型包括 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。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ 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" : "ASIAIOSFODNN7EXAMPLE",  
    "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",  
    "Token" : "token",  
    "Expiration" : "2017-05-17T15:09:54Z"  
}
```

对于实例上运行的应用程序、AWS CLI 和 Windows PowerShell 工具 命令，您无需显式获取临时安全凭证—AWS 开发工具包、AWS CLI 和 Windows PowerShell 工具 会自动从 EC2 实例元数据服务中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 \(p. 499\)](#)。

允许 IAM 用户将 IAM 角色传递给实例

若要支持 IAM 用户启动带有 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 策略将授权用户启动带有 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，应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。

目录

- [创建 IAM 角色 \(p. 752\)](#)
- [启动带有 IAM 角色的实例 \(p. 754\)](#)
- [将 IAM 角色附加到实例 \(p. 755\)](#)
- [替换 IAM 角色 \(p. 755\)](#)
- [分离 IAM 角色 \(p. 756\)](#)

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该角色附加到该实例。

使用 IAM 控制台创建 IAM 角色

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Roles 和 Create role。
3. 在 Select role type 页面上，选择 EC2 和 EC2 使用案例。选择下一步：权限。
4. 在附加权限策略页面上，选择向实例授予对所需资源的访问权的 AWS 托管策略。
5. 在 Review (审核) 页面上，为角色输入一个名称，然后选择 Create role (创建角色)。

或者，您可以使用 AWS CLI 创建 IAM 角色。

创建 IAM 角色和实例配置文件 (AWS CLI)

- 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. 将访问策略附加到角色。

```
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 CLI Command 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（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 (配置实例详细信息) 页面上，为 IAM role (IAM 角色) 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 软件开发工具包创建了 IAM 角色，则可能对实例配置文件指定了不同名称。

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 安全凭证，并使用它们签署请求。AWS 开发工具包将为您执行此操作。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

IMDSv1

```
[ec2-user ~]$ 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。

启动带有 IAM 角色的实例 (AWS CLI)

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 安全凭证，并使用它们签署请求。AWS 开发工具包将为您执行此操作。

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

将 IAM 角色附加到实例

要将 IAM 角色附加到没有角色的实例，该实例可以处于 stopped 或 running 状态。

将 IAM 角色附加到实例（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 Instances（实例）。
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 角色，然后选择 Apply（应用）。

将 IAM 角色附加到实例（AWS CLI）

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](#) 并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 Amazon 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](#)

替换 IAM 角色

要替换已附加了 IAM 角色的实例上的 IAM 角色，实例必须处于 running 状态。如果要更改实例的 IAM 角色而先不分离现有角色，则您可以执行此操作。例如，您可以执行此操作，以确保正在实例上运行的应用程序所执行的 API 操作不会被中断。

替换实例的 IAM 角色（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 Instances（实例）。

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 角色，然后选择 Apply (应用)。

替换实例的 IAM 角色 (AWS CLI)

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](#) 命令并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](#)

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分离。

从实例中分离 IAM 角色 (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 Instances (实例)。
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。

从实例中分离 IAM 角色 (AWS CLI)

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](#)

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 或 HTTPS 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。

您的默认安全组和新创建的安全组包含不支持您从 Internet 访问实例的默认规则。有关更多信息，请参阅 [默认安全组 \(p. 770\)](#) 和 [自定义安全组 \(p. 771\)](#)。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“什么是我的 IP 地址”，或使用以下服务：[检查 IP](#)。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

如果使用 `0.0.0.0/0`，则允许所有 IPv4 地址使用 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。在生产环境中，您仅授权特定 IP 地址或地址范围访问您的实例。

决定您是否支持使用 EC2 Instance Connect 对实例进行 SSH 访问。如果您将不使用 EC2 Instance Connect，则考虑卸载它或在 IAM 策略中拒绝以下操作：`ec2-instance-connect:SendSSHPublicKey`。有关更多信息，请参阅 [卸载 EC2 Instance Connect \(p. 435\)](#) 和 [为 EC2 Instance Connect 配置 IAM 权限 \(p. 432\)](#)。

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。您必须向安全组添加可让您使用 SSH 从 IP 地址连接到 Linux 实例的规则。

在安全组中为通过 IPv4 的入站 SSH 流量添加规则（控制台）

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 inbound rules (查看入站规则)，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 \(p. 757\)](#)。

5. 选择 Save。

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。

在安全组中为通过 IPv6 的入站 SSH 流量添加规则（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 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。

Note

请确保以下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 \(p. 3\)](#)。

使用命令行向安全组添加规则

1. 使用以下命令之一找到与您的实例关联的安全组：

- [describe-instance-attribute \(AWS CLI\)](#)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute groupSet
```

- [Get-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId instance_id -Attribute groupSet).Groups
```

两个命令均返回一个安全组 ID，您将在下一步中使用该 ID。

2. 使用以下命令之一向安全组添加规则：

- [authorize-security-group-ingress \(AWS CLI\)](#)

```
aws ec2 authorize-security-group-ingress --group-id security_group_id --protocol tcp  
--port 22 --cidr cidr_ip_range
```

- [Grant-EC2SecurityGroupIngress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

Grant-EC2SecurityGroupIngress 命令需要 IpPermission 参数，该参数描述要用于安全组规则的协议、端口范围和 IP 地址范围。以下命令创建 IpPermission 参数：

```
PS C:\> $ip1 = @{ IpProtocol="tcp"; FromPort="22"; ToPort="22";  
IpRanges="cidr_ip_range" }
```

```
PS C:\> Grant-EC2SecurityGroupIngress -GroupId security_group_id -IpPermission  
@($ip1)
```

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。

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 密钥对

Amazon EC2 使用公有密钥加密方法加密和解密登录信息。公有密钥加密方法使用公有密钥加密某个数据，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。通过公有密钥加密方法，您能够使用私有密钥安全地访问实例，而不是使用密码。

启动实例时，您指定密钥对。您可以指定现有的密钥对，也可以指定在启动时创建的新密钥对。在启动时，公有密钥内容放在实例上 `~/.ssh/authorized_keys` 中的条目内。要登录实例，您必须在连接到实例时指定私有密钥。有关更多信息，请参阅[启动实例 \(p. 374\)](#)和[连接到 Linux 实例 \(p. 423\)](#)。

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 \(p. 760\)](#)。

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 \(p. 761\)](#)。

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。连接到该实例时，您必须指定与在启动该实例时指定的密钥对相应的私有密钥。

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 \(p. 765\)](#)。

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 \(p. 469\)](#)。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的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。

目录

- [使用 Amazon EC2 创建密钥对 \(p. 760\)](#)
- [将您自己的公有密钥导入 Amazon EC2 \(p. 761\)](#)
- [在 Linux 上检索密钥对的公有密钥 \(p. 762\)](#)
- [在 Windows 上检索密钥对的公有密钥 \(p. 763\)](#)
- [从实例检索密钥对的公有密钥 \(p. 763\)](#)
- [验证您的密钥对指纹 \(p. 763\)](#)
- [删除您的密钥对 \(p. 764\)](#)
- [添加或替换实例的密钥对 \(p. 764\)](#)
- [丢失私有密钥时连接到 Linux 实例 \(p. 765\)](#)

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[添加或替换实例的密钥对 \(p. 764\)](#)。

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。

Note

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. 对于 Key pair name (密钥对名称)，为新密钥对输入一个名称，然后选择 Create (创建)。
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
```

如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅[错误：未保护的私钥文件 \(p. 959\)](#)。

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。例如，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 和很多其他提供标准库的编程语言来创建 RSA 密钥对。

要求

- 支持以下格式：
 - OpenSSH 公有密钥格式 (格式为 ~/.ssh/authorized_keys)。如果您在使用 EC2 Instance Connect API 时使用 SSH 进行连接，则也支持 SSH2 公司。
 - Base64 编码的 DER 格式
 - SSH 公有密钥文件格式如 [RFC4716](#) 所指定
 - SSH 私有密钥文件格式必须为 PEM (例如，使用 ssh-keygen -m PEM 将 OpenSSH 密钥转换为 PEM 格式)
- 创建一个 RSA 密钥。Amazon EC2 不接受 DSA 密钥。
- 支持的长度为 1024、2048 和 4096。如果您在使用 EC2 Instance Connect API 时使用 SSH 进行连接，则支持的长度为 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。

- 将私有密钥保存至另一个扩展名为 .pem 的本地文件。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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
- 选择 Import Key Pair。
- 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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 从导航栏中，选择您在其中创建密钥对的区域。
- 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
- 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

在本地 Linux 或 Mac 计算机上，可使用 ssh-keygen 命令检索密钥对的公有密钥。指定您已在其中下载私有密钥的路径 (.pem 文件)。

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

命令将返回公有密钥。例如：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtXJMLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxxPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

如果该命令失败，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
```

在 Windows 上检索密钥对的公有密钥

在本地 Windows 计算机上，您可以使用 PuTTYgen 获取密钥对的公有密钥。

启动 PuTTYgen 并选择 Load (加载)。选择 .ppk 或 .pem 文件。PuTTYgen 在 Public key for pasting into OpenSSH authorized_keys file (粘贴到 OpenSSH authorized_keys 文件的公有密钥) 下方显示公有密钥。也可以通过以下方式查看公有密钥：选择 Save public key (保存公有密钥)，指定文件的名称，然后打开文件。

从实例检索密钥对的公有密钥

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：

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUZofz221CBt5IMucxxXPkX4rWi+z7wB3Rb
B9oQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYicNYwI3f05p6KLxEXAMPLE my-key-pair
```

如果您更改用于连接到实例的密钥对，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。

有关更多信息，请参阅 [检索实例元数据 \(p. 503\)](#)。

或者，在 Linux/ 实例中，公有密钥内容放在 ~/.ssh/authorized_keys 内的条目中。您可以在编辑器中打开此文件。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 AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUZofz221CBt5IMucxxXPkX4rWi+z7wB3Rb
B9oQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYicNYwI3f05p6KLxEXAMPLE my-key-pair
```

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。

您可以使用显示在 Key Pairs (密钥对) 页面上的 SSH2 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。在您在其中已下载私有密钥文件的计算机中，从私有密钥文件生成 SSH2 指纹。输出应与控制台中显示的指纹匹配。

如果您使用 AWS 创建了密钥对，则可以使用 OpenSSL 工具生成指纹，如下所示：

```
$ 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 工具生成指纹，如下所示：

```
$ openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

如果您使用 OpenSSH 7.8 或更高版本创建了 OpenSSH 密钥对并将公有密钥上传到 AWS，则可以使用 ssh-keygen 生成指纹，如下所示：

```
$ ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER | openssl md5 -c
```

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。Amazon EC2 Auto Scaling 检测到运行不正常的实例时会启动替换实例；但是，如果找不到密钥对，实例启动将失败。

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 \(p. 469\)](#)。

添加或替换实例的密钥对

您可以更改用于访问实例默认系统账户的密钥对。例如，如果组织中用户需要使用单独的密钥对访问系统用户账户，您可以向实例中添加一个密钥对。或者，如果某人有 .pem 文件的副本，而您想要防止他们访问实例（例如在他们已离开组织的情况下），您可以将其替换为新密钥对。

Note

这些程序用于修改默认用户账户的密钥对，例如 `ec2-user`。有关向实例添加用户账户的更多信息，请参阅 [在 Linux 实例上管理用户账户 \(p. 469\)](#)。

在开始前，使用 [Amazon EC2 控制台 \(p. 760\)](#) 或 [第三方工具 \(p. 761\)](#) 创建新的密钥对。

添加或替换密钥对

1. 从新密钥对检索公有密钥。有关更多信息，请参阅 [在 Linux 上检索密钥对的公有密钥 \(p. 762\)](#) 或 [在 Windows 上检索密钥对的公有密钥 \(p. 763\)](#)。
2. 使用现有的私有密钥文件连接到实例。
3. 使用您选择的文本编辑器，在实例上打开 `.ssh/authorized_keys` 文件。将新密钥对的公有密钥信息粘贴到现有公有密钥信息下。保存文件。
4. 从实例分离，并测试能否使用新的私有密钥文件连接到实例。
5. (可选) 如果您要替换现有密钥对，请连接到实例并从 `.ssh/authorized_keys` 文件中删除原始密钥对的公有密钥信息。

Note

如果您使用的是 Auto Scaling 组（例如，在 Elastic Beanstalk 环境中），请确保您要替换的密钥对未在启动配置中指定。Amazon EC2 Auto Scaling 检测到运行不正常的实例时会启动替换实例；但是，如果找不到密钥对，实例启动将失败。

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的实例的访问权限。您必须停止实例，分离卷并将其作为数据卷附加到另一个实例，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 \(p. 370\)](#)。

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. 从 Description (说明) 选项卡中，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-xxxxxxxxxxxxxxxxxxxx`)。
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。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

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 \(p. 102\)](#)。
 - 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 (操作)、Detach Volume (分离卷)，然后选择 Yes, Detach (是，分离)。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 (设备) 下指定的设备名称（例如，/dev/sdf），然后选择 Attach (附加)。

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。

- 连接到临时实例。
- 在临时实例中，挂载附加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挂载为 /mnt/tempvol。

Note

您的实例上显示的设备名称可能不同。例如，作为 /dev/sdf 挂载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/xvd~~f~~k。

- 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 
xvdg   202:96   0  30G  0 disk
```

在以上示例中，/dev/xvda 和 /dev/xvdf 是分区卷，而 /dev/xvdg 不是。如果您的卷已分区，则应在后续步骤中挂载分区 (/dev/xvdf1)，而不是原始设备 (/dev/xvdf)。

- 创建临时目录以挂载卷。

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

- 使用之前确定的卷名称或设备名称在临时挂载点挂载卷（或分区）。所需命令取决于操作系统的文件系统。

- Amazon Linux、Ubuntu 和 Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2、CentOS、SLES 12 和 RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

Note

如果您收到说明文件系统受损的错误，请运行以下命令以使用 fsck 实用程序检查文件系统并修复任何问题：

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

10. 在临时实例中，借助临时实例 authorized_keys 中的新公有密钥，在已挂载卷上使用以下命令更新 authorized_keys。

Important

以下示例使用 Amazon Linux 用户名 ec2-user。您可能需要使用其他用户名来替换，例如对于 Ubuntu 实例为 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，您需要使用 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，卸载已附加的卷，以将其重新附加到原始实例。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 (操作)、Detach Volume (分离卷)，然后选择 Yes, Detach (是，分离)。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 Attach (附加)。

Important

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. (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，可指定一个或多个安全组；否则，我们将使用默认安全组。您可以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，我们会评估与实例关联的所有安全组中的所有规则。

在 VPC 中启动实例时，您必须指定一个为该 VPC 创建的安全组。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 \(p. 612\)](#)。

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。

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](#)。

目录

- [安全组规则 \(p. 769\)](#)
 - [连接跟踪 \(p. 770\)](#)
- [默认安全组 \(p. 770\)](#)
- [自定义安全组 \(p. 771\)](#)
 - [使用安全组 \(p. 771\)](#)
 - [正在创建安全组 \(p. 771\)](#)
 - [描述您的安全组 \(p. 772\)](#)
 - [向安全组添加规则 \(p. 772\)](#)
 - [更新安全组规则 \(p. 774\)](#)
 - [从安全组中删除规则 \(p. 774\)](#)
 - [正在删除安全组 \(p. 775\)](#)
 - [安全组规则引用 \(p. 775\)](#)
 - [Web 服务器规则 \(p. 775\)](#)
 - [数据库服务器规则 \(p. 776\)](#)
 - [用于从您的计算机连接到实例的规则 \(p. 777\)](#)
 - [用于在具有相同安全组的实例之间进行连接的规则 \(p. 777\)](#)
 - [用于路径 MTU 发现的规则 \(p. 777\)](#)
 - [用于 Ping/ICMP 的规则 \(p. 778\)](#)
 - [DNS 服务器规则 \(p. 778\)](#)
 - [Amazon EFS 规则 \(p. 778\)](#)
 - [Elastic Load Balancing 规则 \(p. 779\)](#)
 - [VPC 对等规则 \(p. 780\)](#)

安全组规则

安全组规则可控制允许到达与安全组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。
- 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 \(p. 770\)](#)。
- 您可以随时添加和删除规则。您所做的更改将会自动应用于与安全组关联的实例中。

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 \(p. 770\)](#)。

- 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。您必须使用 /32 前缀长度；例如 203.0.113.1/32。
 - 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。
 - 采用 CIDR 块表示法的 IPv6 地址范围；例如，2001:db8:1234:1a00::/64。
- AWS 服务的前缀列表 ID；例如，p1-1a2b3c4d。有关更多信息，请参阅Amazon VPC 用户指南中的[网关 VPC 终端节点](#)。
- 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
 - 同一 VPC 的其他安全组
 - VPC 对等连接中的对等 VPC 的其他安全组
- （可选）描述：您可以添加规则的说明；例如，用于帮助您在以后识别它。描述的长度最多为 255 个字符。允许的字符包括 a-z、A-Z、0-9、空格和 _-:/()#@[]+=;{}!\$*。

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 \(p. 574\)](#)。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通信 (0.0.0.0/0) 的 TCP 或 UDP 流，并且另一个方向存在允许所有端口 (0-65535) 的所有响应通信 (0.0.0.0/0) 的对应规则，则不会跟踪该通信流。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 TCP 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)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
ICMP	全部	0.0.0.0/0

出站规则		
协议类型	端口号	目的地 IP
全部	全部	0.0.0.0/0

将会跟踪端口 22 (SSH) 上流入和流出实例的 TCP 流量，因为入站规则只允许来自 203.0.113.1/32 的流量，而不是所有 IP 地址 (0.0.0.0/0)。不会跟踪端口 80 (HTTP) 上流入和流出实例的 TCP 流量，因为入站和出站规则都允许所有流量 (0.0.0.0/0)。无论规则如何，始终跟踪 ICMP 流量。如果您从安全组删除出站规则，则将跟踪往返于实例上的所有流量，包括端口 80 (HTTP) 上的流量。

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个主机 (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。

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 账户在每个区域的默认 VPC 中都自动拥有一个默认安全组。如果您在启动实例时没有指定安全组，实例会自动与 VPC 的默认安全组关联。

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和出站规则。

您无法删除默认安全组。如果您尝试删除默认安全组，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：

a-z、A-Z、0-9、空格和 `_:-/()#,@[]+=&{}!$^*`

安全组名称不能以 `sg-` 开头。安全组名称在 VPC 中必须是唯一的。

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。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的更多信息，请参阅[安全组规则引用 \(p. 775\)](#)。

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。

任务

- [正在创建安全组 \(p. 771\)](#)
- [描述您的安全组 \(p. 772\)](#)
- [向安全组添加规则 \(p. 772\)](#)
- [更新安全组规则 \(p. 774\)](#)
- [从安全组中删除规则 \(p. 774\)](#)
- [正在删除安全组 \(p. 775\)](#)

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。您必须指定您正在为其创建安全组的 VPC。

使用控制台创建新安全组

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. 对于 VPC，选择 VPC 的 ID。
6. 您可以开始添加规则，也可以选择 Create (创建) 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 \(p. 772\)](#)。

使用命令行创建安全组

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

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。

使用控制台复制安全组

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。对于 VPC，选择 VPC 的 ID。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。

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。

描述您的安全组

您可以使用 Amazon EC2 控制台或命令行查看有关安全组的信息。

使用控制台描述您的安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. (可选) 从筛选条件列表中选择 VPC ID，然后选择 VPC 的 ID。
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，在 Outbound (出站) 选项卡上显示出站规则，并在 Tags (标签) 选项卡上显示标签。

使用命令行描述一个或多个安全组

- [describe-security-groups](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

向安全组添加规则

当您向安全组添加规则时，该新规则会在经过一小段时间之后自动应用于与该安全组关联的任何实例。

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 \(p. 775\)](#)。

使用控制台向安全组添加规则

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。使用该选项后，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 Anywhere (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`)，另一个用于 IPv6 流量 (`::/0`)。

- 我的 IP：自动添加本地计算机的公有 IPv4 地址。
- 对于描述，您可以选择指定规则的描述。

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 \(p. 775\)](#)。

5. 选择 Save。
6. 您也可以指定出站规则。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。该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 Anywhere (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`)，另一个用于 IPv6 流量 (`::/0`)。

- 我的 IP：自动添加本地计算机的 IP 地址。
- 对于描述，您可以选择指定规则的描述。

7. 选择 Save。

使用命令行向安全组添加一条或多条传入规则

- [authorize-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行向安全组添加一条或多条出口规则

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

更新安全组规则

使用控制台修改现有安全组规则的协议、端口范围或者源或目标时，控制台会删除现有规则并为您添加新规则。

使用控制台更新安全组规则

1. 打开 Amazon EC2 控制台 [https://console.aws.amazon.com/ec2/。](https://console.aws.amazon.com/ec2/)
2. 在导航窗格中，选择 Security Groups。
3. 选择要更新的安全组，然后选择 Inbound Rules 更新入站流量的规则，或者选择 Outbound Rules 更新出站流量的规则。
4. 选择 Edit。根据需要修改规则条目，然后选择 Save。

要使用 Amazon EC2 API 或命令行工具更新现有规则的协议、端口范围或者源或目标，您无法修改规则。相反，您必须删除该现有规则并添加新规则。要仅更新规则描述，您可以使用 [update-security-group-rule-descriptions-ingress](#) 和 [update-security-group-rule-descriptions-egress](#) 命令。

使用命令行更新传入安全组规则的说明

- [update-security-group-rule-descriptions-ingress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行更新出口安全组规则的说明

- [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleEgressDescription](#) (适用于 Windows PowerShell 的 AWS 工具)

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关联的任何实例。

使用控制台更新安全组规则

1. 打开 Amazon EC2 控制台 [https://console.aws.amazon.com/ec2/。](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。

使用命令行从安全组删除一条或多条传入规则

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行从安全组删除一条或多条出口规则

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

正在删除安全组

您不能删除与实例关联的安全组。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。

使用控制台删除安全组

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。

使用命令行删除安全组

- [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。

示例

- [Web 服务器规则 \(p. 775\)](#)
- [数据库服务器规则 \(p. 776\)](#)
- [用于从您的计算机连接到实例的规则 \(p. 777\)](#)
- [用于在具有相同安全组的实例之间进行连接的规则 \(p. 777\)](#)
- [用于路径 MTU 发现的规则 \(p. 777\)](#)
- [用于 Ping/ICMP 的规则 \(p. 778\)](#)
- [DNS 服务器规则 \(p. 778\)](#)
- [Amazon EFS 规则 \(p. 778\)](#)
- [Elastic Load Balancing 规则 \(p. 779\)](#)
- [VPC 对等规则 \(p. 780\)](#)

Web 服务器规则

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	端口	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。
TCP	6	443 (HTTPS)	0.0.0.0/0	允许来自任何 IPv4 地址的入站 HTTPS 访问

协议类型	协议编号	端口	源 IP	备注
TCP	6	80 (HTTP)	::/0	允许来自任何 IPv6 地址的入站 HTTP 访问
TCP	6	443 (HTTPS)	::/0	允许来自任何 IPv6 地址的入站 HTTPS 访问

数据库服务器规则

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 RDS 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	端口	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 集群数据库的默认端口。
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

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	端口	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	端口	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

用于从您的计算机连接到实例的规则

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	端口	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，并且您的实例有一个 IPv6 地址，则可以输入一个 IPv6 地址或范围。

用于在具有相同安全组的实例之间进行连接的规则

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相互通信的安全组的入站规则。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

用于路径 MTU 发现的规则

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

用于 Ping/ICMP 的规则

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 命令对您的实例的 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 服务器规则

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 IP 地址或 IP 地址范围
- 您网络中需要访问 DNS 服务器的实例组的安全组 ID。

协议类型	协议编号	端口
TCP	6	53
UDP	17	53

Amazon EFS 规则

如果您将 Amazon EFS 文件系统与 Amazon EC2 实例结合使用，与 Amazon EFS 挂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 实例上挂载 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 规则

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 Classic Load Balancer 用户指南中的[为您的传统负载均衡器配置安全组](#)以及 Application Load Balancer 用户指南中的[您的应用程序负载均衡器的安全组](#)。

VPC 对等规则

您可以更新 VPC 安全组的入站或出站规则以引用对等的 VPC 中的安全组。此操作将允许流量流入和流出与对等的 VPC 中的已引用安全组关联的实例。有关如何为 VPC 对等配置安全组的更多信息，请参阅[更新安全组以引用对等 VPC 组](#)。

Amazon EC2 中的更新管理

我们建议您定期修补、更新和保护 EC2 实例上的操作系统和应用程序。您可以使用 [AWS Systems Manager Patch Manager](#) 自动执行为操作系统和应用程序安装安全相关更新的过程。或者，您也可以使用任何自动更新服务或建议的过程安装应用程序供应商提供的更新。

Amazon EC2 的合规性验证

作为多个 AWS 合规性计划的一部分，第三方审核员将评估 Amazon EC2 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 AWS 服务列表，请参阅[合规性计划范围内的 AWS 服务](#)。有关常规信息，请参阅[AWS 合规性计划](#)。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅[下载 AWS Artifact 中的报告](#)。

您在使用 Amazon EC2 时的合规性责任是由您的数据敏感性、您的公司的合规性目标以及适用的法律和法规决定的。AWS 提供了以下资源以帮助满足合规性要求：

- [安全性与合规性快速入门指南](#) – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- [《设计符合 HIPAA 安全性和合规性要求的架构》白皮书](#) – 此白皮书介绍公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- [AWS 合规性资源](#) – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config Developer Guide 中的[使用规则评估资源](#) – AWS Config；评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- [AWS Security Hub](#) – 此 AWS 服务提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

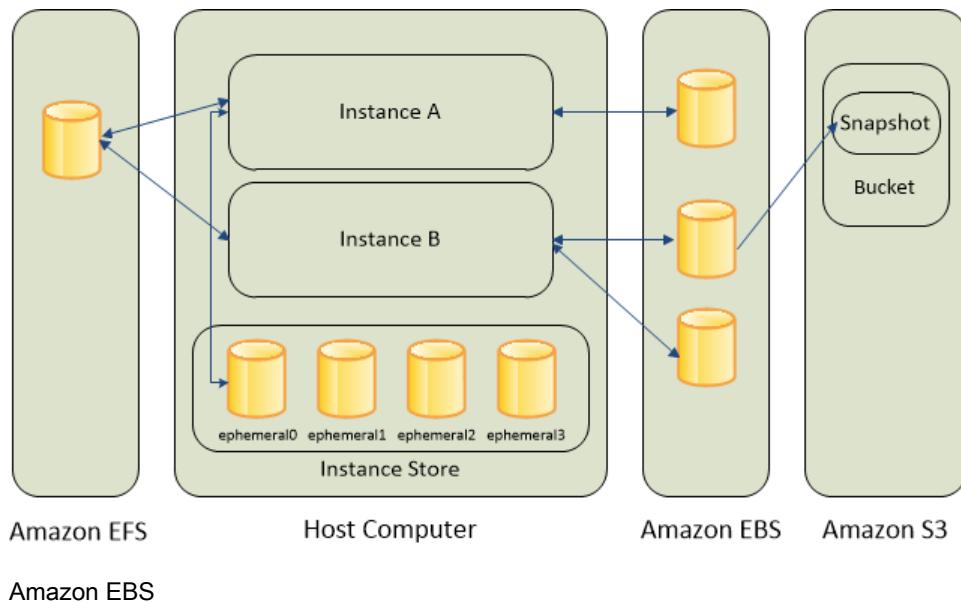
存储

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 \(p. 782\)](#)
- [Amazon EC2 实例存储 \(p. 903\)](#)
- [Amazon Elastic File System \(Amazon EFS\) \(p. 916\)](#)
- [Amazon Simple Storage Service \(Amazon S3\) \(p. 919\)](#)

下图显示了这些存储选项和您的实例之间的关系。



Amazon EBS

Amazon EBS 提供块级别的持久存储卷，您可将这些卷附加到正在运行的实例。可以使用 Amazon EBS 作为主要存储设备，以获取需要频繁更新和精细更新的数据。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，可附加到单个实例。卷始终不受实例运行时间的影响。将 EBS 卷附加到实例后，您可以像使用其他物理硬盘一样使用它。如上图所示，可以将多个卷附加到一个实例。您也可以将 EBS 卷从实例中分离，并将其附加到另一个实例。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 \(p. 851\)](#)。

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，并将其附加到另一个实例。有关更多信息，请参阅[Amazon Elastic Block Store \(p. 782\)](#)。

Amazon EC2 实例存储

很多实例可以访问物理附加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 \(p. 903\)](#)。

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装载文件系统。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 \(Amazon EFS\) \(p. 916\)](#)。

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 快照以及由实例存储支持的 AMI。有关更多信息，请参阅 [Amazon Simple Storage Service \(Amazon S3\) \(p. 919\)](#)。

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 \(p. 923\)](#)。

您还可以将 EBS 卷附加到运行中的实例。有关更多信息，请参阅 [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。

Amazon Elastic Block Store (Amazon EBS)

Amazon Elastic Block Store (Amazon EBS) 提供了块级存储卷以用于 EC2 实例。EBS 卷的行为类似于原始、未格式化的块储存设备。您可以将这些卷作为设备挂载在实例上。您可以在同一实例上安装多个卷，但每个卷一次只能附加到一个实例。您可以在这些卷上创建文件系统，或者以使用块储存设备（如硬盘）的任何方式使用这些卷。您可以动态更改附加到实例的卷的配置。

EBS 卷是高度可用、可靠的存储卷，您可以将其附加到同一可用区域中任何正在运行的实例。附加到 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 页面](#) 的“预计费用”部分。

您可以将多个卷附加到同一实例，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](#)。

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、未格式化的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。

目录

- [Amazon EBS 的功能 \(p. 782\)](#)
- [Amazon EBS 卷 \(p. 783\)](#)
- [Amazon EBS 快照 \(p. 812\)](#)
- [Amazon EBS 数据服务 \(p. 841\)](#)
- [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)
- [Amazon EBS 优化的实例 \(p. 863\)](#)
- [Linux 实例上的 Amazon EBS 卷性能 \(p. 875\)](#)
- [Amazon EBS 的 Amazon CloudWatch 指标 \(p. 889\)](#)
- [Amazon EBS 的 Amazon CloudWatch Events \(p. 893\)](#)

Amazon EBS 的功能

- EBS 卷在特定可用区中创建，随后可以附加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，您可以创建一个快照并将该快照还原到该区域中任意位置处的新卷。您可以将快照复制到其他区域，再将

它们还原到该区域中的新卷，从而更轻松地利用多个 AWS 区域来实现地理扩展、数据中心迁移和灾难恢复。

- 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) 和 Cold HDD (sc1)。以下是每种卷类型的性能和使用案例摘要。
- 通用型 SSD 卷提供 3 IOPS/GiB 的基本性能，并且能够长时间突增到 3,000 IOPS。这些卷适用于广泛的使用案例，例如，引导卷、中小型数据库以及开发和测试环境。有关更多信息，请参阅[通用型 SSD \(gp2\) 卷 \(p. 787\)](#)。
- 预配置 IOPS SSD 卷支持高达 64,000 IOPS 和 1,000 MiB/s 的吞吐量。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 \(p. 789\)](#)。
- 吞吐优化 HDD 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。这些卷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 \(p. 790\)](#)。
- Cold HDD 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。这些卷非常适合大型顺序冷数据工作负载。如果您不需要经常访问数据并希望节约成本，这些卷提供价格低廉的块存储。有关更多信息，请参阅[Cold HDD \(sc1\) 卷 \(p. 792\)](#)。
- 您可以创建 EBS 卷以作为加密卷，以便满足监管/审核的数据和应用程序的各种静态数据加密要求。创建加密 EBS 卷并将它附加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，对从 EC2 实例传输到 EBS 存储的数据进行加密。有关更多信息，请参阅[Amazon EBS Encryption \(p. 851\)](#)。
- 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 \(p. 812\)](#)。
- 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 \(p. 875\)](#)。

Amazon EBS 卷

Amazon EBS 卷是一种耐用的数据块级存储设备，可以附加到单个 EC2 实例。可以将 EBS 卷用作需要频繁更新的数据的主存储（如实例的系统驱动器或数据库应用程序的存储）。还可以将它们用于执行连续磁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。

将卷附加到实例后，您可以像使用其他物理硬盘一样使用它。EBS 卷非常灵活。对于附加到当前一代实例类型的当前一代卷，您可以动态增加大小、修改预配置 IOPS 容量以及更改实际生产卷上的卷类型。

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 为上一代类型）。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 \(p. 785\)](#)。

目录

- [使用 EBS 卷的优势 \(p. 784\)](#)
- [Amazon EBS 卷类型 \(p. 785\)](#)
- [针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)
- [创建 Amazon EBS 卷 \(p. 798\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 799\)](#)
- [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)
- [使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#)
- [查看有关 Amazon EBS 卷的信息 \(p. 803\)](#)
- [监控您的卷状态 \(p. 804\)](#)
- [将 Amazon EBS 卷与实例分离 \(p. 810\)](#)
- [删除 Amazon EBS 卷 \(p. 812\)](#)

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，可将其附加到同一可用区内的任何 EC2 实例。附加后，该卷显示为类似于硬盘或其他物理设备的本机块储存设备。这时，实例就像与本地驱动器交互一样与该卷交互。实例还可以使用文件系统（例如 ext3）将 EBS 卷格式化，然后安装应用程序。

一个 EBS 卷一次只能附加到一个实例，但多个卷可附加到单个实例。如果您将多个卷附加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。

EBS 卷和它附加到的实例必须位于同一可用区内。

您可以获取针对 EBS 卷（包括 EBS 支持的实例的根设备卷）的监控数据，而无需额外付费。有关监控指标的更多信息，请参阅[Amazon EBS 的 Amazon CloudWatch 指标 \(p. 889\)](#)。有关跟踪卷状态的信息，请参阅[Amazon EBS 的 Amazon CloudWatch Events \(p. 893\)](#)。

- **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。

如果您在 EC2 控制台中为您的实例配置 EBS 卷时取消选中了 Delete on Termination（终止时删除）复选框，则在运行的实例终止时，附加到该实例的 EBS 卷会自动从该实例分离，并保持数据完整。然后，可将卷重新附加到新的实例，从而快速恢复数据。如果选中 Delete on Termination（终止时删除）复选框，则在 EC2 实例终止时删除卷。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其附加的卷中保存的数据。在从停止到启动的整个周期中，该卷均为已附加状态。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 \(p. 851\)](#)。

默认情况下，当一个实例终止时，将删除在启动时创建并附加到该实例的根 EBS 卷。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，也可将该卷保留下来并附加到其他实例。

默认情况下，当一个实例终止时，不会删除在启动时创建并附加到该实例的额外 EBS 卷。您可以修改此行为，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 更改为 `true`。此修改的值会导致在实例终止时删除卷。

- **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 \(p. 851\)](#)。

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。不必将该卷附加到运行中的实例，也可以制作快照。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准。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，新卷是制作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 账户共享这些快照或使其公开可用。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[标记您的 Amazon EC2 资源 \(p. 940\)](#)。

- 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

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 \(p. 875\)](#)。

有关定价的更多信息，请参阅[Amazon EBS 定价](#)。

卷特性

下表列出了每个卷类型的使用案例和性能特点。默认卷类型为 通用型 SSD (gp2)。

	固态硬盘 (SSD)		硬盘驱动器 (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，可用于多种工作负载	最高性能 SSD 卷，可用于任务关键型低延迟或高吞吐量工作负载	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引导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 16,000 IOPS 或 250 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引导卷	<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引导卷

	固态硬盘 (SSD)		硬盘驱动器 (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
每个卷的最大 IOPS	16,000 (16 KiB I/O) [*]	64,000 (16 KiB I/O) †	500 (1 MiB I/O)	250 (1 MiB I/O)
每个卷的最大吞吐量	250 MiB/s *	1,000 MiB/s †	500 MiB/s	250 MiB/s
每个实例的最大 IOPS ‡‡	80,000	80,000	80,000	80,000
每个实例的最大吞吐量 ‡‡	2375 MB/s	2375 MB/s	2375 MB/s	2375 MB/s
管理性能属性	IOPS	IOPS	MiB/s	MiB/s

* 吞吐量限制介于 128 MiB/s 和 250 MiB/s 之间，具体取决于卷大小。小于 170 GiB 的卷提供最大 128 MiB/s 的吞吐量。如果有突增积分可用，大于 170 GiB 但小于 334 GiB 的卷将提供 250 的最大吞吐量。大于或等于 334 GiB 的卷提供 250 MiB/s 的吞吐量，不论是否有突增积分。除非您修改较旧的 gp2 卷，否则该卷可能无法实现完全性能。有关更多信息，请参阅[Amazon EBS 弹性卷 \(p. 841\)](#)。

† 仅保证在 [基于 Nitro 的实例 \(p. 163\)](#) 上实现最大 IOPS 和吞吐量。其他实例保证最高为 32,000 IOPS 和 500 MiB/s。除非您修改较旧的 io1 卷，否则该卷可能无法实现完全性能。有关更多信息，请参阅[Amazon EBS 弹性卷 \(p. 841\)](#)。

‡‡ 要实现此吞吐量，您必须要有支持 [EBS 优化 \(p. 863\)](#) 的实例。

上一代卷类型

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](#)。

硬盘驱动器 (HDD)	
卷类型	磁介质
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
每个卷的最大 IOPS	40–200
每个卷的最大吞吐量	40–90 MiB/s
每个实例的最大 IOPS	80,000
每个实例的最大吞吐量	1,750 MiB/s
管理性能属性	IOPS

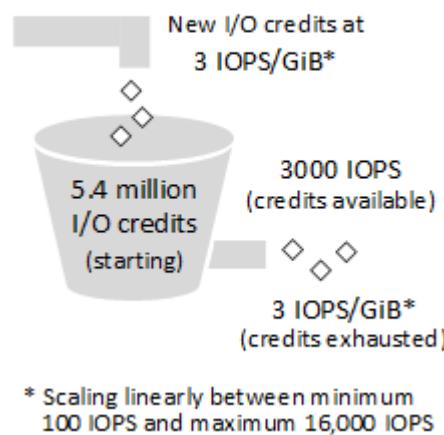
通用型 SSD (gp2) 卷

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 16,000 IOPS (以 5334 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。AWS 对 gp2 卷进行了设计，以在 99% 的时间内提供 90% 的预配置性能。gp2 卷的大小范围为 1 GiB 到 16 TiB。

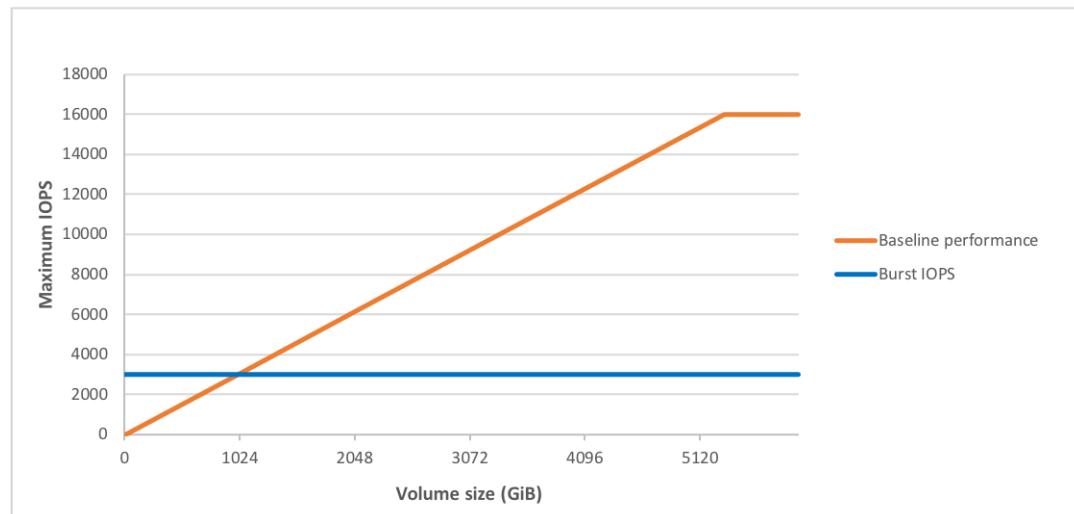
I/O 积分和突增性能

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 积分的速度；卷越大，基准性能级别就越高，I/O 积分积累速度也越快。I/O 积分表示您的 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。

GP2 burst bucket



每个卷都有 540 万 I/O 点的初始 I/O 积分余额，这足以维持 3000 IOPS 的最大突增性能 30 分钟。设计初始积分余额的目的是为引导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 积分。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，它会使用积分余额中的 I/O 积分突增到所需的性能水平，最大为 3000 IOPS。如果卷在一秒内使用的 I/O 积分少于它所赚取的积分，未使用的 I/O 积分会加到 I/O 积分余额中。卷的最大 I/O 积分余额等于初始积分余额 (540 万 I/O 积分)。

当卷的基准性能超过最大突发性能时，绝不会使用 I/O 分数。如果卷附加到基于 Nitro 的实例 (p. 163)，则不报告突发余额。对于非基于 Nitro 的实例，报告的突发余额为 100%。

卷的突增持续时间取决于卷的大小、所需的突增 IOPS 以及突增开始时的积分余额。如下面的等式所示：

$$\text{Burst duration} = \frac{(\text{Credit balance})}{(\text{Burst IOPS}) - 3(\text{Volume size in GiB})}$$

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 积分的速度)、在最大 3000 IOPS 时的突增持续时间 (从完整积分余额开始时) 以及卷重新填满空积分余额所需的秒数。

卷大小 (GiB)	基准性能 (IOPS)	提供持续的 3,000 IOPS 时的突增持续时间 (秒)	在未执行 IO 时填充空积分余额的秒数
1	100	1802	54000
100	300	2000	18000
250	750	2400	7200
334 (最大吞吐量的最小大小)	1002	2703	5389
500	1500	3600	3600
750	2250	7200	2400
1000	3000	不适用*	不适用*
5334 (最大 IOPS 的最小大小)	16,000	不适用*	不适用*
16384 (16 TiB, 最大卷大小)	16,000	不适用*	不适用*

*卷的基准性能超过了最大突发性能。

如果我清空我的 I/O 积分余额，会发生什么情况？

如果您的 gp2 卷使用其所有 I/O 积分余额，则该卷的最大 IOPS 性能将保持在基准 IOPS 性能水平 (亦即您的卷获得积分的速率)，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。吞吐量绝不会超过 250 MiB/s。当 I/O 需求下降到基准水平以下并且未使用的积分添加到 I/O 积分余额中时，该卷的最大 IOPS 性能会再次超出基准。例如，积分余额为空的 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，补充积分余额的速度也越快。有关如何测量 IOPS 的更多信息，请参阅 [I/O 特征和监控 \(p. 878\)](#)。

如果您注意到卷性能常常受限于基准水平 (由于空 I/O 积分余额)，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 16,000 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 \(p. 795\)](#)。

吞吐量性能

gp2 卷的吞吐量可以使用以下公式计算，吞吐量上限为 250 MiB/s：

$$\text{Throughput in MiB/s} = ((\text{Volume size in GiB}) \times (\text{IOPS per GiB}) \times (\text{I/O size in KiB}))$$

假定 V = 卷大小 , I = I/O 大小 , R = I/O 速率 , 并且 T = 吞吐量 , 这可以简化为 :

$$T = VIR$$

实现最大吞吐量的最小卷大小可通过以下方式得出 :

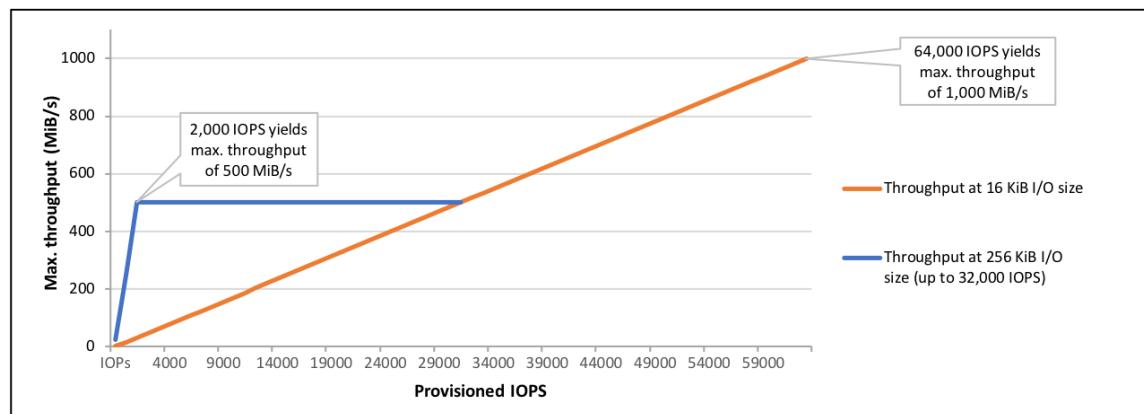
$$\begin{aligned} V &= \frac{T}{IR} \\ &= \frac{250 \text{ MiB/s}}{(256 \text{ KiB})(3 \text{ IOPS/GiB})} \\ &= \frac{[(250)(2^{20})(\text{Bytes})]/s}{(256)(2^{10})(\text{Bytes})([3 \text{ IOP/s}]/[(2^{30})(\text{Bytes})])} \\ &= \frac{(250)(2^{20})(2^{30})(\text{Bytes})}{(256)(2^{10})(3)} \\ &= 357,913,941,333 \text{ Bytes} \\ &= 333\# \text{ GiB } (334 \text{ GiB in practice because volumes are provisioned in whole gibibytes}) \end{aligned}$$

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。与使用存储桶和积分模型计算性能的 gp2 不同 , io1 卷允许您在创建卷时指定一致的 IOPS 速率 , 并且 Amazon EBS 在超过 99.9% 的时间里可提供预配置的 IOPS 性能。

io1 卷的大小范围是 4 GiB 到 16 TiB。您可以在 [基于 Nitro 的实例 \(p. 163\)](#) 实例上为每个卷预置 100 IOPS 到 64,000 IOPS , 并在其他实例上最多预置 32,000。预配置 IOPS 与请求的卷大小 (GiB) 的最大比率为 50:1。例如 , 100 GiB 卷可以预配置为最高 5,000 IOPS。在支持的实例类型上 , 任何大小为 1280 GiB 或更大的卷可以预配置为最大值 64,000 IOPS ($50 \times 1280 \text{ GiB} = 64000$)。

任何预配置了最高 32000 IOPS 的 io1 卷支持 256 KiB 的最大 I/O 大小 , 可以得到最高 500 MiB/s 的吞吐量。当 I/O 大小达到最大时 , 吞吐量也将达到峰值 2000 IOPS。任何预配置了超过 32000 IOPS (最高为上限 64000 IOPS) 的卷支持 16 KiB 的最大 I/O 大小 , 可以得到最高 1000 MiB/s 的吞吐量。下图说明了这些性能特性 :



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。该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。

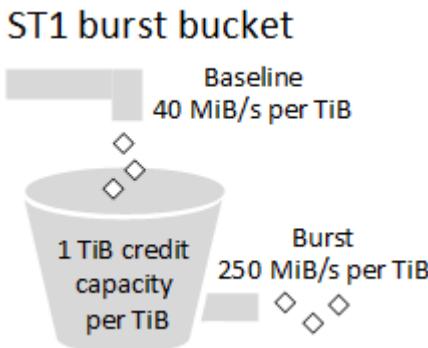
吞吐优化 HDD (st1) 卷虽然与 Cold HDD (sc1) 卷类似，但其设计用于支持频繁访问的数据。

该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 \(p. 795\)](#)。

吞吐量积分和突增性能

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，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，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积分上限的限制，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 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 500 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 40 MiB/s。

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，如下所示：

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

突增吞吐量从 125 MiB/s 到上限 500 MiB/s 变化，2 TiB 时达到上限，如下所示：

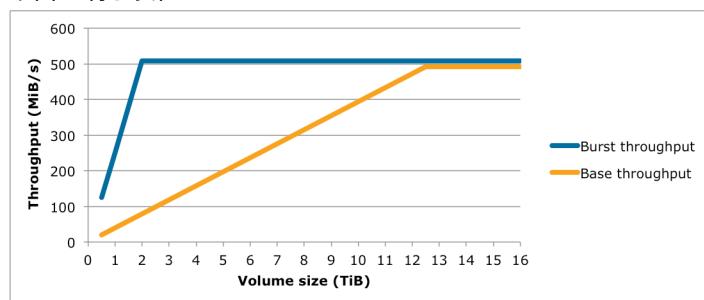
$$250 \text{ MiB/s}$$

$$2 \text{ TiB} \times \frac{\text{---}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

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
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 \(p. 795\)](#)。

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绝佳选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的块存储。不支持可启动的 sc1 卷。

Cold HDD (sc1) 卷虽然与 吞吐优化 HDD (st1) 卷类似，但其设计用于支持不频繁 访问的数据。

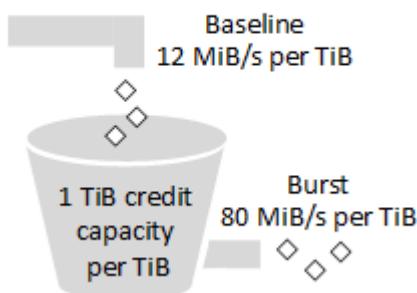
Note

该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 \(p. 795\)](#)。

吞吐量积分和突增性能

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，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。

SC1 burst bucket



sc1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，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 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 250 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 12 MiB/s。

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，如下所示：

$$12 \text{ MiB/s} \\ 16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

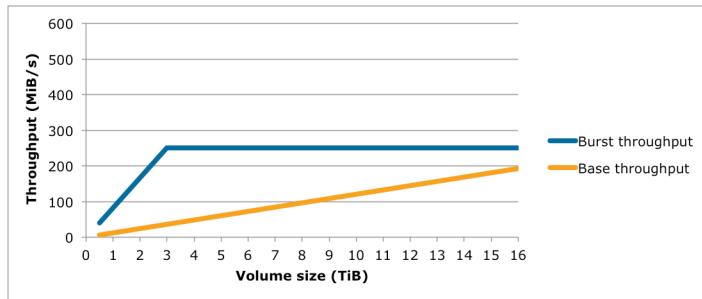
突增吞吐量从 40 MiB/s 到上限 250 MiB/s 变化，3.125 TiB 时达到上限，如下所示：

$$80 \text{ MiB/s} \\ 3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

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 \(p. 795\)](#)。

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 \(p. 795\)](#)。

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

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)*
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
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 积分。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 积分。

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 优化的实例 \(p. 863\)](#)。

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 积分百分比 (对于 `gp2`) 或吞吐量积分 (对于

st1 和 sc1)。有关 BurstBalance 指标以及与 I/O 相关的其他指标的更多信息，请参阅 [I/O 特征和监控 \(p. 878\)](#)。CloudWatch 还允许您设置警报，以便在 BurstBalance 值降到特定水平时通知您。有关更多信息，请参阅[创建 Amazon CloudWatch 警报](#)。

针对 EBS 卷的大小和配置的限制

Amazon EBS 卷的大小受制于块数据存储的物理和算术特性，以及操作系统 (OS) 和文件系统设计者的实现决策。AWS 对卷大小施加了额外的限制，以保证其服务的可靠性。

以下部分介绍了限制 EBS 卷的可用大小并提供配置 EBS 卷的建议的最重要因素。

目录

- [存储容量 \(p. 796\)](#)
- [服务限制 \(p. 796\)](#)
- [分区方案 \(p. 797\)](#)
- [数据块大小 \(p. 797\)](#)

存储容量

下表总结了 Amazon EBS 上的最常用文件系统的理论和实现存储容量 (假定 4096 字节块大小)。

分区方案	最大可寻址块数	理论最大大小 (块数 x 块大小)	Ext4 实现的最大大小*	XFS 实现的最大大小**	NTFS 实现的最大大小	EBS 支持的最大大小
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB	1 EiB = 1024 ² TiB (在 RHEL7 上认证的 50 TiB)	500 TiB (在 RHEL7 上认证)	256 TiB	16 TiB

* https://ext4.wiki.kernel.org/index.php/Ext4_Howto 和 <https://access.redhat.com/solutions/1532>

** <https://access.redhat.com/solutions/1532>

服务限制

Amazon EBS 将数据中心的大规模分布式存储提取到虚拟硬盘驱动器中。对安装在 EC2 实例上的操作系统而言，附加的 EBS 卷似乎是包含 512 字节磁盘扇区的物理硬盘驱动器。操作系统通过其存储管理实用程序对数据块 (或集群) 分配到这些虚拟扇区进行管理。分配与卷分区方案 (如主启动记录 (MBR) 或 GUID 分区表 (GPT)) 一致，并且属于已安装文件系统 (ext4、NTFS 等) 的功能。

EBS 不知道其虚拟磁盘扇区中包含的数据；它只会确保扇区的完整性。这意味着 AWS 操作和操作系统操作是彼此独立的。在您选择卷大小时，请注意二者的功能和限制，如以下情况中所示：

- EBS 当前支持最大卷大小 16 TiB。这意味着您可以创建一个大小为 16 TiB 的 EBS 卷，但操作系统是否能够识别该容量的全部取决于其自身的设计特征以及该卷的分区方式。
- Linux 引导卷可以使用 MBR 或 GPT 分区方案。MBR 支持最大为 2047 GiB (2 TiB - 1 GiB) 的引导卷。带 GRUB 2 的 GPT 支持 2 TiB 或更大的引导卷。如果您的 Linux AMI 使用 MBR，则引导卷限制为 2047 GiB，但您的非引导卷没有此限制。有关更多信息，请参阅[使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#)。

分区方案

除其他影响之外，分区方案还确定了可以在单个卷中唯一寻址的逻辑数据块的数量。有关更多信息，请参阅[数据块大小 \(p. 797\)](#)。正在使用的常见分区方案是主启动记录 (MBR) 和 GUID 分区表 (GPT)。这两个方案之间的重要差别可归纳如下。

MBR

MBR 使用 32 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{32} 个可能整数之一。卷的最大可寻址大小由以下公式指定：

$$(2^{32} - 1) \times \text{Block size} = \text{Number of addressable blocks}$$

MBR 卷的块大小通常限制为 512 字节。因此：

$$(2^{32} - 1) \times 512 \text{ bytes} = 2 \text{ TiB} - 512 \text{ bytes}$$

工程解决办法是提高 MBR 卷的这个 2 TiB 限制，但还没有被行业广泛采用。因此，即使 AWS 显示 MBR 卷的大小大于 2 TiB，Linux 和 Windows 也绝不会检测到它。

GPT

GPT 使用 64 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{64} 个可能整数之一。卷的最大可寻址大小由以下公式指定：

$$(2^{64} - 1) \times \text{Block size} = \text{Number of addressable blocks}$$

GPT 卷的块大小通常限制为 4,096 字节。因此：

$$\begin{aligned} & (2^{64} - 1) \times 4,096 \text{ bytes} \\ &= 2^{64} \times 4,096 \text{ bytes} - 1 \times 4,096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} - 4,096 \text{ bytes} \\ &= 2^{70} \times 2^6 \text{ bytes} - 4,096 \text{ bytes} \\ &= 64 \text{ ZiB} - 4,096 \text{ bytes} \end{aligned}$$

现实世界中的计算机系统不支持任何接近这个理论最大值的值。实现的文件系统大小目前仅限于 50 TiB（对于 ext4）和 256 TiB（对于 NTFS），这两个值都超过了 AWS 所施加的 16 TiB 限制。

数据块大小

现代硬盘驱动器上的数据存储是通过逻辑块寻址 来管理的，逻辑块寻址是一个抽象层，它允许操作系统在逻辑块中读取和写入数据，而无需详细了解底层硬件。操作系统依赖存储设备将块映射到其物理扇区。EBS 将 512 字节的扇区通告给操作系统，操作系统使用数据块（是扇区大小的数倍）将数据读写到磁盘。

逻辑数据块的行业默认大小当前为 4096 字节 (4 KiB)。由于某些工作负载受益于较小或较大的块大小，因此文件系统支持可在格式化期间指定的非默认块大小。应使用非默认块大小的情况不在本主题的范围之内，但块大小的选择会对卷的存储容量产生影响。下表显示了存储容量随不同块大小的变化：

块大小	最大卷大小
4 KiB (默认)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB

块大小	最大卷大小
64 KiB (最大)	256 TiB

EBS 对卷大小 (16 TiB) 施加的限制目前等于 4 KiB 数据块启用的最大大小。

创建 Amazon EBS 卷

您可以创建一个 Amazon EBS 卷，然后将它附加到同一可用区内的任何 EC2 实例。您可以选择创建加密 EBS 卷，但是加密卷只能附加到支持的实例类型。有关更多信息，请参阅[支持的实例类型 \(p. 852\)](#)。

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) 卷并将它附加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 Gb 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 EBS 优化的实例 \(p. 863\)](#)。

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块必须先进行初始化 (从 Amazon S3 提取并写入到卷)，然后您才能访问该块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。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 \(p. 879\)](#)。

创建卷的方法

- 您可以创建一个 EBS 卷并将其附加到正在运行的实例。有关更多信息，请参阅下面的过程。
- 如果通过指定块储存设备映射启动实例，则可以创建并附加 EBS 卷。有关更多信息，请参阅[使用启动实例向导启动实例 \(p. 375\)](#) 和[块储存设备映射 \(p. 923\)](#)。
- 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 \(p. 799\)](#)。

使用控制台创建新的 (空) 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。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
3. 在导航窗格中，选择 Elastic Block Store 和卷。
4. 选择 Create Volume。
5. 对于 Volume Type，选择卷类型。有关更多信息，请参阅[Amazon EBS 卷类型 \(p. 785\)](#)。
6. 对于 Size(GiB)，键入卷的大小。有关更多信息，请参阅[针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。
7. 对于 预配置 IOPS SSD 卷，在 IOPS 中，键入该卷应支持的每秒输入/输出操作数 (IOPS) 的最大值。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。EBS 卷只能附加到同一可用区中的 EC2 实例。
9. (可选) 如果实例类型支持 EBS 加密，并且您想要对卷进行加密，请选择加密此卷并选择一个 CMK。如果在此区域中启用了默认加密，则启用 EBS 加密并选择默认的 EBS 加密 CMK。您可以从主密钥中选择不同的 CMK，也可以粘贴您可以访问的任何密钥的完整 ARN。有关更多信息，请参阅[Amazon EBS Encryption \(p. 851\)](#)。
10. (可选) 选择 Create additional tags 以将标签添加到卷。对于每个标签，提供标签键和标签值。有关更多信息，请参阅[标记您的 Amazon EC2 资源 \(p. 940\)](#)。
11. 选择 Create Volume。卷状态为可用后，您可以将卷附加到实例。有关更多信息，请参阅[将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。

使用命令行创建新的 (空) 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。您必须知道快照的 ID，并且您必须具有快照的访问权限。有关快照的更多信息，请参阅 [Amazon EBS 快照 \(p. 812\)](#)。

考虑到速度、便利性和成本，EBS 快照是 Amazon EC2 上首选的备份工具。从快照还原卷时，您将重新创建其在过去特定时间点的状态，其所有数据都完整无缺。通过将已还原的卷附加到实例，您可以跨区域复制数据、创建测试环境、完整替换受损或损坏的生产卷，或检索特定文件和目录并将其传输到另一个附加的卷。有关更多信息，请参阅[Amazon EBS 快照 \(p. 812\)](#)。

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，附加的实例即可开始访问该卷及其所有数据。如果您的实例访问尚未加载的数据，卷会立即从 Amazon S3 下载请求的数据，然后在后台继续加载卷数据的剩余部分。

EBS 性能

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)。

对于从快照还原的卷，必须先从 Amazon S3 下载存储块并将其写入到卷中，然后才能访问这些块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。

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。为了避免最初在生产环境中出现这种性能下降，您可以使用以下其中一种方案：

- 强制立即初始化整个卷。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 879\)](#)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅 [Amazon EBS 快速快照还原 \(p. 859\)](#)。

EBS 加密

将自动加密从加密的快照中还原的新 EBS 卷。您还可以在从未加密的快照还原卷的同时对卷进行动态加密。加密的卷只能附加到支持 EBS 加密的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 852\)](#)。

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 [加密和快照复制 \(p. 820\)](#)。

从快照中创建卷

可以使用以下过程从快照中创建卷。

使用控制台从快照中创建 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。

要将快照还原到在不同区域的某个卷，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 \(p. 819\)](#)。

3. 在导航窗格中，选择 Elastic Block Store 和卷。
4. 选择 Create Volume。
5. 对于 Volume Type，选择卷类型。有关更多信息，请参阅[Amazon EBS 卷类型 \(p. 785\)](#)。
6. 对于 Snapshot ID (快照 ID)，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。

7. (可选) 选择加密此卷以更改卷的加密状态。如果启用了[默认加密 \(p. 853\)](#)，这是可选的。从主密钥中选择一个 CMK，以指定 EBS 加密的非默认 CMK。
8. 对于 Size (GiB)，键入卷的大小，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，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时，最小和最大卷大小将显示在 Size 旁边。有关更多信息，请参阅[针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。
9. 对于 预配置 IOPS SSD 卷，在 IOPS 中，键入该卷应支持的每秒输入/输出操作数 (IOPS) 的最大值。
10. 对于 Availability Zone，选择要在其中创建卷的可用区。EBS 卷只能附加到位于相同可用区中的 EC2 实例。
11. (可选) 选择 Create additional tags 以将标签添加到卷。对于每个标签，提供标签键和标签值。
12. 选择 Create Volume。
13. 从快照恢复某个卷后，您可以将其附加到实例上并开始使用。有关更多信息，请参阅[将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。
14. 如果您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，则必须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[Amazon EBS 弹性卷 \(p. 841\)](#)。

使用命令行从快照中创建 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

将 Amazon EBS 卷附加到实例

您可以将可用的 EBS 卷附加到与该卷处于同一可用区中的任一实例。

先决条件

- 确定您可以将多少个卷附加到您的实例。有关更多信息，请参阅[实例卷限制 \(p. 921\)](#)。
- 如果卷是加密的，则只能将它附加到支持 Amazon EBS 加密的实例。有关更多信息，请参阅[支持的实例类型 \(p. 852\)](#)。
- 如果某个卷有 AWS Marketplace 产品代码：
 - 卷只能附加到已停止的实例。
 - 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，然后将其附加到 Linux 实例。
 - AWS Marketplace 产品代码从卷复制到实例。

使用控制台将 EBS 卷附加到实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic Block Store 和卷。
3. 选择可用卷，然后选择 操作、附加卷。
4. 对于实例，开始键入实例的名称或 ID。从选项列表中选择实例 (仅显示与卷位于同一可用区域中的实例)。
5. 对于设备，您可以保留推荐的设备名称，也可以键入其他受支持的设备名称。有关更多信息，请参阅[Linux 实例上的设备命名 \(p. 922\)](#)。
6. 选择 Attach。

7. 连接到您的实例并安装卷。有关更多信息，请参阅[使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#)。

使用命令行将 EBS 卷附加到实例

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 卷可在 Linux 上使用

将某个 Amazon EBS 卷附加到您的实例后，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，然后进行挂载。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。

您可以制作 EBS 卷的快照以进行备份或在您创建其他卷时作为基准。有关更多信息，请参阅[Amazon EBS 快照 \(p. 812\)](#)。

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。

格式化并附加到附加卷

假设您的根设备 /dev/xvda 拥有一个具有 EBS 卷的 EC2 实例，并且您已使用 /dev/sdf 将一个空的 EBS 卷添加到了该实例。按照以下过程使新附加的卷可用。

在 Linux 上格式化并挂载 EBS 卷

1. 使用 SSH 连接到您的实例。有关更多信息，请参阅[连接到 Linux 实例 \(p. 423\)](#)。
2. 设备可附加到设备名称与您在块储存设备映射中指定的设备名称不同的实例。有关更多信息，请参阅[Linux 实例上的设备命名 \(p. 922\)](#)。使用 lsblk 命令可查看可用磁盘设备及其挂载点（如果适用），以帮助您确定要使用的正确设备名称。lsblk 的输出从完整的设备路径中去掉了 /dev/ 前缀。

以下是[基于 Nitro 的实例 \(p. 163\)](#)的示例输出，输出将 EBS 卷显示为 NVMe 块储存设备。根设备为 /dev/nvme0n1。如果尚未附加，则附加卷为 /dev/nvme1n1。

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1    259:0   0  10G  0 disk
nvme0n1    259:1   0   8G  0 disk
-nvme0n1p1  259:2   0   8G  0 part /
-nvme0n1p28 259:3   0   1M  0 part
```

以下是 T2 实例的示例输出。根设备为 /dev/xvda。如果尚未附加，则附加卷为 /dev/xvdf。

```
[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  10G  0 disk
```

3. 确定卷上是否存在文件系统。新卷为原始的块储存设备，您必须先在这种设备上创建文件系统，然后才能够挂载并使用它们。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 file -s 命令获取设备信息，例如其文件系统类型。如果输出仅显示 data（如以下示例输出），则说明设备上没有文件系统，您必须创建一个文件系统。

```
[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data
```

如果设备有文件系统，该命令会显示有关文件系统类型的信息。例如，以下示例输出显示具有 XFS 文件系统的根设备。

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

4. (有条件) 如果您在上一步中发现设备上存在文件系统，请跳过此步骤。如果您有一个空卷，请使用 mkfs -t 命令在该卷上创建一个文件系统。

Warning

如果要挂载已具有数据的磁盘（例如，通过快照还原的磁盘），请勿使用此命令。否则，您会格式化卷并删除现有数据。

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

如果出现“找不到 mkfs.xfs”错误，请使用以下命令安装 XFS 工具，然后重复上一命令：

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. 使用 mkdir 命令创建卷的挂载点目录。挂载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。下面的示例创建一个名为 /data 的目录。

```
[ec2-user ~]$ sudo mkdir /data
```

6. 使用以下命令在您在上一步中创建的目录挂载卷。

```
[ec2-user ~]$ sudo mount /dev/xvdf /data
```

7. 检查新卷挂载的文件权限，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](#)。
8. 重启实例后，挂载点不会自动保留。要在重启后自动挂载此 EBS 卷，请使用[重启后自动附加附加卷 \(p. 802\)](#)。

重启后自动附加附加卷

要在每次系统重启时附加附加的 EBS 卷，可在 /etc/fstab 文件中为该设备添加一个条目。

您可以在 /etc/fstab 中使用设备名称（如 /dev/xvdf），但建议改为使用设备的 128 位通用唯一标识符 (UUID)。设备名称可以更改，但 UUID 会在整个分区的使用寿命期间保留。通过使用 UUID，您可以减少系统在硬件重新配置后无法启动的机会。有关更多信息，请参阅[识别 EBS 设备 \(p. 861\)](#)。

重启后自动附加附加卷

1. (可选) 创建 /etc/fstab 文件的备份，以便在编辑时误损坏或删除此文件时使用。

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. 使用 blkid 命令查找设备的 UUID。

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

```
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"  
PARTLABEL="Linux" PARTUUID="02dc3d367-e87c-4f2e-9a72-a3cf8f299c10"  
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

对于 Ubuntu 18.04，请使用 `lsblk` 命令。

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

- 使用任何文本编辑器（如 `nano` 和 `vim`）打开 `/etc/fstab` 文件。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

- 将以下条目添加到 `/etc/fstab` 以在指定的挂载点挂载设备。这些字段是 `blkid`（或用于 Ubuntu 18.04 的 `lsblk`）返回的 UUID 值、挂载点、文件系统以及建议的文件系统挂载选项。有关更多信息，请参阅 `fstab` 的手册页（运行 `man fstab`）。

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2
```

Note

如果您要在未附加此卷的情况下启动实例（例如，将卷移动到另一个实例之后），`nofail` 附加选项允许该实例即使在卷附加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。

- 要检查条目是否有效，请在 `/etc/fstab` 中运行以下命令以卸载设备，然后挂载所有文件系统。如果未产生错误，则说明 `/etc/fstab` 文件正常，您的文件系统会在重启后自动挂载。

```
[ec2-user ~]$ sudo umount /data  
[ec2-user ~]$ sudo mount -a
```

如果收到错误消息，请解决文件中的错误。

Warning

`/etc/fstab` 文件中的错误可能显示系统无法启动。请勿关闭 `/etc/fstab` 文件中有错误的系统。

如果您无法确定如何更正 `/etc/fstab` 中的错误并且您在此过程的第一步中创建了一个备份文件，则可以使用以下命令从您的备份文件还原。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

查看有关 Amazon EBS 卷的信息

您可以查看有关您的 EBS 卷的描述信息。例如，您可以查看有关特定区域中所有卷的信息，或者查看有关单个卷的详细信息，包括其大小、卷类型、卷是否加密、加密卷所用的主密钥以及卷附加到的特定实例。

您可以获得有关您的 EBS 卷的其他信息，例如该实例的操作系统上有多少空间磁盘可用。

查看描述性信息

使用控制台查看有关 EBS 卷的信息

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 `Volumes`。
- 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。

4. 在详细信息窗格中，您可以检查所提供的关于卷的信息。

查看已附加到实例的 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 Instances (实例)。
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)

查看可用磁盘空间

您可以获得有关您的 EBS 卷的其他信息，例如该实例的 Linux 操作系统上有多少空间磁盘可用。例如，使用以下命令：

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1      xfs       8.0G  1.2G  6.9G  15% /
```

监控您的卷状态

Amazon Web Services (AWS) 自动提供可用于监控 Amazon Elastic Block Store (Amazon EBS) 卷的数据。

目录

- [EBS 卷状态检查 \(p. 804\)](#)
- [EBS 卷事件 \(p. 806\)](#)
- [使用一个受损卷工作 \(p. 807\)](#)
- [使用自动启用 IO 卷属性 \(p. 809\)](#)

有关其他监控信息，请参阅[Amazon EBS 的 Amazon CloudWatch 指标 \(p. 889\)](#)和[Amazon EBS 的 Amazon CloudWatch Events \(p. 893\)](#)。

EBS 卷状态检查

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，默认禁用从任何附加的 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到该卷的 I/O 来解决卷的损坏状态。我们将等待您启用 I/O，在此期间您有机会决定是继续让您的实例使用该卷，还是在使用该卷之前先使用命令（如 fsck）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）。

如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是“受损”，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 I/O 卷属性（在 API 中为 autoEnableIO），那么该卷会继续通过状态检查。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 不会自动启用。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 \(p. 879\)](#)。

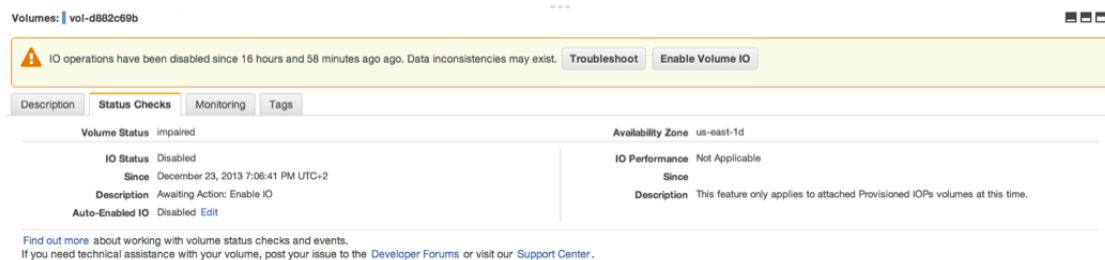
下表列出了 Amazon EBS 卷的状态。

卷状态	I/O 使能状态	I/O 性能状态 (只适用于预配置 IOPS 卷)
ok	使能 (I/O 使能或 I/O 自动使能)	正常 (卷的期望性能)
warning	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)
impaired	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)
insufficient-data	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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择卷。卷状态列显示每个卷的运行状态。
- 要查看卷的状态详细信息，请选中该卷，然后选择状态检查。



4. 如果您的卷状态检查返回故障 (状态是受损) , 请参阅[使用一个受损卷工作 \(p. 807\)](#)。

另外 , 您还可以在导航器中选择事件来查看实例和卷所有的事件。有关更多信息 , 请参阅[EBS 卷事件 \(p. 806\)](#)。

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)

EBS 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 , 它将会禁用从任何附加的 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。

想要自动使能具有潜在不一致性卷上的 I/O , 您可以改变自动启用 IO 卷属性 (在 API 中为 `autoEnableIO`) 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 \(p. 807\)](#)。

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。当您明确启用 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。列出具有事件的所有实例和卷。

3. 可以按卷进行筛选以便仅查看卷状态。您也可以筛选指定的状态类型。
4. 选择一个卷以查看其特定事件。

The screenshot shows the AWS CloudWatch Events console with a list of events. The first event is selected, showing detailed information:

Availability Zone	us-east-1d
Event Type	potential-data-inconsistency
Event Status	Awaiting Action: Enable IO
IO status	IO Disabled
Attached to	i-93aae4ea
Start Time	December 23, 2013 7:09:20 PM UTC+2
End time	

Below the table, there is a note: "Find out more about [monitoring volume events](#).

如果您的卷 I/O 被禁用，请参阅[使用一个受损卷工作 \(p. 807\)](#)。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

如果卷受损，请使用以下选项，因为卷的数据可能不一致。

选项

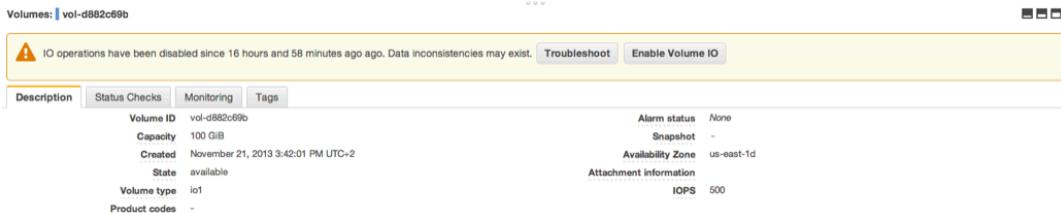
- [选择 1：在附加到它的实例上的卷上进行一次一致性检查。 \(p. 807\)](#)
- [选择 2：使用其他实例在该卷上进行一次一致性检查 \(p. 808\)](#)
- [选择 3：如果您不再需要它，请删除该卷 \(p. 809\)](#)

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，选择卷。
 - c. 选择要使能 I/O 操作的卷。
 - d. 在详细信息窗格中，选择启用卷 IO，然后选择是，请启用。



3. 检查卷上数据。

- a. 运行 fsck 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 AWS 支持中心。选择问题排查，然后在状态检查故障排除对话框上选择联系客户服务提交一个支持案例。

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

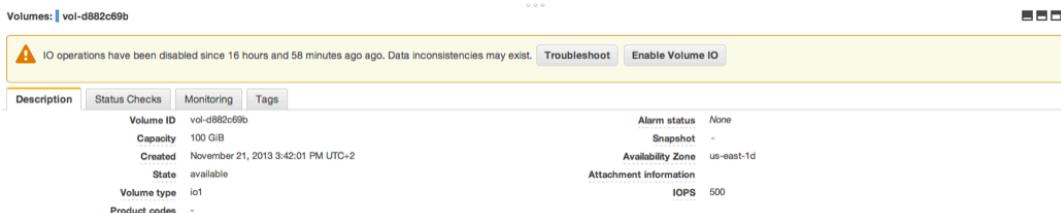
按照以下程序在您的产品环境外检查该卷。

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，选择卷。
 - 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，选择卷。
 - b. 选择您在之前的步骤中分离的卷。
 - c. 在详细信息窗格中，选择启用卷 IO，然后选择是，请启用。



4. 将该卷附加到另一个实例。有关更多信息，请参阅 [启动实例 \(p. 374\)](#) 和 [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。

5. 检查卷上数据。
 - a. 运行 fsck 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 AWS 支持中心。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 \(p. 812\)](#)。

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 \(p. 799\)](#)。

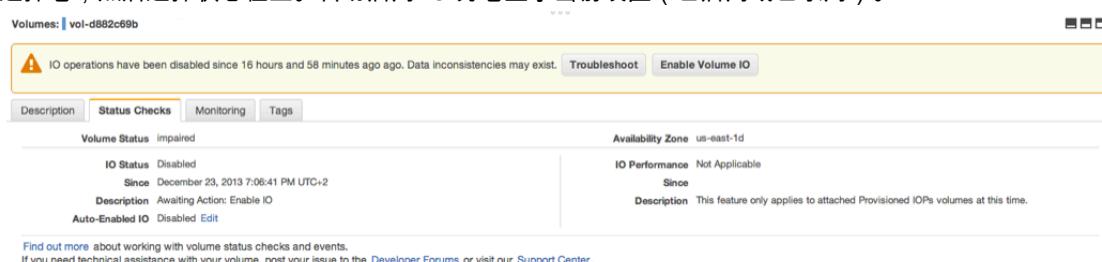
使用自动启用 IO 卷属性

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何附加的 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查明故障的原因。如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态为受损，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 IO 卷属性（在 API 中为 autoEnableIO），在卷和实例之间的 I/O 会自动重新启用，并且卷将通过状态检查。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[EBS 卷事件 \(p. 806\)](#)。

该过程介绍如何查看和修改卷的自动启用 IO 属性。

在控制台中查看卷的自动启用 IO 属性

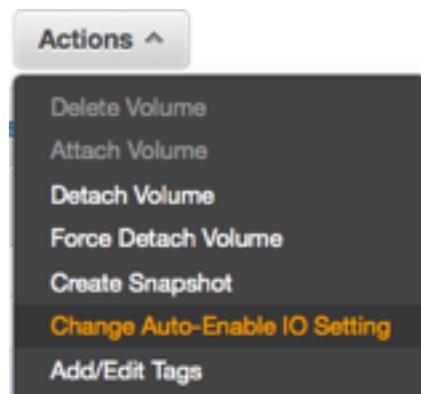
1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择卷。
3. 选择卷，然后选择状态检查。自动启用 IO 为卷显示当前设置（已启用或已禁用）。



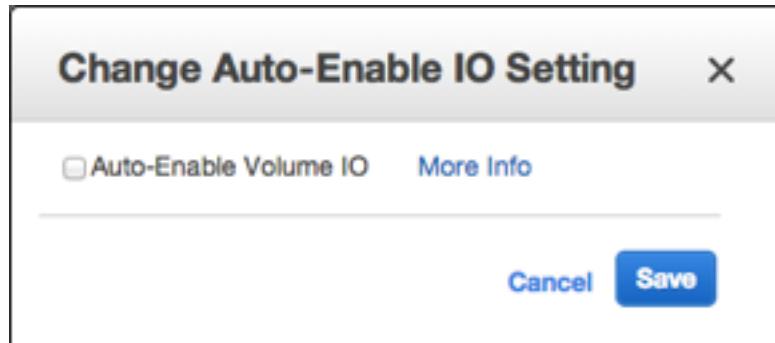
在控制台中修改卷的自动启用 IO 属性

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择卷。

3. 选择卷并选择操作、更改自动启用 IO 设置。此外，选择状态检查选项卡，对于自动启用 IO，选择编辑。



4. 选中自动启用卷 IO 复选框以为受损卷自动启用 I/O。想要禁用该功能，请清除复选框。



5. 选择保存。

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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

将 Amazon EBS 卷与实例分离

您可以明确地将 Amazon EBS 卷与实例分离，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，则在分离卷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 \(p. 812\)](#)。

该示例卸载了卷，然后明确地将其从实例分离。当您要终止实例或将卷附加到其他实例时，这会非常有用。要验证该卷是否不再附加到该实例，可参阅[查看有关 Amazon EBS 卷的信息 \(p. 803\)](#)。

您可以重新附加分离的卷（无需卸载），但可能不能获得相同挂载点。如果分离时正在写入卷，那么卷上的数据可能不同步。

使用控制台将 EBS 卷分离

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 卷从实例分离

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

以下内容介绍在分离卷时遇到的常见问题并以及如何解决这些问题。

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制作快照。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附加新卷。

- 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。请将该选项仅用作在不得已的情况下从故障实例分离卷的方法，或是在要删除卷的情况下分离卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用该选项，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。
- 如果尝试分离仍挂载的卷，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：

```
aws ec2 describe-volumes --region us-west-2 --volume-ids vol-1234abcd
{
    "Volumes": [
        {
            "Status": "in-use"
        }
    ]
}
```

```
"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，并且再也不能附加到任何实例。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（未附加到实例）。有关更多信息，请参阅[将 Amazon EBS 卷与实例分离 \(p. 810\)](#)。

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)

Amazon EBS 快照

您可以通过拍摄时间点快照将 Amazon 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。由于无需复制数据，这将最大限度缩短创建快照所需的时间和增加存储成本节省。删除快照时，仅会删除该快照特有的数据。每个快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。

当您基于快照创建新 EBS 卷时，新卷将开始作为用于创建快照的原始卷的精确副本。复制的卷将在后台加载数据，让您立即开始使用数据。如果您访问尚未加载的数据，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 \(p. 815\)](#)。

多卷快照

快照可用于创建关键工作负载的备份，如跨多个 EBS 卷的大型数据库或文件系统。利用多卷快照，您可以跨附加到 EC2 实例的多个 EBS 卷拍摄准确的时间点、数据协调和崩溃一致性快照。您不再需要停止实例或在多个卷之间协调来确保崩溃一致性，因为快照将跨多个 EBS 卷自动进行拍摄。有关更多信息，请参阅[创建 Amazon EBS 快照 \(p. 815\)](#)下创建多卷 EBS 快照的步骤。

您可以通过 CloudWatch Events 跟踪 EBS 快照的状态。有关更多信息，请参阅[Amazon EBS 的 Amazon CloudWatch Events \(p. 893\)](#)。

目录

- [增量快照的工作原理 \(p. 813\)](#)
- [复制和共享快照 \(p. 814\)](#)
- [快照的加密支持 \(p. 815\)](#)
- [创建 Amazon EBS 快照 \(p. 815\)](#)
- [删除 Amazon EBS 快照 \(p. 817\)](#)
- [复制 Amazon EBS 快照 \(p. 819\)](#)
- [查看 Amazon EBS 快照信息 \(p. 822\)](#)
- [共享 Amazon EBS 快照 \(p. 822\)](#)
- [访问 EBS 快照的内容 \(p. 824\)](#)
- [自动化 Amazon EBS 快照生命周期 \(p. 831\)](#)

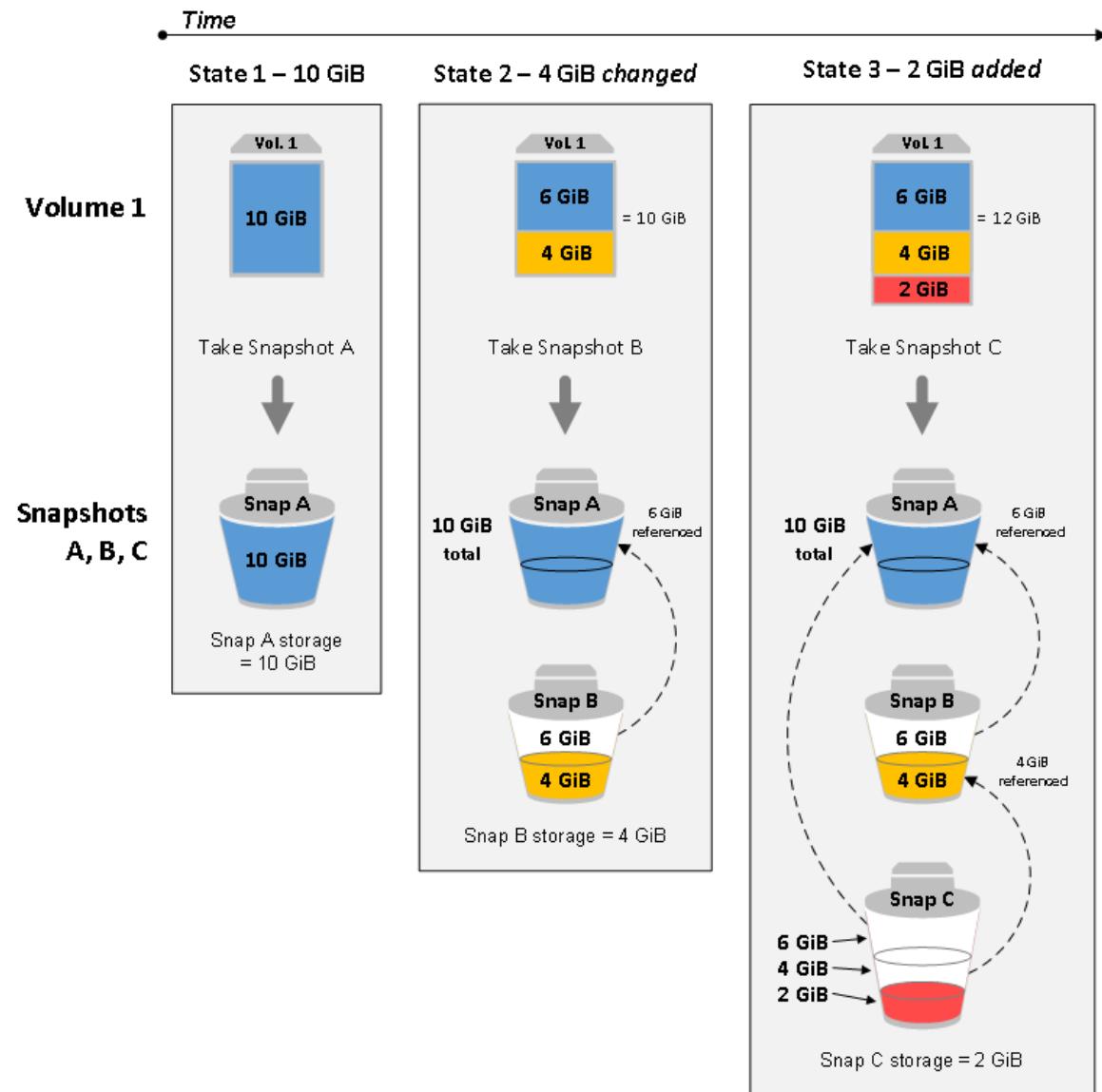
增量快照的工作原理

本节阐述 EBS 快照如何捕获卷在某一时间点的状态，以及正在更改的卷的连续快照如何创建这些更改的历史记录。

在下图中，卷 1 在三个时间点上显示。为这三个卷状态分别制作快照。

- 在状态 1 中，该卷具有 10 GiB 数据。因为快照 A 是为该卷制作的首个快照，因此必须复制所有 10 GiB 数据。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，4 GiB 数据已更改。快照 B 只需复制并存储制作快照 A 后更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已复制并存储在快照 A 中）将由快照 B 引用而不是再次复制。这通过虚线箭头指示。
- 在状态 3 中，2 GiB 数据已添加到该卷中，共计 12 GiB 数据。快照 C 需要复制制作快照 B 之后添加的 2 GiB 数据。如虚线箭头所示，快照 C 还引用了存储在快照 B 中的 4 GiB 数据和存储在快照 A 中的 6 GiB 数据。
- 三个快照共需 16 GiB 存储空间。

卷的多个快照之间的关系



Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

有关删除快照后如何管理数据的更多信息，请参阅[删除 Amazon EBS 快照 \(p. 817\)](#)。

复制和共享快照

您可通过修改快照的访问权限来跨 AWS 账户共享快照。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 \(p. 822\)](#)。

快照受限于创建它的 AWS 区域。在您创建 EBS 卷的快照之后，可在同一个区域中使用它来创建新卷。有关更多信息，请参阅[从快照还原 Amazon EBS 卷 \(p. 799\)](#)。您还可以跨区域复制快照，从而能够使用多个区域进行地理扩展、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 \(p. 819\)](#)。

快照的加密支持

EBS 快照完全支持 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。
- 您从已拥有或有权访问的未加密快照创建的卷可进行动态加密。
- 在复制您拥有的未加密快照时，您可以在复制过程中对其加密。
- 在复制您拥有或有权访问的加密快照时，可在复制过程中使用其他密钥对其进行重新加密。
- 对于从未加密的快照中创建的加密卷，拍摄的第一个快照始终是完整快照。
- 为重新加密的卷拍摄的第一个快照（具有与源快照不同的 CMK）始终是完整快照。

Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

[创建 Amazon EBS 快照 \(p. 815\)](#) 和 [复制 Amazon EBS 快照 \(p. 819\)](#) 中提供了可能的快照加密方案的完整文档。

有关更多信息，请参阅 [Amazon EBS Encryption \(p. 851\)](#)。

创建 Amazon EBS 快照

您可以创建 EBS 卷的时间点快照，并将其用作新卷的基准或用于数据备份。如果您定期为卷拍摄快照，则快照为增量快照，新快照上仅保存自上次快照后已更改的块。

快照是异步制作的；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。

您可以制作正在使用的已附加卷的快照。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制作快照，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，您可以重新挂载并使用卷。

要简化快照的管理，您可以在创建期间为快照添加标签，也可在创建后添加。例如，您可以应用标记，描述该快照对应的原始卷，或描述用于将原始卷附加到实例上的设备名称。有关更多信息，请参阅 [标记您的 Amazon EC2 资源 \(p. 940\)](#)。

快照加密

从加密卷制作的快照会自动加密。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 Encryption \(p. 851\)](#)。

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 \(p. 822\)](#)。

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 \(p. 822\)](#)。

Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

多卷快照

您可以创建多卷快照，这些快照是连接到单个 EC2 实例的所有 EBS 卷的时间点快照。您还可以创建生命周期策略以自动化多卷快照的创建和保留。有关更多信息，请参阅 [自动化 Amazon EBS 快照生命周期 \(p. 831\)](#)。

创建快照后，每个快照将视为单个快照。您可以执行所有快照操作，如还原、删除和跨区域/账户复制，就像您使用单个卷快照执行的操作一样。您还可以标记多卷快照，就像您使用单个卷快照执行的操作一样。我们建议您标记多个卷快照以在还原、复制或保留操作期间集中管理它们。

多卷、崩溃一致性快照通常以集的形式进行还原。这有助于通过使用实例 ID、名称或其他相关详细信息标记您的集，以标识位于崩溃一致性快照集中的快照。还可以选择自动将标签从源卷复制到相应的快照。这将帮助您设置快照元数据（如访问策略、附件信息和成本分配）以匹配源卷。

创建多卷快照后，其行为方式与任何其他快照类似。您可以执行所有操作，如跨区域和账户还原、删除和复制。还可以标记快照。我们建议您标记多卷快照以在还原、复制或保留操作期间集中管理它们。

创建快照后，它们会在确切的时间点创建时显示在您的 EC2 控制台中。这些快照将统一进行管理，因此，如果卷集中的任一快照失败，所有其他快照会显示错误状态。

注意事项

创建快照时需考虑以下事项：

- 当您为充当根设备的 EBS 卷创建快照时，应在拍摄快照之前停止实例。
- 无法从启用了休眠的实例创建快照。
- 无法从已休眠实例创建快照。
- 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 个 pending 快照，而一个 st1 或 sc1 卷只能有 1 个 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。
- 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。

创建快照

使用以下过程从指定的卷中创建快照。

使用控制台创建快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 Elastic Block Store (弹性数据块存储) 下选择 Snapshots (快照)。
3. 选择 Create Snapshot (创建快照)。
4. 对于选择资源类型，选择卷。
5. 对于卷，选择此卷。
6. (可选) 输入快照的描述。
7. (可选) 选择添加标签以向快照添加标签。对于每个标签，提供标签键和标签值。
8. 选择 Create Snapshot (创建快照)。

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)

创建多卷快照

使用以下过程从实例的卷中创建一个快照。

使用控制台创建多卷快照

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 (弹性数据块存储) 下选择 Snapshots (快照)。
3. 选择 Create Snapshot (创建快照)。
4. 对于选择资源类型，选择实例。
5. 选择要为所有已附加的 EBS 卷创建同步备份的实例 ID。多卷快照对于每个实例支持多达 40 个 EBS 卷。
6. (可选) 设置 Exclude root volume (排除根卷)。
7. (可选) 设置 Copy tags from volume (从卷复制标签) 标记，以自动将标签从源卷复制到相应快照。这将设置快照元数据 (如访问策略、附件信息和成本分配) 以匹配源卷。
8. (可选) 选择添加标签以向快照添加标签。对于每个标签，提供标签键和标签值。
9. 选择 Create Snapshot (创建快照)。

快照创建期间，将一起管理快照。如果卷集中的其中一个快照失败，则其他快照将移至卷集的错误状态。您可以使用 [CloudWatch Events](#) 监控快照的进度。在快照创建过程完成后，CloudWatch 将生成一个事件，其中包含受影响实例的状态及所有相关的快照详细信息。

使用命令行创建多卷快照

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-snapshots](#) (AWS CLI)
- [New-EC2SnapshotBatch](#) (适用于 Windows PowerShell 的 AWS 工具)

删除 Amazon EBS 快照

删除快照时，仅删除快照专门引用的数据。除非引用该数据的所有快照都删除，否则不会删除唯一数据。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。

删除卷的快照对卷无任何影响。删除卷对从它生成的快照无任何影响。

如果定期拍摄卷快照，则这些快照为增量快照。这意味着仅在您的上一个快照后更改的设备数据块将保留在新快照中。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。存在于卷上、保存在较早快照中或快照系列中的数据，以后从该卷上删除时，仍视为较早快照的唯一数据。此唯一数据不从快照序列中删除，除非引用该唯一数据的所有快照都删除。

删除快照可能不会降低组织的数据存储成本。其他快照可引用已删除快照的数据，已引用的数据总是会被保留。如果您删除了一个快照，而该快照包含以后的快照使用的数据，那么与所引用数据关联的成本将分配到后来的快照。有关快照如何存储数据的更多信息，请参阅[增量快照的工作原理 \(p. 813\)](#)和下面的示例。

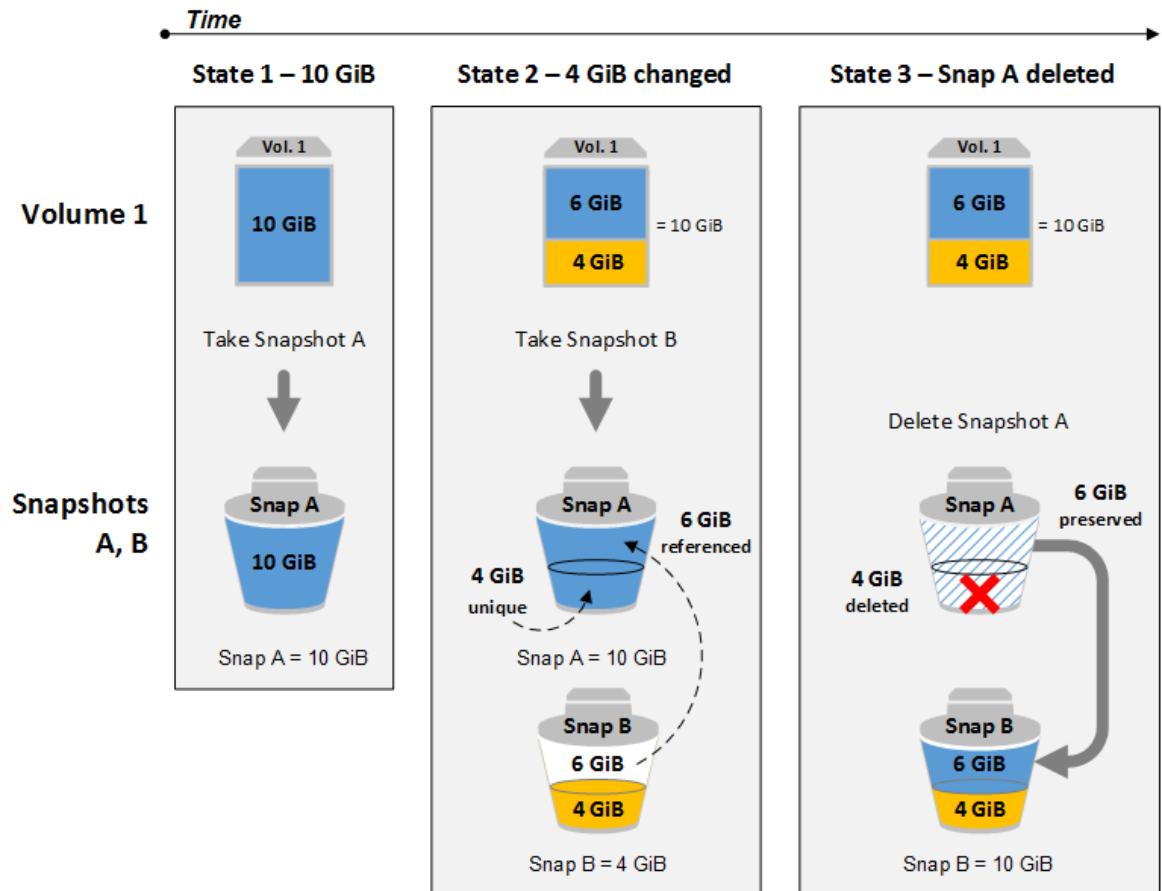
要删除多卷快照，请使用您在创建快照时应用于多卷组的标签检索组的所有快照。然后，分别删除这些快照。系统不会阻止您删除多卷快照组中的各个快照。

在下图中，卷 1 在三个时间点上显示。某个快照已捕获前两种状态，在第三种状态中，某个快照已被删除。

- 在状态 1 中，该卷具有 10 GiB 数据。因为快照 A 是为该卷制作的首个快照，因此必须复制所有 10 GiB 数据。

- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，4 GiB 数据已更改。快照 B 只需复制并存储制作快照 A 后更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已复制并存储在快照 A 中）将由快照 B 引用而不是再次复制。这通过虚线箭头指示。
- 在状态 3 中，卷自状态 2 以来未更改，但快照 A 已被删除。快照 B 引用的存储在快照 A 中的 6 GiB 数据现已移至快照 B，如粗箭头所示。因此，您仍需支付存储 10 GiB 数据的费用；快照 A 中保留的 6 GiB 未更改数据和快照 B 中的 4 GiB 已更改数据。

示例 1：删除快照及其由其他快照引用的部分数据



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 Linux AMI \(p. 142\)](#)。

如需使用控制台删除快照

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Snapshots (快照)。
- 选择快照，然后从 Actions 列表中选择 Delete。
- 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)

Note

尽管您可以删除仍在制作的快照，但该快照必须先完成，删除才能生效。这可能需要很长时间。如果您还具有并发快照限制（最多同时制作 5 个快照），而您尝试再制作一个快照，则可能遇到 `ConcurrentSnapshotLimitExceeded` 错误。

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 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 区域复制到另一个区域，也可在相同区域内复制。Amazon S3 服务器端加密（256 位 AES）可在复制操作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 ID。

要将多卷快照复制到另一个 AWS 区域，请使用您在创建快照时应用于多卷快照组的标签检索快照。然后分别将快照复制到另一个区域。

有关复制 Amazon RDS 快照的信息，请参阅 Amazon RDS 用户指南 中的 [复制数据库快照](#)。

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 \(p. 822\)](#)。

有关在 AWS 区域和账户之间复制快照的定价信息，请参阅 [Amazon EBS 定价](#)。请注意，只要快照副本的加密状态不更改，单个账户和区域内的快照复制操作就完全不会复制任何实际数据，因此是免费的。

Note

如果将快照复制到新的区域，则将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

使用案例

- 地理扩展：在新的 AWS 区域中启动您的应用程序。
- 迁移：将应用程序迁移到新区域，以实现更好的可用性以及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。出现灾难情况时，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。

先决条件

- 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。

限制

- 每个账户最多可以向单个目标区域进行 5 个并发快照复制请求。

- 用户定义的标签不会从源快照复制到新快照。您可以在复制操作期间或之后添加用户定义的标签。有关更多信息，请参阅 [标记您的 Amazon EC2 资源 \(p. 940\)](#)。
- 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。

跨区域增量复制

快照副本是否为增量副本是由最近完成的快照复制决定的。在跨区域复制快照时，如果满足以下条件，则副本为增量副本：

- 快照以前已复制到目标区域。
- 最新的快照副本仍位于目标区域中。
- 目标区域中的所有快照副本均未加密，或者是使用同一 CMK 加密的。

如果删除了最新的快照副本，则下一个副本是完整副本，而不是增量副本。如果在启动另一个副本时第一个副本仍处于待处理状态，则第二个副本也是完整副本。如果第一个副本已完成，但在启动另一个副本时第二个副本仍处于待处理状态，则第三个副本是第一个副本的增量副本。

我们建议您使用卷 ID 和创建时间来标记快照，以便在目标区域中跟踪卷的最新快照副本。

要确定快照副本是否为增量副本，请检查 [copySnapshot \(p. 899\)](#) CloudWatch 事件。

加密和快照复制

在复制快照时，您可以加密副本，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会生成完整（非增量）副本，这可能产生更多的数据传输和存储费用。

要复制从其他 AWS 账户共享的加密快照，您必须拥有使用该快照以及用于加密快照的客户主密钥（CMK）的权限。使用与您共享的加密快照时，我们建议您使用您拥有的 CMK 复制快照以对其进行重新加密。这样，即使原始 CMK 泄露或拥有者将其撤销，您也不会失去对使用快照创建的任何加密卷的访问权限。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 822\)](#)。

通过将 `Encrypted` 参数设置为 `true`，您可以将加密应用于 EBS 快照。（如果启用 [默认加密 \(p. 853\)](#)，则 `Encrypted` 参数是可选的）。

（可选）您可以使用 `KmsKeyId` 指定用于加密快照副本的自定义密钥。（即使启用了默认加密，也必须将 `Encrypted` 参数设置为 `true`。）如果未指定 `KmsKeyId`，则用于加密的密钥取决于源快照的加密状态及其所有权。

下表描述了每种可能的设置组合的加密结果。

加密结果：复制快照

是否已设置 <code>Encrypted</code> 参数？	是否已默认设 置加密？	源快照	默认（未指定 <code>KmsKeyId</code> ）	自定义（指定 <code>KmsKeyId</code> ）
否	否	您拥有的未加密快照	未加密	不适用
否	否	您拥有的加密快照	按相同密钥加密	
否	否	与您共享的未加密快 照	未加密	
否	否	与您共享的加密快照	按默认 CMK 加密*	
是	否	您拥有的未加密快照	按默认 CMK 加密	按指定的 CMK 加密**

是否已设置 Encrypted 参数 ?	是否已默认设 置加密 ?	源快照	默认 (未指定 KmsKeyId)	自定义 (指定 KmsKeyId)
是	否	您拥有的加密快照	按相同密钥加密	
是	否	与您共享的未加密快 照	按默认 CMK 加密	
是	否	与您共享的加密快照	按默认 CMK 加密	
否	是	您拥有的未加密快照	按默认 CMK 加密	不适用
否	是	您拥有的加密快照	按相同密钥加密	
否	是	与您共享的未加密快 照	按默认 CMK 加密	
否	是	与您共享的加密快照	按默认 CMK 加密	
是	是	您拥有的未加密快照	按默认 CMK 加密	按指定的 CMK 加密
是	是	您拥有的加密快照	按相同密钥加密	
是	是	与您共享的未加密快 照	按默认 CMK 加密	
是	是	与您共享的加密快照	按默认 CMK 加密	

* 这是用于对 AWS 账户和区域进行 EBS 加密的默认 CMK。默认情况下，这是用于 EBS 的唯一 AWS 托管 CMK，您也可以指定自定义的托管 CMK。有关更多信息，请参阅 [用于 EBS 加密的默认密钥 \(p. 853\)](#)。

** 这是为复制操作指定的客户托管的 CMK。此 CMK 替代默认的 CMK 用于 AWS 账户和区域。

复制快照

使用以下过程，通过 Amazon EC2 控制台复制快照。

使用控制台复制快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
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：
 - 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。如果启用了 [默认加密 \(p. 853\)](#)，则会设置加密选项，无法从快照控制台中取消设置该选项。如果设置了 Encryption (加密) 选项，则可以选择将其加密到客户托管 CMK (方法为在字段中选择一个 CMK)，如下所述。

无法从加密的快照中去除加密。

Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整 (非增量) 副本，从而导致额外的延迟和存储成本。

- Master Key (主密钥)：将用于对此快照进行加密的客户主密钥 (CMK)。最初会显示您账户的默认密钥，但您可以选择性地从账户中的主密钥中选择，也可以从其他账户键入/粘贴密钥的 ARN。您可在 IAM 控制台 <https://console.aws.amazon.com/iam/> 中创建新的加密主密钥。
5. 选择 Copy。
 6. 在复制快照确认对话框中，选择快照以转至指定区域的快照页面，或选择关闭。

要查看复制过程的进度，请切换到目标区域，然后刷新快照页面。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，如以下示例所示。

```
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”。

在复制加密的快照时，您必须对默认 CMK 具有 `DescribeKey` 权限。显式拒绝这些权限将导致复制失败。有关管理 CMK 密钥的信息，请参阅[控制对客户主密钥的访问权限](#)。

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 (快照)。
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. 要查看有关快照的更多信息，请选择该选项。

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

通过修改快照的权限，您可以与您指定的 AWS 账户共享快照。您已授权的用户可以使用您共享的快照作为基础来创建自己的 EBS 卷，同时您的原始快照不受影响。如选择，您可使您的未加密快照对所有 AWS 用户公开可用。您不能使加密快照公开可用。

共享加密快照时，还必须共享用于加密快照的客户托管 CMK。您可以在创建客户托管 CMK 时或以后的某个时间向客户托管 CMK 应用跨账户权限。

Important

共享快照时，您可以让其他人访问快照上的所有数据。仅与您要与其共享所有快照数据的人共享快照。

注意事项

共享快照时需考虑以下事项：

- 快照受限于在其中创建它们的区域。要与其他区域共享快照，请将快照复制到该区域。有关更多信息，请参阅[复制 Amazon EBS 快照 \(p. 819\)](#)。
- 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 \(p. 933\)](#)。
- 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客户托管 CMK 加密。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[创建密钥](#)。
- 必须为正在访问加密快照的共享 CMK 用户授予对密钥执行以下操作的权限：kms:DescribeKey、kms>CreateGrant、GenerateDataKey 和 kms:ReEncrypt。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[控制对客户主密钥的访问权限](#)。

使用控制台共享未加密快照

使用控制台共享快照

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 **Snapshots** (快照)。
- 选择快照，然后依次选择操作、修改权限。
- 使快照公开可用或与特定 AWS 账户共享快照，如下所示：
 - 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。
 - 要与一个或多个 AWS 账户共享快照，请选择 **Private (私有)**，在 **AWS Account Number (AWS 账号)** 中输入 AWS 账户 ID (无连字符)，然后选择 **Add Permission (添加权限)**。对任何其他 AWS 账户重复此步骤。
- 选择 **Save (保存)**。

使用与您私下共享的未加密快照

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 **Snapshots** (快照)。
- 选择私有快照筛选条件。
- 按 ID 或描述查找快照。您可以像使用任何其他快照一样使用此快照；例如，您可以从快照创建卷或将快照复制到其他区域。

使用控制台共享加密快照

使用控制台共享加密快照

- 从 <https://console.aws.amazon.com/kms> 打开 AWS KMS 控制台。
- 要更改 AWS 区域，请使用页面右上角的区域选择器。

3. 在导航窗格中，选择 Customer managed keys (客户托管密钥)。
4. 选择用于加密快照的客户托管密钥的别名。
5. 选择 Add other AWS accounts (添加其他 AWS 账户)，并按提示输入 AWS 账户 ID。要添加另一个 AWS 账户，选择 Add another AWS account (添加另一个 AWS 账户) 并输入 AWS 账户 ID。添加完所有 AWS 账户后，选择 Save changes (保存更改)。
6. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
7. 在导航窗格中，选择 Snapshots (快照)。
8. 选择快照，然后依次选择 Actions (操作)、Modify Permissions (修改权限)。
9. 对于每个 AWS 账户，在 AWS Account Number (AWS 账号) 中输入 AWS 账户 ID，然后选择 Add Permission (添加权限)。添加完所有 AWS 账户时，选择 Save (保存)。

使用与您共享的加密快照

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots (快照)。
3. 选择私有快照筛选条件。（可选）添加加密筛选条件。
4. 按 ID 或描述查找快照。
5. 选择快照，然后依次选择操作、复制。
6. （可选）选择一个目标区域。
7. 使用显示在 Master Key (主密钥) 中的密钥加密快照的副本。默认情况下，所选密钥是您账户的默认 CMK。要选择客户托管 CMK，请在输入框内单击以查看可用密钥的列表。
8. 选择 Copy (复制)。

使用命令行共享快照

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要将快照与特定 AWS 账户共享，请将用户设置为 AWS 账户的 ID。

使用命令行修改快照权限

使用以下命令之一：

- [modify-snapshot-attribute](#) (AWS CLI)
- [Edit-EC2SnapshotAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行查看快照权限

使用以下命令之一：

- [describe-snapshot-attribute](#) (AWS CLI)
- [Get-EC2SnapshotAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

访问 EBS 快照的内容

您可以使用 Amazon Elastic Block Store (EBS) 直接 API 直接读取 EBS 快照上的数据，并识别两个快照之间的差异。您可以查看 EBS 快照中数据块的详细信息，比较两个快照之间的数据块差异，并直接访问快照中的数据。如果您是为 EBS 提供备份服务的独立软件供应商 (ISV)，则利用 EBS direct APIs，可以更轻松、更具成本效益地通过 EBS 快照跟踪 EBS 卷上的增量更改。无需从 EBS 快照创建新卷，然后使用 EC2 实例来比较差异，即可完成此操作。

本用户指南概述了构成 EBS direct APIs 的元素，并提供了如何有效使用这些元素的示例。有关 API 的操作、数据类型、参数和错误的更多信息，请参阅 [EBS direct APIs 参考](#)。

- [了解 EBS direct APIs \(p. 825\)](#)
- [IAM 用户的权限 \(p. 826\)](#)
- [通过命令行使用 EBS direct APIs \(p. 828\)](#)
- [通过 API 或 AWS 开发工具包使用 EBS direct APIs \(p. 830\)](#)
- [EBS direct APIs 常见问题 \(p. 830\)](#)

了解 EBS direct APIs

下面是您在开始使用 EBS direct APIs 前应了解的关键元素。

快照

快照是备份 EBS 卷中的数据的主要方式。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的数据。有关更多信息，请参阅 [Amazon EBS 快照 \(p. 812\)](#)。

Note

EBS direct APIs 不支持公有快照。

数据块

数据块是快照中的数据片段。每个快照可以包含数千个数据块。快照中的所有数据块都具有固定大小。

数据块索引

数据块索引是数据块在快照中的偏移位置，它用于标识数据块。将 `BlockIndex` 值与 `BlockSize` 值相乘 (`BlockIndex * BlockSize`) 来确定数据在逻辑数据块中的逻辑偏移。

数据块令牌

数据块令牌是快照中的数据块的标识哈希，它用于查找数据块数据。

Note

EBS direct APIs 返回的数据块令牌是临时的。如果您对同一快照运行另一个 `ListSnapshotBlocks` 或 `ListChangedBlocks` 请求，数据块令牌会更改。

列出快照数据块

`ListSnapshotBlocks` API 操作返回指定快照中的数据块的数据块索引和数据块令牌。有关更多信息，请参阅 EBS direct APIs 参考 中的 [ListSnapshotBlocks](#)。

列出已更改的数据块

`ListChangedBlocks` API 操作返回同一卷/快照谱系的两个指定快照之间不同的数据块的数据块索引和数据块令牌。有关更多信息，请参阅 EBS direct APIs 参考 中的 [ListChangedBlocks](#)。

获取快照数据块

`GetSnapshotBlock` API 操作返回指定快照 ID、数据块索引和数据块令牌的数据块中的数据。有关更多信息，请参阅 EBS direct APIs 参考 中的 [GetSnapshotBlock](#)。

使用 API

使用 `ListSnapshotBlocks` 或 `ListChangedBlocks` API 操作来确定要获取其数据的数据块的数据块索引和数据块令牌。然后，使用 `GetSnapshotBlock` API 操作从快照中的这些数据块获取数据。本指南后面提供了如何使用 AWS CLI 运行这些操作的示例。

IAM 用户的权限

IAM 用户必须具有以下策略才能使用 EBS direct APIs。

Important

向 IAM 用户分配以下策略时要小心。通过分配这些策略，您可以向通过 EC2 API（例如 CopySnapshot 或 CreateVolume 操作）拒绝其访问同一资源的用户授予访问权限。

以下策略授予对 EBS direct APIs 的完全访问权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:*"  
            ],  
            "Resource": "arn:aws:ec2:*:::snapshot/*"  
        }  
    ]  
}
```

以下策略授予对特定 AWS 区域中的特定快照的访问权限。在策略中，将 `<SnapshotID>` 替换为快照的 ID，并将 `<Region>` 替换为快照的区域。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs>ListSnapshotBlocks"  
            ],  
            "Resource": "arn:aws:ec2:<Region>::snapshot/<SnapshotID>"  
        }  
    ]  
}
```

以下策略为 EBS direct APIs 授予对具有特定键/值标签的快照的访问权限。在策略中，将 `<Key>` 替换为标签的键值，并将 `<Value>` 替换为标签的值。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs>ListChangedBlocks",  
                "ebs>ListSnapshotBlocks",  
                "ebs>GetSnapshotBlock"  
            ],  
            "Resource": "arn:aws:ec2:*:::snapshot/*",  
            "Condition": {  
                "StringEqualsIgnoreCase": {  
                    "aws:ResourceTag/<Key>": "<Value>"  
                }  
            }  
        }  
    ]  
}
```

```
}
```

以下权限拒绝 EBS direct APIs 对特定快照的访问。在策略中，将 `<SnapshotID>` 替换为快照的 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs>ListSnapshotBlocks",
                "ebs>ListChangedBlocks",
                "ebs>GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ebs>ListSnapshotBlocks",
                "ebs>ListChangedBlocks",
                "ebs>GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:us-east-2::<SnapshotID>"
        }
    ]
}
```

以下策略授予对特定时间范围内的所有快照的访问权限。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs>ListChangedBlocks",
                "ebs>ListSnapshotBlocks",
                "ebs>GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

以下策略授予使用 AWS Key Management Service (AWS KMS) 中的特定密钥 ID 解密已加密快照的权限。在策略中，将 `<AccountId>` 替换为 AWS KMS 密钥的 AWS 账户的 ID，并将 `<KeyId>` 替换为用于加密要使用 EBS direct APIs 访问的快照的密钥的 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {

```

```
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "arn:aws:kms:us-west-2:<AccountID>:key/<KeyId>"
    }
}
```

有关更多信息，请参阅 IAM 用户指南 中的[更改 IAM 用户的权限](#)。

通过命令行使用 EBS direct APIs

以下示例显示如何通过 AWS Command Line Interface (AWS CLI) 使用 EBS direct APIs。有关安装和配置 AWS CLI 的更多信息，请参阅[安装 AWS CLI 版本 1](#) 和[快速配置 AWS CLI](#)。

Example 示例：获取快照中的数据块的数据块索引和数据块令牌

以下 `list-snapshot-blocks` 命令示例返回 `us-east-1` AWS 区域中 `snap-0987654321` 快照中的数据块的数据块索引和数据块令牌。`--starting-block-index` 和 `--max-results` 参数将结果限制为数据块索引大于 `1000` 的前 `100` 个数据块。

```
aws ebs list-snapshot-blocks --region us-east-1 --snapshot-id snap-0987654321 --starting-block-index 1000 --max-results 100
```

以下为响应示例：要获取数据块中的数据，请使用 `get-snapshot-block` 命令并指定数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
    "Blocks": [
        {
            "BlockIndex": 1001,
            "BlockToken": "AAABAV3/PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
        },
        {
            "BlockIndex": 1002,
            "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
        },
        {
            "BlockIndex": 1007,
            "BlockToken": "AAABAZ9CTuQtUvp/dXqRWw4d07e0gTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
        },
        {
            "BlockIndex": 1012,
            "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
        },
        {
            "BlockIndex": 1030,
            "BlockToken": "AAABAAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L+CbXnvpkswA6iDID523d"
        },
        {
            "BlockIndex": 1031,
            "BlockToken": "AAABATgWZC0XcFwUKvtJbUXMiSPg59KVxJGL+BWBClkw6spzCxJVqDVaTskJ"
        },
        ...
    ],
    "ExpiryTime": 1576287332.806,
    "VolumeSize": 32212254720,
    "BlockSize": 524288
}
```

Example 示例：获取同一卷/快照谱系的两个快照之间不同的数据块的数据块索引和数据块令牌。

以下 `list-changed-blocks` 命令示例返回 `us-east-1` AWS 区域中快照 `snap-1234567890` 和 `snap-0987654321` 之间不同的数据块的数据块索引和数据块令牌。`--starting-block-index` 和 `--max-results` 参数将结果限制为数据块索引大于 0 的前 500 个数据块。

```
aws ebs list-changed-blocks --region us-east-1 --first-snapshot-id snap-1234567890 --second-snapshot-id snap-0987654321 --starting-block-index 0 --max-results 500
```

以下为响应示例：它显示数据块索引 0、6000、6001、6002 和 6003 在两个快照之间是不同的。此外，数据块索引 6001、6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

要获取数据块中的数据，请使用 `get-snapshot-block` 命令并指定数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{  
    "ChangedBlocks": [  
        {  
            "BlockIndex": 0,  
            "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/  
KN3uygGlS0QOYWesbzBbDnX2dGpmC",  
            "SecondBlockToken":  
"AAABAf8o0o6UFlrDbSZGIRaCedDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGsr"  
        },  
        {  
            "BlockIndex": 6000,  
            "FirstBlockToken": "AAABAbYSiZvJ0/  
R9tz8suI8dSzecLjN4kkazK8inFXvintPkdaVFLfCMQsKe",  
            "SecondBlockToken":  
"AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"  
        },  
        {  
            "BlockIndex": 6001,  
            "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/  
T4sU25Bnb8jB5Q6FRXHFqAIaqE04hJoR"  
        },  
        {  
            "BlockIndex": 6002,  
            "FirstBlockToken": "AAABASqX4/  
NWjvNceoyMULjcRd0DnwbswNnes1UkoP62CrQxvn47BY5435aw"  
        },  
        {  
            "BlockIndex": 6003,  
            "FirstBlockToken":  
"AAABASmJ005JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKof4PBROuiCb2A"  
        },  
        ...  
    ],  
    "ExpiryTime": 1576308931.973,  
    "VolumeSize": 32212254720,  
    "BlockSize": 524288,  
    "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//O6Mdi/  
BbJarBnp8h"  
}
```

Example 示例：获取数据块中的数据

以下 `get-snapshot-block` 命令示例返回 `us-east-1` AWS 区域的快照 `snap-1234567890` 中数据块令牌为 `AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIaqE04hJoR` 的数据块索引 6001 中的数据。二进制数据将输出到 Windows 计算机上的 `C:\Temp` 目录中的 `output.txt` 文件。如果您在

Linux 或 Unix 计算机上运行该命令，请将输出路径替换为 `/tmp/output.txt` 以将数据输出到 `/tmp` 目录中的 `output.txt` 文件。

```
aws ebs get-snapshot-block --region us-east-1 --snapshot-id snap-1234567890 --block-index 6001 --block-token AAAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoRC:/Temp/output.txt
```

以下为响应示例：它显示返回的数据的大小、用于验证数据的校验和以及用于生成校验和的校验和算法。二进制数据会自动保存到您在请求命令中指定的目录和文件中。

```
{  
    "DataLength": "524288",  
    "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTf1PTKzxGv2OKowXc=",  
    "ChecksumAlgorithm": "SHA256"  
}
```

通过 API 或 AWS 开发工具包使用 EBS direct APIs

EBS direct APIs 参考 提供了服务的每个操作和数据类型的描述和语法。您还可以使用一个 AWS 开发工具包来访问适用于您所用编程语言或平台的 API。有关更多信息，请参阅 [AWS 开发工具包](#)。

EBS direct APIs 需要 AWS 签名版本 4 签名。有关创建这些签名的更多信息，请参阅 AWS 一般参考 中的 [签名版本 4 签名流程](#)。

仅当您打算手动创建 HTTP 请求时，才需要了解如何签署这些请求。当您使用 AWS 命令行界面 (AWS CLI) 或一个 AWS 开发工具包来向 AWS 发出请求时，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。当您使用这些工具时，您不必了解如何亲自签署这些请求。

EBS direct APIs 常见问题

如果快照具有挂起状态，是否可以使用 EBS direct APIs 访问该快照？

不可以。仅当快照具有已完成状态时，才能访问该快照。

EBS direct APIs 是否按数字顺序返回数据块索引？

是。返回的数据块索引是唯一的，并按数字顺序排列。

我是否可以提交 `MaxResults` 参数值低于 100 的请求？

不可以。您可以使用的最小 `MaxResult` 参数值为 100。如果您提交 `MaxResult` 参数值低于 100 的请求，并且快照中的数据块超过 100 个，则 API 将返回至少 100 个结果。

我是否可以并发运行 API 请求？

您可以并发运行 API 请求。请确保考虑账户中可能运行的其他工作负载，以避免瓶颈。您还应将重试机制内置到 EBS direct APIs 工作流中，以处理限制、超时和服务不可用性。

运行 `ListChangedBlocks` 操作时，是否即使快照中有数据块，也有可能获得空响应？

是。如果快照中更改的数据块很少，则响应可能为空，但 API 将返回下一页令牌值。使用下一页令牌值来继续转到下一页结果。当 API 返回的下一页令牌值为 null 时，您可以确认已到达最后一页结果。

如果同时指定了 `NextToken` 参数和 `StartingBlockIndex` 参数，将使用这两者中的哪一个？

将使用 `NextToken`，并忽略 `StartingBlockIndex`。

数据块令牌和下一个令牌的有效期是多久？

数据块令牌的有效期为七天，下一个令牌的有效期为 60 分钟。

是否支持已加密快照？

是。可以使用 EBS 直接 API 访问已加密快照。

要访问已加密快照，用户必须有权访问用于加密快照的密钥和 AWS KMS 解密操作。有关要分配给用户的 AWS KMS 策略，请参阅本指南前面的

使用 `ListSnapshotBlocks` 或 `ListChangedBlocks` API 操作来确定要获取其数据的数据块的数据块索引和数据块令牌。然后，使用 `GetSnapshotBlock` API 操作从快照中的这些数据块获取数据。本指南后面提供了如何使用 AWS CLI 运行这些操作的示例。

(p. 831) 部分。

是否支持公有快照？

否。不支持公有快照。

`list snapshot block` 是返回快照中的所有数据块索引和数据块令牌，还是仅返回那些写入数据的数据块索引和数据块令牌？

它只返回写入数据的数据块索引和令牌。

自动化 Amazon EBS 快照生命周期

您可以使用 Amazon 数据生命周期管理器 来自动创建、保留和删除为备份 Amazon EBS 卷而制作的快照。自动化快照管理可以帮助您：

- 通过实施定期备份计划来保护重要数据。
- 按照审核员的要求或内部合规性保留备份。
- 通过删除过时的备份来降低存储成本。

与 Amazon CloudWatch Events 和 AWS CloudTrail 的监控功能结合使用，Amazon 数据生命周期管理器 可为 EBS 卷提供完整备份解决方案，而无需额外费用。

目录

- [Amazon 数据生命周期管理器 的工作原理 \(p. 831\)](#)
- [Amazon 数据生命周期管理器 的注意事项 \(p. 832\)](#)
- [先决条件 \(p. 833\)](#)
- [创建和维护生命周期策略 \(p. 834\)](#)
- [创建和维护多卷快照 \(p. 838\)](#)
- [监控快照生命周期 \(p. 840\)](#)

Amazon 数据生命周期管理器 的工作原理

以下是 Amazon 数据生命周期管理器 的关键要素。

快照

快照是备份 EBS 卷中的数据的主要方式。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。在您删除卷的一系列快照中的一个快照时，只删除该快照独有的数据。将保留卷的其余捕获历史记录。

有关更多信息，请参阅 [Amazon EBS 快照 \(p. 812\)](#)。

定位资源标签

Amazon 数据生命周期管理器 使用资源标签来标识要备份的 EBS 卷。标签是可分配到 AWS 资源（包括 EBS 卷和快照）的可自定义元数据。Amazon 数据生命周期管理器 策略（如下所述）使用单个标签定位某个卷用于备份。如果您希望在某个卷上运行多个策略，可以为其分配多个标签。

在标签键中不能使用“\”或“=”字符。

有关更多信息，请参阅 [标记您的 Amazon EC2 资源 \(p. 940\)](#)。

快照标签

Amazon 数据生命周期管理器 对通过策略创建的所有快照应用以下标签，以与通过任何其他方法创建的快照区分开来：

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`

还可以在创建时指定要应用于快照的自定义标签。

在标签键中不能使用“\”或“=”字符。

Amazon 数据生命周期管理器 用于将卷与策略关联的目标标签可以选择性地应用于策略创建的快照。

生命周期策略

生命周期策略包括以下核心设置：

- 资源类型 - 由策略管理的 AWS 资源的类型。支持的类型是 EBS 卷和 EC2 实例。
- 目标标签 - 必须与 EBS 卷或 EC2 实例关联才能由策略管理的标签。
- 计划 - 创建快照的开始时间和间隔。
- 保留 - 您可以基于快照的总计数或每个快照的存在时间保留快照。

例如，您可以创建一个策略，它管理具有标签 `account=Finance` 的所有 EBS 卷，每隔 24 小时在 9:00 创建一次快照，并保留 5 个最新快照。快照创建会最晚在 0959 开始。

Amazon 数据生命周期管理器 的注意事项

您的 AWS 账户具有与 Amazon 数据生命周期管理器 相关的以下配额：

- 您最多可以为每个区域创建 100 个生命周期策略。
- 您最多可以为每个资源添加 50 个标签。
- 您可以为每个生命周期策略创建一个计划。

以下注意事项适用于生命周期策略：

- 在您将策略的激活状态设置为已启用后，策略才开始创建快照。您可以在创建时将策略配置为已启用。
- 第一个快照是由策略在指定的开始时间之后的一小时内创建的。
- 如果您通过删除或更改目标标签来修改策略，则具有该标签的 EBS 卷将不再受此策略的影响。
- 如果您修改策略的计划名称，则在旧计划名称下创建的快照将不再受此策略的影响。
- 如果您根据时间修改保留计划以使用新的时间间隔，则新的间隔仅用于新快照。新的计划不会影响该策略创建的现有快照的保留计划。
- 您无法将策略的保留计划从快照计数更改为每个快照的存在时间。要进行该更改，您必须创建新的策略。
- 如果您禁用了其保留计划基于每个快照的存在时间的策略，则会无限期保留在禁用该策略时其保留期过期的快照。您必须手动删除这些快照。再次启用该策略时，Amazon 数据生命周期管理器 会在快照保留期过期时继续删除快照。
- 如果删除策略适用的资源，则策略不再管理以前创建的快照。如果不再需要使用快照，您必须手动删除这些快照。

- 您可以创建多个策略以备份 EBS 卷或 EC2 实例。例如，如果 EBS 卷有两个标签，其中标签 A 是每隔 12 小时创建一次快照的策略 A 的目标，标签 B 是每隔 24 小时创建一次快照的策略 B 的目标，则 Amazon 数据生命周期管理器 将根据这两个策略的计划创建快照。

以下注意事项适用于生命周期策略和[快速快照还原 \(p. 859\)](#)：

- 即使您删除或禁用生命周期策略，为生命周期策略禁用快速快照还原，或者为可用区禁用快速快照还原，已启用快速快照还原的快照也会保持启用状态。您可以手动为这些快照禁用快速快照还原。
- 如果您启用快速快照还原，并且超过可启用快速快照还原的最大快照数，Amazon 数据生命周期管理器 将按计划创建快照，但不会为其启用快速快照还原。在删除启用了快速快照还原的快照后，将为 Amazon 数据生命周期管理器 创建的下一个快照启用快速快照还原。
- 在为快照启用快速快照还原时，每个 TiB 需要 60 分钟来优化快照。我们建议您创建一个计划，以确保在 Amazon 数据生命周期管理器 创建下一个快照之前对每个快照进行完全优化。

先决条件

Amazon 数据生命周期管理器 需要满足以下先决条件。

Amazon 数据生命周期管理器 权限

Amazon 数据生命周期管理器 使用 IAM 角色来获取代表您管理快照所需的权限。在您首次使用 AWS 管理控制台创建生命周期策略时，Amazon 数据生命周期管理器 会创建 AWSDataLifecycleManagerDefaultRole 角色。您还可以使用以下 [create-default-role](#) 命令创建此角色。

```
aws dlm create-default-role
```

或者，您可以在创建生命周期策略时创建具有所需权限的自定义 IAM 角色并选择它。

创建自定义 IAM 角色

- 创建具有以下权限的角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeVolumes",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        }
    ]
}
```

有关更多信息，请参阅 IAM 用户指南 中的[创建角色](#)。

2. 向角色添加信任关系。

- a. 在 IAM 控制台中，选择角色。
- b. 选择您创建的角色，然后选择信任关系。
- c. 选择编辑信任关系，添加以下策略，然后选择更新信任策略。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "dlm.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

IAM 用户的权限

IAM 用户必须具有以下权限才能使用 Amazon 数据生命周期管理器。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["iam:PassRole", "iam>ListRoles"],  
            "Resource": "arn:aws:iam::123456789012:role/AWSDataLifecycleManagerDefaultRole"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "dlm:*",  
            "Resource": "*"  
        }  
    ]  
}
```

有关更多信息，请参阅 IAM 用户指南 中的[更改 IAM 用户的权限](#)。

创建和维护生命周期策略

以下示例说明如何使用 Amazon 数据生命周期管理器 执行典型过程来管理您的 EBS 卷的备份。

使用控制台

创建生命周期策略

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 Lifecycle Manager (生命周期管理器)，然后选择 Create snapshot lifecycle policy (创建快照生命周期策略)。
3. 根据需要，为您的策略提供以下信息：
 - Description (描述) – 策略的描述。
 - Resource type (资源类型) – 资源的类型：卷或实例。
 - Target with these tags (具有这些标签的目标) – 标识要备份的卷或实例的资源标签。
 - Lifecycle policy tags (生命周期策略标签) – 生命周期策略的标签。

- Schedule name (计划名称) – 计划的名称。
- Run policy every n Hours (每 n 小时运行一次策略) – 运行两次策略间隔的小时数。支持的值为 2、3、4、6、8、12 和 24。
- Starting at hh:mm UTC (开始时间 - 小时:分钟 UTC) – 计划开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。
- 保留 – 您可以基于快照的总计数或每个快照的存在时间保留快照。对于基于计数的保留，范围是 1 到 1000。在达到最大计数后，将在创建新快照时删除最早的快照。对于基于存在时间的保留，范围是 1 天到 100 年。在每个快照的保留期过期后，将删除它。保留期应大于或等于创建间隔。
- Cross Region copy (跨区域复制) – 您可以将每个快照复制到最多三个其他区域。对于每个区域，您可以选择不同的保留策略，以及是复制所有标签还是不复制任何标签。如果源快照已加密或默认启用加密，则会加密快照副本。如果源快照未加密，您可以启用加密。如果未指定 CMK，则会在每个目标区域中使用 EBS 加密的默认密钥对快照进行加密。您必须确保没有超过每个区域的并发快照副本数。
- Tagging information (标记信息) – 选择是否将源卷上的所有用户定义的标签复制到该策略创建的快照。除了 Amazon 数据生命周期管理器应用的标签以外，您还可以为快照指定其他标签。如果资源类型是实例，您可以选择使用实例 ID 和时间戳自动标记快照。
- Fast snapshot restore (快速快照还原) – 选择是否启用快速快照还原以及在哪个可用区中启用。您还可以指定可启用快速快照还原的最大快照数。
- IAM role (IAM 角色) – 有权创建、删除和描述快照以及描述卷的 IAM 角色。AWS 提供一个默认角色 AWSDataLifecycleManagerDefaultRole，您也可以创建自定义 IAM 角色。
- Policy status after creation (创建后的策略状态) – 选择 Enable policy (启用策略) 以在下个计划时间开始运行策略，或者选择 Disable policy (禁用策略) 以禁止运行策略。

4. 选择创建策略。

显示生命周期策略

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 和生命周期管理器。
3. 从列表中选择生命周期策略。Details (详细信息) 选项卡显示有关策略的信息。

修改生命周期策略

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 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择 Actions (操作)，然后选择 Modify Snapshot Lifecycle Policy (修改快照生命周期策略)。
5. 根据需要，修改策略设置。例如，您可以修改计划，添加或删除标签，或者启用或禁用策略。
6. 选择 Update policy。

删除生命周期策略

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 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择 Actions (操作)，然后选择 Delete Snapshot Lifecycle Policy (删除快照生命周期策略)。
5. 在提示确认时，选择 Delete Snapshot Lifecycle Policy (删除快照生命周期策略)。

使用 AWS CLI

以下示例说明如何使用 Amazon 数据生命周期管理器 执行典型过程来管理您的 EBS 卷的备份。

Example 示例：创建生命周期策略

可使用 [create-lifecycle-policy](#) 命令创建生命周期策略。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetails.json`。

```
aws dlm create-lifecycle-policy --description "My first policy" --state ENABLED --  
execution-role-arn arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole --  
policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{  
    "ResourceTypes": [  
        "VOLUME"  
    ],  
    "TargetTags": [  
        {  
            "Key": "costcenter",  
            "Value": "115"  
        }  
    ],  
    "Schedules": [  
        {  
            "Name": "DailySnapshots",  
            "TagsToAdd": [  
                {  
                    "Key": "type",  
                    "Value": "myDailySnapshot"  
                }  
            ],  
            "CreateRule": {  
                "Interval": 24,  
                "IntervalUnit": "HOURS",  
                "Times": [  
                    "03:00"  
                ]  
            },  
            "RetainRule": {  
                "Count": 5  
            },  
            "CopyTags": false  
        }  
    ]  
}
```

成功后，此命令将返回新创建的策略的 ID。下面是示例输出。

```
{  
    "PolicyId": "policy-0123456789abcdef0"  
}
```

Example 示例：显示生命周期策略

可使用 [get-lifecycle-policy](#) 命令来显示有关生命周期策略的信息。

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

下面是示例输出。它包括您指定的信息以及 AWS 插入的元数据。

```
{  
    "Policy": {
```

```
"Description": "My first policy",
"DateCreated": "2018-05-15T00:16:21+0000",
"State": "ENABLED",
"ExecutionRoleArn":
"arn:aws:iam::210774411744:role/AWSDataLifecycleManagerDefaultRole",
"PolicyId": "policy-0123456789abcdef0",
"DateModified": "2018-05-15T00:16:22+0000",
"PolicyDetails": {
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Value": "115",
            "Key": "costcenter"
        }
    ],
    "Schedules": [
        {
            "TagsToAdd": [
                {
                    "Value": "myDailySnapshot",
                    "Key": "type"
                }
            ],
            "RetainRule": {
                "Count": 5
            },
            "CopyTags": false,
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "03:00"
                ]
            },
            "Name": "DailySnapshots"
        }
    ]
}
```

Example 修改生命周期策略

可使用 `update-lifecycle-policy` 命令来修改生命周期策略中的信息。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetailsUpdated.json`。

```
aws dlm update-lifecycle-policy --state DISABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole --policy-details
file://policyDetailsUpdated.json
```

以下是 `policyDetailsUpdated.json` 文件的示例。

```
{
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Key": "costcenter",
            "Value": "120"
        }
    ]
}
```

```
        },
    ],
    "Schedules": [
        {
            "Name": "DailySnapshots",
            "TagsToAdd": [
                {
                    "Key": "type",
                    "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 12,
                "IntervalUnit": "HOURS",
                "Times": [
                    "15:00"
                ]
            },
            "RetainRule": {
                "Count": 5
            },
            "CopyTags": false
        }
    ]
}
```

要查看更新后的策略，请使用 `get-lifecycle-policy` 命令。您可以看到更改了状态、标签的值、快照时间间隔和快照开始时间。

Example 示例：删除生命周期策略

可使用 `delete-lifecycle-policy` 命令来删除生命周期策略并释放策略中指定的目标标签以供重复使用。

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

使用 API

Amazon 数据生命周期管理器 API 参考 提供了 Amazon 数据生命周期管理器 查询 API 的各种操作和数据类型的描述和语法。

或者，您可以使用 AWS 开发工具包之一，通过适用于您所用编程语言或平台的方法来访问该 API。有关更多信息，请参阅 [AWS 开发工具包](#)。

创建和维护多卷快照

您可以创建生命周期策略以自动创建和删除多卷快照。

使用控制台

以下过程说明了如何使用 AWS 管理控制台通过 Amazon 数据生命周期管理器 自动创建和删除多卷快照。

使用控制台自动处理多卷快照

1. 登录 AWS 管理控制台并通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic Block Store (弹性数据块存储)。然后选择 Lifecycle Manager (生命周期管理器) 和 Create snapshot lifecycle policy (创建快照生命周期策略)。
3. 根据需要，为您的策略提供以下信息：
 - Description (描述) – 策略的描述。
 - Target with tags (具有标签的目标) – 标识要备份的卷或实例的资源标签。

- Schedule Name (计划名称) – 备份计划的名称。
- Create snapshots every n Hours (每隔 n 小时创建快照) – 策略运行之间的小时数。支持的值为 2、3、4、6、8、12 和 24。
- Snapshot creation start time hh:mm UTC (快照创建开始时间 hh:mm UTC) – 策略运行计划开始的当日时间。策略运行在计划时间后的 1 小时内开始。
- Retention rule (保留规则) – 每个卷或实例保留的最大快照数。支持的范围为 1 至 1000。在到达限制后，当创建新的快照时，会删除最旧的快照。
- Copy tags (复制标签) – 将源卷上所有用户定义的标签复制到由此策略创建的卷的快照。
- Tag created snapshots (标记创建的快照) – 应用于创建的快照的资源标签。这些标签作为 Amazon 数据生命周期管理器 应用的标签的补充。您还可以选择变量标签，以使用相应的 instance-id 或 timestamp 自动标记所有快照。
- IAM role (IAM 角色) – 一个 IAM 角色，具有创建、删除和描述快照以及描述卷的权限。AWS 提供一个默认角色 AWSDataLifecycleManagerDefaultRole，您也可以创建自定义 IAM 角色。
- Policy status after creation (创建后的策略状态) – 选择 Enable policy (启用策略) 以在下次计划时间启动策略运行，或者选择 Disable policy (禁用策略) 以禁止策略运行。

4. 选择创建策略。

使用 AWS CLI

以下示例说明了如何使用 AWS CLI 通过 Amazon 数据生命周期管理器 自动创建和删除多卷快照。

Example 示例：创建生命周期策略

可使用 `create-lifecycle-policy` 命令创建生命周期策略。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetails.json`。

```
aws dlm create-lifecycle-policy --description My multi-volume snapshots policy --state ENABLED --execution-role-arn arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole --policy-details file://multi-volume-policy.json
```

以下是 `multi-volume-policy.json` 文件的示例。

```
{  
    "ResourceTypes": [  
        "INSTANCE"  
    ],  
    "TargetTags": [  
        {  
            "Key": "costcenter",  
            "Value": "115"  
        }  
    ],  
    "Schedules": [  
        {  
            "Name": "DailySnapshots",  
            "TagsToAdd": [  
                {  
                    "Key": "type",  
                    "Value": "Daily-Multi-Volume Snapshots"  
                }  
            ],  
            "VariableTags": [  
                {  
                    "Key": "timestamp",  
                    "Value": "$(timestamp)"  
                },  
                {  
                    "Key": "volumeid",  
                    "Value": "$volumeId"  
                }  
            ]  
        }  
    ]  
}
```

```
        "Key": "instance-id",
        "Value": "${instance-id}"
    },
],
"Interval": 24,
"IntervalUnit": "HOURS",
"Times": [
"03:00"
]
},
"RetainRule": {
"Count": 5
},
"CopyTags": false
}
]
"Parameters": {
"ExcludeBootVolume": true
}
}
```

成功后，此命令将返回新创建的策略的 ID。下面是示例输出。

```
{
    "PolicyId": "policy-0123456789abcdef0"
}
```

监控快照生命周期

您可以使用以下功能来监控快照的生命周期。

使用控制台和 AWS CLI

您可以使用 Amazon EC2 控制台或 AWS CLI 来查看生命周期策略。策略创建的每个快照均具有时间戳以及与策略相关的标签。您可以使用标签来筛选快照以验证是否按预期创建备份。有关使用控制台查看生命周期策略的信息，请参阅[显示生命周期策略 \(p. 835\)](#)。有关使用 CLI 显示生命周期策略相关信息的信息，请参阅[示例：显示生命周期策略 \(p. 836\)](#)。

使用 CloudWatch Events

Amazon EBS 和 Amazon 数据生命周期管理器 发出与生命周期策略操作相关的事件。您可以使用 AWS Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。有关更多信息，请参阅[Amazon CloudWatch Events 用户指南](#)。

提供的事件如下：

- `createSnapshot` – 当 CreateSnapshot 操作成功或失败时，会发出 Amazon EBS 事件。有关更多信息，请参阅[Amazon EBS 的 Amazon CloudWatch Events \(p. 893\)](#)。
- `DLM Policy State Change` – 当生命周期策略进入错误状态时，会发出 Amazon 数据生命周期管理器事件。此事件包含有关导致错误的问题的描述。下面是在 IAM 角色授予的权限不足时发出的事件的示例：

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ]
}
```

```
],
  "detail": {
    "state": "ERROR",
    "cause": "Role provided does not have sufficient permissions",
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  }
}
```

下面是在超过限制时发出的事件的示例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "DLM Policy State Change",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2018-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  ],
  "detail": {
    "state": "ERROR",
    "cause": "Maximum allowed active snapshot limit exceeded",
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  }
}
```

使用 AWS CloudTrail

使用 AWS CloudTrail，您可以跟踪用户活动和 API 使用率来证明符合内部策略和监管标准。有关更多信息，请参阅 [AWS CloudTrail User Guide](#)。

Amazon EBS 数据服务

Amazon EBS 提供以下数据服务。

数据服务

- [Amazon EBS 弹性卷 \(p. 841\)](#)
- [Amazon EBS Encryption \(p. 851\)](#)
- [Amazon EBS 快速快照还原 \(p. 859\)](#)

Amazon EBS 弹性卷

通过使用 Amazon EBS 弹性卷，您可以增加卷大小，更改卷类型或调整 EBS 卷的性能。如果您的实例支持弹性卷，您可以执行这些操作，而无需分离卷或重新启动实例。这样，您就可以在更改生效时继续使用应用程序。

修改卷配置是免费的。卷修改开始后，您需要支付新卷配置的费用。有关更多信息，请参阅 [Amazon EBS 定价页面](#)。

目录

- [修改卷时的要求 \(p. 842\)](#)
- [对您的 EBS 卷请求修改 \(p. 843\)](#)
- [监控卷修改的进度 \(p. 845\)](#)
- [调整卷大小后扩展 Linux 文件系统 \(p. 848\)](#)

修改卷时的要求

您修改 Amazon EBS 卷时存在以下要求和限制。若要了解有关 EBS 卷的常规要求的更多信息，请参阅 [针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。

Amazon EC2 实例支持

以下实例上支持弹性卷：

- [所有当前一代实例 \(p. 161\)](#)
- 上一代实例系列 C1、C3、CC2、CR1、G2、I2、M1、M3 和 R3

如果您的实例类型不支持弹性卷，请参阅[在不支持弹性卷的情况下修改 EBS 卷 \(p. 845\)](#)。

针对 Linux 卷的要求

Linux AMI 需要将 GUID 分区表 (GPT) 和 GRUB 2 用于 2 TiB (2048 GiB) 或更大的引导卷。现在的很多 Linux AMI 仍使用 MBR 分区方案，此方案仅支持最高 2 TiB 的引导卷大小。如果您的实例不通过大于 2 TiB 的引导卷启动，您要使用的 AMI 可能限制为小于 2 TiB 的引导卷大小。非引导卷对 Linux 实例没有这种限制。有关影响 Windows 卷的要求，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[针对 Windows 卷的要求](#)。

在尝试调整超过 2 TiB 的引导卷大小之前，您可以通过在您的实例上运行以下命令来决定该卷是使用 MBR 分区还是使用 GPT 分区：

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

使用 GPT 分区的 Amazon Linux 实例返回以下信息：

```
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.
```

使用 MBR 分区的 SUSE 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.8

Partition table scan:
  MBR: MBR only
  BSD: not present
  APM: not present
  GPT: not present
```

限制

- 新卷大小不能超出支持的卷容量。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。
- 如果卷是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的，您必须初始化弹性卷支持。有关更多信息，请参阅[初始化弹性卷支持 \(p. 844\)](#)。
- 如果您使用的是不受支持的上一代实例类型，或者如果您在尝试修改卷时遇到错误，请参阅[在不支持弹性卷的情况下修改 EBS 卷 \(p. 845\)](#)。

- 作为根卷附加到实例的 gp2 卷无法修改为 st1 或 sc1 卷。如果分离了 gp2 并将其修改为 st1 或 sc1，则无法将其作为根卷附加到实例。
- 如果请求的卷大小小于 st1 和 sc1 卷的最小大小，gp2 卷无法修改为 st1 或 sc1 卷。
- 在某些情况下，您必须分离卷或停止实例才能继续进行修改。如果在尝试修改 EBS 卷时遇到错误消息，或者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。
 - 对于根（引导）卷，停止实例，应用修改，然后重新启动实例。
- 在现有 io1 卷上预配置超过 32,000 IOPS 后，您可能需要执行以下操作之一来实现全部性能改进：
 - 分离和附加卷。
 - 重新启动实例。
- 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）将数据迁移到该卷。
- 如果修改尚未完全初始化的卷，则修改时间会增加。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 879\)](#)。
- 修改卷后，等待至少六个小时并确保卷处于 in-useavailable 状态，然后再对同一个卷进行其他修改。
- 虽然 m3.medium 实例完全支持卷修改，但 m3.large、m3.xlarge 和 m3.2xlarge 实例可能不支持所有卷修改功能。

对您的 EBS 卷请求修改

对于弹性卷，您可以在不分离 Amazon EBS 卷的情况下动态修改卷的大小、性能和卷类型。

修改卷时使用以下过程：

- 1.（可选）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）。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 815\)](#)。
2. 请求卷修改。
3. 监控卷修改进度。有关更多信息，请参阅 [监控卷修改的进度 \(p. 845\)](#)。
4. 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 \(p. 848\)](#)。

目录

- [使用弹性卷修改 EBS 卷（控制台）\(p. 843\)](#)
- [使用弹性卷修改 EBS 卷（AWS CLI）\(p. 844\)](#)
- [初始化弹性卷支持（如果需要）\(p. 844\)](#)
- [在不支持弹性卷的情况下修改 EBS 卷 \(p. 845\)](#)

使用弹性卷修改 EBS 卷（控制台）

要修改 EBS 卷，请按照以下过程操作。

使用控制台修改 EBS 卷

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。

- 如果选择预配置 IOPS SSD (io1) 作为卷类型，请为 IOPS 输入一个允许的整数值。
4. 完成更改卷设置后，请选择 **Modify** (修改)。当系统提示您确认时，请选择 Yes。
5. 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 \(p. 848\)](#)。

使用弹性卷修改 EBS 卷 (AWS CLI)

使用 `modify-volume` 命令修改卷的一个或多个配置设置。如果您有一个类型为 `gp2` 且大小为 100 GiB 的卷，以下命令会将其配置更改为类型为 `io1`、包含 10000 IOPS 且大小为 200 GiB 的卷。

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-id vol-1111111111111111
```

下面是示例输出：

```
{  
    "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  
    }  
}
```

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 \(p. 848\)](#)。

初始化弹性卷支持 (如果需要)

您必须先使用以下操作之一初始化卷修改支持，然后才能修改在 UTC 时间 2016 年 11 月 3 日 23:40 前附加到实例的卷：

- 分离和附加卷
- 停止和启动实例

使用以下过程之一来确定您的实例是否已准备好进行卷修改。

使用控制台确定您的实例是否已准备就绪

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择实例。
- 选择 Show/Hide Columns 图标 (齿轮)。选择 Launch Time 和 Block Devices 属性，然后选择 Close。
- 按 Launch Time 列对实例列表进行排序。对于在截止日期前启动的实例，请检查附加设备的时间。在以下示例中，您必须为第一个实例初始化卷修改，因为该实例是在截止日期前启动的，并且其根卷是在截止日期前附加的。其他实例已准备就绪，因为它们是在截止日期后启动的。

Instance ID	Launch Time	Block Devices
i-e905622e	February 25, 2016 at 1:49:35 PM UTC-8	/dev/xvda=vol-e6b46410.attached:2016-02-25T21:49:35.000Z:true
i-719f9a8	December 8, 2016 at 2:21:51 PM UTC-8	/dev/xvda=vol-bad60e7a.attached:2016-01-15T18:36:12.000Z:true
i-006b02c1b78381e57	May 17, 2017 at 1:52:52 PM UTC-7	/dev/sda1=vol-0de9250441c73024c.attached:2017-05-17T20:52:53.000Z:true, xvdb=vol-0863a86c393496d3d.attached:2017-05-17T20:52:53.000Z:false
i-e3d172ed	May 17, 2017 at 2:48:54 PM UTC-7	/dev/sda1=vol-04c34d0b.attached:2015-01-21T21:19:46.000Z:true

使用 CLI 确定您的实例是否已准备就绪

使用以下 [describe-instances](#) 命令确定卷是否是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的。

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*][Ebs.AttachTime<='2016-11-01']]"
--output text
```

每个实例的输出的第一行都将显示其 ID，无论实例是否在截止日期前启动（True 或 False）。第一行后跟一行或多行，以显示是否在截止日期前已附加每个 EBS 卷（True 或 False）。在以下示例输出中，您必须为第一个实例初始化卷修改，因为该实例是在截止日期前启动的，并且其根卷是在截止日期前附加的。其他实例已准备就绪，因为它们是在截止日期后启动的。

```
i-e905622e      True
True
i-719f99a8      False
True
i-006b02c1b78381e57  False
False
False
i-e3d172ed      False
True
```

在不支持弹性卷的情况下修改 EBS 卷

如果您使用的是支持的实例类型，则可以使用弹性卷来在不分离 Amazon EBS 卷的情况下动态修改卷的大小、性能和卷类型。

如果您无法使用弹性卷但需要修改根（启动）卷，则必须停止实例，修改卷，然后重新启动实例。

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 \(p. 848\)](#)。

监控卷修改的进度

当您修改 EBS 卷时，它将经历一系列状态。卷将依次进入 `modifying` 状态、`optimizing` 状态和 `completed` 状态。此时，卷已准备好做进一步的修改。

Note

在极少数情况下，暂时的 AWS 故障可能会导致 `failed` 状态。这并不指示卷的运行状况；它仅指示卷修改失败。如果发生这种情况，请重试卷修改。

当卷处于 `optimizing` 状态时，卷性能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，则过渡卷的性能不会低于目标卷的性能。

卷修改更改将生效，如下所示：

- 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。
- 新配置生效最长需要 24 个小时，在某些情况下可能会更长，例如在未完全初始化卷的情况下。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。

使用以下方法之一监控卷修改的进度。

目录

- [监控卷修改的进度 \(控制台 \) \(p. 846\)](#)
- [监控卷修改的进度 \(AWS CLI\) \(p. 846\)](#)
- [监控卷修改的进度 \(CloudWatch Events\) \(p. 847\)](#)

监控卷修改的进度 (控制台)

使用以下过程查看一个或多个卷修改的进度。

使用控制台监控修改的进度

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。卷状态显示在详细信息窗格的 State (状态) 列和 State (状态) 字段。在此示例中，修改状态为 completed (已完成)。
4. 打开 State (状态) 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，如本示例所示。

The screenshot shows the AWS EC2 Volumes page. A specific volume, 'vol-065fc28c...', is selected. The 'State' field shows 'available - completed (100%)'. A tooltip titled 'Volume modification details' is displayed, listing the following information:

Original Volume Type	gp2
Original Size	100
Original IOPS	300
Target Volume Type	gp2
Target Size	1000
Target IOPS	3000
Status message	-

监控卷修改的进度 (AWS CLI)

使用 `describe-volumes-modifications` 命令查看一个或多个卷修改的进度。以下示例描述了两个卷的卷修改。

```
aws ec2 describe-volumes-modifications --volume-id vol-1111111111111111 vol-2222222222222222
```

在以下示例输出中，卷修改仍处于 modifying 状态。

```
{  
    "VolumesModifications": [  
        {  
            "TargetSize": 200,  
            "TargetVolumeType": "io1",  
            "ModificationState": "modifying",  
            "VolumeId": "vol-1111111111111111",  
            "TargetIops": 10000,  
            "ModificationId": "mod-1111111111111111",  
            "ModificationArn": "arn:aws:ec2:us-east-1:123456789012:modification/mod-1111111111111111",  
            "ModificationType": "size",  
            "ModificationTimestamp": "2017-01-25T12:00:00Z",  
            "ModificationStatus": "in-progress",  
            "ModificationProgress": 100  
        }  
    ]  
}
```

```
"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
}
]
```

下一个示例描述了修改状态为 `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" --query "VolumesModifications[?
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

以下是包含有关两个卷的信息的示例输出：

```
[
{
    "STATE": "optimizing",
    "ID": "vol-06397e7a0eEXAMPLE"
},
{
    "STATE": "completed",
    "ID": "vol-ba74e18c2aEXAMPLE"
}]
```

监控卷修改的进度 (CloudWatch Events)

利用 CloudWatch Events，您可以为卷修改事件创建通知规则。您可以使用规则生成使用 Amazon SNS 的通知消息，或调用 [Lambda 函数](#) 来响应匹配事件。

使用 CloudWatch Events 监控修改进度

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 (构建自定义事件模式)，将内容替换为以下内容并选择 Save (保存)。

```
{
    "source": [
        "aws.ec2"
    ],
    "detail-type": [
        "EBS Volume Notification"
    ],
    "detail": {
        "event": [

```

```
        "modifyVolume"
    ]
}
```

下面是示例事件数据：

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "2017-01-12T21:09:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
    ],
    "detail": {
        "result": "optimizing",
        "cause": "",
        "event": "modifyVolume",
        "request-id": "01234567-0123-0123-0123-0123456789ab"
    }
}
```

调整卷大小后扩展 Linux 文件系统

在增加 EBS 卷的大小后，您必须使用特定于文件系统的命令来将文件系统扩展到较大小。一旦卷进入 `optimizing` 状态，您即可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，最佳实践是创建卷的快照（如果您需要回滚您的更改）。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 815\)](#)。如果您的 Linux AMI 使用 MBR 分区方案，您的引导卷大小限制为最高 2 TiB。有关更多信息，请参阅 [针对 Linux 卷的要求 \(p. 842\)](#) 和 [针对 EBS 卷的大小和配置的限制 \(p. 796\)](#)。

有关扩展 Windows 文件系统的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [调整卷大小后扩展 Windows 文件系统](#)。

对于以下任务，假设您将实例的引导卷的大小从 8 GB 调整为 16 GB，并将一个额外卷的大小从 8 GB 调整为 30 GB。

任务

- [标识卷的文件系统 \(p. 848\)](#)
- [扩展分区（如果需要）\(p. 849\)](#)
- [扩展文件系统 \(p. 850\)](#)

标识卷的文件系统

要验证文件系统是否用于您实例上的每个卷，请[连接到您的实例 \(p. 423\)](#)并运行 `file -s` 命令。

Example 示例：基于 Nitro 的实例上的文件系统

以下示例显示了一个[基于 Nitro 的实例 \(p. 163\)](#)，该实例具有带 XFS 文件系统的引导卷和带 XFS 文件系统的额外卷。

```
[ec2-user ~]$ sudo file -s /dev/nvme?n*
```

```
/dev/nvme0n1:      x86 boot sector ...
/dev/nvme0n1p1:    SGI XFS filesystem data ...
/dev/nvme0n1p128:  data
/dev/nvme1n1:      SGI XFS filesystem data ...
```

Example 示例 : T2 实例上的文件系统

以下示例显示了一个 T2 实例，该实例具有带 ext4 文件系统的引导卷和带 XFS 文件系统的额外卷。

```
[ec2-user ~]$ sudo file -s /dev/xvd*
/dev/xvda:  DOS/MBR boot sector ..
/dev/xvda1: Linux rev 1.0 ext4 filesystem data ...
/dev/xvdf:  SGI XFS filesystem data ...
```

扩展分区 (如果需要)

您的 EBS 卷可能有一个包含文件系统和数据的分区。增加卷的大小不会增加分区的大小。在调整大小后的卷上扩展文件系统之前，请检查卷是否具有必须扩展到卷的新大小的分区。

使用 lsblk 命令显示有关附加到实例的块储存设备的信息。如果调整大小后的卷有一个分区且该分区不反映卷的新大小，请使用 growpart 命令扩展该分区。有关扩展 LVM 分区的信息，请参阅[扩展逻辑卷](#)。

Example 示例 : 基于 Nitro 的实例上的分区

以下示例显示了基于 Nitro 的实例上的卷：

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1   259:0    0   30G  0 disk /data
nvme0n1   259:1    0   16G  0 disk
##nvme0n1p1 259:2    0   8G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
```

- 根卷 /dev/nvme0n1 具有一个分区 /dev/nvme0n1p1。当根卷的大小反映新大小 16 GB 时，分区的小会反映原始大小 8 GB 并且必须先进行扩展，然后才能扩展文件系统。
- 卷 /dev/nvme1n1 没有分区。卷的大小反映新大小 30 GB。

要在根卷上扩展分区，请使用以下 growpart 命令。请注意，设备名称和分区编号之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

您可以再次使用 lsblk 命令来验证分区是否反映增加的卷大小。

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1   259:0    0   30G  0 disk /data
nvme0n1   259:1    0   16G  0 disk
##nvme0n1p1 259:2    0   16G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
```

Example 示例 : T2 实例上的分区

以下示例显示了 T2 实例上的卷：

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0   16G  0 disk
##xvda1 202:1    0   8G  0 part /
```

```
xvdf    202:80    0  30G  0 disk
##xvdf1 202:81    0   8G  0 part /data
```

- 根卷 /dev/xvda 具有一个分区 /dev/xvda1。当卷的大小为 16 GB 时，分区的大小仍为 8 GB 且必须进行扩展。
- 卷 /dev/xvdf 具有一个分区 /dev/xvdf1。当卷的大小为 30G 时，分区的大小仍为 8 GB 且必须进行扩展。

要在每个卷上扩展分区，请使用以下 growpart 命令。请注意，设备名称和分区编号之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
[ec2-user ~]$ sudo growpart /dev/xvdf 1
```

您可以再次使用 lsblk 命令来验证分区是否反映增加的卷大小。

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0  16G  0 disk
##xvda1  202:1    0  16G  0 part /
xvdf     202:80   0  30G  0 disk
##xvdf1  202:81   0  30G  0 part /data
```

扩展文件系统

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。有关此处显示的示例以外的文件系统，请参阅文件系统的文档以了解相关说明。

Example 示例：扩展 ext2、ext3 或 ext4 文件系统

使用 df -h 命令验证每个卷的文件系统的大小。在此示例中，/dev/xvda1 和 /dev/xvdf 均反映卷的原始大小 8 GB。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       8.0G  1.9G  6.2G  24% /
/dev/xvdf1       8.0G   45M  8.0G   1% /data
...
```

使用 resize2fs 命令扩展每个卷上的文件系统。

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
[ec2-user ~]$ sudo resize2fs /dev/xvdf1
```

您可以再次使用 df -h 命令来验证每个文件系统是否反映增加的卷大小。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       16G  1.9G  6.2G  12% /
/dev/xvdf1       30G   45M  8.0G   1% /data
...
```

Example 示例：扩展 XFS 文件系统

使用 df -h 命令验证每个卷的文件系统的大小。在此示例中，每个文件系统均反映原始卷大小 8 GB。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
```

```
/dev/nvme0n1p1  8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    8.0G   33M   8.0G   1% /data
...
```

要扩展 XFS 文件系统，请按以下方式安装 XFS 工具（如果尚未安装）。

```
[ec2-user ~]$ sudo yum install xfsprogs
```

使用 xfs_growfs 命令扩展每个卷上的文件系统。在此示例中，/ 和 /data 是 df -h 的输出中显示的卷挂载点。

```
[ec2-user ~]$ sudo xfs_growfs -d /
[ec2-user ~]$ sudo xfs_growfs -d /data
```

您可以再次使用 df -h 命令来验证每个文件系统是否反映增加的卷大小。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p1   16G  1.6G   15G  10% /
/dev/nvme1n1     30G   33M   30G   1% /data
...
```

Amazon EBS Encryption

Amazon EBS 加密 提供了直接用于 EBS 资源的加密解决方案，无需您构建、维护和保护自己的密钥管理基础设施。它在创建加密卷和快照时使用 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK)。

加密操作在托管 EC2 实例的服务器上进行，用于确保静态数据安全性以及在实例和其附加的 EBS 存储之间传输的数据的安全性。

目录

- [EBS 加密的工作原理 \(p. 851\)](#)
- [要求 \(p. 852\)](#)
- [用于 EBS 加密的默认密钥 \(p. 853\)](#)
- [默认加密 \(p. 853\)](#)
- [加密 EBS 资源 \(p. 854\)](#)
- [加密方案 \(p. 854\)](#)
- [使用 API 和 CLI 设置加密默认值 \(p. 859\)](#)

EBS 加密的工作原理

您可以加密 EC2 实例的引导卷和数据卷。在创建加密的 EBS 卷并将其附加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
- 从这些快照创建的所有卷

EBS 通过行业标准的 AES-256 算法，利用数据密钥加密您的卷。您的数据密钥与您的加密数据一起存储在磁盘上，但并非在 EBS 利用您的 CMK 对数据密钥进行加密之前。数据密钥绝不会以纯文本形式出现在磁盘上。同一数据密钥将由从这些快照创建的卷和后续卷的快照共享。有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[数据密钥](#)。

Amazon EBS 与 AWS KMS 结合使用以加密和解密您的 EBS 卷，如下所示：

1. Amazon EBS 将 [CreateGrant](#) 请求发送到 AWS KMS，以便它能够解密数据密钥。
2. Amazon EBS 将 [GenerateDataKeyWithoutPlaintext](#) 请求发送到 AWS KMS，同时指定用于加密卷的 CMK。
3. AWS KMS 生成一个新的数据密钥，使用指定的 CMK 对其进行加密，并将加密的数据密钥发送给 Amazon EBS，以便与卷元数据一起存储。
4. 当您将加密卷附加到实例时，Amazon EBS 将 [Decrypt](#) 请求发送到 AWS KMS，同时指定加密的数据密钥。
5. AWS KMS 解密加密的数据密钥，然后将解密的数据密钥发送到 Amazon EBS。
6. Amazon EBS 使用管理程序内存中的明文数据密钥来加密卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的 [Amazon Elastic Block Store \(Amazon EBS\) 如何使用 AWS KMS 和 AWS KMS 日志文件条目](#)。

要求

在您开始之前，确认您满足以下要求。

支持的卷类型

所有 EBS 卷类型都支持加密。您可能希望加密卷具有与未加密卷相同的 IOPS 性能，同时对延迟的影响最低。您可以采用与访问未加密卷相同的方式来访问加密卷。加密和解密是以透明方式处理的，并且不需要您或您的应用程序执行额外操作。

支持的实例类型

Amazon EBS 加密 适用于以下所列的实例类型。您可以同时将加密卷和未加密卷附加到这些实例类型。

- 通用 : A1、M3、M4、M5、M5a、M5ad、M5d、M5dn、M5n、T2、T3 和 T3a
- 计算优化 : C3、C4、C5、C5d 和 C5n
- 内存优化 : `cr1.8xlarge`、R3、R4、R5、R5a、R5ad、R5d、R5dn、R5n、`u-6tb1.metal`、`u-9tb1.metal`、`u-12tb1.metal` 和 z1d
- 存储优化 : D2、`h1.2xlarge`、`h1.4xlarge`、I2、I3 和 I3en
- 加速计算 : F1、G2、G3、G4、P2 和 P3

IAM 用户的权限

当您将 CMK 配置为用于 EBS 加密的默认密钥时，默认密钥策略允许任何有权访问所需 KMS 操作的 IAM 用户使用此密钥加密或解密 EBS 资源。您必须授予 IAM 用户调用以下操作的权限才能使用 EBS 加密：

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 AWS 服务代表用户创建授权时，才允许用户在 CMK 上创建授权，如以下示例所示：

```
{  
    "Version": "2012-10-17",
```

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": "kms>CreateGrant",
        "Resource": [
            "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
        ],
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": true
            }
        }
    }
]
```

有关更多信息，请参阅 AWS Key Management Service Developer Guide 中的[默认密钥策略](#)。

用于 EBS 加密的默认密钥

Amazon EBS 自动在您存储 AWS 资源的每个区域中创建唯一的 AWS 托管 CMK。此密钥具有别名 alias / aws/ebs。默认情况下，Amazon EBS 使用此密钥进行加密。或者，您也可以将您创建的对称客户托管 CMK 指定为用于 EBS 加密的默认密钥。使用您自己的 CMK 可以提高灵活性，包括提供创建、轮换和禁用密钥的能力。

Important

Amazon EBS 不支持非对称 CMK。有关更多信息，请参阅 AWS Key Management Service 开发人员指南 中的[使用对称和非对称密钥](#)。

针对某个区域配置用于 EBS 加密的默认密钥

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. 依次选择 Account Attributes (账户属性) 和 Settings (设置)。
4. 选择 Change the default key (更改默认密钥)，然后选择可用密钥。
5. 选择 Update (更新)。

默认加密

您可以配置 AWS 账户对您创建的新 EBS 卷和快照副本进行加密。例如，Amazon EBS 加密当您启动实例时创建的 EBS 卷以及您从未加密的快照复制的快照。有关从未加密转换为加密 EBS 资源的示例，请参阅[加密未加密的资源 \(p. 854\)](#)。

默认情况下，加密对现有 EBS 卷或快照没有影响。

注意事项

- 默认加密是区域特定的设置。如果您为某个区域启用了它，则无法为该区域中单独的卷或快照禁用。
- 当您启用默认加密时，您只能在实例类型支持 EBS 加密时启动实例。有关更多信息，请参阅[支持的实例类型 \(p. 852\)](#)。
- 在使用 AWS Server Migration Service (SMS) 迁移服务器时，默认情况下不会启用加密。如果默认情况下已启用加密，并且您遇到增量复制失败，请默认关闭加密。改为在创建复制作业时启用 AMI 加密。

默认为某个区域启用加密

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 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择设置。
5. 在 EBS Storage (EBS 存储) 下，选择 Always encrypt new EBS volumes (始终加密新的 EBS 卷)。
6. 选择 Update (更新)。

您无法更改与现有快照或加密卷关联的 CMK。但是，您可在快照复制操作期间关联另一个 CMK，从而使生成的已复制快照由新 CMK 进行加密。

加密 EBS 资源

您可以通过启用加密来加密 EBS 卷：[使用默认加密 \(p. 853\)](#)，或者在创建要加密的卷时启用加密。

加密卷时，可以指定用于加密卷的对称 CMK。如果未指定 CMK，则用于加密的密钥取决于源快照的加密状态及其所有权。有关更多信息，请参阅[加密结果表 \(p. 858\)](#)。

您无法更改与现有快照或卷关联的 CMK。但是，您可在快照复制操作期间关联另一个 CMK，从而使生成的已复制快照由新 CMK 进行加密。

创建具有加密的新空卷

创建新的空 EBS 卷时，可以通过为特定卷创建操作启用加密来对其进行加密。如果您默认启用了 EBS 加密，则会自动加密卷。默认情况下，已使用用于 EBS 加密的默认密钥对卷加密。或者，您可以为特定的卷创建操作指定不同的对称 CMK。卷从其首次可用时开始加密，因此您的数据始终安全。有关详细步骤，请参阅[创建 Amazon EBS 卷 \(p. 798\)](#)。

默认情况下，您在创建卷时选择的 CMK 会对从该卷拍摄的快照加密，并对从这些加密的快照还原的卷加密。您无法从加密卷或快照删除加密，这意味着从加密快照还原的卷或者加密快照的副本始终加密。

加密卷的快照无法公开，但您可以与特定账户共享加密快照。有关详细指导，请参阅[共享 Amazon EBS 快照 \(p. 822\)](#)。

加密未加密的资源

虽然没有直接的方法可以加密现有的未加密卷或快照，但您可以通过创建卷或快照来加密它们。如果您启用了默认加密，Amazon EBS 使用您用于 EBS 加密的默认密钥对生成的新卷或快照实施加密。即使您未启用默认加密，也可以在创建单个卷或快照时启用加密。无论是启用默认加密还是在单独创建操作中启用加密，您都可以覆盖用于 EBS 加密的默认密钥并选择对称的客户托管 CMK。有关更多信息，请参阅[创建 Amazon EBS 卷 \(p. 798\)](#) 和[复制 Amazon EBS 快照 \(p. 819\)](#)。

要将快照副本加密到客户托管的 CMK，您必须同时启用加密并指定密钥，如[复制未加密的快照（未启用默认加密）\(p. 856\)](#) 中所示。

Important

Amazon EBS 不支持非对称 CMK。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的[使用对称和非对称密钥](#)。

在从由 EBS 支持的 AMI 启动实例时，您还可以应用新的加密状态。这是因为 EBS 支持的 AMI 包括可以按照所述进行加密的 EBS 卷的快照。有关更多信息，请参阅[将加密与 EBS 支持的 AMI 结合使用 \(p. 134\)](#)。

加密方案

创建加密 EBS 资源时，除非您在卷创建参数或 AMI 或实例的块设备映射中指定了不同的客户托管 CMK，否则它将使用您账户的用于 EBS 加密的默认密钥进行加密。有关更多信息，请参阅[用于 EBS 加密的默认密钥 \(p. 853\)](#)。

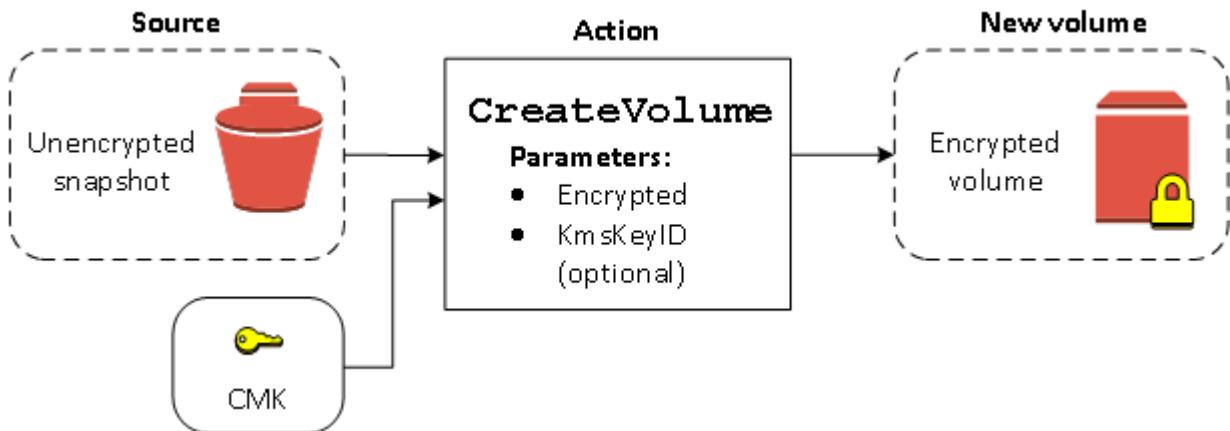
以下示例说明如何管理卷和快照的加密状态。有关加密案例的完整列表，请参阅[加密结果表 \(p. 858\)](#)。

示例

- 还原未加密的卷 (未启用默认加密) (p. 855)
- 还原未加密的卷 (启用了默认加密) (p. 855)
- 复制未加密的快照 (未启用默认加密) (p. 856)
- 复制未加密的快照 (启用了默认加密) (p. 856)
- 重新加密已加密卷 (p. 857)
- 重新加密已加密快照 (p. 857)
- 在加密卷与未加密卷之间迁移数据 (p. 858)
- 加密结果 (p. 858)

还原未加密的卷 (未启用默认加密)

未启用默认加密时，从未加密快照还原的卷在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的卷。下图说明了该过程。

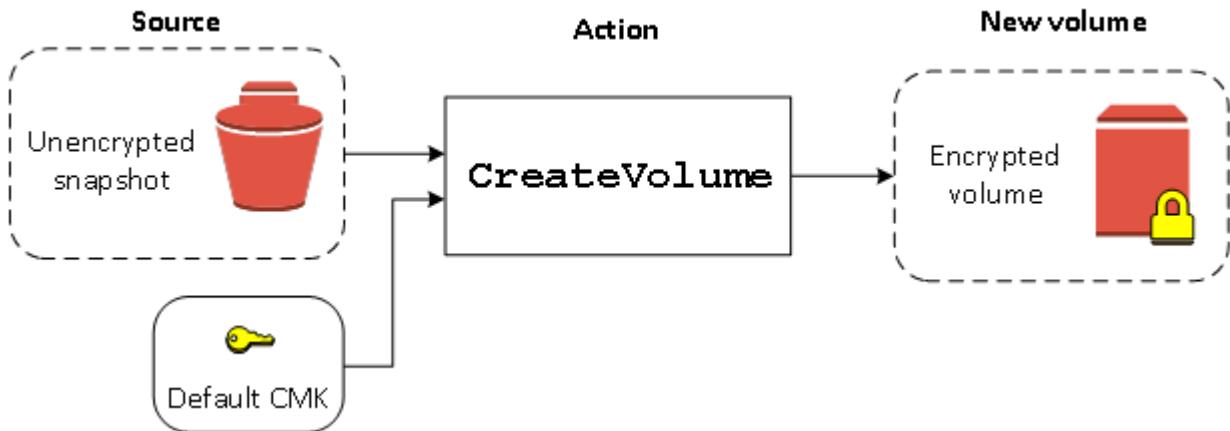


如果您省略 `KmsKeyId` 参数，则将使用您用于 EBS 加密的默认密钥加密生成的卷。您必须指定密钥 ID 以使用不同的 CMK 加密卷。

有关更多信息，请参阅 [从快照还原 Amazon EBS 卷 \(p. 799\)](#)。

还原未加密的卷 (启用了默认加密)

在您启用了默认加密时，从未加密快照还原的卷必须加密，无需使用默认 CMK 的加密参数。下图说明了这种简单默认案例：

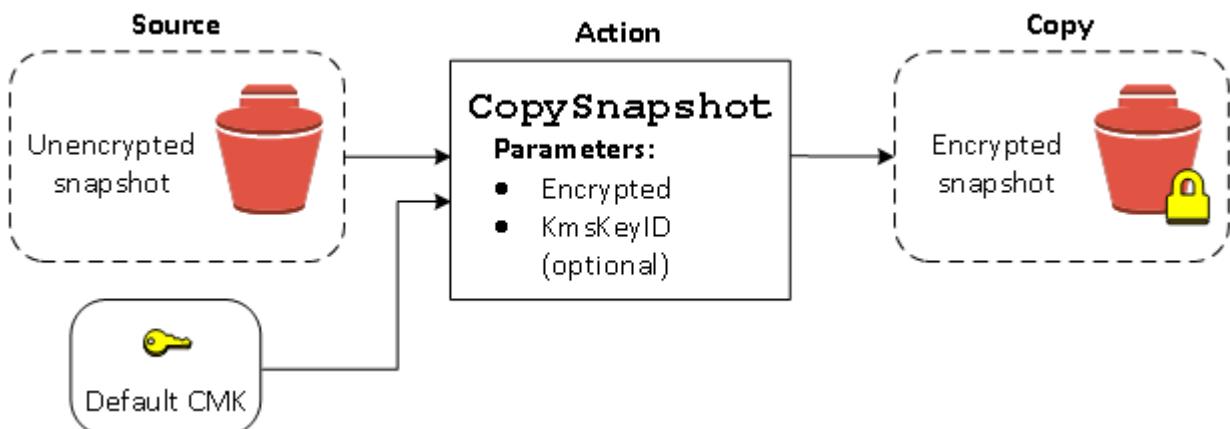


如果您要使用对称的客户托管 CMK 加密还原的卷，则必须提供 `Encrypted` 和 `KmsKeyId` 参数，如[还原未加密的卷 \(未启用默认加密\) \(p. 855\)](#)中所示。

复制未加密的快照 (未启用默认加密)

未启用默认加密时，未加密快照的副本在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的快照。如果省略 `KmsKeyId`，则使用默认 CMK 加密生成的快照。您必须指定密钥 ID 以使用不同的对称 CMK 加密卷。

下图说明了该过程。



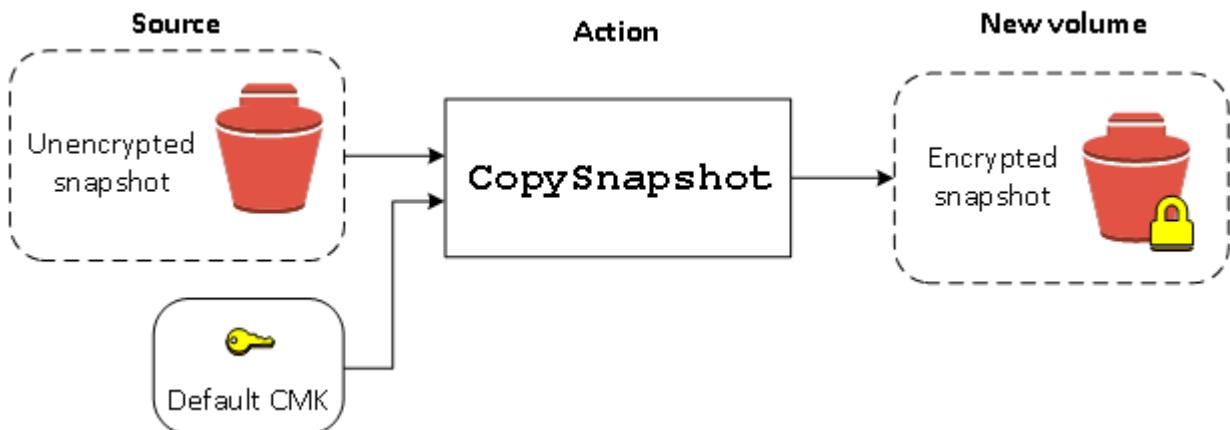
Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整 (非增量) 副本，从而导致额外的延迟和存储成本。

您可以将未加密的快照复制到加密的快照，然后从加密的快照中创建卷来加密 EBS 卷。有关更多信息，请参阅[复制 Amazon EBS 快照 \(p. 819\)](#)。

复制未加密的快照 (启用了默认加密)

在您启用了默认加密时，未加密快照的副本必须加密，无需使用默认 CMK 的加密参数。下图说明了这种默认情况：

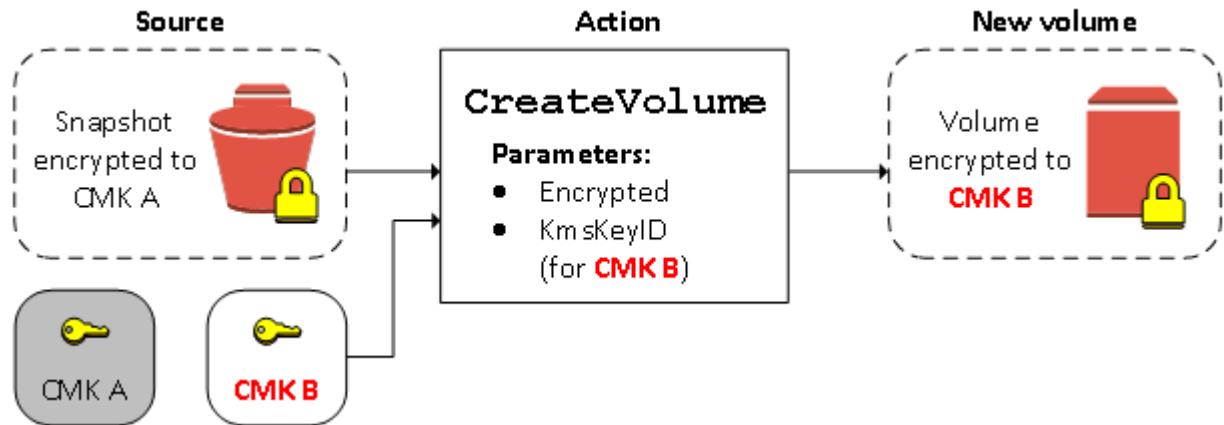


Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整 (非增量) 副本，从而导致额外的延迟和存储成本。

重新加密已加密卷

对加密快照执行 `CreateVolume` 操作时，您可以选择使用不同 CMK 重新加密它。下图说明了该过程。在本例中，您拥有两个 CMK，即 CMK A 和 CMK B。源快照由 CMK A 加密。在卷创建期间，由于 CMK B 的密钥 ID 被指定为一个参数，因此源数据被自动解密，然后由 CMK B 重新加密。



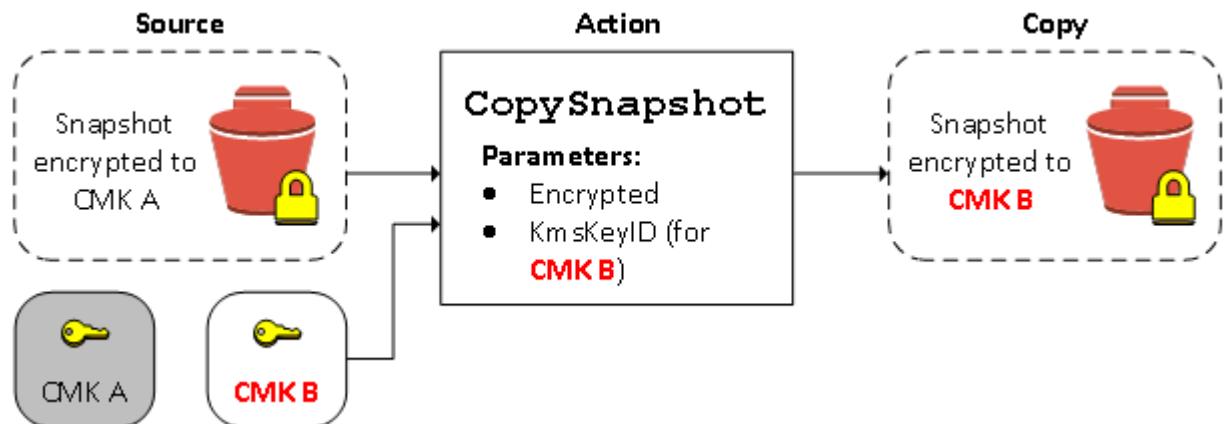
Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

有关更多信息，请参阅 [从快照还原 Amazon EBS 卷 \(p. 799\)](#)。

重新加密已加密快照

由于能够在复制过程中加密快照，您可以将新的对称 CMK 应用于您拥有的已加密过的快照。从生成的副本还原的卷只能使用新的 CMK 进行访问。下图说明了该过程。在本例中，您拥有两个 CMK，即 CMK A 和 CMK B。源快照由 CMK A 加密。在复制期间，由于 CMK B 的密钥 ID 被指定为一个参数，因此源数据被 CMK B 自动重新加密。



Note

如果快照复制到新的 CMK 并将其加密，将始终创建完整（非增量）副本，从而导致额外的延迟和存储成本。

在相关的场景中，您可以选择将新加密参数应用于已与您共享的快照的副本。默认情况下，系统会使用快照所有者共享的 CMK 对该副本进行加密。但是，我们建议您使用您控制的其他 CMK 创建共享快照的副本。这样，即使原始 CMK 遭到泄露或所有者出于任何原因撤销了 CMK，您也不会失去对卷的访问权限。有关更多信息，请参阅 [加密和快照复制 \(p. 820\)](#)。

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。

例如，使用 rsync 命令复制数据。在以下命令中，源数据位于 /mnt/source 中，目标卷挂载在 /mnt/destination 中。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

加密结果

下表描述了每种可能的设置组合的加密结果。

是否启用加密？	是否默认启用加密？	卷源	默认值（不指定 CMK）	自定义（指定 CMK）
否	否	新（空）卷	未加密	不适用
否	否	您拥有的未加密快照	未加密	
否	否	您拥有的加密快照	按相同密钥加密	
否	否	与您共享的未加密快照	未加密	
否	否	与您共享的加密快照	按默认 CMK 加密*	
是	否	新卷	按默认 CMK 加密	按指定的 CMK 加密**
是	否	您拥有的未加密快照	按默认 CMK 加密	
是	否	您拥有的加密快照	按相同密钥加密	
是	否	与您共享的未加密快照	按默认 CMK 加密	
是	否	与您共享的加密快照	按默认 CMK 加密	
否	是	新（空）卷	按默认 CMK 加密	
否	是	您拥有的未加密快照	按默认 CMK 加密	
否	是	您拥有的加密快照	按相同密钥加密	
否	是	与您共享的未加密快照	按默认 CMK 加密	
否	是	与您共享的加密快照	按默认 CMK 加密	
是	是	新卷	按默认 CMK 加密	按指定的 CMK 加密
是	是	您拥有的未加密快照	按默认 CMK 加密	
是	是	您拥有的加密快照	按相同密钥加密	
是	是	与您共享的未加密快照	按默认 CMK 加密	
是	是	与您共享的加密快照	按默认 CMK 加密	

* 这是用于对 AWS 账户和区域进行 EBS 加密的默认 CMK。默认情况下，这是用于 EBS 的唯一 AWS 托管 CMK，您也可以指定自定义的托管 CMK。有关更多信息，请参阅 [用于 EBS 加密的默认密钥 \(p. 853\)](#)。

** 这是在发布时为卷指定的客户托管的 CMK。此 CMK 替代默认的 CMK 用于 AWS 账户和区域。

使用 API 和 CLI 设置加密默认值

您可以使用以下 API 操作和 CLI 命令默认管理加密和默认客户主密钥 (CMK)。

API 操作	CLI 命令	描述
DisableEbsEncryptionByDefault	disable-ebs-encryption-by-default	默认禁用加密。
EnableEbsEncryptionByDefault	enable-ebs-encryption-by-default	默认启用加密。
GetEbsDefaultKmsKeyId	get-ebs-default-kms-key-id	描述默认 CMK。
GetEbsEncryptionByDefault	get-ebs-encryption-by-default	指示是否默认启用了加密。
ModifyEbsDefaultKmsKeyId	modify-ebs-default-kms-key-id	更改用于加密 EBS 卷的默认 CMK。
ResetEbsDefaultKmsKeyId	reset-ebs-default-kms-key-id	将 AWS 托管默认 CMK 重置为用于加密 EBS 卷的默认 CMK。

Amazon EBS 快速快照还原

Amazon EBS 快速快照还原使您能够在创建时从已初始化的快照创建卷。这会消除首次访问块时对其执行 I/O 操作的延迟。使用快速快照还原创建的卷可以立即交付其所有预配置性能。

要使用快速快照还原，请在特定可用区中为特定快照启用此功能。您可以为每个区域的最多 5 个快照启用快速快照还原。

目录

- [快速快照还原状态 \(p. 859\)](#)
- [卷创建积分 \(p. 859\)](#)
- [管理快速快照还原 \(p. 860\)](#)

快速快照还原状态

在为快照启用快速快照还原后，它可能处于以下状态之一。

- `enabling` — 发出了启用快速快照还原的请求。
- `optimizing` — 正在启用快速快照还原。对于快照优化，每个 TiB 需要 60 分钟的时间。
- `enabled` — 启用了快速快照还原。
- `disabling` — 发出了禁用快速快照还原的请求，或者启用快速快照还原的请求失败。
- `disabled` — 禁用了快速快照还原。您可以根据需要再次启用快速快照还原。

卷创建积分

获得快速快照还原的全部性能优势的卷数是由快照的卷创建积分决定的。每个可用区的每个快照具有一个积分存储桶。从快照中创建并启用了快速快照还原的每个卷使用积分存储桶中的一个积分。

积分存储桶大小取决于快照的大小，而不是取决于从快照中创建的卷的大小。每个快照的积分存储桶大小计算如下：

```
MAX (1, MIN (10, FLOOR(1024/snapshot_size_gib)))
```

在使用积分时，将随着时间的推移重新填充积分存储桶。每个积分存储桶的重新填充率计算如下：

```
MIN (10, 1024/snapshot_size_gib)
```

例如，如果为 100 GiB 大小的快照启用快速快照还原，则其积分存储桶的最大大小为 10 个积分，重新填充率为每小时 10 个积分。如果积分存储桶已满，您可以同时从该快照中创建 10 个初始化的卷。

您可以使用 Cloudwatch 指标来监控积分余额存储桶的大小以及各个存储桶中可用的积分数量。有关更多信息，请参阅 [快速快照还原指标 \(p. 892\)](#)。

从启用了快速快照还原的存储桶创建卷之后，您可以使用 [describe-volumes](#) 来描述卷，并检查输出中的 `fastRestored` 字段以确定是否使用快速快照还原将该卷创建为已初始化卷。

管理快速快照还原

使用以下过程为快照启用快速快照还原。您必须拥有快照。无法在与您共享的快照上启用快速快照还原。

管理快速快照还原

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择快照。
4. 选择操作，然后选择管理快速快照还原。
5. 选择或取消选择可用区，然后选择保存。
6. 要在启用了快速快照还原时跟踪其状态，请查看描述选项卡上的快速快照还原。

使用 AWS CLI 管理快速快照还原

- [enable-fast-snapshot-restores](#)
- [disable-fast-snapshot-restores](#)
- [describe-fast-snapshot-restores](#)
- [describe-volumes](#)

Linux 实例上的 Amazon EBS 和 NVMe

在[基于 Nitro 的实例 \(p. 163\)](#)上，EBS 卷显示为 NVMe 块储存设备。设备名称为 `/dev/nvme0n1`、`/dev/nvme1n1`，以此类推。您在块储存设备映射中指定的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。块储存设备驱动程序可以使用不同于您在块储存设备映射中为卷指定的顺序来分配 NVMe 设备名称。

Note

无论块储存设备接口如何，[Amazon EBS 产品详细信息](#) 中所述的 EBS 性能保证都有效。

目录

- [安装或升级 NVMe 驱动程序 \(p. 861\)](#)
- [识别 EBS 设备 \(p. 861\)](#)
- [使用 NVMe EBS 卷 \(p. 862\)](#)
- [I/O 操作超时 \(p. 863\)](#)

安装或升级 NVMe 驱动程序

要访问 NVMe 卷，必须安装 NVMe 驱动程序。实例可以支持 NVMe EBS 卷和 NVMe 实例存储卷（要么两种类型的 NVMe 卷均支持，要么均不支持）。有关更多信息，请参阅 [联网和存储功能总结 \(p. 165\)](#)。

以下 AMI 包含所需的 NVMe 驱动程序：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 `linux-aws` 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

有关 Windows 实例上的 NVMe 驱动程序的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 [Windows 实例上的 Amazon EBS 和 NVMe](#)。

如果您使用的是不包含 NVMe 驱动程序的 AMI，则可以使用以下过程将该驱动程序安装在实例上。

安装 NVMe 驱动程序

1. 连接到您的实例。
2. 更新程序包缓存以获取必需程序包更新，如下所示。

- 对于 Amazon Linux 2、Amazon Linux、CentOS 和 Red Hat Enterprise Linux：

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

- 对于 Ubuntu 和 Debian：

```
[ec2-user ~]$ sudo apt-get update -y
```

3. Ubuntu 16.04 及更高版本包含 `linux-aws` 程序包，该程序包包含基于 Nitro 的实例所需的 NVMe 和 ENA 驱动程序。升级 `linux-aws` 程序包以接收最新版本，如下所示：

```
[ec2-user ~]$ sudo apt-get upgrade -y linux-aws
```

对于 Ubuntu 14.04，您可以安装最新的 `linux-aws` 程序包，如下所示：

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. 重启实例以加载最新内核版本。

```
sudo reboot
```

5. 重启之后重新连接到实例。

识别 EBS 设备

EBS 使用单一根 I/O 虚拟化 (SR-IOV) 在使用 NVMe 规范的基于 Nitro 的实例上提供卷附加。这些设备依赖于操作系统上的标准 NVMe 驱动程序。这些驱动程序通常在实例启动期间通过扫描 PCI 总线来发现附加的

设备，然后根据设备响应的顺序创建设备节点，而不是按照在块储存设备映射中指定设备的顺序。在 Linux 中，NVMe 设备名称遵循 `/dev/nvme<x>n<y>` 模式，其中 `<x>` 是枚举顺序，对于 EBS，`<y>` 为 1。有时候，在接下来的实例启动时，设备会以不同顺序响应发现过程，这会导致设备名称更改。

建议您在实例中为 EBS 卷使用静态标识符，例如以下之一：

- 对基于 Nitro 的实例，您在附加 EBS 卷或者在 `AttachVolume` 或 `RunInstances` API 调用期间通过 Amazon EC2 控制台指定的块储存设备映射，将在 NVMe 控制器标识的供应商特定数据字段中捕获。对版本高于 2017.09.01 的 Amazon Linux AMI，我们提供了 `udev` 规则，该规则读取此数据并创建指向块储存设备映射的符号链接。
- NVMe EBS 卷在设备标识中将 EBS 卷 ID 设置为序列号。
- 格式化设备时，将生成在文件系统的使用寿命内保持的 UUID。此时可指定设备标签。有关更多信息，请参阅 [使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#) 和 [正在从错误的卷启动 \(p. 985\)](#)。

Amazon Linux AMI

利用 Amazon Linux AMI 2017.09.01 或更高版本（包括 Amazon Linux 2），您可以按下面所示运行 `ebsnvme-id` 命令以将 NVMe 设备名称映射到卷 ID 和设备名称：

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-01324f611e2463981
/dev/sdf
```

Amazon Linux 还将创建从块储存设备映射中的设备名称（例如，`/dev/sdf`）到 NVMe 设备名称的符号链接。

其他 Linux AMI

利用内核版本 4.2 或更高版本，您可以按下面所示运行 `nvme id-cntl` 命令以将 NVMe 设备映射到卷 ID。首先，使用您的 Linux 发行版的程序包管理工具安装 NVMe 命令行程序包 `nvme-cl`。

以下示例将获取卷 ID 和设备名称。设备名称通过特定于 NVMe 控制器供应商的扩展（控制器标识的字节 384:4095）提供：

```
[ec2-user ~]$ sudo nvme id-cntl -v /dev/nvme1n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn       : vol01234567890abcdef
mn       : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

`lsblk` 命令可列出可用设备及其挂载点（如果适用）。这有助于确定要使用的正确设备名称。在本示例中，`/dev/nvme0n1p1` 作为根设备挂载，`/dev/nvme1n1` 会附加但不会挂载。

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1   259:3    0 100G  0 disk
nvme0n1   259:0    0    8G  0 disk
  nvme0n1p1 259:1    0    8G  0 part /
  nvme0n1p128 259:2   0    1M  0 part
```

使用 NVMe EBS 卷

要格式化并挂载 NVMe EBS 卷，请参阅 [使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#)。

如果您使用的是 Linux 内核 4.2 或更高版本，您对 NVMe EBS 卷的卷大小进行的所有更改将自动在实例中反映。对于旧版 Linux 内核，您可能需要分离然后附加 EBS 卷或者重启实例才能反映大小更改。对于 Linux 内核 3.19 或更高版本，您可以按下面所示使用 `hdparm` 命令强制重新扫描 NVMe 设备：

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

当您分离 NVMe EBS 卷时，实例在分离卷之前将没有机会刷新文件系统缓存或元数据。在分离 NVMe EBS 卷之前，您应该首先同步并卸载它。如果卷无法分离，您可以按照[将 Amazon EBS 卷与实例分离 \(p. 810\)](#)中所述尝试执行 `force-detach` 命令。

I/O 操作超时

附加到基于 Nitro 系统的实例的 EBS 卷使用操作系统提供的默认 NVMe 驱动程序。大多数操作系统为提交到 NVMe 设备的 I/O 操作指定一个超时。默认超时为 30 秒，可以使用 `nvme_core.io_timeout` 引导参数更改该超时。对于 4.6 版之前的 Linux 内核版本，此参数为 `nvme.io_timeout`。

如果 I/O 延迟超过了此超时参数的值，则 Linux NVMe 驱动程序会使 I/O 失败，并将错误返回文件系统或应用程序。根据 I/O 操作，您的文件系统或应用程序可以重试错误。在某些情况下，您的文件系统可能会通过只读方式重新挂载。

为了获得与附加到 Xen 实例的 EBS 卷类似的体验，我们建议将 `nvme_core.io_timeout` 设置为可能的最大值。对于当前内核，最大值为 4294967295，而对于较早的内核，最大值为 255。根据 Linux 版本的不同，超时时间可能已设置为支持的最大值。例如，对于 Amazon Linux AMI 2017.09.01 以及更高的版本，超时时间默认设置为 4294967295。

您可以通过将高于建议最大值的值写入 `/sys/module/nvme_core/parameters/io_timeout` 并在尝试保存文件时检查 `Numerical result out of range` (数值结果超出范围) 错误，以此来验证您的 Linux 发行版的最大值。

Amazon EBS 优化的实例

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。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

EBS 优化的实例将专用带宽提供给 Amazon EBS。当附加到 EBS 优化实例时，通用型 SSD (gp2) 卷可在 99% 的时间内提供其基准性能和突增性能，而预配置 IOPS SSD (io1) 卷可在 99.9% 的时间内提供其预配置性能。吞吐优化 HDD (st1) 和 Cold HDD (sc1) 都可确保 99% 的时间内 90% 突增性能的性能一致性。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。有关更多信息，请参阅[Amazon EBS 卷类型 \(p. 785\)](#)。

目录

- [支持的实例类型 \(p. 863\)](#)
- [在启动时启用 EBS 优化 \(p. 874\)](#)
- [为正在运行的实例启用 EBS 优化 \(p. 875\)](#)

支持的实例类型

下面的表显示了支持 EBS 优化的实例类型。它们包括针对 Amazon EBS 的专用带宽、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，以及实例可以支持的最大 IOPS (如果使用的是 16 KiB I/O 大小)。请选择提供的专用 Amazon 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。

默认为 EBS 优化

下表列出了支持 EBS 优化的实例类型，默认情况下启用了 EBS 优化。无需启用 EBS 优化，禁用 EBS 优化也没有效果。

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
a1.medium *	3,500	437.5	20000
a1.large *	3,500	437.5	20000
a1.xlarge *	3,500	437.5	20000
a1.2xlarge *	3,500	437.5	20000
a1.4xlarge	3,500	437.5	20000
c4.large	500	62.5	4000
c4.xlarge	750	93.75	6000
c4.2xlarge	1000	125	8000
c4.4xlarge	2000	250	16000
c4.8xlarge	4,000	500	32000
c5.large *	4750	593.75	20000
c5.xlarge *	4750	593.75	20000
c5.2xlarge *	4750	593.75	20000
c5.4xlarge	4750	593.75	20000
c5.9xlarge	9500	1187.5	40000
c5.12xlarge	9500	1187.5	40000
c5.18xlarge	19000	2375	80,000
c5.24xlarge	19000	2375	80,000
c5.metal	19000	2375	80,000
c5d.large *	4750	593.75	20000
c5d.xlarge *	4750	593.75	20000
c5d.2xlarge *	4750	593.75	20000
c5d.4xlarge	4750	593.75	20000
c5d.9xlarge	9500	1187.5	40000
c5d.12xlarge	9500	1187.5	40000
c5d.18xlarge	19000	2375	80,000
c5d.24xlarge	19000	2375	80,000
c5d.metal	19000	2375	80,000
c5n.large *	4750	593.75	20000
c5n.xlarge *	4750	593.75	20000

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
c5n.2xlarge *	4750	593.75	20000
c5n.4xlarge	4750	593.75	20000
c5n.9xlarge	9500	1187.5	40000
c5n.18xlarge	19000	2375	80,000
c5n.metal	19000	2375	80,000
d2.xlarge	750	93.75	6000
d2.2xlarge	1000	125	8000
d2.4xlarge	2000	250	16000
d2.8xlarge	4,000	500	32000
f1.2xlarge	1,700	212.5	12000
f1.4xlarge	3,500	400	44,000
f1.16xlarge	14,000	1,750	75000
g3s.xlarge	850	100	5000
g3.4xlarge	3,500	437.5	20000
g3.8xlarge	7,000	875	40000
g3.16xlarge	14,000	1,750	80,000
g4dn.xlarge	3,500	437.5	10,000
g4dn.2xlarge	3,500	437.5	20000
g4dn.4xlarge	3,500	437.5	20000
g4dn.8xlarge	7,000	875	40000
g4dn.12xlarge	7,000	875	40000
g4dn.16xlarge	7,000	875	40000
h1.2xlarge	1,750	218.75	12000
h1.4xlarge	3,500	437.5	20000
h1.8xlarge	7,000	875	40000
h1.16xlarge	14,000	1,750	80,000
i3.large	425	53.13	3000
i3.xlarge	850	106.25	6000
i3.2xlarge	1,700	212.5	12000
i3.4xlarge	3,500	437.5	16000

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
i3.8xlarge	7,000	875	32,500
i3.16xlarge	14,000	1,750	65000
i3.metal	14,000	1,750	65000
i3en.large *	3,500	437.5	20000
i3en.xlarge *	3,500	437.5	20000
i3en.2xlarge *	3,500	437.5	20000
i3en.3xlarge *	3,500	437.5	20000
i3en.6xlarge	3,500	437.5	20000
i3en.12xlarge	7,000	875	40000
i3en.24xlarge	14,000	1,750	80,000
i3en.metal	14,000	1,750	80,000
m4.large	450	56.25	3600
m4.xlarge	750	93.75	6000
m4.2xlarge	1000	125	8000
m4.4xlarge	2000	250	16000
m4.10xlarge	4,000	500	32000
m4.16xlarge	10000	1250	65000
m5.large *	4750	593.75	18,750
m5.xlarge *	4750	593.75	18,750
m5.2xlarge *	4750	593.75	18,750
m5.4xlarge	4750	593.75	18,750
m5.8xlarge	6800	850	30000
m5.12xlarge	9500	1187.5	40000
m5.16xlarge	13600	1,700	60000
m5.24xlarge	19000	2375	80,000
m5.metal	19000	2375	80,000
m5a.large *	2,120	265	16000
m5a.xlarge *	2,120	265	16000
m5a.2xlarge *	2,120	265	16000
m5a.4xlarge	2,120	265	16000

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
m5a.8xlarge	3,500	437.5	20000
m5a.12xlarge	5000	625	30000
m5a.16xlarge	7,000	875	40000
m5a.24xlarge	10000	1250	60000
m5ad.large *	2,120	265	16000
m5ad.xlarge *	2,120	265	16000
m5ad.2xlarge *	2,120	265	16000
m5ad.4xlarge	2,120	265	16000
m5ad.12xlarge	5000	675	30000
m5ad.24xlarge	10000	1250	60000
m5d.large *	4750	593.75	18,750
m5d.xlarge *	4750	593.75	18,750
m5d.2xlarge *	4750	593.75	18,750
m5d.4xlarge	4750	593.75	18,750
m5d.8xlarge	6800	850	30000
m5d.12xlarge	9500	1187.5	40000
m5d.16xlarge	13600	1,700	60000
m5d.24xlarge	19000	2375	80,000
m5d.metal	19000	2375	80,000
m5dn.large *	4750	593.75	18,750
m5dn.xlarge *	4750	593.75	18,750
m5dn.2xlarge *	4750	593.75	18,750
m5dn.4xlarge	4750	593.75	18,750
m5dn.8xlarge	6800	850	30000
m5dn.12xlarge	9500	1187.5	40000
m5dn.16xlarge	13600	1,700	60000
m5dn.24xlarge	19000	2375	80,000
m5n.large *	4750	593.75	18,750
m5n.xlarge *	4750	593.75	18,750
m5n.2xlarge *	4750	593.75	18,750

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
m5n.4xlarge	4750	593.75	18,750
m5n.8xlarge	6800	850	30000
m5n.12xlarge	9500	1187.5	40000
m5n.16xlarge	13600	1,700	60000
m5n.24xlarge	19000	2375	80,000
p2.xlarge	750	93.75	6000
p2.8xlarge	5000	625	32,500
p2.16xlarge	10000	1250	65000
p3.2xlarge	1,750	218	10000
p3.8xlarge	7,000	875	40000
p3.16xlarge	14,000	1,750	80,000
p3dn.24xlarge	19000	2375	80,000
r4.large	425	53.13	3000
r4.xlarge	850	106.25	6000
r4.2xlarge	1,700	212.5	12000
r4.4xlarge	3,500	437.5	18,750
r4.8xlarge	7,000	875	37,500
r4.16xlarge	14,000	1,750	75000
r5.large *	4750	593.75	18,750
r5.xlarge *	4750	593.75	18,750
r5.2xlarge *	4750	593.75	18,750
r5.4xlarge	4750	593.75	18,750
r5.8xlarge	6800	850	30000
r5.12xlarge	9500	1187	40000
r5.16xlarge	13600	1,700	60000
r5.24xlarge	19000	2375	80,000
r5.metal	19000	2375	80,000
r5a.large *	2,120	265	16000
r5a.xlarge *	2,120	265	16000
r5a.2xlarge *	2,120	265	16000

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
r5a.4xlarge	2,120	265	16000
r5a.8xlarge	3,500	437.5	32000
r5a.12xlarge	5000	625	30000
r5a.16xlarge	7,000	875	40000
r5a.24xlarge	10000	1250	60000
r5ad.large *	2,210	265	16000
r5ad.xlarge *	2,210	265	16000
r5ad.2xlarge *	2,210	265	16000
r5ad.4xlarge	2,210	265	16000
r5ad.12xlarge	5000	625	30000
r5ad.24xlarge	10000	1250	60000
r5d.large *	4750	593.75	18,750
r5d.xlarge *	4750	593.75	18,750
r5d.2xlarge *	4750	593.75	18,750
r5d.4xlarge	4750	593.75	18,750
r5d.8xlarge	6800	850	30000
r5d.12xlarge	9500	1187	40000
r5d.16xlarge	13600	1,700	60000
r5d.24xlarge	19000	2375	80,000
r5d.metal	19000	2375	80,000
r5dn.large *	4750	593.75	18,750
r5dn.xlarge *	4750	593.75	18,750
r5dn.2xlarge *	4750	593.75	18,750
r5dn.4xlarge	4750	593.75	18,750
r5dn.8xlarge	6800	850	30000
r5dn.12xlarge	9500	1187	40000
r5dn.16xlarge	13600	1,700	60000
r5dn.24xlarge	19000	2375	80,000
r5n.large *	4750	593.75	18,750
r5n.xlarge *	4750	593.75	18,750

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
r5n.2xlarge *	4750	593.75	18,750
r5n.4xlarge	4750	593.75	18,750
r5n.8xlarge	6800	850	30000
r5n.12xlarge	9500	1187	40000
r5n.16xlarge	13600	1,700	60000
r5n.24xlarge	19000	2375	80,000
t3.nano *	1,536	192	11,800
t3.micro *	1,536	192	11,800
t3.small *	1,536	192	11,800
t3.medium *	1,536	192	11,800
t3.large *	2,048	256	15,700
t3.xlarge *	2,048	256	15,700
t3.2xlarge *	2,048	256	15,700
t3a.nano *	1,536	192	11,800
t3a.micro *	1,536	192	11,800
t3a.small *	1,536	192	11,800
t3a.medium *	1,536	192	11,800
t3a.large *	2,048	256	15,700
t3a.xlarge *	2,048	256	15,700
t3a.2xlarge *	2,048	256	15,700
u-6tb1.metal	19000	2375	80,000
u-9tb1.metal	19000	2375	80,000
u-12tb1.metal	19000	2375	80,000
u-18tb1.metal	28000	3,500	160000
u-24tb1.metal	28000	3,500	160000
x1.16xlarge	7,000	875	40000
x1.32xlarge	14,000	1,750	80,000
x1e.xlarge	500	62.5	3,700
x1e.2xlarge	1000	125	7,400
x1e.4xlarge	1,750	218.75	10000

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
x1e.8xlarge	3,500	437.5	20000
x1e.16xlarge	7,000	875	40000
x1e.32xlarge	14,000	1,750	80,000
z1d.large *	2,333	291	13,333
z1d.xlarge *	2,333	291	13,333
z1d.2xlarge	2,333	292	13,333
z1d.3xlarge	3,500	438	20000
z1d.6xlarge	7,000	875	40000
z1d.12xlarge	14,000	1,750	80,000
z1d.metal	14,000	1,750	80,000

* 这些实例类型可以至少每 24 小时一次支持 30 分钟的最大性能。如果您的工作负载需要超过 30 分钟的持续最大性能，请根据基准性能选择一个实例类型，如下表所示。

实例大小	基准带宽 (Mbps)	基准吞吐量 (MB/s , 128 KiB I/O)	基准 IOPS (16 KiB I/O)
a1.medium	300	37.5	2,500
a1.large	525	65.625	4000
a1.xlarge	800	100	6000
a1.2xlarge	1,750	218.75	10000
c5.large	650	81.25	4,000
c5.xlarge	1,150	143.75	6000
c5.2xlarge	2,300	287.5	10000
c5d.large	650	81.25	4,000
c5d.xlarge	1,150	143.75	6000
c5d.2xlarge	2,300	287.5	10000
c5n.large	650	81.25	4,000
c5n.xlarge	1,150	143.75	6000
c5n.2xlarge	2,300	287.5	10000
i3en.large	425	53.125	3000
i3en.xlarge	850	106.25	6000
i3en.2xlarge	1,700	212.5	12000

实例大小	基准带宽 (Mbps)	基准吞吐量 (MB/s , 128 KiB I/O)	基准 IOPS (16 KiB I/O)
i3en.3xlarge	2,800	350	15000
m5.large	650	81.25	3600
m5.xlarge	1,150	143.75	6000
m5.2xlarge	2,300	287.5	12000
m5a.large	480	60	3600
m5a.xlarge	800	100	6000
m5a.2xlarge	1,166	146	8,333
m5ad.large	480	60	3600
m5ad.xlarge	800	100	6000
m5ad.2xlarge	1,166	146	8,333
m5d.large	650	81.25	3600
m5d.xlarge	1,150	143.75	6000
m5d.2xlarge	2,300	287.5	12000
m5dn.large	650	81.25	3600
m5dn.xlarge	1,150	143.75	6000
m5dn.2xlarge	2,300	287.5	12000
m5n.large	650	81.25	3600
m5n.xlarge	1,150	143.75	6000
m5n.2xlarge	2,300	287.5	12000
r5.large	650	81.25	3600
r5.xlarge	1,150	143.75	6000
r5.2xlarge	2,300	287.5	12000
r5a.large	480	60	3600
r5a.xlarge	800	100	6000
r5a.2xlarge	1,166	146	8,333
r5ad.large	480	60	3600
r5ad.xlarge	800	100	6000
r5ad.2xlarge	1,166	146	8,333
r5d.large	650	81.25	3600
r5d.xlarge	1,150	143.75	6000

实例大小	基准带宽 (Mbps)	基准吞吐量 (MB/s , 128 KiB I/O)	基准 IOPS (16 KiB I/O)
r5d.2xlarge	2,300	287.5	12000
r5dn.large	650	81.25	3600
r5dn.xlarge	1,150	143.75	6000
r5dn.2xlarge	2,300	287.5	12000
r5n.large	650	81.25	3600
r5n.xlarge	1,150	143.75	6000
r5n.2xlarge	2,300	287.5	12000
t3.nano	32	4	250
t3.micro	64	8	500
t3.small	128	16	1000
t3.medium	256	32	2000
t3.large	512	64	4000
t3.xlarge	512	64	4000
t3.2xlarge	512	64	4000
t3a.nano	32	4	250
t3a.micro	64	8	500
t3a.small	128	16	1000
t3a.medium	256	32	2000
t3a.large	512	64	4000
t3a.xlarge	512	64	4000
t3a.2xlarge	512	64	4000
z1d.large	583	73	3,333
z1d.xlarge	1,167	146	6,667

EBSIOBalance% 和 EBSByteBalance% 指标可以帮助您确定是否正确调整了实例大小。您可以在 CloudWatch 控制台中查看这些指标，并设置将根据您指定的阈值触发的警报。这些指标以百分比形式表示。具有持续低余额百分比的实例是上调大小的候选对象。余额百分比从未低于 100% 的实例是下调大小的候选对象。有关更多信息，请参阅[使用 CloudWatch 监控您的实例 \(p. 538\)](#)。

支持的 EBS 优化

下表列出了支持 EBS 优化的实例类型，但默认情况下不启用 EBS 优化。您可以在启动这些实例时或在它们运行后启用 EBS 优化。实例必须启用了 EBS 优化才能实现所述的性能级别。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[按需实例的 Amazon EC2 定价页面](#)上的 EBS 优化实例。

实例大小	最大带宽 (Mbps)	最大吞吐量 (MB/s , 128 KiB I/O)	最大 IOPS (16 KiB I/O)
c1.xlarge	1000	125	8000
c3.xlarge	500	62.5	4000
c3.2xlarge	1000	125	8000
c3.4xlarge	2000	250	16000
g2.2xlarge	1000	125	8000
i2.xlarge	500	62.5	4000
i2.2xlarge	1000	125	8000
i2.4xlarge	2000	250	16000
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
r3.xlarge	500	62.5	4000
r3.2xlarge	1000	125	8000
r3.4xlarge	2000	250	16000

i2.8xlarge、c3.8xlarge 和 r3.8xlarge 实例没有专用 EBS 带宽，因此不提供 EBS 优化。在这些实例上，网络流量和 Amazon EBS 流量将共用同一 10 Gb 网络接口。

在启动时启用 EBS 优化

您可以通过针对 EBS 优化设置某个实例的属性来为该实例启用优化。

使用控制台在启动实例时启用 Amazon EBS 优化

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance。
3. 在步骤 1：选择 Amazon 系统映像 (AMI) 中，选择 AMI。
4. 在步骤 2：选择实例类型 中，选择作为支持性 Amazon EBS 优化列出的实例类型。
5. 在 Step 3: Configure Instance Details 中，填写所需的字段并选择 Launch as EBS-optimized instance。如果您在上一步中选择的实例类型不支持 Amazon EBS 优化，则该选项将不存在。如果您选择的实例类型在默认情况下会进行 Amazon EBS 优化，则会选择此选项，并且无法取消选择。
6. 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)
- 带 [New-EC2Instance](#) 的 `-EbsOptimized` (适用于 Windows PowerShell 的 AWS 工具)

为正在运行的实例启用 EBS 优化

您可以修改正在运行的实例的 Amazon EBS 优化实例属性，以便为该实例启用或禁用优化。

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。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

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，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是经过 Amazon EBS 优化的实例类型，则将选择 EBS 优化，并且您无法更改它。您可以选择取消，因为已为该实例启用 Amazon EBS 优化。
 - 如果您的实例的实例类型支持 Amazon EBS 优化，请选择 EBS 优化、应用。
 - 如果您的实例的实例类型不支持 Amazon EBS 优化，则您无法选择 EBS 优化。您可以从实例类型中选择一个支持 Amazon EBS 优化的实例类型，然后选择 EBS 优化、应用。
7. 依次选择 Actions、Instance State、Start。

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)

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。

Note

EBS 卷类型性能的 AWS 更新可能不会立即在您的现有卷上生效。要查看较早卷上的全部性能，您需要先在其上执行 `ModifyVolume` 操作。有关更多信息，请参阅[在 Linux 上修改 EBS 卷的大小、IOPS 或类型](#)。

目录

- [Amazon EBS 性能提示 \(p. 876\)](#)
- [I/O 特征和监控 \(p. 878\)](#)
- [初始化 Amazon EBS 卷 \(p. 879\)](#)
- [Linux 上的 RAID 配置 \(p. 881\)](#)
- [对 EBS 卷进行基准测试 \(p. 884\)](#)

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、C5 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 EBS 优化的实例 \(p. 863\)](#)。

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 特征和监控 \(p. 878\)](#)。

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 \(p. 884\)](#)。

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。您可以使用以下其中一个选项来避免这一性能下降：

- 在将卷部署到生产环境之前访问每个块。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 \(p. 879\)](#)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅[Amazon EBS 快速快照还原 \(p. 859\)](#)。

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 卷吞吐量的更多信息，请参阅[Amazon EBS 卷类型 \(p. 785\)](#)。

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）。有关确保稳定的卷性能的更多信息，请参阅 [I/O 特征和监控 \(p. 878\)](#)。

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。

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 3.8 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 特征和监控 \(p. 878\)](#)。

要在 st1 或 sc1 卷上实现最大吞吐量，建议您将值 256 应用于 xen_blkfront.max 参数（对于低于 4.6 的 Linux 内核版本）或 xen_blkfront.max_indirect_segments 参数（对于 Linux 内核版本 4.6 及更高版本）。可在操作系统 boot 命令行中设置相应的参数。

例如，在具有较早内核的 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
```

对于更高版本的内核，该命令将类似于以下内容：

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
xen_blkfront.max_indirect_segments=256
```

重启实例，让此设置生效。

有关更多信息，请参阅 [配置 GRUB \(p. 155\)](#)。对于其他 Linux 发行版（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内核参数。

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 \(p. 881\)](#)。

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 \(p. 804\)](#)。

I/O 特征和监控

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。这些操作以 KiB 进行度量，而底层驱动器技术决定了卷类型将作为单个 I/O 计数的最大数据量。由于 SSD 卷处理小型或随机 I/O 比 HDD 卷更有效，因此 SSD 卷的 I/O 大小上限为 256 KiB，而 HDD 卷的 I/O 大小上限为 1,024 KiB。

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 操作，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 ($1024 \div 256 = 4$)，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，您就可以将它附加到一个 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，对于具有可用突增积分的 1000 GiB 以下的 gp2 卷，IOPS 限制为 3000，卷吞吐量限制为 250 MiB/s。

如果您正在使用 256 KiB 的 I/O 大小，则您的卷在 IOPS 为 1000 时将达到其吞吐量限制 ($1000 \times 256 \text{ KiB} = 250 \text{ MiB}$)。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 250 MiB/s。（这些示例都假设卷的 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 \(p. 785\)](#)。

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。

如果您的工作负载在 HDD 支持的 st1 和 sc1 卷上使用顺序 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 EBS 优化的实例 \(p. 863\)](#)。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 \(p. 804\)](#) 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 和 sc1 卷的突增存储桶余额。当您的突增存储桶耗尽时，卷 I/O（对于 gp2 卷）或卷吞吐量（对于 st1 和 sc1 卷）会限定在基准水平。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 卷经过特别设计，旨在对使用 1024 KiB 最大 I/O 大小的工作负载提供最佳性能。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）。

对于从快照还原的卷，必须先从 Amazon S3 下载存储块并将其写入到卷中，然后才能访问这些块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。

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 (I/O 性能) 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 [EBS 卷状态检查 \(p. 804\)](#)。

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。为了避免最初在生产环境中出现这种性能下降，您可以使用以下其中一种方案：

- 强制立即初始化整个卷。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 879\)](#)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅 [Amazon EBS 快速快照还原 \(p. 859\)](#)。

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. 将新还原的卷附加到您的 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 已附加，但是未挂载（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，因为它允很多线程读取。

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。

[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。

Important

不当使用 dd 可能容易损坏卷的数据。请务必严格遵循下面的示例命令。只有 if=/dev/**xvdf** 参数将因您要读取的设备的名称而异。

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] 如果您在系统上安装了 fio，请使用以下命令初始化您的卷。应将 --filename（输入文件）参数设置为要初始化的驱动器。

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=128k --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

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
```

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 卷可在 Linux 上使用 \(p. 801\)](#)。

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](#)。

目录

- [RAID 配置选项 \(p. 881\)](#)
- [在 Linux 上创建 RAID 阵列 \(p. 882\)](#)
- [创建 RAID 阵列中卷的快照 \(p. 884\)](#)

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和 IOPS。	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 4,000 的两个 500 GiB Amazon EBS io1 卷将创建可用带宽为 8,000 IOPS、吞吐量为 1,000 MiB/s 的 1000 GiB RAID 0 阵列，或创建可用带宽为 4,000 IOPS、吞吐量为 500 MiB/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 \(p. 798\)](#)。

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 EBS 优化的实例 \(p. 863\)](#)。

2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅[将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。
3. 使用 mdadm 命令从新附加的 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，--level=0 选项用于将阵列条带化）：

```
[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，--level=1 选项用于将阵列镜像化）：

```
[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
```

下面是示例输出：

```
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
```

下面是示例输出：

```
/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  
...  

```

- 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装载该文件系统时使用的标签。例如，要使用标签 **MY_RAID** 创建 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，您可以使用其他文件系统类型，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)。

- 要确保 RAID 阵列在启动时自动重组，请创建一个包含 RAID 信息的配置文件：

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

Note

如果您使用的是 Linux 发行版而不是 Amazon Linux，此文件可能需要被放在不同的位置。有关更多信息，请参阅您的 Linux 系统上的 man mdadm.conf。

- 创建新的 Ramdisk Image 以为新的 RAID 配置正确地预加载块储存设备模块：

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

- 为 RAID 阵列创建装载点。

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

- 最后，在已创建的装载点上安装 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。

- (可选)要在每次系统重启时装载此 Amazon 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. 使用您常用的文本编辑器（如 nano 或 vim）打开 `/etc/fstab` 文件。
c. 注释掉任何以“`UUID=`”开头的行，然后，在文件末尾，使用以下格式为您的 RAID 卷添加新行：

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

此行的最后三个字段分别是文件系统装载选项、文件系统转储频率和启动时的文件系统检查顺序。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` 手册页面（通过在命令行上输入 `man fstab`）。例如，要在设备上的装载点 `/mnt/raid` 装载带 `MY_RAID` 标签的 `ext4` 文件系统，请将以下条目添加到 `/etc/fstab`。

Note

如果您要在未附加该卷的情况下启动实例（例如，以便该卷可以在不同实例之间向后和向前移动），则应添加 `nofail` 装载选项，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` 装载选项。

LABEL=MY_RAID	/mnt/raid	ext4	defaults, nofail	0	2
---------------	-----------	------	------------------	---	---

- d. 在您将新条目添加到 `/etc/fstab` 后，需要检查您的条目是否有效。运行 `sudo mount -a` 命令以在 `/etc/fstab` 中装载所有文件系统。

```
[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装载。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` 文件中的错误可能显示系统无法启动。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
```

创建 RAID 阵列中卷的快照

如果要使用快照备份 RAID 阵列中 EBS 卷上的数据，则必须确保快照的一致性。原因在于这些卷的快照是独立创建的。从不同步的快照恢复 RAID 阵列中的 EBS 卷会降低阵列的完整性。

要为 RAID 阵列创建一组一致的快照，请使用 [EBS 多卷快照](#)。利用多卷快照，您可以跨附加到 EC2 实例的多个 EBS 卷拍摄时间点、数据协调和崩溃一致性快照。您不需要停止实例以在多个卷之间协调来确保一致性，因为快照将跨多个 EBS 卷自动拍摄。有关更多信息，请参阅[创建 Amazon EBS 快照](#)下有关创建多卷快照的步骤。

对 EBS 卷进行基准测试

您可以通过模拟 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. 将这些卷附加到您的 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

某些过程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 优化的实例在 Amazon EC2 与 Amazon EBS 之间提供了专用带宽，其规格取决于实例类型。有关更多信息，请参阅 [Amazon EBS 优化的实例 \(p. 863\)](#)。

要创建 EBS 优化实例，可在使用 Amazon EC2 控制台启动实例时选择作为 EBS 优化的实例启动，或在使用命令行时指定 `--ebs-optimized`。请确保您启动的实例是支持该选项的最新一代实例。有关更多信息，请参阅 [Amazon EBS 优化的实例 \(p. 863\)](#)。

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 64,000 之间的整数。有关 EBS 卷规格的详细信息，请参阅 [Amazon EBS 卷类型 \(p. 785\)](#)。有关创建 EBS 卷的信息，请参阅 [创建 Amazon EBS 卷 \(p. 798\)](#)。有关将这些卷附加到实例的信息，请参阅 [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。

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、挂载 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 \(p. 798\)](#)。有关将这些卷附加到您的实例的信息，请参阅[将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。

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](#)并将其另存为 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，然后将该卷附加到 `/dev/xvdf` 处的实例。

使用模板创建 HDD 卷

1. 从 <https://console.aws.amazon.com/cloudformation> 打开 AWS CloudFormation 控制台。
2. 选择创建堆栈。
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，选择输出以获得新实例的公有 DNS 条目，新实例将附加一个 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 \(p. 886\)](#)。

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	描述
fio	<p>用于测试 I/O 性能。（请注意，fio 依赖于 libaio-devel。）</p> <p>要在 Amazon Linux 上安装 fio，请运行以下命令：</p> <div style="border: 1px solid black; padding: 5px;"><pre>[ec2-user ~]\$ sudo yum install -y fio</pre></div> <p>要在 Ubuntu 上安装 fio，请执行以下命令：</p> <div style="border: 1px solid black; padding: 5px;"><pre>sudo apt-get install -y fio</pre></div>
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 1000 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 3,000 IOPS 的卷应该将队列长度设置为 3。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。

禁用 C 状态

在运行基准测试之前，您应禁用处理器 C 状态。支持此功能的 CPU 中的核心在暂时空闲时，会进入 C 状态以节省功耗。在调用核心以恢复处理时，将经过一段特定的时间，核心才能再次全速运行。此延迟可能会干扰处理器基准测试例程。有关 C 状态以及哪些 EC2 实例类型支持此状态的更多信息，请参阅 [EC2 实例的处理器状态控制](#)。

在 Linux 系统上禁用 C 状态

您可在 Amazon Linux、RHEL 和 CentOS 上按以下所示禁用 C 状态：

1. 获取 C 状态数。

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. 从 c1 到 cN 禁用 C 状态。理想情况下，核心应处于状态 c0。

```
$ for i in `seq 1 $((N-1))` ; do cpupower idle-set -d $i; done
```

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。

对附加了 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 \(p. 879\)](#)。

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 \(p. 812\)](#)和[终止您的实例 \(p. 458\)](#)。

对 io1 卷进行基准测试

在您创建的条带集上运行 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 \(p. 877\)](#)所述在实例上设置缓冲 I/O。

以下命令针对附加的 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
```

以下命令针对附加的 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 指标

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	描述
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 (<code>io1</code>) 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。只有在卷附加到实例时，才会向 CloudWatch 报告数据。

其中一些指标在基于 Nitro 的实例上会有所不同。有关基于 Nitro 系统的实例类型列表，请参阅[基于 Nitro 的实例 \(p. 163\)](#)。

AWS/EBS 命名空间包括以下指标。

Metrics

- [卷指标 \(p. 889\)](#)
- [快速快照还原指标 \(p. 892\)](#)

卷指标

指标	说明
<code>VolumeReadBytes</code>	提供有关指定时间段内的读取操作的信息。Sum 统计数据将报告该时间段内传输的总字节数。Average 统计数据报告该时间段内的每个读取操作的平均大小，附加到基于 Nitro 的实例的卷除外，其中的平均值表示指定时间段的平均值。SampleCount 统计数据报告该时间段内的读取操作总数，但附加到基于 Nitro 的实例的卷除外，其中的样本数表示在统计计算中使用的数据点数。对于 Xen 实例，只有在卷上有读取活动时才报告数据。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。

指标	说明
	单位 : 字节
VolumeWriteBytes	<p>提供有关指定时间段内的写入操作的信息。Sum 统计数据将报告该时间段内传输的总字节数。Average 统计数据报告该时间段内的每个写入操作的平均大小，附加到基于 Nitro 的实例的卷除外，其中的平均值表示指定时间段的平均值。SampleCount 统计数据报告该时间段内的写入操作总数，但附加到基于 Nitro 的实例的卷除外，其中的样本数表示在统计计算中使用的数据点数。对于 Xen 实例，只有在卷上有写入活动时才报告数据。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</p> <p>单位 : 字节</p>
VolumeReadOps	<p>在指定时间的读取操作总数。</p> <p>要计算该时间段的平均每秒读取操作数 (读取 IOPS)，请将该时间段的总读取操作数除以秒数。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</p> <p>单位 : 计数</p>
VolumeWriteOps	<p>在指定时间的写入操作总数。</p> <p>要计算该时间段的平均每秒写入操作数 (写入 IOPS)，请将该时间段的总写入操作数除以秒数。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</p> <p>单位 : 计数</p>
VolumeTotalReadTime	<p>指定时间段中所有读取操作耗费的总秒数。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。对于 Xen 实例，只有在卷上有读取活动时才报告数据。</p> <p>该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</p> <p>单位 : 秒</p>

指标	说明
VolumeTotalWriteTime	<p>指定时间段中所有写入操作耗时的总秒数。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。对于 Xen 实例，只有在卷上有写入活动时才报告数据。</p> <p>该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</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>该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</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>该指标的 Sum 统计数据与附加到基于 Nitro 的实例的卷无关。</p> <p>仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。</p> <p>单位：计数</p>
VolumeThroughputPercentage	<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 10% 以内的预置 IOPS 性能。</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 性能可能由于已执行的操作而暂时下降 (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，或者首次访问卷上的数据)。</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>

指标	说明
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 积分百分比 (对于 gp2) 或吞吐量积分 (对于 st1 和 sc1) 的信息。仅当卷处于活动状态时将数据报告给 CloudWatch。如果未附加卷，则不会报告任何数据。</p> <p>该指标的 Sum 统计数据与附加到基于 Nitro 的实例的卷无关。</p> <p>如果卷的基准性能超过了最大突发性能，则绝不会使用积分。报告的突发余额为 0% (基于 Nitro 的实例) 或 100% (非基于 Nitro 的实例)。有关更多信息，请参阅 I/O 积分和突增性能 (p. 787)。</p> <p>单位：百分比</p>

快速快照还原指标

指标	说明
FastSnapshotRestoreCreditsBucket	<p>可以累积的最大卷创建积分数。将为每个可用区的每个快照报告该指标。</p> <p>最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。</p>
FastSnapshotRestoreCreditsAvailable	<p>可用的卷创建积分数。将为每个可用区的每个快照报告该指标。</p> <p>最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。</p>

Amazon EBS 指标的维度

支持的维度是卷 ID (volumeId)。所有可用的统计数据都是按卷 ID 筛选的。

对于 [卷指标 \(p. 889\)](#)，支持的维度是卷 ID (volumeId)。所有可用的统计数据都是按卷 ID 筛选的。

对于 [快速快照还原指标 \(p. 892\)](#)，支持的维度是快照 ID (SnapshotId) 和可用区 (AvailabilityZone)。

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)	$\text{Sum}(\text{VolumeReadBytes}) / \text{Period} / 1024$
写入带宽 (KiB/s)	$\text{Sum}(\text{VolumeWriteBytes}) / \text{Period} / 1024$
读取吞吐量 (IOPS)	$\text{Sum}(\text{VolumeReadOps}) / \text{Period}$
写入吞吐量 (IOPS)	$\text{Sum}(\text{VolumeWriteOps}) / \text{Period}$

图表	使用原始指标描述
平均队列长度 (操作数)	Avg(VolumeQueueLength)
空闲花费时间百分比	Sum(VolumeIdleTime) / Period × 100
平均读取大小 (KiB/操作)	<p>Avg(VolumeReadBytes) / 1024</p> <p>对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均读取大小：</p> $(\text{Sum}(\text{VolumeReadBytes}) / \text{Sum}(\text{VolumeReadOps})) / 1024$ <p>在 EBS CloudWatch 控制台中提供了 VolumeReadBytes 和 VolumeReadOps 指标。</p>
平均写入大小 (KiB/操作)	<p>Avg(VolumeWriteBytes) / 1024</p> <p>对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均写入大小：</p> $(\text{Sum}(\text{VolumeWriteBytes}) / \text{Sum}(\text{VolumeWriteOps})) / 1024$ <p>在 EBS CloudWatch 控制台中提供了 VolumeWriteBytes 和 VolumeWriteOps 指标。</p>
平均读取延迟 (毫秒/操作)	<p>Avg(VolumeTotalReadTime) × 1000</p> <p>对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均读取延迟：</p> $(\text{Sum}(\text{VolumeTotalReadTime}) / \text{Sum}(\text{VolumeReadOps})) \times 1000$ <p>在 EBS CloudWatch 控制台中提供了 VolumeTotalReadTime 和 VolumeReadOps 指标。</p>
平均写入延迟 (毫秒/操作)	<p>Avg(VolumeTotalWriteTime) × 1000</p> <p>对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均写入延迟：</p> $(\text{Sum}(\text{VolumeTotalWriteTime}) / \text{Sum}(\text{VolumeWriteOps})) * 1000$ <p>在 EBS CloudWatch 控制台中提供了 VolumeTotalWriteTime 和 VolumeWriteOps 指标。</p>

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。

Amazon EBS 的 Amazon CloudWatch Events

Amazon EBS 根据 Amazon CloudWatch Events 发送通知，以告知一系列卷、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，从而响应卷、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。

CloudWatch 中的事件表示为 JSON 对象。该事件独有的字段包含在 JSON 对象的“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。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南 中的 [CloudWatch Events 中的事件模式](#)。

有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [使用事件](#)。

目录

- [EBS 卷事件 \(p. 894\)](#)
- [EBS 快照事件 \(p. 897\)](#)
- [EBS 卷修改事件 \(p. 900\)](#)
- [EBS 快速快照还原事件 \(p. 901\)](#)
- [使用 Amazon Lambda 处理 CloudWatch Events \(p. 902\)](#)

EBS 卷事件

在发生以下卷事件时，Amazon EBS 会向 CloudWatch Events 发送事件。

事件

- [创建卷 \(createVolume\) \(p. 894\)](#)
- [删除卷 \(deleteVolume\) \(p. 895\)](#)
- [卷附加或重新附加 \(attachVolume , reattachVolume\) \(p. 896\)](#)

创建卷 (createVolume)

当创建卷的操作完成后，系统会将 `createVolume` 事件发送至您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 `available` 或 `failed`。如果提供的 KMS 密钥无效，创建操作将失败，如以下示例所示。

事件数据

下面的列表是 EBS 为成功的 `createVolume` 事件发送的 JSON 对象示例。

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "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-1:012345678901:volume/vol-01234567"  
    ],  
    "detail": {  
        "result": "available",  
        "cause": "",  
        "event": "createVolume",  
        "request-id": "01234567-0123-0123-0123-0123456789ab"  
    }  
}
```

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",
    }
}
```

删除卷 (`deleteVolume`)

当删除卷的操作完成后，系统会将 `deleteVolume` 事件发送至您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件具有 `deleted` 结果。如果删除操作未完成，绝不会发送此事件。

事件数据

下面的列表是 EBS 为成功的 `deleteVolume` 事件发送的 JSON 对象示例。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "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-1:012345678901:volume/vol-01234567"
    ],
    "detail": {
```

```
        "result": "deleted",
        "cause": "",
        "event": "deleteVolume",
        "request-id": "01234567-0123-0123-0123-0123456789ab"
    }
}
```

卷附加或重新附加 (attachVolume , reattachVolume)

如果卷无法附加或重新附加到实例，系统会将 attachVolume 或 reattachVolume 事件发送至您的 AWS 账户。不过，不会保存、记录或存档该事件。如果您使用 KMS 密钥加密 EBS 卷并且该密钥变为无效，则日后使用该密钥将卷附加或重新附加到实例时，EBS 会发送一个事件，如以下示例所示。

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 可能会尝试重新附加卷。

```
{
    "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": ""  
}  
}
```

EBS 快照事件

在发生以下卷事件时，Amazon EBS 会向 CloudWatch Events 发送事件。

事件

- [创建快照 \(createSnapshot\) \(p. 897\)](#)
- [创建快照 \(createSnapshots\) \(p. 897\)](#)
- [复制快照 \(copySnapshot\) \(p. 899\)](#)
- [共享快照 \(shareSnapshot\) \(p. 900\)](#)

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。不过，不会保存、记录或存档该事件。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。在 `detail` 部分，`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"    }  
}
```

创建快照 (createSnapshots)

当创建多卷快照的操作完成后，系统会将 `createSnapshots` 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 `createSnapshots` 事件发送的 JSON 对象的示例。在 `detail` 部分中，`source` 字段包含多卷快照集的源卷的 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 Multi-Volume Snapshots Completion Status",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
        "arn:aws:ec2::us-east-1:snapshot/snap-012345678"  
    ],  
    "detail": {  
        "event": "createSnapshots",  
        "result": "succeeded",  
        "cause": "",  
        "request-id": "",  
        "startTime": "yyyy-mm-ddThh:mm:ssZ",  
        "endTime": "yyyy-mm-ddThh:mm:ssZ",  
        "snapshots": [  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",  
                "status": "completed"  
            },  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",  
                "status": "completed"  
            }  
        ]  
    }  
}
```

下面的列表是 EBS 在 createSnapshots 事件失败后发送的 JSON 对象的示例。失败的原因是一个或多个快照未能完成。snapshot_id 的值是失败的快照的 ARN。StartTime 和EndTime 表示创建快照操作开始和结束的时间。

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Multi-Volume Snapshots Completion Status",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
        "arn:aws:ec2::us-east-1:snapshot/snap-012345678"  
    ],  
    "detail": {  
        "event": "createSnapshots",  
        "result": "failed",  
        "cause": "Snapshot snap-01234567 is in status deleted",  
        "request-id": "",  
        "startTime": "yyyy-mm-ddThh:mm:ssZ",  
        "endTime": "yyyy-mm-ddThh:mm:ssZ",  
        "snapshots": [  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",  
                "status": "error"  
            },  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",  
                "status": "error"  
            }  
        ]  
    }  
}
```

```
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "deleted"
    }
]
}
```

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。不过，不会保存、记录或存档该事件。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 事件成功后发送的 JSON 对象的示例。snapshot_id 的值为新创建快照的 ARN。在 detail 部分中，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": "succeeded",
    "cause": "",
    "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",
    "Incremental": "True"
  }
}
```

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。在 detail 部分中，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 invalid."
  }
}
```

```
"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。不过，不会保存、记录或存档该事件。结果始终是 succeeded。

事件数据

下面是 EBS 在 shareSnapshot 事件完成后发送的 JSON 对象的示例。在 detail 部分中，source 的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",
    "source": "012345678901",
    "StartTime": "yyyy-mm-ddThh:mm:ssZ",
    "EndTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

EBS 卷修改事件

当修改卷时，Amazon EBS 会向 CloudWatch Events 发送 modifyVolume 事件。不过，不会保存、记录或存档该事件。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "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-1:012345678901:volume/vol-03a55cf56513fa1b6"
  ],
}
```

```
"detail": {  
    "result": "optimizing",  
    "cause": "",  
    "event": "modifyVolume",  
    "request-id": "01234567-0123-0123-0123-0123456789ab"  
}  
}
```

EBS 快速快照还原事件

在快照的快速快照还原状态发生变化时，Amazon EBS 向 CloudWatch Events 发送事件。

以下是此事件的示例数据。

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Fast Snapshot Restore State-change Notification",  
    "source": "aws.ec2",  
    "account": "123456789012",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"  
    ],  
    "detail": {  
        "snapshot-id": "snap-1234567890abcdef0",  
        "state": "optimizing",  
        "zone": "us-east-1a",  
        "message": "Client.UserInitiated - Lifecycle state transition",  
    }  
}
```

可能的 state 值为 enabling、optimizing、enabled、disabling 和 disabled。

可能的 message 值如下所示：

`Client.InvalidSnapshot.InvalidState` – The requested snapshot transitioned to an invalid state (Error)

启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。无法为该快照启用快速快照还原。

`Client.UserInitiated`

状态成功转换为 enabling 或 disabling。

`Client.UserInitiated - Lifecycle state transition`

状态成功转换为 optimizing、enabled 或 disabled。

`Server.InsufficientCapacity` – There was insufficient capacity available to satisfy the request

由于容量不足而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Server.InternalError` – An internal error caused the operation to fail

由于内部错误而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

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。

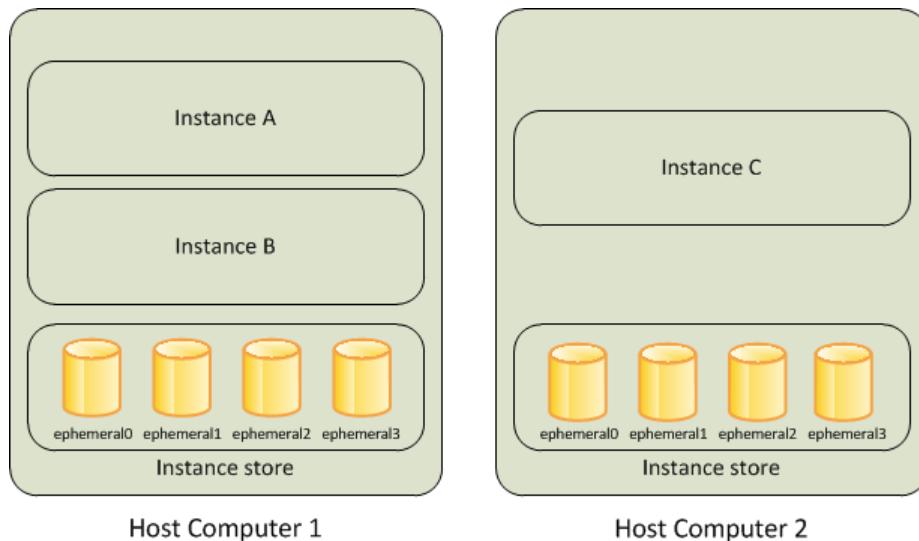
现在，您的规则应该会显示在规则选项卡中。在所示的示例中，当您下次复制快照时，EBS 应该会发送您所配置的事件。

Amazon EC2 实例存储

实例存储为您的实例提供临时性块级存储。此存储位于已物理附加到主机的磁盘上。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。

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。



目录

- [实例存储生命周期 \(p. 904\)](#)
- [实例存储卷 \(p. 904\)](#)
- [将实例存储卷添加到您的 EC2 实例 \(p. 909\)](#)
- [SSD 实例存储卷 \(p. 912\)](#)
- [实例存储交换卷 \(p. 913\)](#)
- [优化实例存储卷的磁盘性能 \(p. 915\)](#)

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附加到另一个实例。

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 , 在以下任一情况下 , 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。

如果更改实例类型 , 实例存储不会附加到新实例类型。有关更多信息 , 请参阅[更改实例类型 \(p. 233\)](#)。

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使用成本中。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)。

之后设置实例存储卷的格式并挂载这些卷，然后再使用这些卷。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 \(p. 909\)](#)。

某些实例类型使用基于 NVMe 或 SATA 的固态硬盘 (SSD) 来提供高随机 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 \(p. 912\)](#)。

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 (1.6 TB)	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	✓	
c3.4xlarge	2 x 160 GB (320 GB)	SSD	✓	
c3.8xlarge	2 x 320 GB (640 GB)	SSD	✓	
c5d.large	1 x 50GB	NVMe SSD		✓
c5d.xlarge	1 x 100GB	NVMe SSD		✓
c5d.2xlarge	1 x 200GB	NVMe SSD		✓
c5d.4xlarge	1 x 400GB	NVMe SSD		✓
c5d.9xlarge	1 x 900GB	NVMe SSD		✓
c5d.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
c5d.18xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
c5d.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
c5d.metal	4 x 900 GB (3.6 TB)	NVMe SSD		✓
cc2.8xlarge	4 x 840 GB (3.36 TB)	HDD	✓	
cr1.8xlarge	2 x 120 GB (240 GB)	SSD	✓	
d2.xlarge	3 x 2,000 GB (6 TB)	HDD		
d2.2xlarge	6 x 2,000 GB (12 TB)	HDD		
d2.4xlarge	12 x 2,000 GB (24 TB)	HDD		
d2.8xlarge	24 x 2,000 GB (48 TB)	HDD		
f1.2xlarge	1 x 470GB	NVMe SSD		✓
f1.4xlarge	1 x 940 GB	NVMe SSD		✓
f1.16xlarge	4 x 940 GB (3.76 TB)	NVMe SSD		✓
g2.2xlarge	1 x 60 GB	SSD	✓	

实例类型	实例存储卷	类型	需要初始化 *	TRIM Support**
g2.8xlarge	2 x 120 GB (240 GB)	SSD	✓	
g4dn.xlarge	1 x 125 GB	NVMe SSD		✓
g4dn.2xlarge	1 x 225 GB	NVMe SSD		✓
g4dn.4xlarge	1 x 225 GB	NVMe SSD		✓
g4dn.8xlarge	1 x 900GB	NVMe SSD		✓
g4dn.12xlarge	1 x 900GB	NVMe SSD		✓
g4dn.16xlarge	1 x 900GB	NVMe SSD		✓
h1.2xlarge	1 x 2000 GB (2 TB)	HDD		
h1.4xlarge	2 x 2000 GB (4 TB)	HDD		
h1.8xlarge	4 x 2000 GB (8 TB)	HDD		
h1.16xlarge	8 x 2000 GB (16 TB)	HDD		
hs1.8xlarge	24 x 2,000 GB (48 TB)	HDD	✓	
i2.xlarge	1 x 800 GB	SSD		✓
i2.2xlarge	2 x 800 GB (1.6 TB)	SSD		✓
i2.4xlarge	4 x 800 GB (3.2 TB)	SSD		✓
i2.8xlarge	8 x 800 GB (6.4 TB)	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		✓
i3.8xlarge	4 x 1,900 GB (7.6 TB)	NVMe SSD		✓
i3.16xlarge	8 x 1,900 GB (15.2 TB)	NVMe SSD		✓
i3.metal	8 x 1,900 GB (15.2 TB)	NVMe SSD		✓
i3en.large	1 x 1,250 GB	NVMe SSD		✓
i3en.xlarge	1 x 2,500 GB	NVMe SSD		✓
i3en.2xlarge	2 x 2,500 GB (5 TB)	NVMe SSD		✓
i3en.3xlarge	1 x 7,500 GB	NVMe SSD		✓
i3en.6xlarge	2 x 7,500 GB (15 TB)	NVMe SSD		✓
i3en.12xlarge	4 x 7,500 GB (30 TB)	NVMe SSD		✓
i3en.24xlarge	8 x 7,500 GB (60 TB)	NVMe SSD		✓
i3en.metal	8 x 7,500 GB (60 TB)	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化 *	TRIM Support**
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 (1.6 TB)	HDD	✓	
m2.xlarge	1 x 420 GB	HDD	✓	
m2.2xlarge	1 x 850 GB	HDD	✓	
m2.4xlarge	2 x 840 GB (1.68 TB)	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	✓	
m5ad.large	1 x 75GB	NVMe SSD		✓
m5ad.xlarge	1 x 150GB	NVMe SSD		✓
m5ad.2xlarge	1 x 300GB	NVMe SSD		✓
m5ad.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
m5ad.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
m5ad.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
m5d.large	1 x 75GB	NVMe SSD		✓
m5d.xlarge	1 x 150GB	NVMe SSD		✓
m5d.2xlarge	1 x 300GB	NVMe SSD		✓
m5d.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
m5d.8xlarge	2 x 600 GB (1.2 TB)	NVMe SSD		✓
m5d.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
m5d.16xlarge	4 x 600 GB (2.4 TB)	NVMe SSD		✓
m5d.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
m5d.metal	4 x 900 GB (3.6 TB)	NVMe SSD		✓
m5dn.large	1 x 75GB	NVMe SSD		✓
m5dn.xlarge	1 x 150GB	NVMe SSD		✓
m5dn.2xlarge	1 x 300GB	NVMe SSD		✓
m5dn.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
m5dn.8xlarge	2 x 600 GB (1.2 TB)	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化 *	TRIM Support**
m5dn.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
m5dn.16xlarge	4 x 600 GB (2.4 TB)	NVMe SSD		✓
m5dn.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
p3dn.24xlarge	2 x 900 GB (1.8 TB)	NVMe 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		✓
r5ad.large	1 x 75GB	NVMe SSD		✓
r5ad.xlarge	1 x 150GB	NVMe SSD		✓
r5ad.2xlarge	1 x 300GB	NVMe SSD		✓
r5ad.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
r5ad.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
r5ad.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
r5d.large	1 x 75GB	NVMe SSD		✓
r5d.xlarge	1 x 150GB	NVMe SSD		✓
r5d.2xlarge	1 x 300GB	NVMe SSD		✓
r5d.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
r5d.8xlarge	2 x 600 GB (1.2 TB)	NVMe SSD		✓
r5d.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
r5d.16xlarge	4 x 600 GB (2.4 TB)	NVMe SSD		✓
r5d.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
r5d.metal	4 x 900 GB (3.6 TB)	NVMe SSD		✓
r5dn.large	1 x 75GB	NVMe SSD		✓
r5dn.xlarge	1 x 150GB	NVMe SSD		✓
r5dn.2xlarge	1 x 300GB	NVMe SSD		✓
r5dn.4xlarge	2 x 300 GB (600 GB)	NVMe SSD		✓
r5dn.8xlarge	2 x 600 GB (1.2 TB)	NVMe SSD		✓
r5dn.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
r5dn.16xlarge	4 x 600 GB (2.4 TB)	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化 *	TRIM Support**
r5dn.24xlarge	4 x 900 GB (3.6 TB)	NVMe SSD		✓
x1.16xlarge	1 x 1,920 GB	SSD		
x1.32xlarge	2 x 1,920 GB (3.84 TB)	SSD		
x1e.xlarge	1 x 120GB	SSD		
x1e.2xlarge	1 x 240GB	SSD		
x1e.4xlarge	1 x 480GB	SSD		
x1e.8xlarge	1 x 960GB	SSD		
x1e.16xlarge	1 x 1,920 GB	SSD		
x1e.32xlarge	2 x 1,920 GB (3.84 TB)	SSD		
z1d.large	1 x 75GB	NVMe SSD		✓
z1d.xlarge	1 x 150GB	NVMe SSD		✓
z1d.2xlarge	1 x 300GB	NVMe SSD		✓
z1d.3xlarge	1 x 450GB	NVMe SSD		✓
z1d.6xlarge	1 x 900GB	NVMe SSD		✓
z1d.12xlarge	2 x 900 GB (1.8 TB)	NVMe SSD		✓
z1d.metal	2 x 900 GB (1.8 TB)	NVMe SSD		✓

* 如果附加到特定实例的卷没有初始化，将会进行初始写入。有关更多信息，请参阅[优化实例存储卷的磁盘性能 \(p. 915\)](#)。

** 有关更多信息，请参阅[实例存储卷 TRIM 支持 \(p. 913\)](#)。

† 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 \(p. 913\)](#)。

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。

某个实例类型支持的所有 NVMe 实例存储卷将在实例启动时自动枚举并为其分配设备名称；将这些卷包含在 AMI 或实例的块储存设备映射中不起作用。有关更多信息，请参阅[块储存设备映射 \(p. 923\)](#)。

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 \(p. 85\)](#)。将自动挂载根卷。对于根卷的具有实例存储卷的实例，该卷的大小因 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附加额外的 EBS 卷。有关更多信息，请参阅[Amazon EBS 卷 \(p. 783\)](#)。

您只能在启动实例时为其指定实例存储卷。无法在启动实例后将实例存储卷附加到该实例。

如果更改实例类型，实例存储不会附加到新实例类型。有关更多信息，请参阅[更改实例类型 \(p. 233\)](#)。

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。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他卷将被忽略。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 \(p. 904\)](#)。

如果为您的实例选择的实例类型支持非 NVMe 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。NVMe 实例存储卷在默认情况下是可用的。在启动实例后，您必须先确保已格式化和挂载实例的实例存储卷，然后才能使用这些存储卷。将自动挂载实例存储支持的实例的根卷。

目录

- [将实例存储卷添加到 AMI \(p. 910\)](#)
- [将实例存储卷添加到实例 \(p. 910\)](#)
- [使实例存储卷在您的实例上可用 \(p. 911\)](#)

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。如果使用支持实例存储卷的实例类型和在其块储存设备映射中指定实例存储卷的 AMI 启动一个实例，则该实例包括这些实例存储卷。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他实例存储卷将被忽略。

注意事项

- 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。
- 启动实例时，可忽略 AMI 块储存设备映射中指定的非 NVMe 实例存储卷，或添加实例存储卷。

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，为您的映像键入有意义的名称和描述。
5. 对于要添加的每个实例存储卷，选择 Add New Volume，从 Volume Type 中选择实例存储卷，并从 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 \(p. 922\)](#)。) 可用的实例存储卷数量取决于实例类型。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。您还可忽略 AMI 块储存设备映射中指定的设备。

注意事项

- 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。

- 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

- 打开 Amazon EC2 控制台。
- 在控制面板中，选择 Launch Instance。
- 在 Step 1: Choose an Amazon Machine Image (AMI) 中，选择要使用的 AMI，然后选择 Select。
- 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。
- 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，选择 Add New Volume，从 Volume Type 中选择实例存储卷，并从 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。
- 完成向导并启动实例。
- (可选) 要查看实例上可用的实例存储卷，请运行 `lsblk` 命令。

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)
- 带 `New-EC2Instance` 的 -BlockDeviceMapping (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，但是必须先挂载该卷，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挂载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。

很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 \(p. 913\)](#)。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 \(p. 930\)](#)。

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

- 使用 SSH 客户端连接到实例。
- 使用 `df -h` 命令查看已格式化并挂载的卷。使用 `lsblk` 查看在启动时已映射但未格式化和挂载的所有卷。
- 要格式化并挂载仅映射的实例存储卷，请执行以下操作：
 - 使用 `mkfs` 命令在设备上创建文件系统。
 - 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) 来提供高随机 I/O 性能的实例存储卷：C、G2、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 \(p. 904\)](#)。

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 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为其映射 SSD 实例存储卷。SSD 实例卷上的数据仅在其关联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 \(p. 909\)](#)。

NVMe SSD 卷

以下实例提供非易失性存储规范 (NVMe) SSD 实例存储卷：

C5d、I3、I3en、F1、M5ad、M5d、p3dn.24xlarge、R5ad、R5d 和 z1d。要访问 NVMe 卷，必须安装[NVMe 驱动程序 \(p. 861\)](#)。以下 AMI 满足此要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (具有 `linux-aws` 内核) 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

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 PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 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，请使用以下命令验证是否已加载 NVMe 模块。

- Amazon Linux、Amazon Linux 2、Ubuntu 14/16、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、CentOS 7

```
$ lsmod | grep nvme
nvme           48813   0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

NVMe 卷符合 NVMe 1.0e 规范。您可以对 NVMe 卷使用 NVMe 命令。利用 Amazon Linux，您可以使用 yum install 命令从存储库安装 nvme-cli 程序包。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）。

NVMe 实例存储上的数据是使用在实例上的硬件模块中实施的 XTS-AES-256 数据块密码加密的。加密密钥是使用硬件模块生成的，并且对每台 NVMe 实例存储设备都是唯一的。当实例停止或终止并且无法恢复时，将销毁所有加密密钥。无法禁用此加密，并且无法提供自己的加密密钥。

实例存储卷 TRIM 支持

以下实例支持带 TRIM 的 SSD 卷：

C5d、F1、I2、I3、I3en、M5ad、M5d、p3dn.24xlarge、R3、R5ad、R5d 和 z1d。

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，而后才能挂载和使用。为了更快地访问这些卷，您在格式化它们时应跳过 TRIM 操作。

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。在 Linux 上，使用 fstrim 命令启用定期 TRIM。

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。启用交换空间后，Linux 系统可以将很少使用的内存页面从物理内存交换至交换空间（现有文件系统中的专用分区或交换文件），并为需要高速访问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[更改实例类型 \(p. 233\)](#)。

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 AMIs 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 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附加并启用的 900 MiB 交换卷。如果您没有通过该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

您必须在 lsblk 列出的设备名称前加上 /dev/。设备的命名可以不同，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 ~]$ 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，以便在每次系统启动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 \(p. 904\)](#)。

1. 列出附加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 处格式化并挂载；并不是所有 Linux 操作系统都自动执行这一操作。

- 2.（可选）如果您挂载了实例存储卷（它将在 lsblk 命令输出中列出 MOUNTPOINT），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 swapspace version 1, size = 4188668 KiB
```

```
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

- 启用新的交换空间。

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

- 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
```

- 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. 914) 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. 914) 到 Step 5 (p. 915)。

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附加的固态硬盘 (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 \(p. 904\)](#)。

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，具体取决于要初始化的存储 (如 /dev/sdb 或 /dev/nvme1n1)。

Note

请确保先卸载硬盘，然后再执行该命令。

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
```

文件存储

云文件存储是一种在云中存储数据的方法，允许服务器和应用程序通过共享文件系统访问数据。这种兼容性使得云文件存储非常适合依赖共享文件系统的工作负载，并且实现了无需更改代码的简单集成。

存在许多文件存储解决方案，范围从使用块存储作为基础的计算实例上的单节点文件服务器（没有扩展性或一些冗余来保护数据），到自助集群解决方案再到完全托管的解决方案（如 [Amazon Elastic File System \(Amazon EFS\) \(p. 916\)](#) 或 [Amazon FSx for Windows File Server \(p. 919\)](#)）。

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装载文件系统。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 EC2 用户指南 (适用于 Linux 实例) 和 [Amazon Elastic File System \(Amazon EFS\)](#)。

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 \(p. 916\)](#)
- [步骤 1：创建 EFS 文件系统 \(p. 916\)](#)
- [步骤 2：装载文件系统 \(p. 917\)](#)
- [步骤 3：测试文件系统 \(p. 918\)](#)
- [步骤 4：清除 \(p. 918\)](#)

先决条件

- 创建安全组（例如 efs-sg）以便关联到 EC2 实例和 EFS 挂载目标，然后添加以下规则：
 - 允许从您计算机到 EC2 实例的入站 SSH 连接（源是您的网络的 CIDR 块）
 - 允许从与此安全组关联的 EC2 实例（源是安全组本身）通过 EFS 挂载目标向文件系统的入站 NFS 连接。有关更多信息，请参阅[Amazon EFS 规则 \(p. 778\)](#)以及Amazon Elastic File System 用户指南中的[Amazon EC2 实例和装载目标的安全组](#)。
- 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 \(p. 19\)](#)。

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装载并访问的文件系统。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 \(p. 916\)](#)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：装载文件系统

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装载到两个实例并且在实例重启之后更新 /etc/fstab 以确保重新装载文件系统。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

还有其他装载卷的方式 (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[装载文件系统](#)。

启动两个实例并装载 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 (选择一个 Amazon 系统映像) 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 (子网) 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 (高级详细信息) 下选择 As text (以文本形式)，然后将以下脚本粘贴到 User data (用户数据) 中。使用您文件系统的 ID 更新 FILE_SYSTEM_ID。您可以选择用您装载的文件系统的一个目录更新 MOUNT_POINT。

```
#!/bin/bash
yum update -y
yum install -y nfs-utils
```

```
FILE_SYSTEM_ID=fs-xxxxxxx
AVAILABILITY_ZONE=$(curl -s http://169.254.169.254/latest/meta-data/placement/
availability-zone)
REGION=${AVAILABILITY_ZONE:0:-1}
MOUNT_POINT=/mnt/efs
mkdir -p ${MOUNT_POINT}
chown ec2-user:ec2-user ${MOUNT_POINT}
echo ${FILE_SYSTEM_ID}.efs.${REGION}.amazonaws.com:/ ${MOUNT_POINT} nfs4
nfsvers=4.1,rsize=1048576,wszie=1048576,hard,timeo=600,retrans=2,_netdev 0 0 >> /
etc/fstab
mount -a -t nfs4
```

- e. 转到向导的步骤 6。
6. 在 Configure Security Group (配置安全组) 页面上，选择 Select an existing security group (选择现有安全组)，然后选择您在[先决条件 \(p. 916\)](#)中创建的安全组，再选择 Review and Launch (查看并启动)。
 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装载到您指定的目录 (例如，/mnt/efs)。

验证文件系统是否已装载

1. 连接到您的实例。有关更多信息，请参阅[连接到 Linux 实例 \(p. 423\)](#)。
2. 从每个实例的终端窗口，运行 df -T 命令以验证 EFS 文件系统是否已装载。

```
$ 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：

```
file-system-id.efs.aws-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 (操作)、Instance State (实例状态) 和 Terminate (终止)。
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 FSx for Windows File Server

Amazon FSx for Windows File Server 提供完全托管的 Windows 文件服务器，由完全原生的 Windows 文件系统支持，具有功能、性能和兼容性，可轻松提升企业应用程序并将其转移到 AWS。

Amazon FSx 支持一系列广泛的企业 Windows 工作负载，并在 Microsoft Windows Server 上构建了完全托管的文件存储。Amazon FSx 本机支持 Windows 文件系统功能和行业标准服务器消息块 (SMB) 协议以通过网络访问文件存储。Amazon FSx 已针对 AWS 云中的企业应用程序进行优化，具有本机 Windows 兼容性、企业性能和功能以及一致的亚毫秒级延迟。

利用 Amazon FSx 上的文件存储，Windows 开发人员和管理员今天使用的代码、应用程序和工具可以继续保持不变。适用于 Amazon FSx 的 Windows 应用程序和工作负载包括业务应用程序、主目录、Web 服务、内容管理、数据分析、软件构建设置和媒体处理工作负载。

作为一项完全托管的服务，Amazon FSx for Windows File Server 消除了设置并预置文件服务器和存储卷的管理开销。此外，它可使 Windows 软件保持最新，检测并排除硬件故障以及执行备份。它还提供与其他 AWS 服务（包括 AWS Directory Service for Microsoft Active Directory、Amazon WorkSpaces、AWS Key Management Service 和 AWS CloudTrail）的丰富集成。

有关更多信息，请参阅 [Amazon FSx for Windows File Server 用户指南](#)。

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。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 系统映像 (AMI)。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准来创建多个数据卷，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 \(p. 782\)](#)。

对象是 Amazon S3 中存储的基本实体。Amazon S3 中存储的每个对象都包含在存储桶中。存储桶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 存储桶类似于 Internet 域名。

存储在存储桶中的对象具有唯一的密钥值，可以使用 HTTP URL 地址进行检索。举例来说，如果密钥值为 /photos/mygarden.jpg 的对象存储在 **aws-s3-bucket1** 存储桶中，则可使用 URL `http://aws-s3-bucket1.s3.amazonaws.com/photos/mygarden.jpg` 对该对象进行寻址。

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 下载公用对象。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）。

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

此方法要求您请求的对象是公用的；如果对象不是公用的，您会收到“ERROR 403: Forbidden”（错误 403：禁止访问）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 Command Line Interface

AWS Command Line Interface (AWS CLI) 是用于管理 AWS 服务的统一工具。AWS CLI 能让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 Command Line Interface 详细信息页](#)。

aws s3 cp 命令与 Unix cp 命令类似。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，可以将文件在不同 Amazon S3 位置之间复制。

使用以下命令可将一个对象从 Amazon S3 复制到您的实例。

```
[ec2-user ~]$ 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。

```
[ec2-user ~]$ aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.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。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。

```
[ec2-user ~]$ aws s3 sync s3://remote_s3_bucket local_directory
```

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，可将其与其他 API 和 SDK（如 boto Python 接口）集成。

实例卷限制

您的实例可以具有的卷的最大数量取决于操作系统和实例类型。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。

目录

- [特定于 Linux 的卷限制 \(p. 921\)](#)
- [特定于 Windows 的卷限制 \(p. 921\)](#)
- [实例类型限制 \(p. 921\)](#)
- [带宽与容量 \(p. 922\)](#)

特定于 Linux 的卷限制

附加的卷数超出 40 会导致启动失败。请注意，此数字包括根卷以及所有附加的实例存储卷和 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，分离所有在启动过程中不必要的卷，然后在实例运行之后重新附加这些卷。

Important

如果将 40 个以上的卷附加到 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附加的实例存储卷和 EBS 卷。

Important

如果附加到 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](#)。

实例类型限制

A1、C5、C5d、C5n、G4、I3en、Inf1、M5、M5a、M5ad、M5d、M5dn、M5np3dn.24xlarge、R5、R5a、R5ad、R5dn 和 z1d 实例最多支持 28 个附件，包括网络接口、EBS 卷和 NVMe 实例存储卷。每个实例至少附加 1 个网络接口。NVMe 实例存储卷将自动附加。例如，如果在仅限 EBS 的实例上没有附加其他网络接口，您可以将多达 27 个 EBS 卷附加到该实例。如果带有 2 个 NVMe 实例存储卷的实例上还有一个网络接口，您可以将 24 个 EBS 卷附加到该实例。有关更多信息，请参阅[弹性网络接口 \(p. 595\)](#) 和 [实例存储卷 \(p. 904\)](#)。

i3.metal、m5.metal、m5d.metal、r5.metal、r5d.metal 和 z1d.metal 实例最多支持 31 个 EBS 卷。

u-6tb1.metal、u-9tb1.metal 和 u-12tb1.metal 实例支持最多 13 个 EBS 卷。u-18tb1.metal 和 u-24tb1.metal 实例支持最多 19 个 EBS 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 EBS 优化的实例 \(p. 863\)](#) 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

当您将卷附加到实例时，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。

您的实例可支持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 \(p. 921\)](#)。

目录

- [可用设备名称 \(p. 922\)](#)
- [设备名称注意事项 \(p. 923\)](#)

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

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。支持 HVM AMI 的所有实例类型。上一代的某些实例类型支持半虚拟化 AMI。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 \(p. 87\)](#)。

下表列出了在块储存设备映射中或附加 EBS 卷时您可指定的可用设备名称。

虚拟化类型	Available	根预留	建议用于 EBS 卷	实例存储卷
半虚拟化	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
全虚拟化	/dev/sd[a-z] /dev/xvd[b-c][a-z]	不同的 AMI /dev/sda1 或 /dev/xvda	/dev/sd[f-p] * /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge)	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge)

虚拟化类型	Available	根预留	建议用于 EBS 卷	实例存储卷
				/dev/sd[b-i] (i2.8xlarge) **

* 您在块储存设备映射中为 NVMe EBS 卷指定的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。块储存设备驱动程序可以使用不同于您在块储存设备映射中为卷指定的顺序来分配 NVMe 设备名称。

** 将自动枚举 NVMe 实例存储卷并为其分配 NVMe 设备名称。

有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 903\)](#)。有关 NVMe EBS 卷的更多信息，请参阅 [Linux 实例上的 Amazon EBS 和 NVMe \(p. 860\)](#)。

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附加实例存储卷的设备名附加 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。
- 实例的 NVMe 实例存储卷数取决于该实例的大小。将自动枚举 NVMe 实例存储卷并为其分配 NVMe 设备名称 (`/dev/nvme[0-26]n1`)。
- 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 `/dev/sdh` 的设备名称，则设备可能命名为 `/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，即使尾部字母可能发生改变 (`/dev/sda` 可能变为 `/dev/xvde`)。在这些情况下，每个设备名称的尾部字母都会递增相同次数。例如，如果 `/dev/sdb` 重命名为 `/dev/xvdf`，则 `/dev/sdc` 重命名为 `/dev/xvdg`。Amazon Linux 为您对重命名设备指定的名称创建符号链接。其他操作系统的行方式可能有所不同。
- HVM AMI 不支持在设备名称中使用尾部数字，除为根设备保留的 `/dev/sda1` 和 `/dev/sda2` 以外。尽管可以使用 `/dev/sda2`，但我们不建议将此设备映射与 HVM 实例结合使用。
- 使用 PV AMI 时，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，如果您将一个卷附加为 `/dev/sdc`，另一个卷附加为 `/dev/sdc1`，则只有 `/dev/sdc` 将对实例可见。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 (例如 `/dev/sdc1`、`/dev/sdc2`、`/dev/sdc3`)。
- 一些自定义内核可能会包含限制，限制使用 `/dev/sd[f-p]` 或 `/dev/sd[f-p][1-6]`。如果您在使用 `/dev/sd[q-z]` 或 `/dev/sd[q-z][1-6]` 时遇到问题，请尝试切换为 `/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 卷附加到运行中的实例，请参阅 [将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。然而，将实例存储卷附加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 \(p. 15\)](#)。

目录

- [块储存设备映射的概念 \(p. 924\)](#)
- [AMI 块储存设备映射 \(p. 926\)](#)
- [实例块储存设备映射 \(p. 928\)](#)

块储存设备映射的概念

块储存设备是一种以字节或位（块）为单位移动数据的存储设备。这些设备支持随机访问并广泛使用缓存 I/O。例如，包括硬盘、CD-ROM 盘和闪存盘。块储存设备可以实际附加到计算机，或者就像实际附加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，其底层硬件实际附加到该实例的主机）
- 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，某个实例类型支持的所有 NVMe 实例存储卷将在实例启动时自动枚举并为其分配设备名称；将这些卷包含在您的块储存设备映射中不起作用。

目录

- [块储存设备映射条目 \(p. 924\)](#)
- [块储存设备映射实例存储注意事项 \(p. 924\)](#)
- [块储存设备映射示例 \(p. 925\)](#)
- [如何使设备在操作系统可用 \(p. 925\)](#)

块储存设备映射条目

当您创建块储存设备映射时，可以为需要附加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。在装载卷时，实例的块储存设备驱动程序将分配实际卷名称。分配的名称可以与 Amazon EC2 建议的名称不同。有关更多信息，请参阅[Linux 实例上的设备命名 \(p. 922\)](#)。
- [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] 这些卷将自动枚举并分配设备名称；将这些卷包含在您的块储存设备映射中不起作用。
- [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，附加的卷的默认值为 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。默认值为 gp2。
- [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 AMIs 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。

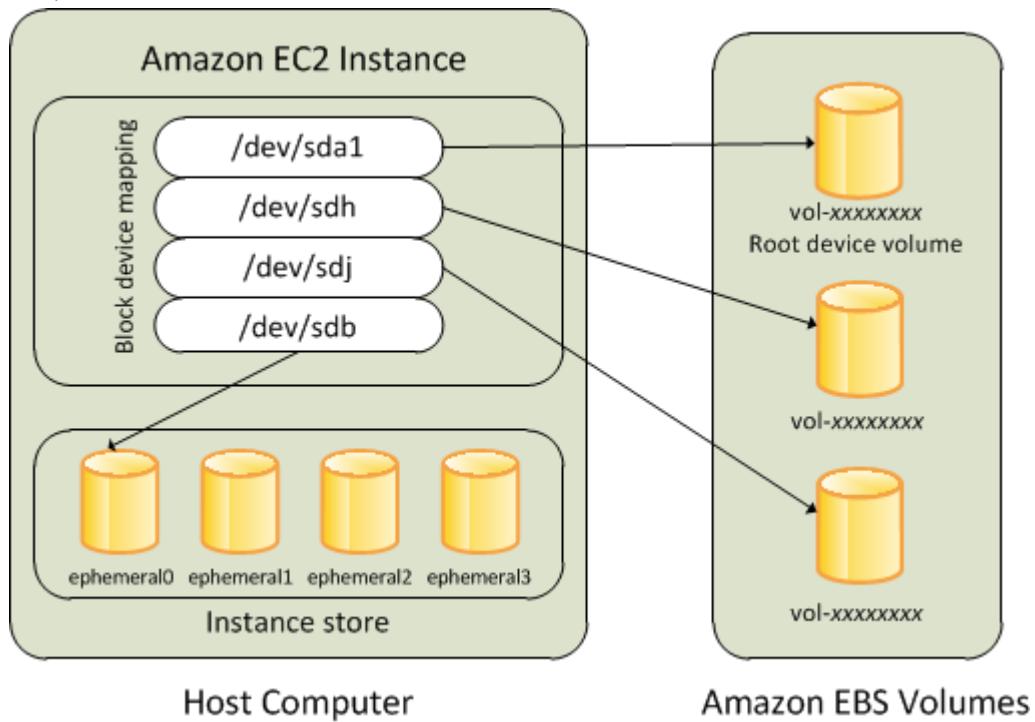
Note

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 并映射两个 EBS 卷，一个映射到 /dev/sdh，另一个映射到 /dev/sdj。它还显示了作为根设备卷的 EBS 卷，即 /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 \(p. 926\)](#)和[在启动实例时更新块储存设备映射 \(p. 928\)](#)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 使用设备名称（如 /dev/sdh 和 xvdh）来描述块储存设备。Amazon EC2 使用块储存设备映射来指定要附加到 EC2 实例的块储存设备。当块储存设备附加到实例后，您必须先将其装载到操作系统，然后才可以访问此存储设备。当块储存设备从实例分离后，就被操作系统卸载下来，而您也不能再访问该存储设备。

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。默认情况下，实例类型决定要格式化并装载哪个实例存储卷。您可以在启动时装载额外的实例存储卷，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. 903)。实例的块储存设备驱动程序决定在格式化和装载卷时要使用哪些设备。有关更多信息，请参阅将 Amazon EBS 卷附加到实例 (p. 800)。

AMI 块储存设备映射

各个 AMI 都拥有块储存设备映射，指定实例启动时要附加的块储存设备。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。

目录

- [为 AMI 指定块储存设备映射 \(p. 926\)](#)
- [查看 AMI 块储存设备映射中的 EBS 卷 \(p. 927\)](#)

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 前已将卷附加到运行中的实例，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

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances。
3. 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 `--block-device-mappings` 参数指定块储存设备映射。以 JSON 编码的参数可以直接在命令行上提供，也可以通过引用文件提供：

```
--block-device-mappings [mapping, ...]  
--block-device-mappings [file://mapping.json]
```

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 gp2 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，您可以将 `-BlockDeviceMapping` 参数与以下命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用：

- [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 (根设备类型) (ebs)
 - Root Device Name (例如，/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

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存储设备（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。

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。

目录

- [在启动实例时更新块储存设备映射 \(p. 928\)](#)
- [更新正在运行的实例的块储存设备映射 \(p. 929\)](#)
- [查看实例块储存设备映射中的 EBS 卷 \(p. 930\)](#)
- [查看实例存储卷的实例块储存设备映射 \(p. 930\)](#)

在启动实例时更新块储存设备映射

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

- 打开 Amazon EC2 控制台。
- 在控制面板中，选择 Launch Instance。
- 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
- 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。
- 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。
- 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  
    }  
}
```

要附加额外的实例存储卷 /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，您可以将 `-BlockDeviceMapping` 参数与 [New-EC2Instance](#) 命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用。

更新正在运行的实例的块储存设备映射

您可以使用以下 `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，您可以将 `-BlockDeviceMapping` 参数与 [Edit-EC2InstanceAttribute](#) 命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用。

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。您必须先分离并重新附加该卷，AWS 才能显示块储存设备映射。

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：
 - Root device type (根设备类型) (ebs)
 - Root device (例如，/dev/sda1)
 - Block devices (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具有额外的 EBS 卷，则 Block devices 字段会将这些连接卷也显示为根设备。(请记住，此对话框不显示实例存储卷。)

Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sda1 /dev/sdf

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)
 - Root device type (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在块储存设备映射中查询非 NVMe 实例存储卷。未包含 NVMe 实例存储卷。

所有针对实例元数据的请求的基本 URI 均为 <http://169.254.169.254/latest/>。有关更多信息，请参阅[实例元数据和用户数据 \(p. 499\)](#)。

首先，连接到运行中的实例。从该实例中，使用此查询获取其块储存设备映射。

```
[ec2-user ~]$ 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 设备是实例所看到的根设备。实例存储卷命名为 ephemeral[0-23]。swap 设备用于存储页面文件。如果您还映射了一些 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。

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

实例类型将决定对实例可用的实例存储卷的数量。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他卷将被忽略。要查看实例的实例存储卷，请运行 `lsblk` 命令。要了解每种实例类型支持的实例存储卷数，请参阅[实例存储卷 \(p. 904\)](#)。

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。

目录

- [资源位置 \(p. 932\)](#)
- [资源 ID \(p. 933\)](#)
- [列出并筛选您的资源 \(p. 937\)](#)
- [标记您的 Amazon EC2 资源 \(p. 940\)](#)
- [Amazon EC2 服务限制 \(p. 950\)](#)
- [Amazon EC2 使用率报告 \(p. 951\)](#)

资源位置

有些资源可以在所有地区 (全球) 使用，而有些资源则特定于其所在的区域或可用区。

资源	类型	描述
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	您使用 Amazon EC2 创建的密钥对与您在其中创建它们的区域相关联。您可以创建您自己的 RSA 密钥对并将其上传到您打算在其中使用它的区域；因此，您可以通过将密钥对上传至每个区域而使其在全球范围内可用。 有关更多信息，请参阅 Amazon EC2 密钥对 (p. 759) 。
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。
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. 138) 。
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。

资源	类型	描述
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. 819) 。
EBS 卷	可用区	Amazon EBS 卷与其可用区相关联，只能附加到同一可用区内的实例。
实例	可用区	实例与您在其中启动实例的可用区相关联。但它的实例 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 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。

支持的资源类型有一个选择周期，在此期间您可以选择资源 ID 格式和截止日期，在此之后资源默认为较长 ID 格式。在为特定资源类型传递截止时间后，您不能再对该资源类型禁用较长 ID 格式。

不同的资源类型具有不同的选择周期和截止日期。下表列出受支持的资源类型及其选择周期和截止日期。

资源类型	选择周期	截止日期
instance snapshot reservation volume	不再可用	2016 年 12 月 15 日
bundle conversion-task customer-gateway dhcp-options elastic-ip-allocation elastic-ip-association export-task flow-log image import-task internet-gateway network-acl network-acl-association network-interface network-interface-attachment prefix-list route-table route-table-association security-group subnet subnet-cidr-block-association vpc vpc-cidr-block-association vpc-endpoint vpc-peering-connection vpn-connection vpn-gateway	2018 年 2 月 9 日 - 2018 年 6 月 30 日	2018 年 6 月 30 日

在选择周期内

您可以在选择周期内随时对资源启用或禁用较长 ID。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 ID。

Note

资源 ID 在创建后不会更改。因此，在选择周期内启用或禁用较长 ID 不会影响现有的资源 ID。

根据您创建 AWS 账户的时间，支持的资源类型可能默认为使用较长 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。

在截止日期之后

不能在截止日期结束后对资源类型禁用较长 ID。您创建的所有新资源都是使用较长 ID 创建的。

使用较长的 ID

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。

主题

- [查看较长 ID 设置 \(p. 934\)](#)
- [修改较长 ID 设置 \(p. 935\)](#)

查看较长 ID 设置

您可以使用控制台和命令行工具查看支持较长 ID 的资源类型。

使用控制台查看较长 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，选择您可以查看较长 ID 设置的区域。
3. 在控制面板中的 Account Attributes 下，选择 Resource ID length management。
4. 展开 Advanced Resource ID Management 以查看支持较长 ID 及其截止日期的资源类型。

使用命令行查看较长 ID 设置

使用以下命令之一：

- [describe-id-format \(AWS CLI\)](#)

```
aws ec2 describe-id-format --region region
```

- [Get-EC2IdFormat \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Get-EC2IdFormat -Region region
```

使用命令行查看特定 IAM 用户或 IAM 角色的较长 ID 设置

使用以下命令之一，并在请求中指定 IAM 用户、IAM 角色或根账户用户的 ARN。

- [describe-identity-id-format \(AWS CLI\)](#)

```
aws ec2 describe-identity-id-format --principal-arn arn-of-iam-principal --region region
```

- [Get-EC2IdentityIdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

```
Get-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Region region
```

使用命令行查看特定区域的聚合较长 ID 设置

使用 [describe-aggregate-id-format](#) AWS CLI 命令查看整个区域的聚合较长 ID 设置，以及每个资源类型的所有 ARN 的聚合较长 ID 设置。此命令对于执行快速审核非常有用，可以确定某个特定区域是否针对较长 ID 完全选择加入。

```
aws ec2 describe-aggregate-id-format --region region
```

标识显式定义了自定义较长 ID 设置的用户

使用 [describe-principal-id-format](#) AWS CLI 命令查看根用户以及所有显式指定了较长 ID 首选项的 IAM 角色和 IAM 用户的较长 ID 格式设置。此命令对于标识已覆盖默认较长 ID 设置的 IAM 用户和 IAM 角色非常有用。

```
aws ec2 describe-principal-id-format --region region
```

修改较长 ID 设置

您可以使用控制台和命令行工具修改仍在选择周期内的资源类型的较长 ID 设置。

Note

此部分中的 AWS CLI 和 [适用于 Windows PowerShell 的 AWS 工具](#) 命令是仅针对每个区域的。除非另行指定，否则它们适用于默认区域。要修改其他区域的设置，请在命令中包括 `region` 参数。

使用控制台修改较长 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，选择您可以修改较长 ID 设置的区域。
3. 在控制面板中的 Account Attributes 下，选择 Resource ID length management。
4. 请执行下列操作之一：
 - 要跨所有区域对所有 IAM 用户支持的所有资源类型启用较长 ID，请选择 Switch to longer IDs (切换到加长 ID)、Yes, switch to longer IDs (是，切换到加长 ID)。

Important

IAM 用户和 IAM 角色需要 `ec2:ModifyIdentityIdFormat` 权限来执行此操作。

- 要修改您的 IAM 用户账户的特定资源类型的较长 ID 设置，请展开 Advanced Resource ID Management (高级资源 ID 管理)，然后在 My IAM Role/User (我的 IAM 角色/用户) 列中选择相应的复选框以启用较长 ID，或者清除该复选框以禁用较长 ID。
- 要修改所有 IAM 用户的特定资源类型的较长 ID 设置，请展开 Advanced Resource ID Management (高级资源 ID 管理)，然后在 All IAM Roles/Users (所有 IAM 角色/用户) 列中选择相应的复选框以启用较长 ID，或者清除该复选框以禁用较长 ID。

使用命令行修改您的 IAM 用户账户的较长 ID 设置

使用以下命令之一：

Note

如果您以根用户的身份使用这些命令，则这些更改将适用于整个 AWS 账户，除非 IAM 用户或角色明确为其覆盖这些设置。

- [modify-id-format \(AWS CLI\)](#)

```
aws ec2 modify-id-format --resource resource_type --use-long-ids
```

您还可以使用该命令修改所有受支持资源类型的较长 ID 设置。为此，请将 *resource_type* 参数替换为 *all-current*。

```
aws ec2 modify-id-format --resource all-current --use-long-ids
```

Note

要禁用较长 ID，请将 *use-long-ids* 参数替换为 *no-use-long-ids*。

- [Edit-EC2IdFormat \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Edit-EC2IdFormat -Resource resource_type -UseLongId boolean
```

您还可以使用该命令修改所有受支持资源类型的较长 ID 设置。为此，请将 *resource_type* 参数替换为 *all-current*。

```
Edit-EC2IdFormat -Resource all-current -UseLongId boolean
```

使用命令行修改特定 IAM 用户或 IAM 角色的较长 ID 设置

使用以下命令之一，并在请求中指定 IAM 用户、IAM 角色或根用户的 ARN。

- [modify-identity-id-format \(AWS CLI\)](#)

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --  
resource resource_type --use-long-ids
```

您还可以使用该命令修改所有受支持资源类型的较长 ID 设置。为此，请为 *all-current* 参数指定 *--resource*。

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --resource all-  
current --use-long-ids
```

Note

要禁用较长 ID，请将 *use-long-ids* 参数替换为 *no-use-long-ids*。

- [Edit-EC2IdentityIdFormat \(适用于 Windows PowerShell 的 AWS 工具\)](#)

```
Edit-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Resource resource_type -  
UseLongId boolean
```

您还可以使用该命令修改所有受支持资源类型的较长 ID 设置。为此，请为 *all-current* 参数指定 *-Resource*。

```
Edit-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Resource all-current -  
UseLongId boolean
```

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以下操作的权限，除非他们通过关联的 IAM 策略明确获得了相应权限：

- ec2:DescribeIdFormat
- ec2:DescribeIdentityIdFormat
- ec2:DescribeAggregateIdFormat
- ec2:DescribePrincipalIdFormat
- ec2:ModifyIdFormat
- ec2:ModifyIdentityIdFormat

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",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribePrincipalIdFormat"
            ],
            "Resource": "*"
        }
    ]
}
```

对于以下操作，我们不支持资源级权限：

- ec2:DescribeIdFormat
- ec2:DescribeIdentityIdFormat
- ec2:DescribeAggregateIdFormat
- ec2:DescribePrincipalIdFormat
- ec2:ModifyIdFormat
- ec2:ModifyIdentityIdFormat

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。

目录

- [高级搜索 \(p. 938\)](#)
- [使用控制台列出资源 \(p. 939\)](#)
- [使用控制台筛选资源 \(p. 939\)](#)
- [使用 CLI 和 API 列出并筛选 \(p. 940\)](#)

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、用户定义的标签键以及预定义的资源属性进行筛选。

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

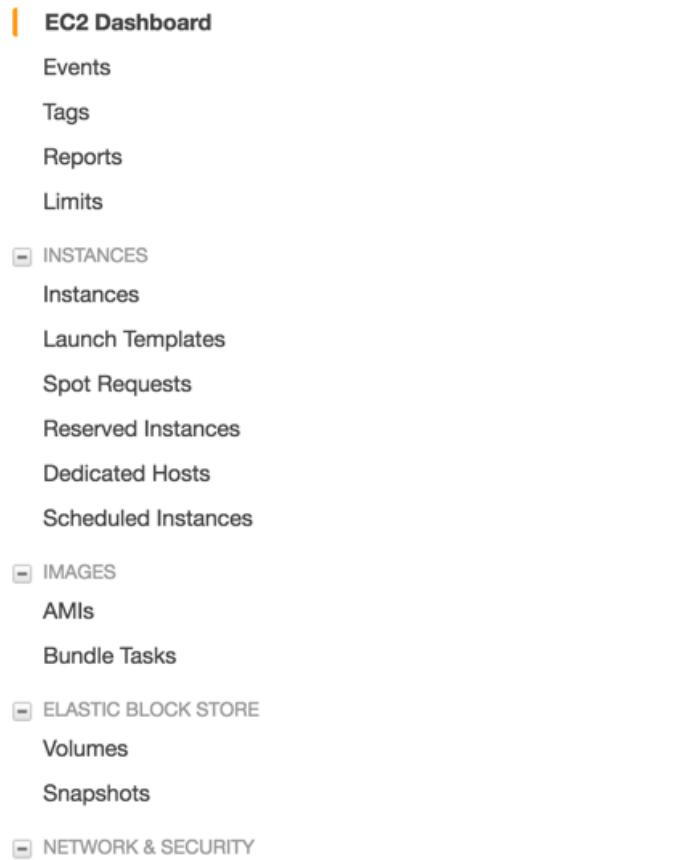
通常，具有相同键字段（例如，tag:Name、search、Instance State）的多个筛选条件会自动以 OR 运算符联接。这是特意设计的，因为绝大部分筛选条件如果以 AND 运算符联接将不合逻辑。例如，如果以“Instance State=running AND Instance State=stopped”为条件进行搜索，将返回零个结果。在许多情况下，您可以对不同键字段使用补充性搜索词来细化搜索结果，此时将自动改用 AND 规则。如果您搜索“tag: Name:=All values AND tag:Instance State=running”，您将获得包含这两个条件的搜索结果。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，从菜单中选择附加状态，然后选择已分离。（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 支持的公有 64 位 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 Windows。
3. 在搜索字段中键入 x86_64。
4. 会显示所有符合此标准的 AMI。

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 (*) 匹配零个或多个字符，而问号 (?) 匹配零个或一个字符。

例如，您可以使用 `database` 作为筛选值仅获取描述为 `database` 的 EBS 快照。如果指定 `*database*`，则会返回描述包括 `database` 的所有快照。如果指定 `database?`，则只会返回描述与以下模式之一匹配的快照：等于 `database` 或等于 `database` 后跟一个字符。

问号数决定结果中包含的最大字符数。例如，如果指定 `database????`，则只会返回描述为 `database` 后跟最多四个字符的快照。`database` 后跟五个或更多字符的描述将从搜索结果中排除。

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 CLI Command Reference](#) 中的相关命令。
- 对于 Windows PowerShell，请参阅 [适用于 PowerShell 的 AWS 工具 Cmdlet 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。

标记您的 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。

Warning

很多不同的 API 调用返回标签键及其值。拒绝访问 `DescribeTags` 不会自动拒绝访问其他 API 返回的标签。作为最佳实践，我们建议您不要在标签中包含敏感数据。

目录

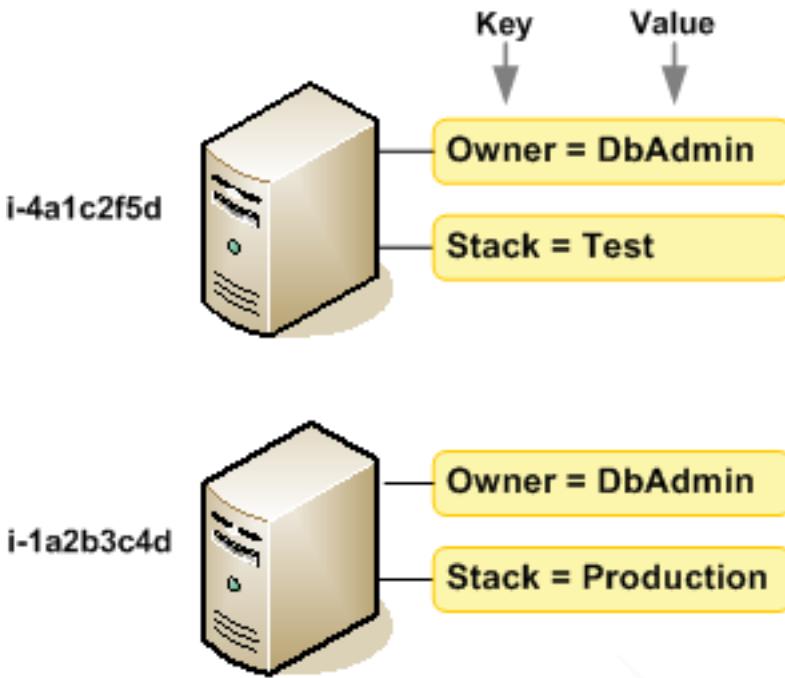
- [有关标签的基本知识 \(p. 941\)](#)
- [标记资源 \(p. 942\)](#)
- [标签限制 \(p. 944\)](#)
- [标记资源以便于计费 \(p. 944\)](#)
- [通过控制台使用标签 \(p. 945\)](#)
- [通过 CLI 或 API 使用标签 \(p. 948\)](#)

有关标签的基本知识

标签是您为 AWS 资源分配的标记。每个标签都包含您定义的一个键 和一个可选值。

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很多资源时会很有用 — 您可以根据分配给资源的标签快速识别特定资源。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。

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 — 一个标签使用键 `Owner`，另一个使用键 `Stack`。每个标签都拥有相关的值。



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。

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[适用于 Amazon EC2 的 Identity and Access Management \(p. 701\)](#)。

标记资源

您可以标记您的账户中已存在的大多数 Amazon EC2 资源。下表 (p. 942)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 (标签) 选项卡或使用 Tags (标签) 屏幕向资源应用标签。在您创建资源时 , 某些资源屏幕能让您为资源指定标签 ; 例如 , 具有 Name 键并且具有您指定的值的标签。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。控制台可能根据 Name 标签对资源进行组织 , 但此标签对于 Amazon EC2 服务没有任何语义意义。

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。这样可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使用 Amazon EC2 API、AWS CLI 或 AWS 软件开发工具包标记的资源。

Amazon EC2 资源标记支持

资源	支持标签	支持在创建时标记
AFI	是	是
AMI	是	否
捆绑任务	否	否
容量预留	是	是
客户端 VPN 终端节点	是	是
客户端 VPN 路由	否	否
客户网关	是	否
专用主机	是	是
专用主机 预留	是	否
DHCP 选项	是	否
EBS 快照	是	是
EBS 卷	是	是
EC2 队列	是	是
仅出口 Internet 网关	否	否
弹性 IP 地址	是	否
Elastic Graphics 加速器	是	否
实例	是	是
实例存储卷	不适用	不适用

资源	支持标签	支持在创建时标记
Internet 网关	是	否
密钥对	是	否
启动模板	是	是
启动模板版本	否	否
NAT 网关	是	否
网络 ACL	是	否
网络接口	是	否
置放群组	是	否
Reserved Instance	是	否
Reserved Instance 清单	否	否
路由表	是	否
Spot 实例请求	是	否
安全组	是	否
子网	是	否
流量镜像筛选	是	是
流量镜像会话	是	是
流量镜像目标	是	是
转换网关	是	是
转换网关路由表	是	是
转换网关 VPC 连接	是	是
虚拟专用网关	是	否
VPC	是	否
VPC 终端节点	是	否
VPC 终端节点服务	是	否
VPC 终端节点服务配置	是	否
VPC 流日志	否	否
VPC 对等连接	是	否
VPN 连接	是	否

您可以在创建时使用 Amazon EC2 控制台中的 Amazon EC2 启动实例向导为实例和卷添加标签。您可以在创建时使用卷屏幕为 EBS 卷添加标签，使用快照屏幕为 EBS 快照添加标签。或者，也可以使用资源创建 Amazon EC2 API (例如 [RunInstances](#)) 在创建资源时应用标签。

对于支持在创建时进行标记的 Amazon EC2 API 操作，您可以在 IAM 策略中应用基于标签的资源级权限，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 \(p. 712\)](#) 和 [使用 AWS CLI 或 AWS SDK 的策略示例 \(p. 714\)](#)。

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：

- 每个资源的最大标签数 – 50
- 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值。
- 最大键长度 – 128 个 Unicode 字符（采用 UTF-8 格式）
- 最大值长度 – 256 个 Unicode 字符（采用 UTF-8 格式）
- 虽然 EC2 允许在其标签中使用任何字符，但其他服务具有更严格的限制。允许在不同的服务中使用的字符包括：可以使用 UTF-8 表示的字母、数字和空格以及以下字符：+ - = . _ : / @。
- 标签键和值区分大小写。
- aws：前缀是专为 AWS 使用预留的。如果某个标签具有带有此标签键，则您无法编辑该标签的键或值。具有 aws：前缀的标签不计入每个资源的标签数限制。

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 \(p. 942\)](#)。

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密钥值的 AWS 账户账单。有关设置带有标签的成本分配报告的更多信息，请参阅 AWS Billing and Cost Management 用户指南中的 [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。

成本分配标签可指示哪些资源导致产生成本，而删除或停用资源并不总是能降低成本。例如，即使删除包含原始数据的快照，其他快照引用的快照数据也将保留。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南中的 [Amazon Elastic Block Store 卷和快照](#)。

Note

标记的弹性 IP 地址不会显示在成本分配报告中。

通过控制台使用标签

通过使用 Amazon EC2 控制台，您可以查看在同一区域的所有 Amazon EC2 资源中使用了哪些标签。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 \(p. 937\)](#)。

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，请参阅开始使用 AWS 管理控制台中的[使用标签编辑器](#)。

目录

- [显示标签 \(p. 945\)](#)
- [为单个资源添加和删除标签 \(p. 946\)](#)
- [为一组资源添加和删除标签 \(p. 946\)](#)
- [在启动实例时添加标签 \(p. 947\)](#)
- [按标签筛选资源列表 \(p. 947\)](#)

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 (实例)，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。控制台中添加了一个新列。
- 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。

Manage Tags						
Filter: <input type="text"/> Search Keys		Search Values		1 to 7 of 7 Tags		
	Tag Key	Tag Value	Total	Instances	AMIs	Volumes
Manage Tag	Name	DNS Server	1	1	0	0
Manage Tag	Owner	TeamB	2	0	0	2
Manage Tag	Owner	TeamA	2	0	0	2
Manage Tag	Purpose	Project2	1	0	0	1
Manage Tag	Purpose	Logs	1	0	0	1
Manage Tag	Purpose	Network Management	1	1	0	0
Manage Tag	Purpose	Project1	2	0	0	2

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. 从导航栏中，选择满足您的需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
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，然后选择标签、添加/编辑标签。
5. 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. 从导航栏中，选择满足您的需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
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，然后选择标签。
5. 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. 从导航栏中，选择满足您的需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
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。

- 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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 从导航栏中，选择满足您的需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
- 在导航窗格中，依次选择 Tags、Manage Tags。
- 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。
- 对于 Filter，选择要删除标签的资源的类型 (如实例)。
- 在资源列表中，选中要删除标签的资源旁边的复选框。
- 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

- 在导航栏中，选择的实例的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。选择满足您的需求的区域。有关更多信息，请参阅[资源位置 \(p. 932\)](#)。
- 选择 Launch Instance。
- 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 \(p. 88\)](#)。
- 在 Configure Instance Details 页面上，根据需要配置实例设置，然后选择 Next: Add Storage。
- 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。
- 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。
- 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。
- 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

- 标签列显示如下：
 - 选择资源。
 - 在详细信息窗格中，选择 Tags。
 - 在列表中查找标签，然后选择 Show Column。
- 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. 937)。

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。

Note

在命令行中输入 JSON 格式参数的方式因操作系统而异。Linux、macOS 或 Unix 和 Windows PowerShell 使用单引号 ('') 括住 JSON 数据结构。在通过 Windows 命令行使用命令时，则不使用单引号。有关更多信息，请参阅为 AWS 命令行界面指定参数值。

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。该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}]'
```

示例 6：将标签添加到资源

此示例将标签 Stack=production 添加到指定图像，或者覆盖该 AMI 的现有标签 (其中标签键为 Stack)。如果命令成功，则不返回任何输出。

```
aws ec2 create-tags --resources ami-78a54011 --tags Key=Stack,Value=production
```

示例 7：将标签添加到多个资源

此示例为 AMI 和实例添加 (或覆盖) 两个标签。其中一个标签仅包含一个键 (webserver)，不包含值 (我们将值设置为空字符串)。另一个标签则包含一个键 (stack) 和值 (Production)。如果命令成功，则不返回任何输出。

```
aws ec2 create-tags --resources ami-1a2b3c4d i-1234567890abcdef0 --tags Key=webserver,Value= Key=stack,Value=Production
```

示例 8：使用特殊字符添加标签

此示例将标签 [Group]=test 添加到实例。方括号 ([和]) 是特殊字符，并且必须使用反斜杠 (\) 进行转义。

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags Key=\[Group\],Value=test
```

如果您使用的是 Windows PowerShell，请使用反斜杠 (\) 隔开字符，使用双引号 ("") 括起来，然后使用单引号 ('') 将整个键和值结构括起来。

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags 'Key=\\"[Group]\\",Value=test'
```

如果您使用的是 Linux 或 OS X，请使用单引号(')将整个键和值结构括起来，然后使用双引号(")将包含特殊字符的元素括起来。

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags 'Key="[Group]",Value=test'
```

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（也称为配额）。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）区域中启动实例时，请求一定不能导致您的用量超出您在该区域中的当前实例限制。

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](#)。

查看您的当前限制

使用 Amazon EC2 控制台中的 EC2 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. 从导航栏中选择一个区域。



3. 从导航窗格中，选择 Limits。

- 在列表中找到资源。您可以使用搜索字段按资源名称或资源组筛选列表。当前限制列显示您的账户对该资源的当前最大限制。

Note

如果您选择为按需实例使用基于 vCPU 的实例限制，则可以看到五个基于 vCPU 的按需实例限制。每种限制指定了一个或多个实例系列的 vCPU 限制。有关更多信息，请参阅[个按需实例限制 \(p. 241\)](#)。

申请提高限制

使用 Amazon EC2 控制台中的限制页面可按区域请求提高 Amazon EC2 或 Amazon VPC 提供的资源的限制。

申请提高限制

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 从导航栏中选择一个区域。
- 从导航窗格中，选择 Limits。
- 在列表中选择资源，然后选择请求提高限制。
- 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。

对使用端口 25 发送的电子邮件的限制

默认情况下，Amazon EC2 会限制所有实例的端口 25 上的流量。您可以请求删除此限制。有关更多信息，请参阅 AWS 知识中心内的[如何从 EC2 实例删除端口 25 上的限制？](#)

Amazon EC2 使用率报告

AWS 提供了称为 Cost Explorer 的免费报告工具，该工具可让您分析 EC2 实例的成本和使用率以及预留实例的使用率。

Cost Explorer 是一款免费工具，可用于查看使用率和成本的图表。您最多可以查看过去 13 个月的数据，并预测您在接下来三个月内可能产生的费用。您可以使用 Cost Explorer 查看一段时间内在 AWS 资源方面的费用模式，确定需要进一步查询的方面，并查看可用于了解您的成本的趋势。您还可以指定数据的时间范围，并按天或按月查看时间数据。

下面是您可以使用 Cost Explorer 回答的一些问题的示例：

- 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？
- 我的预留实例使用情况如何？
- 预留实例是否在帮助我节省开支？

在 Cost Explorer 中查看 Amazon EC2 报告

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择 Reports，然后选择要查看的报告。

报告将在 Cost Explorer 中打开。它根据固定的筛选器设置提供预配置的视图，其中显示有关您的使用率和成本趋势的信息。

有关在 Cost Explorer 中使用报告 (包括保存报告) 的更多信息，请参阅[使用 Cost Explorer 分析您的成本](#)。

排查实例问题

以下文档可帮助您排查实例存在的问题。

目录

- [排查实例启动问题 \(p. 953\)](#)
- [排查实例的连接问题 \(p. 955\)](#)
- [排查实例的停止问题 \(p. 961\)](#)
- [排查实例的终止 \(关闭\) 问题 \(p. 963\)](#)
- [通过故障状态检查排查实例故障 \(p. 963\)](#)
- [对无法访问的实例进行故障排除 \(p. 983\)](#)
- [正在从错误的卷启动 \(p. 985\)](#)
- [使用 EC2Rescue for Linux \(p. 986\)](#)
- [发送诊断中断 \(仅限高级用户\) \(p. 995\)](#)

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](#)。

排查实例启动问题

以下问题将阻止您启动实例。

启动问题

- [超出实例限制 \(p. 953\)](#)
- [实例容量不足 \(p. 953\)](#)
- [实例立即终止 \(p. 954\)](#)

超出实例限制

描述

在尝试启动新实例或重新启动已停止的实例时，您将收到 `InstanceLimitExceeded` 错误。

原因

在尝试启动新实例或重新启动已停止的实例时，如果您已达到可在区域中启动的实例的数目，则将收到 `InstanceLimitExceeded` 错误。在创建 AWS 账户时，我们根据区域设置可运行的实例数的默认限制。

解决方案

您可以根据区域请求提高实例限制。有关更多信息，请参阅 [Amazon EC2 服务限制 \(p. 950\)](#)。

实例容量不足

描述

在尝试启动新实例或重新启动已停止的实例时，您将收到 `InsufficientInstanceCapacity` 错误。

原因

如果您在尝试启动实例或重新启动已停止的实例时收到 `InsufficientInstanceCapacity` 错误，则表示 AWS 当前没有足够的可用按需容量来服务您的请求。

解决方案

要解决该问题，请尝试以下操作：

- 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 [更改实例类型 \(p. 233\)](#)。
- 如果您将实例启动到集群置放群组中，则会获得容量不足错误。有关更多信息，请参阅 [置放群组规则和限制 \(p. 664\)](#)。
- 尝试创建按需容量预留，这使您能够将 Amazon EC2 容量预留任意持续时间。有关更多信息，请参阅 [按需容量预留 \(p. 360\)](#)。
- 尝试购买作为长期容量预留的预留实例。有关更多信息，请参阅 [Amazon EC2 预留实例](#)。

实例立即终止

描述

您的实例在重新启动后，状态将立即从 `pending` 转至 `terminated`。

原因

下面是实例可能立即终止的一些原因：

- 您已达到 EBS 卷限额。
- EBS 快照受损。
- 将对根 EBS 卷进行加密，并且您无权访问用于解密的 KMS 密钥。
- 您用来启动实例的由实例存储支持的 AMI 缺少必需部分（一个 `image.part.xx` 文件）

解决方案

您可以使用 Amazon EC2 控制台或 AWS Command Line Interface 获得终止原因。

使用 Amazon EC2 控制台了解终止原因

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. 在 `Description`（描述）选项卡上，记下 `State transition reason`（状态转换原因）标签旁边的原因。

使用 AWS Command Line Interface 控制台了解终止原因

1. 使用 `describe-instances` 命令并指定实例 ID。

```
aws ec2 describe-instances --instance-id instance_id
```

2. 检查命令返回的 JSON 响应，并记下 StateReason 响应元素中的值。

下面的代码块显示了 StateReason 响应元素的示例。

```
"StateReason": {  
    "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",  
    "Code": "Server.InternalError"  
},
```

解决问题

根据您记下的终止原因执行下列操作之一：

- 如果原因是 **Client.VolumeLimitExceeded: Volume limit exceeded**，则表示您已达到 EBS 卷限制。有关更多信息，请参阅[实例卷限制 \(p. 921\)](#)。要提交请求以提升 Amazon EBS 卷限制，请填写 AWS 支持中心[创建案例](#)表单。有关更多信息，请参阅 [Amazon EC2 服务限制 \(p. 950\)](#)。
- 如果原因是 **Client.InternalError: Client error on launch**，这通常表示根卷已加密，并且您无权访问用于解密的 KMS 密钥。要获得对所需的 KMS 密钥的访问权限，请将相应的 KMS 权限添加您的 IAM 用户。有关更多信息，请参阅 [AWS Key Management Service Developer Guide 中的使用 AWS KMS 中的密钥策略](#)。

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。

目录

- [连接到您的实例时出错：连接超时 \(p. 955\)](#)
- [错误：无法加载密钥...预期：任何私有密钥 \(p. 957\)](#)
- [错误：服务器无法识别用户密钥 \(p. 957\)](#)
- [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 \(p. 958\)](#)
- [错误：未保护的私钥文件 \(p. 959\)](#)
- [错误：私有密钥的格式必须以“----BEGIN RSA PRIVATE KEY----”开头，以“----END RSA PRIVATE KEY----”结尾 \(p. 960\)](#)
- [错误：服务器拒绝我们的密钥或 没有支持的身份验证方法 \(p. 960\)](#)
- [无法使用我的浏览器进行连接 \(p. 961\)](#)
- [无法对实例执行 Ping 操作 \(p. 961\)](#)
- [错误：服务器意外关闭了网络连接 \(p. 961\)](#)

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](#)。

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. 在屏幕底部的 Description (描述) 选项卡中，在 Security groups (安全组) 旁，选择 view inbound rules (查看入站规则) 以显示对所选实例生效的规则列表。
 4. 对于 Linux 实例：当您选择 view inbound rules (查看入站规则) 时，将会出现一个窗口，其中显示了允许流量到哪些端口。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：当您选择 view inbound rules (查看入站规则) 时，将会出现一个窗口，其中显示了允许流量到哪些端口。验证是否有允许流量从您的计算机到端口 3389 (RDP) 的规则。

每次重新启动实例时，将分配新的 IP 地址（和主机名）。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 \(p. 757\)](#)。

有关安全组规则的更多信息，请参阅Amazon VPC 用户指南中的[安全组规则](#)。

- 查看子网的路由表。您需要使用某个路由，以将发往 VPC 外部的所有流量发送到 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 网关附加到您的 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 0.0.0.0/0 的路由是否为目的地以及您的 VPC 的 Internet 网关是否为目标。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。否则请执行以下操作：
 - a. 选择路由表的 ID (rtb-xxxxxxxx) 以导航到路由表。
 - b. 在 Routes (路由) 选项卡上，选择 Edit routes (编辑路由)。选择 Add route (添加路由)，将 0.0.0.0/0 用作目的地并将 Internet 网关用作目标。对于 IPv6，选择 Add route (添加路由)，将 ::/0 用作目的地并将 Internet 网关用作目标。
 - c. 选择 Save routes (保存路由)。
- 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 Subnets，然后选择您的子网。
 3. 在 Description (描述) 选项卡上，找到 Network ACL (网络 ACL)，然后选择其 ID (acl-xxxxxxxx)。
 4. 选择网络 ACL。对于 Inbound Rules，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. 对于 Outbound Rules，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 \(p. 590\)](#)。
- 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 \(p. 538\)](#)。
- 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[更改实例类型 \(p. 233\)](#)。

要使用 IPv6 地址连接实例，请检查以下各项：

- 您的子网必须与一个路由表关联，此表中具有一个将 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：无法加载密钥...预期：任何私有密钥

如果您尝试连接到您的实例并收到错误消息 `unable to load key ... Expecting: ANY PRIVATE KEY`，则说明未正确配置用于存储私有密钥的文件。如果私有密钥文件以 `.pem` 为结尾，则它可能仍未正确配置。未正确配置私有密钥文件的一个可能原因是缺少证书。

如果未正确配置私有密钥文件，请按照下列步骤解决该错误

1. 创建新的密钥对。有关更多信息，请参阅[使用 Amazon EC2 创建密钥对 \(p. 760\)](#)。
2. 将新密钥对添加到您的实例。有关更多信息，请参阅[丢失私有密钥时连接到 Linux 实例 \(p. 765\)](#)。
3. 使用新的密钥对连接到实例。

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: bogus.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: bogus.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 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 \(p. 436\)](#)。

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 2 或 Amazon Linux AMI，用户名是 ec2-user。
 - 对于 CentOS AMI，用户名是 centos。
 - 对于 Debian AMI，用户名是 admin 或 root。
 - 对于 Fedora AMI，用户名为 ec2-user 或 fedora。
 - 对于 RHEL AMI，用户名是 ec2-user 或 root。
 - 对于 SUSE AMI，用户名是 ec2-user 或 root。
 - 对于 Ubuntu AMI，用户名是 ubuntu。
 - 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 \(p. 757\)](#)。

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。

正确的用户名如下所示：

- 对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 ec2-user。
- 对于 CentOS AMI，用户名是 centos。

- 对于 Debian AMI，用户名是 `admin` 或 `root`。
- 对于 Fedora AMI，用户名为 `ec2-user` 或 `fedora`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
- 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名是 `ubuntu`。
- 另外，如果 `ec2-user` 和 `root` 无法使用，请与 AMI 供应商核实。

例如，要使用 SSH 客户端连接到从 Amazon Linux 实例，请使用以下命令：

```
ssh -i /path/my-key-pair.pem ec2-user@public-dns-hostname
```

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。

1. 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 \(p. 765\)](#)。

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 \(p. 445\)](#) 和[将 Amazon EBS 卷与实例分离 \(p. 810\)](#)。
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），并将根卷附加到此临时实例。有关更多信息，请参阅[将 Amazon EBS 卷附加到实例 \(p. 800\)](#)。
3. 连接临时实例，创建一个挂载点并挂载您附加的卷。有关更多信息，请参阅[使 Amazon EBS 卷可在 Linux 上使用 \(p. 801\)](#)。
4. 在临时实例中，检查附加的卷的 `/home/ec2-user/` 目录的权限。如有必要，按如下方式调整权限：

```
[ec2-user ~]$ chmod 600 mount_point/home/ec2-user/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/ec2-user/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/ec2-user
```

5. 卸载该卷，将其与临时实例分离，然后将其重新附加到原来的实例。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。上述示例利用 `.ssh/my_private_key.pem` 文件权限使用私钥 0777，这可使任何人都能读取或写入此文件。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。

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

错误：私有密钥的格式必须以“----BEGIN RSA PRIVATE KEY----”开头，以“----END RSA PRIVATE KEY----”结尾

如果您使用第三方工具（如 `ssh-keygen`）创建 RSA 密钥对，则它会生成 OpenSSH 密钥格式的私有密钥。当您连接到实例时，如果使用 OpenSSH 格式的私有密钥来解密密码，您将收到错误 `Private key must begin with "----BEGIN RSA PRIVATE KEY----" and end with "----END RSA PRIVATE KEY----"`。

要解决该错误，私有密钥必须采用 PEM 格式。使用以下命令创建 PEM 格式的私有密钥：

```
ssh-keygen -m 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

如果您使用 PuTTY 连接到您的实例时收到以下任一错误：错误：服务器拒绝了我们的密钥或错误：没有支持的身份验证方法，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) 中键入用户名。

正确的用户名如下所示：

- 对于 Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。
- 对于 CentOS AMI，用户名是 `centos`。
- 对于 Debian AMI，用户名是 `admin` 或 `root`。
- 对于 Fedora AMI，用户名为 `ec2-user` 或 `fedora`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
- 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名是 `ubuntu`。
- 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 \(p. 436\)](#)。

无法使用我的浏览器进行连接

Amazon EC2 控制台提供了一个选项，以使用 Java SSH 客户端直接从浏览器连接到实例。如果您的浏览器不支持 NPAPI，则在连接时您将看到在 Chrome 上弃用 NPAPI 的错误消息。该消息建议您使用其他浏览器。但是，这些浏览器的最新版本也不支持 NPAPI，因此您无法使用它们连接到您的实例，而必须选择其他方法连接到您的实例。

有关更多信息，请参阅以下资源：

- 一般：[NPAPI Wikipedia 文章](#)
- Chrome：[NPAPI 弃用文章](#)
- Firefox：[NPAPI 弃用文章](#)
- Safari：[NPAPI 弃用文章](#)

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。

错误：服务器意外关闭了网络连接

如果您使用 Putty 连接到您的实例并接收到错误“服务器意外关闭了网络连接”，则请确认您已在 Putty 配置的“Connection”(连接) 页上启用 keepalives 以避免断开连接。有些服务器如果在指定的时间内未接收到任何数据，将会断开与客户端的连接。将“Seconds between keepalives”(keepalives 之间的秒数) 设置为 59 秒。

如果在启用 keepalives 之后仍然出现问题，请尝试在 Putty 配置的“Connection”(连接) 页上禁用 Nagle 的算法。

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，这说明底层主机可能存在问题。

当实例未处于 running 状态时，不会收取任何实例使用费用。

强制实例使用控制台或 AWS CLI 停止。

- 要强制实例使用控制台停止，请选择卡住的实例，然后选择 Actions、Instance State、Stop 和 Yes, Forcefully Stop。
- 要使用 AWS CLI 强制实例停止，请使用 `stop-instances` 命令和 `--force` 选项，如下所示：

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

如果在 10 分钟后，实例未停止，请在 [Amazon EC2 forum](#) 中寻求帮助。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。此外，如果您有支持计划，则可在[支持中心](#)创建技术支持案例。

创建替代实例

要在等待 [Amazon EC2 forum](#) 或[支持中心](#)的帮助时尝试解决此问题，请创建替代实例。创建卡住实例的 AMI，并使用新的 AMI 启动一个新实例。

使用控制台创建替代实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择卡住实例。
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。

有关更多信息，请参阅[从实例创建 Linux AMI \(p. 103\)](#)。

5. 从 AMI 启动新实例，验证新实例是否正常运行。
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。

使用 CLI 创建替代实例

1. 使用 `create-image` (AWS CLI) 命令和 `--no-reboot` 选项从卡住实例创建 AMI，如下所示：

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --description "AMI for replacement instance" --no-reboot
```

2. 使用 `run-instances` (AWS CLI) 命令从 AMI 启动新实例，如下所示：

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large --key-name MyKeyPair --security-groups MySecurityGroup
```

3. 验证新实例是否正常运行。
4. 使用 `terminate-instances` (AWS CLI) 命令终止卡住实例，如下所示：

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

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：

(替代) 使用控制台创建替代实例

1. 选择实例并选择 Description、Block devices。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，选择快照。选择您刚刚创建的快照，然后依次选择 Actions、Create Volume。
4. 使用与粘滞的实例相同的操作系统启动实例。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，然后将其附加到新实例以作为其根卷（使用记下的设备名称）。将任何其他非根卷附加到该实例。
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。

排查实例的终止 (关闭) 问题

当实例未处于 `running` 状态时，不会向您收取任何实例使用费用。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。此外，如果您有支持计划，则可在[支持中心](#)创建技术支持案例。

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 Amazon EC2 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 [Amazon EC2 Auto Scaling 用户指南](#) 或 [AWS Elastic Beanstalk 开发人员指南](#)。

通过故障状态检查排查实例故障

如果您的实例未能通过状态检查，以下信息可帮助您解决问题。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，请查看状态检查信息和系统日志。

目录

- [查看状态检查信息 \(p. 964\)](#)
- [检索系统日志 \(p. 964\)](#)
- [诊断基于 Linux 的实例的系统日志错误 \(p. 965\)](#)
- [内存不足：终止进程 \(p. 965\)](#)
- [错误：mmu_update 失败 \(内存管理更新失败\) \(p. 966\)](#)
- [I/O 错误 \(块储存设备故障\) \(p. 967\)](#)
- [I/O 错误：既不是本地磁盘也不是远程磁盘 \(破损的分布式块储存设备\) \(p. 968\)](#)
- [request_module : runaway loop modprobe \(在较旧的 Linux 版本上循环旧内核 modprobe\) \(p. 968\)](#)
- [“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”\(内核与 AMI 不匹配\) \(p. 969\)](#)
- [“FATAL: Could not load /lib/modules”或者“BusyBox”\(内核模块缺失\) \(p. 970\)](#)
- [ERROR：无效内核 \(EC2 不兼容内核\) \(p. 971\)](#)
- [fsck：尝试打开时没有找到此文件或目录...\(未找到文件系统\) \(p. 972\)](#)

- 挂载文件系统时出现一般性错误 (挂载失败) (p. 973)
- VFS：无法在未知块上挂载根 fs (根文件系统不匹配) (p. 975)
- 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. 976)
- XENBUS：设备没有驱动程序... (p. 976)
- ... 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. 977)
- fsck 卡在退出状态... (设备缺失) (p. 978)
- GRUB 提示 (grubdom>) (p. 979)
- 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. 980)
- 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. 981)
- XENBUS：连接设备时超时 (Xenbus 超时) (p. 982)

查看状态检查信息

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 [创建停止、终止、重启或恢复实例的警报 \(p. 555\)](#)。
- 如果您将实例类型更改为了[基于 Nitro 的实例 \(p. 163\)](#)，则您在从没有所需的 ENA 和 NVMe 驱动程序的实例中迁移时状态检查会失败。有关更多信息，请参阅[调整大小的实例的兼容性 \(p. 234\)](#)。
- 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](#)。
- 如果您的实例位于 Auto Scaling 组中，则 Amazon EC2 Auto Scaling 服务会自动启动替换实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 [Auto Scaling 实例的运行状况检查](#)。
- 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

对于无法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. 965](#))
- 错误：mmu_update 失败 (内存管理更新失败) ([p. 966](#))

设备错误

- I/O 错误 (块储存设备故障) ([p. 967](#))
- I/O 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. 968](#))

内核错误

- request_module : runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) ([p. 968](#))
- “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. 969](#))
- “FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) ([p. 970](#))
- ERROR : 无效内核 (EC2 不兼容内核) ([p. 971](#))

文件系统错误

- fsck : 尝试打开时没有找到此文件或目录...(未找到文件系统) ([p. 972](#))
- 挂载文件系统时出现一般性错误 (挂载失败) ([p. 973](#))
- VFS : 无法在未知块上挂载根 fs (根文件系统不匹配) ([p. 975](#))
- 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. 976](#))
- XENBUS : 设备没有驱动程序... ([p. 976](#))
- ... 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. 977](#))
- fsck 卡在退出状态... (设备缺失) ([p. 978](#))

操作系统错误

- GRUB 提示 (grubdom>) ([p. 979](#))
- 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. 980](#))
- 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. 981](#))
- XENBUS : 连接设备时超时 (Xenbus 超时) ([p. 982](#))

内存不足：终止进程

指示内存不足错误的系统日志条目与下方显示的内容类似。

```
[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	请执行该操作
由 Amazon EBS 支持	<p>请执行下列操作之一：</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>请执行下列操作之一：</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	请执行该操作
由 Amazon EBS 支持	<p>执行以下步骤：</p> <ol style="list-style-type: none">停止实例。分离该卷。尝试恢复该卷。 <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">重新将卷附加到实例。分离该卷。
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>

对于此实例类型	请执行该操作
	<p style="text-align: center;">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>

I/O 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)
```

```
OMB 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	请执行该操作
由 Amazon EBS 支持	<p>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)。</p> <p>选项 1：终止实例并启动新实例，指定 <code>-kernel</code> 和 <code>-ramdisk</code> 参数。</p> <p>选项 2：</p> <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。

“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	请执行该操作
由 Amazon EBS 支持	执行以下步骤：

对于此实例类型	请执行该操作
	<ol style="list-style-type: none"> 1. 停止实例。 2. 修改配置以使用较新的内核。 3. 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. 创建使用较新内核的 AMI。 2. 终止实例。 3. 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... ...
Begin: Running /scripts/init-premount ...
Done.
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/sda1 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 根卷没有正确附加为 /dev/sda1

建议采取的措施

对于此实例类型	请执行该操作
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. 分离并修复该卷。4. 将卷附加到实例。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	请执行该操作
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。

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	请执行该操作
由 Amazon EBS 支持	<p>执行以下步骤：</p> <ol style="list-style-type: none">1. 停止实例，分离根卷，修补/修改 /etc/fstab 该卷，将其附加到实例，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 卷与重启的实例分离。3. (可选) 通过 AWS Support 寻求技术支持以便恢复数据。

挂载文件系统时出现一般性错误 (挂载失败)

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">分离或出故障的 Amazon EBS 卷。文件系统损坏。匹配错误的内存虚拟磁盘与 AMI 组合 (如 Debian 内存虚拟磁盘和 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	请执行该操作
由 Amazon EBS 支持	<p>执行以下步骤：</p> <ol style="list-style-type: none">停止实例。分离根卷。将根卷附加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分离卷。将卷附加到已停止的实例。启动实例。重新检查实例的状态。

对于此实例类型	请执行该操作
实例存储支持的	请尝试以下任一操作： <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 : 无法在未知块上挂载根 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/sdal 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">设备附加错误。根设备没有附加到正确的设备点。文件系统不是预期的格式。使用旧内核 (如 2.6.16-XenU)。实例上的近期更新内核 (错误更新或更新错误)
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	请执行该操作
由 Amazon EBS 支持	请执行下列操作之一： <ul style="list-style-type: none">停止实例，然后再重启。修改根卷以附加到正确的设备点，可能是 /dev/sdal，而不是 /dev/sda。停止并修改新内核。请参阅您的 Linux 发行版的文档以检查是否有已知更新错误。更改或重新安装内核。
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)
- 实例内核选择错误

建议采取的措施

对于此实例类型	请执行该操作
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. 分离该卷。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)
- 实例内核选择错误

建议采取的措施

对于此实例类型	请执行该操作
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. 分离该卷。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。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... (设备缺失)

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
- 磁盘故障或者已分离

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	<p>尝试以下一个或多个措施以解决此问题：</p> <ul style="list-style-type: none">停止实例，将该卷附加到正在运行的实例。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	<p>尝试以下一个或多个措施以解决此问题：</p> <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	请执行该操作
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 启动一个新实例。 <p>选项 2：修复现有实例：</p> <ol style="list-style-type: none">停止实例。

对于此实例类型	请执行该操作
	<ol style="list-style-type: none">2. 分离根卷文件系统。3. 将根卷文件系统附加到已知正在工作的实例。4. 挂载文件系统。5. 创建 GRUB 配置文件。6. 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。7. 分离文件系统。8. 附加到原始实例。9. 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）。10. 启动实例。
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">1. 使用位于标准位置（/boot/grub/menu.lst）的 GRUB 配置文件创建新 AMI。2. 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）。3. 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。4. 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	请执行该操作
由 Amazon EBS 支持	<p>请执行下列操作之一：</p> <ul style="list-style-type: none">• 修改 AMI 以删除硬编码并重启实例。• 修改实例以删除硬编码 MAC 地址。 <p>OR</p> <p>执行以下步骤：</p> <ol style="list-style-type: none">1. 停止实例。2. 分离根卷。3. 将卷附加到另一个实例并修改卷以删除硬编码 MAC 地址。4. 将卷附加到原始实例。5. 启动实例。
实例存储支持的	<p>请执行下列操作之一：</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	请执行该操作
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。

对于此实例类型	请执行该操作
	<ol style="list-style-type: none">2. 分离失败的实例的根卷。3. 将根卷附加到另一个 Linux 的运行实例 (之后称为“恢复实例”)。4. 连接到恢复实例并挂载失败的实例的根卷。5. 在挂载的根卷上禁用 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>SELINUX=disabled</code> 文件中设置 <code>/mount_point/etc/sysconfig/selinux</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附加到原始实例。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
- 此实例使用的是旧实例内核

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	<p>请执行下列操作之一：</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。

对于此实例类型	请执行该操作
实例存储支持的	请执行下列操作之一： <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。

对无法访问的实例进行故障排除

您可以使用以下方法对无法访问的实例进行故障排除。

目录

- [实例重启 \(p. 983\)](#)
- [实例控制台输出 \(p. 983\)](#)
- [捕获无法访问的实例的屏幕截图 \(p. 984\)](#)
- [主机发生故障时的实例恢复 \(p. 985\)](#)

实例重启

能够重启无法访问的实例对于故障排除和一般实例管理都非常有用。

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 \(p. 456\)](#)。

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

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。

对于 Linux/Unix，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。控制台输出返回缓冲的信息，该信息在实例转变状态（启动、停止、重新引导和终止）之后很快发布。发布的输出不会持续更新；仅当它可能是最大值时。

对于 Windows 实例，实例控制台输出包括最后三个系统事件日志错误。

您可以选择在实例生命周期中随时检索最新的串行控制台输出。仅在 [基于 Nitro 的实例 \(p. 163\)](#) 上支持该选项。它不是通过 Amazon EC2 控制台受支持的。

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

- 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
- 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 \(p. 965\)](#)。

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。该图像可以让您查看实例的状态，更快地处理问题。您可在实例运行时或在其崩溃后生成屏幕截图。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 100 kb。当实例使用 NVIDIA GRID 驱动程序或在裸机实例 (*.metal 类型的实例) 上时，不支持此功能。以下区域提供此功能：

- 美国东部（弗吉尼亚北部）地区
- 美国东部（俄亥俄）区域
- 美国西部（俄勒冈）区域
- 美国西部（加利福利亚北部）区域
- 欧洲（爱尔兰）区域
- 欧洲（法兰克福）区域
- 亚太区域（东京）
- 亚太区域（首尔）
- 亚太区域（新加坡）
- 亚太区域（悉尼）
- 南美洲（圣保罗）区域
- 亚太地区（孟买）区域
- 加拿大（中部）区域
- 欧洲（伦敦）区域
- 欧洲（巴黎）区域

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 (实例)。
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这类事件。

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。

有关更多信息，请参阅[停止和启动您的实例 \(p. 445\)](#)。

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。

有关更多信息，请参阅[创建由实例存储支持的 Linux AMI \(p. 105\)](#)。

正在从错误的卷启动

在某些情况下，您可能会发现某个并非附加到 /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附加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 / 中定义为 /etc/fstab 的卷，在某些发行版中，这是由附加到卷分区的标签决定的。具体来说，您将发现您的 /etc/fstab 与下面类似：

```
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
```

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从中启动的根设备。要解决此问题，请使用相同的 `e2label` 命令更改您不想从中启动实例的附加卷的标签。

某些情况下，在 `/etc/fstab` 中指定 UUID 可以解决此问题。但是，如果两个卷来自同一快照，或者辅助卷是通过主卷的快照创建的，则它们将共享 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
```

更改已附加 ext4 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/
```

更改已附加 xfs 卷的标签

- 使用 `xfs_admin` 命令将卷的标签更改为 / 之外的其他标签。

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1  
writing all SBs  
new label = "old/"
```

如上所示更改卷标签后，您应该能够重新引导实例并在实例引导时让初始虚拟磁盘选择适当的卷。

Important

如果您要分离使用新标签的卷并将它返回到另一实例以用作根卷，则必须再次执行上述过程并将卷标签更改回其原始值。否则，其他实例将不会启动，因为内存虚拟磁盘无法找到标签为 / 的卷。

使用 EC2Rescue for Linux

EC2Rescue for Linux 是一种易于使用的开源工具，可在 Amazon EC2 Linux 实例上运行此工具以通过其包含 100 多个模块的库来诊断和排查常见问题。适用于 EC2Rescue for Linux 的几个常见使用案例包括：收集 `syslog` 和程序包管理器日志，收集资源利用率数据以及诊断/修复已知的有问题的内核参数和常见的 OpenSSH 问题。

Note

如果您使用的是 Windows 实例，请参阅 [EC2Rescue for Windows Server](#)。

目录

- [安装 EC2Rescue for Linux \(p. 987\)](#)
- [使用 EC2Rescue for Linux \(p. 989\)](#)

- 开发 EC2Rescue 模块 (p. 991)

安装 EC2Rescue for Linux

EC2Rescue for Linux 工具可以安装在满足以下先决条件的 Amazon EC2 Linux 实例上。

先决条件

- 支持的操作系统：
 - Amazon Linux 2
 - Amazon Linux 2016.09+
 - SLES 12+
 - RHEL 7+
 - Ubuntu 16.04+
- 软件要求：
 - Python 2.7.9+ 或 3.2+

如果您的系统具有所需的 Python 版本，可以安装标准构建过程。否则，您可以安装捆绑构建过程，其中包括 Python 的最小副本。

安装标准构建过程

1. 从正常工作的 Linux 实例下载 [EC2Rescue for Linux](#) 工具：

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (可选) 在继续操作之前，您可以选择性地验证 EC2Rescue for Linux 安装文件的签名。有关更多信息，请参阅 [\(可选 \) 验证 EC2Rescue for Linux 的签名 \(p. 987\)](#)。
3. 下载 sha256 哈希文件：

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. 验证 tarball 的完整性：

```
sha256sum -c ec2rl.tgz.sha256
```

5. 解压缩 tarball：

```
tar -xvf ec2rl.tgz
```

6. 通过列出帮助文件来验证安装：

```
cd ec2rl-<version_number>
./ec2rl help
```

安装捆绑构建过程

有关指向下载和限制列表的链接，请参阅 [github 上的 EC2Rescue for Linux](#)。

(可选) 验证 EC2Rescue for Linux 的签名

下面是验证基于 Linux 的操作系统的 EC2Rescue for Linux 软件包是否有效的推荐过程。

当您从 Internet 下载应用程序时，我们建议您验证软件发行商的身份，并检查应用程序在发行后是否已遭更改或损坏。这会保护您免于安装含有病毒或其他恶意代码的应用程序版本。

如果您在执行本主题中的步骤后确定适用于 EC2Rescue for Linux 的软件已遭更改或损坏，请不要运行安装文件。否则，可联系 Amazon Web Services。

适用于基于 Linux 的操作系统的 EC2Rescue for Linux 文件是使用 GnuPG (安全数字签名的 Pretty Good Privacy 的开源式执行 (OpenPGP) 标准) 进行签名的。GnuPG (也称为 GPG) 通过数字签名进行身份验证和完整性检查。AWS 发布了公有密钥和签名，可供您用于验证下载的 EC2Rescue for Linux 程序包。有关 PGP 和 GnuPG (GPG) 的更多信息，请访问 <http://www.gnupg.org>。

第一步是与软件发行商建立信任。下载软件发行商的公有密钥，检查公有密钥的所有人是否真为其人，然后将该公有密钥添加到您的密钥环。密钥环是已知公有密钥的集合。验证公有密钥的真实性后，您可以使用它来验证应用程序的签名。

任务

- 安装 GPG 工具 (p. 988)
- 验证并导入公有密钥 (p. 988)
- 验证软件包的签名 (p. 989)

安装 GPG 工具

如果您的操作系统是 Linux 或 Unix，GPG 工具可能已经安装。要测试系统上是否已安装这些工具，请在命令提示符处输入 gpg2。如果已安装 GPG 工具，您会看到 GPG 命令提示。如果没有安装 GPG 工具，您会看到错误信息，告诉您无法找到命令。您可以从存储库安装 GnuPG 包。

在基于 Debian 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：

```
apt-get install gnupg2
```

在基于 Red Hat 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：

```
yum install gnupg2
```

验证并导入公有密钥

本流程的下一步是验证 EC2Rescue for Linux 公有密钥，并在 GPG 密钥环中将其添加为可信任密钥。

验证并导入 EC2Rescue for Linux 公有密钥

1. 在命令提示符处，使用以下命令获取我们的公共 GPG 生成密钥的副本：

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
```

2. 在保存 ec2rl.key 的目录中的命令提示符处，使用以下命令将 EC2Rescue for Linux 公有密钥导入密钥环：

```
gpg2 --import ec2rl.key
```

该命令返回的结果类似于下方内容：

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>" imported
gpg: Total number processed: 1
gpg:                      imported: 1  (RSA: 1)
```

验证软件包的签名

在安装 GPG 工具、验证并导入 EC2Rescue for Linux 公有密钥以及确认 EC2Rescue for Linux 公有密钥可信后，便可以验证 EC2Rescue for Linux 安装脚本的签名。

验证 EC2Rescue for Linux 安装脚本签名

1. 在命令提示符处，运行以下命令以下载安装脚本的签名文件：

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
```

2. 通过在保存 ec2rl.tgz.sig 和 EC2Rescue for Linux 安装文件的目录中的命令提示符处运行以下命令来验证签名。这两个文件都必须存在。

```
gpg2 --verify ./ec2rl.tgz.sig
```

输出应与以下内容类似：

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:           There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

如果输出包含短语 Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"，则意味着已成功验证签名，您可以继续运行 EC2Rescue for Linux 安装脚本。

如果输出包含短语 BAD signature，则检查是否正确执行了此过程。如果您持续获得此响应，请联系 Amazon Web Services，而不要运行之前下载的安装文件。

下面是有关您可能看到的警告的详细信息：

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. 这表示您坚信自己拥有 EC2Rescue for Linux 的可信公有密钥的个人信任级别。理想情况下，您将前往 Amazon Web Services 办公室并亲自接收此密钥。但更常见的情况是，从网站下载此密钥。在这种情况下，该网站是 Amazon Web Services 网站。
- gpg2: no ultimately trusted keys found. 这意味着您 (或您信任的其他人) 对特定密钥不是“绝对信任”。

有关更多信息，请参阅 <http://www.gnupg.org>。

使用 EC2Rescue for Linux

下面是您可以执行以便开始使用此工具的常见任务。

任务

- [运行 EC2Rescue for Linux \(p. 990\)](#)
- [上传结果 \(p. 990\)](#)
- [创建备份 \(p. 991\)](#)
- [获取帮助 \(p. 991\)](#)

运行 EC2Rescue for Linux

您可以运行 EC2Rescue for Linux , 如以下示例所示。

Example 示例 : 运行所有模块

要运行所有模块 , 请运行 EC2Rescue for Linux (不带任何选项) :

```
./ec2rl run
```

有些模块需要根访问权限。如果您不是根用户 , 请使用 sudo 运行这些模块 , 如下所示 :

```
sudo ./ec2rl run
```

Example 示例 : 运行特定模块

要仅运行特定模块 , 请使用 --only-modules 参数 :

```
./ec2rl run --only-modules=module_name --arguments
```

例如 , 此命令运行 dig 模块以查询 amazon.com 域 :

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example 示例 : 查看结果

您可以在 /var/tmp/ec2rl 中查看结果 :

```
cat /var/tmp/ec2rl/logfile_location
```

例如 , 查看 dig 模块的日志文件 :

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

上传结果

如果 AWS Support 需要您提供结果或者需要您从 S3 存储桶分享结果 , 请使用 EC2Rescue for Linux CLI 工具上传结果。EC2Rescue for Linux 命令的输出应提供您需要使用的命令。

Example 示例 : 将结果上传到 AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example 示例：将结果上传到 S3 存储桶

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

有关为 Amazon S3 生成预签名 URL 的更多信息，请参阅[使用预签名 URL 上传对象](#)。

创建备份

使用以下命令为实例、一个或多个卷或者特定设备 ID 创建备份。

Example 示例：使用 Amazon 系统映像 (AMI) 备份实例

```
./ec2rl run --backup=ami
```

Example 示例：备份与实例关联的所有卷

```
./ec2rl run --backup=allvolumes
```

Example 示例：备份特定卷

```
./ec2rl run --backup=volumeID
```

获取帮助

EC2Rescue for Linux 包括帮助文件，为您提供各可用命令的信息和语法。

Example 示例：显示常规帮助

```
./ec2rl help
```

Example 示例：列出可用模块

```
./ec2rl list
```

Example 示例：显示特定模块的帮助

```
./ec2rl help module_name
```

例如，使用以下命令显示 dig 模块的帮助文件：

```
./ec2rl help dig
```

开发 EC2Rescue 模块

模块使用 YAML 编写，这是一种数据序列化标准。模块的 YAML 文件包括一个文档，用于表示模块及其属性。

添加模块属性

下表列出了可用的模块属性。

属性	描述
name	模块的名称。该名称长度应少于或等于 18 个字符。
version	模块的版本号。
标题	模块的简短说明性标题。此值的长度应少于或等于 50 个字符。
helptext	<p>模块的详细说明。每一行的长度应少于或等于 75 个字符。如果模块使用必需或可选参数，请在 helptext 值中包括这些参数。</p> <p>例如：</p> <div style="border: 1px solid black; padding: 5px;"><pre>helptext: !!str Collect output from ps for system analysis Consumes --times= for number of times to repeat Consumes --period= for time period between repetition</pre></div>
placement	运行模块的阶段。支持的值： <ul style="list-style-type: none">• prediagnostic• run• postdiagnostic
language	编写模块代码使用的语言。支持的值： <ul style="list-style-type: none">• bash• python <p>Note</p> <p>Python 代码必须同时兼容 Python 2.7.9+ 和 Python 3.2+。</p>
remediation	指示模块是否支持修正。支持的值为 True 或 False。 模块默认为 False (如果不存在)，这使其成为那些不支持修正的模块的可选属性。
content	整个脚本代码。
constraint	包含限制值的对象的名称。
domain	说明如何分组或分类模块的描述符。所包括的模块组使用以下域： <ul style="list-style-type: none">• application• net

属性	描述
	<ul style="list-style-type: none"> • os • performance
class	由模块执行的任务类型的描述符。所包括的模块组使用以下类： <ul style="list-style-type: none"> • collect (从程序收集输出) • diagnose (基于一组标准确定通过/失败) • gather (复制文件并写入特定文件)
distro	此模块支持的 Linux 发行版的列表。所包含的模块组使用以下发行版： <ul style="list-style-type: none"> • alami (Amazon Linux) • rhel • ubuntu • suse
required	模块从 CLI 选项使用的必需参数。
optional	模块可使用的可选参数。
software	模块中使用的软件可执行文件。此属性用于指定默认情况下未安装的软件。EC2Rescue for Linux 逻辑在运行模块之前确保这些程序存在并且可执行。
package	可执行文件的源软件包。此属性用于随软件提供软件包的详细信息，包括用于下载或者获取更多信息的 URL。
sudo	指示运行模块是否需要根访问权限。 您无需在模块脚本中实施 sudo 检查。如果值为 true，则 EC2Rescue for Linux 逻辑仅在执行用户具有根访问权限时才运行模块。
perfimpact	指示模块对其运行环境是否会产生重大性能影响。如果值为 true 并且没有 --perfimpact=true 参数，则跳过模块。
parallelexclusive	指定需要互斥的程序。例如，所有指定“bpf”的模块以串行方式运行。

添加环境变量

下表列出了可用的环境变量。

环境变量	描述
EC2RL_CALLPATH	<code>ec2rl.py</code> 的路径。此路径可用于定位 lib 目录和使用分发的 Python 模块。
EC2RL_WORKDIR	诊断工具的主 tmp 目录。 默认值: <code>/var/tmp/ec2rl</code> .

环境变量	描述
EC2RL_RUNDIR	用于存储所有输出的目录。 默认值: /var/tmp/ec2rl/<date×tamp>.
EC2RL_GATHEREDDIR	用于放置收集的模块数据的根目录。 默认值:/var/tmp/ec2rl/<date×tamp>/mod_out/gathered/.
EC2RL_NET_DRIVER	为实例上第一个(按照字母顺序排序)非虚拟网络接口使用的驱动程序。 示例： <ul style="list-style-type: none">• xen_netfront• ixgbevf• ena
EC2RL_SUDO	如果 EC2Rescue for Linux 以根身份运行，则为 true；否则为 false。
EC2RL_VIRT_TYPE	由实例元数据提供的虚拟化类型。 示例： <ul style="list-style-type: none">• default-hvm• default-paravirtual
EC2RL_INTERFACES	系统上的接口枚举列表。该值为包含名称的字符串，例如 eth0、eth1 等。这通过 functions.bash 生成，仅对其来源模块可用。

使用 YAML 语法

在您构建模块 YAML 文件时，应注意以下事项：

- 三个连字符 (---) 表示文档的明确开始位置。
- !ec2rlcore.module.Module 标签指示 YAML 分析器在从数据流创建对象时调用哪个构造函数。您可在 module.py 文件内部查找构造函数。
- !!str 标签告知 YAML 解析器不尝试确定数据的类型，而是将内容解释为字符串文本。
- 坚线字符 (!) 告知 YAML 解析器该值为文字类型的标量。在这种情况下，解析器包括所有空格。对于模块而言这非常重要，因为保留了缩进和换行字符。
- YAML 标准缩进为两个空格，在下例中可以看到。请确保您为脚本保留了标准缩进(例如，对于 Python 为四个空格)，然后在模块文件中将全部内容缩进两个空格。

模块示例

示例 1 (mod.d/ps.yaml)：

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
```

```
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
    Collect output from ps for system analysis
    Requires --times= for number of times to repeat
    Requires --period= for time period between repetition
placement: !!str run
package:
- !!str
language: !!str bash
content: !!str |
#!/bin/bash
error_trap()
{
    printf "%0.s=" {1..80}
    echo -e "\nERROR: \"$BASH_COMMAND\" exited with an error on line ${BASH_LINENO[0]}"
    exit 0
}
trap error_trap ERR

# read-in shared function
source functions.bash
echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every $period
seconds."
for i in $(seq 1 $times); do
    ps auxww
    sleep $period
done
constraint:
requires_ec2: !!str False
domain: !!str performance
class: !!str collect
distro: !!str alami ubuntu rhel suse
required: !!str period times
optional: !!str
software: !!str
sudo: !!str False
perfimpact: !!str False
parallelexclusive: !!str
```

发送诊断中断 (仅限高级用户)

Warning

诊断中断旨在供高级用户使用。使用不正确可能会对实例产生负面影响。向实例发送诊断中断可能使实例崩溃并重新启动，从而导致数据丢失。

您可以将诊断中断发送到无法访问或无响应的 Linux 实例以手动触发内核错误。

在出现内核错误时，Linux 操作系统通常会发生崩溃并重启。操作系统的具体行为取决于其配置。内核错误也可用于使实例的操作系统内核执行任务，例如生成崩溃转储文件。然后，您可以使用崩溃转储文件中的信息进行根本原因分析并调试实例。

崩溃转储数据由操作系统在实例本身上本地生成。

在向您的实例发送诊断中断之前，建议您查阅操作系统的文档，然后进行必要的配置更改。

目录

- [支持的实例类型 \(p. 996\)](#)
- [先决条件 \(p. 996\)](#)
- [发送诊断中断 \(p. 998\)](#)

支持的实例类型

所有基于 Nitro 的实例类型（A1 除外）都支持诊断中断。有关更多信息，请参阅 [基于 Nitro 的实例 \(p. 163\)](#)。

先决条件

在使用诊断中断之前，必须配置实例的操作系统。这可确保它在发生内核错误时执行所需的操作。

将 Amazon Linux 2 配置为在发生内核错误时生成崩溃转储

1. 连接到您的实例。
2. 安装 kexec 和 kdump。

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

3. 配置内核以便为辅助内核预留适当的内存量。要预留的内存量取决于实例的总可用内存。使用首选文本编辑器打开 /etc/default/grub 文件，找到以 GRUB_CMDLINE_LINUX_DEFAULT 开始的行，然后按以下格式添加 crashkernel 参数：crashkernel=*memory_to_reserve*。例如，要预留 160MB，请修改 grub 文件，如下所示：

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. 保存更改并关闭 grub 文件。
5. 重新构建 GRUB2 配置文件。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. 在基于 Intel 和 AMD 处理器的实例上，send-diagnostic-interrupt 命令将未知的非屏蔽中断 (NMI) 发送到实例。您必须将内核配置为在收到未知 NMI 时发生崩溃。使用首选文本编辑器打开 /etc/sysctl.conf 文件，并添加以下内容。

```
kernel.unknown_nmi_panic=1
```

7. 重启实例并重新连接到它。
8. 使用正确的 crashkernel 参数验证是否已启动内核。

```
$ grep crashkernel /proc/cmdline
```

以下示例输出指示成功的配置。

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
rd.shell=0
```

9. 确认 kdump 服务正在运行。

```
[ec2-user ~]$ systemctl status kdump.service
```

以下示例输出显示在 kdump 服务正在运行的情况下结果。

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
             enabled)
     Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
       Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
    Main PID: 2503 (code=exited, status=0/SUCCESS)
```

Note

默认情况下，崩溃转储文件将保存到 /var/crash/。要更改位置，请使用首选文本编辑器修改 /etc/kdump.conf 文件。

将 Amazon Linux 配置为在发生内核错误时生成崩溃转储

1. 连接到您的实例。
2. 安装 kexec 和 kdump。

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

3. 配置内核以便为辅助内核预留适当的内存量。要预留的内存量取决于实例的总可用内存。

```
$ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
```

例如，要为崩溃内核预留 160MB，请使用以下命令。

```
$ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
```

4. 在基于 Intel 和 AMD 处理器的实例上，send-diagnostic-interrupt 命令将未知的非屏蔽中断 (NMI) 发送到实例。您必须将内核配置为在收到未知 NMI 时发生崩溃。使用首选文本编辑器打开 /etc/sysctl.conf 文件，并添加以下内容。

```
kernel.unknown_nmi_panic=1
```

5. 重启实例并重新连接到它。
6. 使用正确的 crashkernel 参数验证是否已启动内核。

```
$ grep crashkernel /proc/cmdline
```

以下示例输出指示成功的配置。

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. 确认 kdump 服务正在运行。

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

如果该服务正在运行，则命令将返回 kdump is operational 响应。

Note

默认情况下，崩溃转储文件将保存到 /var/crash/。要更改位置，请使用首选文本编辑器修改 /etc/kdump.conf 文件。

配置 SUSE Linux Enterprise、Ubuntu 或 Red Hat Enterprise Linux

请参阅以下网站：

- [SUSE Linux Enterprise](#)
- [Ubuntu](#)
- [Red Hat Enterprise Linux \(RHEL\)](#)

发送诊断中断

在完成必要的配置更改后，您可以使用 AWS CLI 或 Amazon EC2 API 将诊断中断发送到实例。

将诊断中断发送到实例 (AWS CLI)

使用 [send-diagnostic-interrupt](#) 命令并指定实例 ID。

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

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	描述	发布日期
会话管理器	2016-11-15	您可以从 Amazon EC2 控制台使用实例来启动会话管理器会话。有关更多信息，请参阅 使用会话管理器连接到 Linux 实例 (p. 444) 。	2019 年 12 月 18 日
EC2 队列 中对 按需容量预留 的支持	2016-11-15	您可以将 EC2 队列 配置为在启动 按需实例 时首先 使用 按需容量预留。有关更多信息，请参阅 对 按需实例 使用 容量预留 (p. 395) 。	2019 年 12 月 16 日
实例类型建议	2016-11-15	AWS Compute Optimizer 提供了 Amazon EC2 实例建议，以帮助您提高性能和/或节省资金。有关更多信息，请参阅 获取实例类型建议 (p. 237) 。	2019 年 12 月 3 日
Inf1 实例	2016-11-15	Inf1 实例采用 AWS Inferentia，AWS Inferentia 是一个机器学习推理芯片，旨在以低成本提供高性能。	2019 年 12 月 3 日
支持 AWS Outposts	2016-11-15	您可以在 Outpost 子网内启动实例。有关更多信息，请参阅 AWS Outposts 用户指南 。	2019 年 12 月 3 日
支持 AWS 本地区域	2016-11-15	您可以在本地区域子网内启动实例。有关更多信息，请参阅 区域、可用区和本地区域	2019 年 12 月 3 日
专用主机 和主机资源组	2016-11-15	专用主机 现在可以与主机资源组一起使用。有关更多信息，请参阅 在主机资源组中启动实例 (p. 339) 。	2019 年 12 月 2 日
专用主机 共享	2016-11-15	您现在可以跨 AWS 账户共享 专用主机。有关更多信息，请参阅 使用共享专用主机 (p. 348) 。	2019 年 12 月 2 日
账户级别的默认积分规范	2016-11-15	您可以在每个 AWS 区域的账户级别设置每个可突增性能实例系列的默认积分规范。有关更多信息，请参阅 设置账户的默认积分规范 (p. 199) 。	2019 年 11 月 25 日
专用主机	2016-11-15	您可以配置专用主机以支持实例系列中的多种实例类型。有关更多信息，请参阅 使用专用主机 (p. 336) 。	2019 年 11 月 21 日
Amazon EBS 快速快照还原	2016-11-15	您可以在 EBS 快照上启用快速快照还原，以确保从快照创建的 EBS 卷在创建时已完全初始化，并立即交付所有预配置性能。有关更多信息，请参阅 Amazon EBS 快速快照还原 (p. 859) 。	2019 年 11 月 20 日
实例元数据服务版本 2	2016-11-15	您可以使用 实例元数据服务版本 2，这是一种面向会话的方法，用于请求实例元数据。有关更多信息，请参阅 配置实例元数据服务 (p. 499) 。	2019 年 11 月 19 日
Elastic Fabric Adapter	2016-11-15	Elastic Fabric Adapter 现在可以与 Intel MPI 2019 Update 6 配合使用。有关更多信息，请参阅 EFA 和 MPI 入门 (p. 640) 。	2019 年 11 月 15 日

功能	API 版本	描述	发布日期
对按需 Windows 实例的休眠支持	2016-11-15	您可以使按需 Windows 实例休眠。有关支持的 Windows AMI 的更多信息，请参阅 休眠先决条件 (p. 449) 。	2019 年 10 月 14 日
排队购买 预留实例	2016-11-15	您最早可以提前三年排队购买 Reserved Instance。有关更多信息，请参阅 排队购买 (p. 255) 。	2019 年 10 月 4 日
G4 实例	2016-11-15	G4 实例使用 NVIDIA Tesla GPU，并为使用 CUDA 或机器学习框架的通用 GPU 计算以及使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。	2019 年 9 月 19 日
诊断中断	2016-11-15	您可以将诊断中断发送到无法访问或无响应的实例以触发内核错误（Linux 实例上）或蓝屏/停止错误（Windows 实例上）。有关更多信息，请参阅 发送诊断中断（仅限高级用户）(p. 995) 。	2019 年 8 月 14 日
容量优化的分配策略	2016-11-15	使用 EC2 队列或 Spot 队列，现在您可以通过为正在启动的实例数量提供最佳容量来从 Spot 池启动 Spot 实例。有关更多信息，请参阅 配置 EC2 队列以实现容量优化 (p. 394) 。	2019 年 8 月 12 日
按需容量预留	2016-11-15	您现在可以跨 AWS 账户共享容量预留。有关更多信息，请参阅 使用共享容量预留 (p. 367) 。	2019 年 7 月 29 日
Elastic Fabric Adapter	2016-11-15	EFA 现在支持 Open MPI 3.1.4 和 Intel MPI 2019 Update 4。有关更多信息，请参阅 Elastic Fabric Adapter (p. 638) 。	2019 年 7 月 26 日
在创建时标记启动模板	2016-11-15	您可以在创建时标记启动模板。有关更多信息，请参阅 标记资源 (p. 942) 。	2019 年 7 月 24 日
最高总价	2016-11-15	您可以为 EC2 队列和 Spot 队列中的所有按需实例和 Spot 实例指定每小时最高价格。有关更多信息，请参阅 EC2 队列中的 控制支出 (p. 396) 和 Spot 队列中的 控制支出 (p. 283) 。	2019 年 7 月 1 日
EC2 Instance Connect	2016-11-15	EC2 Instance Connect 提供了一种简单且安全的方法以使用安全 Shell (SSH) 连接到实例。有关更多信息，请参阅 使用 EC2 Instance Connect 连接到 Linux 实例 (p. 428) 。	2019 年 6 月 27 日
主机恢复	2016-11-15	如果在专用主机上发生意外硬件故障，则在新主机上自动重新启动实例。有关更多信息，请参阅 主机恢复 (p. 351) 。	2019 年 6 月 5 日
Amazon EBS 多卷快照	2016-11-15	跨附加到 EC2 实例的多个 EBS 卷拍摄准确的时间点、数据协调和崩溃一致性快照。	2019 年 5 月 29 日
Amazon EBS 默认加密	2016-11-15	在区域中启用默认加密后，将使用用于 EBS 加密的默认 CMK 加密在区域中创建的所有新 EBS 卷。有关更多信息，请参阅 默认加密 (p. 853) 。	2019 年 5 月 23 日
标记 VPC 终端节点、终端节点服务和终端节点服务配置	2016-11-15	您可以标记 VPC 终端节点、终端节点服务和终端节点服务配置。有关更多信息，请参阅 标记资源 (p. 942) 。	2019 年 5 月 13 日

功能	API 版本	描述	发布日期
I3en 实例	2016-11-15	具有高达 100 Gbps 网络带宽的新实例。	2019 年 5 月 8 日
Elastic Fabric Adapter	2016-11-15	您可以将 Elastic Fabric Adapter 附加到实例以加快高性能计算 (HPC) 应用程序的速度。有关更多信息，请参阅 Elastic Fabric Adapter (p. 638) 。	2019 年 4 月 29 日
T3a 实例	2016-11-15	使用 AMD EYPC 处理器的新实例。	2019 年 4 月 24 日
M5ad 和 R5ad 实例	2016-11-15	使用 AMD EYPC 处理器的新实例。	2019 年 3 月 27 日
标记 专用主机 预留	2016-11-15	您可以标记 专用主机 预留。有关更多信息，请参阅 标记 专用主机预留 (p. 348) 。	2019 年 3 月 14 日
M5、M5d、R5、R5d 和 z1d 裸机实例	2016-11-15	为应用程序提供对主机服务器物理资源的直接访问的新实例。	2019 年 2 月 13 日
分区置放群组	2016-11-15	分区置放群组跨逻辑分区来分配实例，以确保一个分区中的实例不会与其他分区中的实例共享基础硬件。有关更多信息，请参阅 分区置放群组 (p. 663) 。	2018 年 12 月 20 日
p3dn.24xlarge 实例	2016-11-15	新的 p3dn.24xlarge 实例提供 100 Gbps 的网络带宽。	2018 年 12 月 7 日
休眠 EC2 Linux 实例	2016-11-15	如果 Linux 实例已启用休眠并且满足休眠先决条件，则可以休眠该实例。有关更多信息，请参阅 使 Linux 实例休眠 (p. 447) 。	2018 年 11 月 28 日
Amazon Elastic Inference 加速器	2016-11-15	您可以将 Amazon EI 加速器附加到实例上以添加 GPU 支持的加速，从而减少运行深度学习推理的成本。有关更多信息，请参阅 Amazon Elastic Inference (p. 522) 。	2018 年 11 月 28 日
实例具有 100 Gbps 网络带宽	2016-11-15	新 C5n 实例可以使用高达 100 Gbps 的网络带宽。	2018 年 11 月 26 日
实例配有基于 Arm 的处理器	2016-11-15	新 A1 实例可以显著节省成本，非常适合横向扩展和基于 Arm 的工作负载。	2018 年 11 月 26 日
Spot 控制台推荐实例队列	2016-11-15	Spot 控制台根据 Spot 最佳实践（实例多元化）推荐实例队列，以满足您应用程序所需的最低硬件规格（vCPU、内存和存储）。有关更多信息，请参阅 创建Spot 队列请求 (p. 300) 。	2018 年 11 月 20 日
新 EC2 队列请求类型：instant	2016-11-15	EC2 队列现在支持新请求类型 instant，您可用它来跨实例类型和购买模式同步预配置容量。instant 请求在 API 响应中返回启动的实例，不采取更多操作，使您能够控制是否启动实例以及何时启动。有关更多信息，请参阅 EC2 队列请求类型 (p. 393) 。	2018 年 11 月 14 日
实例配有 AMD EYPC 处理器	2016-11-15	新的通用型 (M5a) 和内存优化型实例 (R5a) 为微服务、小到中型数据库、虚拟桌面、开发和测试环境、业务应用程序等提供了更低的价格选项。	2018 年 11 月 6 日

功能	API 版本	描述	发布日期
Spot 节省信息	2016-11-15	您可以查看单个 Spot 队列或所有 Spot 实例通过使用 Spot 实例节省的费用。有关更多信息，请参阅 通过购买 Spot 实例 实现节省 (p. 287) 。	2018 年 11 月 5 日
用于优化 CPU 选项的控制台支持	2016-11-15	启动实例时，您可以使用 Amazon EC2 控制台优化 CPU 选项以适应特定的工作负载或业务需求。有关更多信息，请参阅 优化 CPU 选项 (p. 480) 。	2018 年 10 月 31 日
控制台支持从实例创建启动模板	2016-11-15	您可以通过 Amazon EC2 控制台，以实例为基础创建新的启动模板。有关更多信息，请参阅 创建启动模板 (p. 380) 。	2018 年 10 月 30 日
按需容量预留	2016-11-15	您可在特定可用区中为 Amazon EC2 实例预留容量任意持续时间。这使您能够独立于预留实例 (RI) 提供的账单折扣来创建和管理容量预留。有关更多信息，请参阅 按需容量预留 (p. 360) 。	2018 年 10 月 25 日
自带 IP 地址 (BYOIP)	2016-11-15	您可将自己的全部或部分公有 IPv4 地址从本地网络引入到 AWS 账户中。在将地址范围引入 AWS 中之后，它会在您的账户中显示为地址池。您可从地址池创建弹性 IP 地址，并将其用于您的 AWS 资源。有关更多信息，请参阅 自带 IP 地址 (BYOIP) (p. 587) 。	2018 年 10 月 23 日
g3s.xlarge 实例	2016-11-15	引入 g3s.xlarge 实例，扩展了计算加速型 G3 实例系列的范围。	2018 年 10 月 11 日
在创建时标记专用主机和控制台支持	2016-11-15	您可在创建时标记专用主机，并可以使用 Amazon EC2 控制台管理专用主机标签。有关更多信息，请参阅 分配专用主机 (p. 337) 。	2018 年 10 月 8 日
内存增强型实例	2016-11-15	这些实例专门针对运行大型内存中数据库构建。它们通过直接访问主机硬件提供裸机性能。有关更多信息，请参阅 内存优化型实例 (p. 207) 。	2018 年 9 月 27 日
f1.4xlarge 实例	2016-11-15	f1.4xlarge 实例的引入扩展了计算加速型 F1 实例系列的范围。	2018 年 9 月 25 日
针对 Spot 队列计划扩展的控制台支持。	2016-11-15	根据日期和时间增加或减少队列的当前容量。有关更多信息，请参阅 使用计划扩展功能扩展 Spot 队列 (p. 319) 。	2018 年 9 月 20 日
T3 实例	2016-11-15	T3 实例是下一代可突增的通用实例类型，可提供基准水平的 CPU 性能，并且只要需要，就能够随时突增 CPU 利用率。有关更多信息，请参阅 可突增性能实例 (p. 175) 。	2018 年 8 月 21 日
EC2 队列的分配策略	2016-11-15	您可以指定是按价格（最低价格优先）还是优先级（最高优先级优先）来满足按需容量。您可以指定在其中分配您的目标 Spot 容量的 Spot 池数量。有关更多信息，请参阅 Spot 实例的分配策略 (p. 394) 。	2018 年 7 月 26 日
Spot 队列的分配策略	2016-11-15	您可以指定是按价格（最低价格优先）还是优先级（最高优先级优先）来满足按需容量。您可以指定在其中分配您的目标 Spot 容量的 Spot 池数量。有关更多信息，请参阅 Spot 实例分配策略 (p. 282) 。	2018 年 7 月 26 日

功能	API 版本	描述	发布日期
R5 和 R5d 实例	2016-11-15	R5 和 R5d 实例非常适合高性能数据库、分布式内存中缓存和内存中分析。R5d 实例带有 NVMe 实例存储卷。有关更多信息，请参阅 内存优化型实例 (p. 207) 。	2018 年 7 月 25 日
z1d 实例	2016-11-15	这些实例为需要高每核心性能和大量内存的应用设计，例如电子设计自动化 (EDA) 和关系数据库。这些实例带有 NVME 实例存储卷。有关更多信息，请参阅 内存优化型实例 (p. 207) 。	2018 年 7 月 25 日
自动化快照生命周期	2016-11-15	您可以使用 Amazon 数据生命周期管理器 来自动创建和删除 EBS 卷的快照。有关更多信息，请参阅 自动化 Amazon EBS 快照生命周期 (p. 831) 。	2018 年 7 月 12 日
启动模板 CPU 选项	2016-11-15	在使用命令行工具创建启动模板时，您可以优化 CPU 选项以适合特定工作负载或业务需求。有关更多信息，请参阅 创建启动模板 (p. 380) 。	2018 年 7 月 11 日
标记专用主机	2016-11-15	您可以标记专用主机。有关更多信息，请参阅 标记专用主机 (p. 344) 。	2018 年 7 月 3 日
i3.metal 实例	2016-11-15	i3.metal 实例为应用程序提供对主机服务器的物理资源 (如处理器和内存) 的直接访问。有关更多信息，请参阅 存储优化型实例 (p. 215) 。	2018 年 5 月 17 日
获取最新的控制台输出	2016-11-15	使用 <code>get-console-output</code> AWS CLI 命令时，您可以检索某些实例类型的最新控制台输出。	2018 年 5 月 9 日
优化 CPU 选项	2016-11-15	启动实例时，您可以优化 CPU 选项以适应特定的工作负载或业务需求。有关更多信息，请参阅 优化 CPU 选项 (p. 480) 。	2018 年 5 月 8 日
EC2 队列	2016-11-15	您可以使用 EC2 队列启动一组包含不同 EC2 实例类型和可用区以及不同个按需实例、Reserved Instance 和 Spot 实例购买模型的实例。有关更多信息，请参阅 启动 EC2 队列 (p. 391) 。	2018 年 5 月 2 日
Spot 队列 中的按需实例	2016-11-15	您可以在 Spot 队列请求中包含按需容量请求，以确保始终拥有实例容量。有关更多信息，请参阅 Spot 队列的工作原理 (p. 281) 。	2018 年 5 月 2 日
创建时标记 EBS 快照	2016-11-15	在创建过程中，您可以将标签应用于快照。有关更多信息，请参阅 创建 Amazon EBS 快照 (p. 815) 。	2018 年 4 月 2 日
更改置放群组	2016-11-15	您可以将实例移入或移出置放群组，也可以更改实例的置放群组。有关更多信息，请参阅 更改实例的置放群组 (p. 667) 。	2018 年 3 月 1 日
较长的资源 ID	2016-11-15	您可以为更多资源类型启用较长 ID 格式。有关更多信息，请参阅 资源 ID (p. 933) 。	2018 年 2 月 9 日
网络性能改进	2016-11-15	在其他实例或 Amazon S3 之间发送或接收网络通信时，集群置放群组之外的实例现在可以受益于增加的带宽。有关更多信息，请参阅 联网和存储功能 (p. 164) 。	2018 年 1 月 24 日
标记弹性 IP 地址	2016-11-15	您可以标记您的弹性 IP 地址。有关更多信息，请参阅 标记弹性 IP 地址 (p. 592) 。	2017 年 12 月 21 日

功能	API 版本	描述	发布日期
Amazon Linux 2	2016-11-15	Amazon Linux 2 是 Amazon Linux 的新版本。它可为您的应用程序提供稳定、安全且高性能的基础。有关更多信息，请参阅 Amazon Linux (p. 144) 。	2017 年 12 月 13 日
Amazon Time Sync Service	2016-11-15	您可以使用 Amazon Time Sync Service 在您的实例上保持准确的时间。有关更多信息，请参阅 Linux 实例设置时间 (p. 476) 。	2017 年 11 月 29 日
T2 无限	2016-11-15	T2 无限实例可以突增到基准以上所需的时间。有关更多信息，请参阅 可突增性能实例 (p. 175) 。	2017 年 11 月 29 日
启动模板	2016-11-15	启动模板可以包含用于启动实例的全部或部分参数，而无需在每次启动实例时都指定这些参数。有关更多信息，请参阅 通过启动模板启动实例 (p. 379) 。	2017 年 11 月 29 日
分布置放	2016-11-15	建议在具有少量应单独放置的重要实例的应用程序中使用分布置放群组。有关更多信息，请参阅 分布置放群组 (p. 663) 。	2017 年 11 月 29 日
H1 实例	2016-11-15	H1 实例设计用于高性能大数据工作负载。有关更多信息，请参阅 存储优化型实例 (p. 215) 。	2017 年 11 月 28 日
M5 实例	2016-11-15	M5 实例是下一代通用型计算实例。这些实例兼顾了计算、内存、存储和网络资源。	2017 年 11 月 28 日
Spot 实例休眠	2016-11-15	在发生中断时，Spot 服务可以将 Spot 实例休眠。有关更多信息，请参阅 休眠中断的 Spot 实例 (p. 327) 。	2017 年 11 月 28 日
Spot 队列目标跟踪	2016-11-15	您可以为 Spot 队列设置目标跟踪扩展策略。有关更多信息，请参阅 使用目标跟踪策略扩展Spot 队列 (p. 317) 。	2017 年 11 月 17 日
Spot 队列与 Elastic Load Balancing 集成	2016-11-15	您可以将一个或多个负载均衡器附加到 Spot 队列。	2017 年 11 月 10 日
X1e 实例	2016-11-15	X1e 实例非常适合高性能数据库、内存中数据库和其他内存密集型企业应用程序。有关更多信息，请参阅 内存优化型实例 (p. 207) 。	2017 年 11 月 28 日
C5 实例	2016-11-15	C5 实例专为计算密集型应用程序设计。有关更多信息，请参阅 计算优化型实例 (p. 202) 。	2017 年 11 月 6 日
合并和拆分可转换预留实例	2016-11-15	您可以合并两个或更多可转换预留实例，也可以将其与新可转换预留实例交换。您还可以使用修改过程将可转换预留实例拆分为较小的预留。有关更多信息，请参阅 交换可转换预留实例 (p. 270) 。	2017 年 11 月 6 日
P3 实例	2016-11-15	P3 实例是下一代计算优化型 GPU 实例。有关更多信息，请参阅 Linux 加速计算实例 (p. 222) 。	2017 年 10 月 25 日
修改 VPC 租赁	2016-11-15	可以将 VPC 的实例租赁属性从 <code>dedicated</code> 改为 <code>default</code> 。有关更多信息，请参阅 更改 VPC 的租赁 (p. 360) 。	2017 年 10 月 16 日
按秒计费	2016-11-15	Amazon EC2 按秒对基于 Linux 的使用收费，最低收取一分钟的费用。	2017 年 10 月 2 日

功能	API 版本	描述	发布日期
在中断时停止	2016-11-15	您可以指定在 Spot 实例中断时 Amazon EC2 应将其停止还是终止。有关更多信息，请参阅 中断行为 (p. 326) 。	2017 年 9 月 18 日
给 NAT 网关加标签	2016-11-15	您可以给自己的 NAT 网关加标签。有关更多信息，请参阅 标记资源 (p. 942) 。	2017 年 9 月 7 日
安全组规则说明	2016-11-15	您可以向安全组规则添加说明。有关更多信息，请参阅 安全组规则 (p. 769) 。	2017 年 8 月 31 日
恢复弹性 IP 地址	2016-11-15	如果您释放了一个在 VPC 中使用的弹性 IP 地址，则可能能够恢复它。有关更多信息，请参阅 恢复弹性 IP 地址 (p. 594) 。	2017 年 8 月 11 日
标记 Spot 队列实例。	2016-11-15	您可以将您的 Spot 队列配置为自动标记其启动的实例。	2017 年 7 月 24 日
G3 实例	2016-11-15	G3 实例为使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。G3 实例还提供 NVIDIA GRID 虚拟工作站功能，支持 4 台分辨率高达 4096x2160 的监视器。有关更多信息，请参阅 Linux 加速计算实例 (p. 222) 。	2017 年 7 月 13 日
F1 实例	2016-11-15	F1 实例代表下一代加速计算实例。有关更多信息，请参阅 Linux 加速计算实例 (p. 222) 。	2017 年 4 月 19 日
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 标记资源 (p. 942) 。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. 712) 。	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. 215) 。	2017 年 2 月 23 日
在附加的 EBS 卷上进行修改	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 Amazon EBS 弹性卷 (p. 841) 。	2017 年 2 月 13 日
附加 IAM 角色	2016-11-15	您可以为现有实例附加、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. 749) 。	2017 年 2 月 9 日
专用 Spot 实例	2016-11-15	您可在 Virtual Private Cloud (VPC) 中的单租户硬件上运行 Spot 实例。有关更多信息，请参阅 指定 Spot 实例的租期 (p. 290) 。	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. 574) 。	2016 年 12 月 1 日

功能	API 版本	描述	发布日期
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. 207) 。	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要求的应用程序。有关更多信息，请参阅 可突增性能实例 (p. 175) 。	2016 年 11 月 30 日
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. 222) 。	2016 年 29 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
Spot 队列的自动扩展		现在，您可以为 Spot 队列设置扩展策略。有关更多信息，请参阅 Spot 队列的自动扩展 (p. 315) 。	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. 616) 。	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. 933) 。	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. 819) 。	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. 984) 。	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. 207) 。	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. 785) 。	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. 540) 。	2016 年 3 月 23 日
Spot 队列的 CloudWatch 指标		您现在可以获取 Spot 队列的 CloudWatch 指标。有关更多信息，请参阅 Spot 队列的 CloudWatch 指标 (p. 313) 。	2016 年 3 月 21 日

功能	API 版本	描述	发布日期
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. 274) 。	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. 933) 。	2016 年 1 月 13 日
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 实例与 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. 683) 。	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 可突增性能实例 (p. 175) 。	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. 333) 。	2015 年 11 月 23 日
Spot 实例持续时间	2015-10-01	现在 , 您可以为 Spot 实例指定持续时间。有关更多信息 , 请参阅 定义 Spot 实例的持续时间 (p. 290) 。	2015 年 10 月 6 日
Spot 队列 修改请求	2015-10-01	您现在可以修改 Spot 队列请求的目标容量。有关更多信息 , 请参阅 修改Spot 队列请求 (p. 304) 。	2015 年 9 月 29 日
Spot 队列多样化分配策略	2015-04-15	您现在可以使用单个 Spot 队列请求在多个 Spot 池中分配 Spot 实例。有关更多信息 , 请参阅 Spot 实例分配策略 (p. 282) 。	2015 年 9 月 15 日
Spot 队列实例权重	2015-04-15	您现在可以定义每个实例类型在应用程序性能中所占的容量单位 , 并相应地为每个 Spot 池的 Spot 实例调整愿意支付的金额。有关更多信息 , 请参阅 Spot 队列实例权重 (p. 284) 。	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. 555) 。	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 可突增性能实例 (p. 175) 。	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

功能	API 版本	描述	发布日期
Spot 队列	2015-04-15	您可以管理 Spot 实例的集合或队列，而不必管理单独的 Spot 实例请求。有关更多信息，请参阅 Spot 队列的工作原理 (p. 281) 。	2015 年 5 月 18 日
将弹性 IP 地址迁移至 EC2-Classic	2015-04-15	您无法将已分配为在 EC2-Classic 中使用的弹性 IP 地址迁移到 VPC 中使用。有关更多信息，请参阅 从 EC2-Classic 迁移弹性 IP 地址 (p. 676) 。	2015 年 5 月 15 日
将具有多个磁盘的虚拟机作为 AMI 导入	2015-03-01	虚拟机导入过程现在支持将具有多个磁盘的虚拟机作为 AMI 导入。有关更多信息，请参阅 VM Import/Export 用户指南 中的 使用虚拟机导入/导出将虚拟机作为映像导入 。	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>下一代 Amazon EC2 密集存储实例，经过优化，适用于需要顺序访问直接附加的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. 215)。</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. 463)。</p>	2015 年 1 月 12 日
C4 实例		<p>下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动力学。</p> <p>有关更多信息，请参阅 计算优化型实例 (p. 202)。</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. 678) 。	2015 年 1 月 7 日

功能	API 版本	描述	发布日期
Spot 实例终止通知		<p>防范Spot 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 Spot 实例中断通知，该通知可在 Amazon EC2 必须停止或终止您的 Spot 实例时，提前两分钟发出警告。</p> <p>有关更多信息，请参阅 Spot 实例中断通知 (p. 329)。</p>	2015 年 1 月 5 日
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。有关更多信息，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 可突增性能实例 (p. 175) 。	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。这些卷可提供不超过 10 毫秒的延迟，能突增至 3000 IOPS 很长时间，基准性能为 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. 787) 。	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. 851) 。	2014 年 5 月 21 日
R3 实例	2014-02-01	<p>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。</p> <p>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 实例类型。</p>	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. 951) 。	2014 年 1 月 28 日

功能	API 版本	描述	发布日期
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 实例类型 。	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. 215) 。	2013 年 12 月 19 日
更新了 M3 实例	2013-10-15	M3 实例大小、m3.xlarge 和 m3.2xlarge 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 操作的资源级权限。有关更多信息以及示例策略，请参阅 适用于 Amazon EC2 的 Identity and Access Management (p. 701) 。	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 实例类型 。	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. 389) 。	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. 222) 。	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 使用启动实例向导启动实例 (p. 375) 。	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 修改预留实例 (p. 265) 。	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。有关更多信息，请参阅 修改预留实例 (p. 265) 。	2013 年 9 月 11 日

功能	API 版本	描述	发布日期
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. 578) 。	2013 年 8 月 20 日
授予资源级权限	2013-06-15	Amazon EC2 支持新的亚马逊资源名称 (ARN) 和条件键。有关更多信息，请参阅 Amazon EC2 的 IAM 策略 (p. 704) 。	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. 819) 。	2013 年 6 月 11 日
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 标记您的 Amazon EC2 资源 (p. 940) 。	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	以下实例类型现在可作为 EBS 优化的实例启动：c1.xlarge、m2.2xlarge、m3.xlarge 和 m3.2xlarge。 有关更多信息，请参阅 Amazon EBS 优化的实例 (p. 863) 。	2013 年 3 月 19 日
将 AMI 从一个区域复制到另一个区域	2013-02-01	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。 有关更多信息，请参阅 复制 AMI (p. 138) 。	2013 年 3 月 11 日
在默认 VPC 中启动实例	2013-02-01	根据各区域的情况，您的 AWS 账户可以在 EC2-Classic 或 VPC 中启动实例，或者仅在 VPC 中启动。如果您只能在 VPC 中启动实例，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。	2013 年 3 月 11 日
内存增强型集群 (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. 819) 。	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 年 10 月 1 日	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 Amazon EBS 的 Amazon CloudWatch 指标 (p. 889) 。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 EBS 卷状态检查 (p. 804) 。	2012 年 11 月 20 日

功能	API 版本	描述	发布日期
Linux 内核		已更新了 AKI ID；已重组了发行版内核；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 实例类型 。	2012 年 10 月 31 日
Spot 实例请求状态	2012 年 10 月 1 日	Spot 实例请求状态简化了确定您的 Spot 请求状态的过程。	2012 年 10 月 14 日
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 年 8 月 15 日	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 年 7 月 20 日	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. 785) 。	2012 年 7 月 31 日
适用于 Amazon EC2 的高 I/O 实例	2012 年 6 月 15 日	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 Spot 实例功能。		现在您可以按照以下方式管理您的 Spot 实例： <ul style="list-style-type: none">• 使用 Auto Scaling 启动配置指定您愿意为 Spot 实例支付的金额，并设置计划来指定您愿意为 Spot 实例 支付的金额。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的在 Auto Scaling 组中启动 Spot 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 Spot 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 年 5 月 1 日	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 年 5 月 1 日	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

功能	API 版本	描述	发布日期
八倍超大型集群计算	2012 年 4 月 1 日	添加了对 VPC 中的 <code>cc2.8xlarge</code> 实例的支持。	2012 年 4 月 26 日
AWS Marketplace AMIs	2012 年 4 月 1 日	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
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 年 12 月 15 日	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 年 12 月 15 日	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 年 12 月 1 日	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. 595) 。	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 年 11 月 1 日	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 年 11 月 1 日	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. 527) 。	2011 年 11 月 16 日
Amazon EC2 集群计算实例类型		Amazon EC2 八倍超大型集群计算 (<code>cc2.8xlarge</code>) 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 Spot 实例	2011-07-15	增加了 Amazon VPC 中的 Spot 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 Spot 实例。通过在 VPC 中启动 Spot 实例，Spot 实例的用户可以享受到 Amazon VPC 带来的好处。	2011 年 10 月 11 日
新 Linux AMI 版本		增加了 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

功能	API 版本	描述	发布日期
适用于 CLI 工具用户的简化的虚拟机导入过程	2011-07-15	ImportInstance 和 ImportVolume 的增强功能简化了虚拟机导入过程；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 ResumeImport，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
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，虚拟机导入现在支持 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 虚拟机导入连接器		适用于 VMware vCenter 虚拟设备 (连接器) 的 1.1 版本的 Amazon EC2 虚拟机导入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		增加了 AKI 版本从 1.01 变到 1.02 的有关信息。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 启用您自己的 Linux 内核 (p. 154) 。	2011 年 6 月 20 日
Spot 实例可用区定价更改	2011 年 5 月 15 日	增加了 Spot 实例可用区定价功能的有关信息。在本版本中，我们增加了新的可用区定价选项，当您查询 Spot 实例请求和 Spot 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 Spot 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 适用于 Amazon EC2 的 Identity and Access Management (p. 701) 。	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 启用您自己的 Linux 内核 (p. 154) 。	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. 356) 。	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. 243) 。	2011 年 3 月 27 日

功能	API 版本	描述	发布日期
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 适用于基于 GPU 的加速计算实例的 AMI (p. 226) 。	2011 年 3 月 15 日
元数据信息	2011 年 1 月 1 日	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. 499) 和 实例元数据类别 (p. 514) 。	2011 年 3 月 11 日
适用于 VMware vCenter 的 Amazon EC2 虚拟机导入连接器。		已添加适用于 VMware vCenter 虚拟设备(连接器)的 Amazon EC2 虚拟机导入连接器的有关信息。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 将 Amazon EBS 卷与实例分离 (p. 810) 。	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. 459) 。	2011 年 2 月 23 日
校正 Amazon's CentOS 5.4 AMI 上的集群实例的 Clock Drift		已添加如何为 Amazon's CentOS 5.4 AMI 上的集群实例校正 Clock Drift 的有关信息。	2011 年 1 月 25 日
VM Import	2010-11-15	已添加有关虚拟机导入的信息，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
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. 937) 和 标记您的 Amazon EC2 资源 (p. 940) 。	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 可突增性能实例 (p. 175) 。	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 适用于 Amazon EC2 的 Identity and Access Management (p. 701) 。	2010 年 9 月 2 日

功能	API 版本	描述	发布日期
集群实例	2010-06-15	Amazon EC2 为您的高性能计算 (HPC) 应用程序提供了集群计算实例。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 实例类型 。	2010 年 7 月 12 日
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 Amazon EBS 的 Amazon CloudWatch 指标 (p. 889) 。	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 实例类型 。	2010 年 2 月 22 日