
Amazon Elastic Compute Cloud

Microsoft Windows 实例用户指南



Amazon Elastic Compute Cloud: Microsoft Windows 实例用户指南

Copyright © 2016 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Table of Contents

什么是 Amazon EC2 ?	1
Amazon EC2 的功能	1
如何开始使用 Amazon EC2	2
相关服务	2
访问 Amazon EC2	3
Amazon EC2 定价	3
PCI DSS 合规性	4
基本基础设施	5
Amazon 系统映像和实例	5
地区和可用区域	6
存储	6
根设备卷	8
网络和安全性	10
AWS Identity and Access Management	10
Windows Server 与 Amazon EC2 Windows 实例之间的区别	10
设计您的应用程序以在 Amazon EC2 Windows 实例上运行	11
设置	13
注册 AWS	13
创建 IAM 用户	14
创建密钥对	15
创建 Virtual Private Cloud (VPC)	16
创建安全组	17
入门	19
概述	19
先决条件	20
步骤 1 : 启动实例	20
步骤 2 : 连接到您的实例	21
步骤 3 : 清除您的实例	23
后续步骤	23
最佳实践	24
教程	26
教程 : 部署 WordPress 博客	26
先决条件	26
安装 Microsoft Web 平台安装程序	27
安装 WordPress	27
配置安全密钥	28
配置网站标题和管理员	29
公开您的 WordPress 网站	29
后续步骤	30
教程 : 安装 WAMP 服务器	30
教程 : 安装 WIMP 服务器	33
教程 : 提高应用程序的可用性	36
先决条件	37
对应用程序进行扩展和负载均衡	37
测试负载均衡器	39
教程 : 远程管理您的实例	40
启动新实例	40
向您的用户账户授予对 SSM 的访问权限	41
使用 EC2 控制台发送命令	41
使用适用于 Windows PowerShell 的 AWS 工具发送命令	42
教程 : 设置 Windows HPC 集群	43
先决条件	43
步骤 1 : 设置您的 Active Directory 域控制器	43
步骤 2 : 配置头节点	46
步骤 3 : 设置计算节点	48

步骤 4：扩展您的 HPC 计算节点（可选）	49
运行 Lizard 性能测量应用程序	50
Active Directory 安全组的 IP 权限	50
HPC 集群安全组的 IP 权限	54
Amazon 系统映像	60
使用 AMI	60
创建您自己的 AMI	61
购买、共享和出售 AMI	61
取消注册您的 AMI	61
AWS Windows AMI	61
选择初始 Windows AMI	61
保持您的 AMI 为最新	62
AMI 类型	62
启动许可	62
根设备存储	63
查找 Windows AMI	65
使用 Amazon EC2 控制台查找 Windows AMI	65
使用 AWS CLI 查找 AMI	66
使用适用于 Windows PowerShell 的 AWS 工具 查找 AMI	66
查找 Windows Server 2003 AMI	67
共享 AMI	67
查找共享 AMI	68
将 AMI 设为公用	69
将 AMI 与特定 AWS 账户共享	70
使用书签	71
共享 Windows AMI 指导原则	71
付费 AMI	72
出售 AMI	73
查找付费 AMI	73
购买付费 AMI	74
获取实例的产品代码	74
使用付费支持	74
付费和支持 AMI 的账单	75
管理 AWS Marketplace 订阅	75
创建 Amazon EBS 支持的 Windows AMI	76
创建 Amazon EBS 支持的 AMI 的概述	76
从正在运行的实例创建 Windows AMI	76
创建实例存储支持的 Windows AMI	78
实例存储支持的 Windows AMI	79
准备创建实例存储支持的 Windows AMI	79
捆绑实例存储支持的 Windows 实例	80
注册实例存储支持的 Windows AMI	81
带加密快照的 AMI	82
涉及加密的 EBS 快照的 AMI 情景	82
复制 AMI	84
复制您拥有的 AMI	85
跨 AWS 账户复制 AMI	85
跨区域复制 AMI	85
复制到加密	86
AMI 复制方案	87
使用控制台或命令行复制 AMI	88
停止待处理的 AMI 复制操作	89
取消注册您的 AMI	89
清除由 Amazon EBS 支持的 AMI	89
清除由实例存储支持的 AMI	90
Windows AMI 版本	91
配置设置和驱动程序	92
更新您的 Windows 实例	92

确定实例版本	92
AWS Windows AMI 版本	93
映像更改	103
订阅 Windows AMI 通知	104
升级或迁移 Windows Server 实例	105
使用 Sysprep 创建标准 Amazon 系统映像 (AMI)	105
在您开始之前	105
将 Sysprep 与 EC2Config 服务结合使用	105
将 Sysprep 与 EC2Config 服务一起运行	108
使用 EC2Config 对 Sysprep 进行故障排除	109
实例	110
实例类型	110
可用实例类型	111
硬件规格	112
联网和存储功能	112
实例限量	113
T2 实例	113
C4 实例	116
GPU 实例	118
I2 实例	119
D2 实例	121
Hi1 实例	122
HS1 实例	123
T1 微型实例	124
X1 实例	130
调整实例大小	133
实例购买选项	136
实例生命周期	137
预留实例	138
计划实例	157
竞价型实例	160
专用主机	201
实例生命周期	213
实例启动	214
停止和启动实例 (仅限 Amazon EBS 支持的实例)	214
实例重启	214
实例停用	215
实例终止	215
重启、停止与终止之间的区别	215
启动	216
连接	225
停止和启动	227
重启	230
停用	231
终止	232
恢复	237
配置实例	238
实例元数据和用户数据	239
使用 EC2Config	250
半虚拟化驱动程序	272
设置密码	288
设置时间	292
管理配置	294
加入 AWS 域	299
将日志数据发送到 CloudWatch	308
配置辅助私有 IP 地址	319
升级实例	324
远程管理您的实例	331

组件和概念	332
先决条件	333
设置托管实例	335
安装 SSM 代理	337
委派访问权限	338
执行命令	345
查看命令输出	366
创建 SSM 文档	368
共享 SSM 文档	373
演练	379
取消命令	390
监控命令	391
Run Command 疑难解答	399
导入和导出虚拟机	401
将 VM 作为镜像导入 Amazon EC2	402
将 VM 作为实例导入 Amazon EC2	418
导出 Amazon EC2 实例	431
故障排除	434
监控	440
自动和手动监控	441
自动监控工具	442
手动监控工具	442
监控的最佳实践	443
监控实例状态	443
实例状态检查	444
计划的事件	448
使用 CloudWatch 监控您的实例	452
启用详细监控	452
列出可用指标	453
获取指标的统计数据	459
绘制指标图形	474
创建 CloudWatch 警报	476
创建停止、终止、重启或恢复实例的警报	483
网络与安全性	509
密钥对	510
使用 Amazon EC2 创建密钥对	510
将您自己的密钥对导入 Amazon EC2	512
在 Windows 上检索密钥对的公有密钥	514
验证您的密钥对指纹	514
删除您的密钥对	514
安全组	515
EC2-Classic 安全组	515
EC2-VPC 安全组	516
安全组规则	516
默认安全组	518
自定义安全组	518
正在创建安全组	519
描述您的安全组	520
向安全组添加规则	520
从安全组中删除规则	521
正在删除安全组	521
API 和命令概览	521
Controlling Access	522
网络访问您的实例：	523
Amazon EC2 权限属性	523
IAM 和 Amazon EC2	523
IAM 策略	525
IAM 角色	565

网络访问	570
Amazon VPC	572
使用 VPC 的优势	572
EC2-Classic 与 EC2-VPC 的区别	573
在 EC2-Classic 与 EC2-VPC 之间共享和访问资源	575
实例类型仅在 VPC 中可用	576
Amazon VPC 文档	577
支持的平台	577
ClassicLink	578
从 EC2-Classic 迁移到 VPC	588
实例 IP 寻址	597
私有 IP 地址和内部 DNS 主机名	597
公有 IP 地址和外部 DNS 主机名	598
弹性 IP 地址	599
Amazon DNS 服务器	599
EC2-Classic 和 EC2-VPC 之间的 IP 地址区别	599
确定您的公有、私有和弹性 IP 地址	599
分配公有 IP 地址	601
多个私有 IP 地址	602
弹性 IP 地址	606
弹性 IP 地址基础信息	606
EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别	607
使用弹性 IP 地址	608
将反向 DNS 用于电子邮件应用程序	612
弹性 IP 地址限额	612
弹性网络接口	612
每个实例类型的每个网络接口的私有 IP 地址	613
网络接口的公有 IP 地址	615
创建一个管理网络	615
使用您的 VPC 中的网络和安全设备	616
通过不同子网的工作负载/角色创建双主机实例。	616
创建一个低成本、高可用性解决方案	616
监控您的网络接口上的 IP 流量	616
有关配置弹性网络接口的最佳实践	617
创建弹性网络接口	617
删除弹性网络接口	618
查看有关弹性网络接口的详细信息	618
在启动实例时连接弹性网络接口	618
将弹性网络接口连接至已停止的实例或正在运行的实例	619
从实例中分离弹性网络接口	620
更改弹性网络接口的安全组	621
更改弹性网络接口的源/目标检查	621
将弹性 IP 地址与弹性网络接口相关联	622
解除弹性 IP 地址与弹性网络接口的关联	622
更改弹性网络接口的终止行为	622
添加或编辑弹性网络接口的描述	623
添加或编辑弹性网络接口的标签	623
置放群组	624
置放群组的限制	624
将实例启动到置放群组中	625
删除置放群组	626
网络 MTU	627
极大帧 (9001 MTU)	627
路径 MTU 发现	627
查看两台主机之间的路径 MTU	628
在您的 Amazon EC2 实例上检查并设置 MTU	628
故障排除	630
增强型联网	630

增强联网类型	630
在实例上启用增强联网	630
启用增强联网 : Intel 82599 VF	630
启用增强联网 : ENA	633
存储	637
Amazon EBS	638
Amazon EBS 的功能	639
EBS 卷	640
EBS 快照	676
EBS 优化	683
EBS 加密	686
EBS 性能	689
实例存储	701
实例存储生命周期	702
实例存储卷	702
添加实例存储卷	704
SSD 实例存储卷	707
Amazon S3	707
Amazon S3 和 Amazon EC2	708
实例卷限制	709
特定于 Linux 的卷限制	710
特定于 Windows 的卷限制	710
带宽与容量	710
设备命名	710
可用设备名称	711
设备名称注意事项	711
块储存设备映射	712
块储存设备映射的概念	712
AMI 块储存设备映射	714
实例块储存设备映射	716
将磁盘映射到卷	720
列出使用 Windows 磁盘管理的磁盘	720
使用 Windows PowerShell 列出磁盘	722
磁盘设备到设备名称的映射	724
使用公用数据集	726
公用数据集概念	726
查找公用数据集	726
从快照创建公用数据集卷	727
连接和装载公用数据集卷	728
资源和标签	729
资源位置	729
资源 ID	730
使用较长的 ID	731
控制对较长 ID 设置的访问	733
列出并筛选您的资源	734
高级搜索	734
使用控制台列出资源	735
使用控制台筛选资源	736
使用 CLI 和 API 列出并筛选	737
标记您的成员资源	737
有关标签的基本知识	738
标签限制	738
标记资源以便于计费	740
通过控制台使用标签	740
通过 CLI 或 API 使用标签	745
服务限制	746
查看当前限制	746
申请提高限制	747

使用率报告	747
可用报告	747
开始设置使用率报告	747
向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限	749
实例使用率	750
预留实例使用率	753
AWS Systems Manager for Microsoft System Center VMM	758
特色	758
限制	759
要求	759
入门	759
设置	759
注册 AWS	759
设置用户的访问	760
部署插件	761
提供您的 AWS 证书	762
管理 EC2 实例	763
创建 EC2 实例	763
查看实例	764
连接到您的实例	765
重启您的实例	765
停止实例	766
启动实例	766
终止实例	766
导入 VM	766
先决条件	767
导入您的虚拟机	767
检查导入任务状态	768
备份已导入的实例	768
故障排除	769
错误：无法安装插件	769
安装错误	769
检查日志文件	770
导入 VM 时的错误	770
卸载插件	770
AWS Management Pack	771
适用于 System Center 2012 的 AWS Management Pack 概述	772
适用于 System Center 2007 R2 的 AWS Management Pack 概述	773
下载	774
System Center 2012	774
System Center 2007 R2	775
部署	775
步骤 1：安装 AWS Management Pack	775
步骤 2：配置观察程序节点	777
步骤 3：创建 AWS 运行方式账户	778
步骤 4：运行添加监视向导	780
步骤 5：配置端口和终端节点	784
使用	785
视图	785
发现	799
监视器	800
规则	800
事件	801
运行状况模型	801
自定义 AWS Management Pack	803
升级	803
System Center 2012	804
System Center 2007 R2	804

卸载	805
System Center 2012	805
System Center 2007 R2	805
故障排除	805
错误 4101 和 4105	805
错误 4513	806
事件 623	806
事件 2023 和 2120	806
事件 6024	807
System Center 2012 — Operations Manager 的一般故障排除	807
System Center 2007 R2 的一般故障排除	807
AWS Diagnostics for Microsoft Windows Server	809
分析规则	809
分析当前实例	810
收集来自离线实例的数据	812
数据文件存储	812
故障排除	813
对无法访问的实例进行故障排除	813
如何捕获无法访问的实例的屏幕截图	813
常见的屏幕截图	814
常见问题	820
将 EC2 Windows 实例启动至目录服务还原模式 (DSRM)	820
Windows 启动后，CPU 使用率短时增高	822
无控制台输出	823
实例立即终止	823
远程桌面无法连接到远程计算机	824
RDP 显示黑屏而不是桌面	826
实例失去网络连接或计划的任务不按预期方式运行	826
实例容量不足	827
超出实例限制	827
网络上不可用的 Windows Server 2012 R2	827
常见消息	827
"密码不可用"	827
"密码尚不可用"	828
"无法检索 Windows 密码"	828
"等待元数据服务"	828
"无法激活 Windows"	831
"Windows 不是正版 (0x80070005)"	832
"没有终端服务器许可服务器可提供许可证"	832
文档历史记录	833
AWS 词汇表	845

什么是 Amazon EC2？

Abstract

将 Amazon EC2 用于 AWS 云中可扩展的计算容量，以便在没有硬件约束的情况下开发和部署应用程序。

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 IP 地址，也称为 *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](#)。

Amazon EC2 使您能够在我们的高性能、可靠、经济的云计算平台上运行任何基于 Windows 的兼容解决方案。有关更多信息，请参阅[运行 Windows Server 和 SQL 的 Amazon EC2](#)。

有关在 AWS 上运行网站的更多信息，请参阅[网站和网站托管](#)。

如何开始使用 Amazon EC2

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

设置和运行

- [Amazon EC2 的设置 \(p. 13\)](#)
- [Amazon EC2 Windows 实例入门 \(p. 19\)](#)

基础知识

- [适用于 Windows 的 Amazon EC2 基本基础设施 \(p. 5\)](#)
- [实例类型 \(p. 110\)](#)
- [标签 \(p. 737\)](#)

网络和安全性

- [Amazon EC2 密钥对和 Windows 实例 \(p. 510\)](#)
- [安全组 \(p. 515\)](#)
- [弹性 IP 地址 \(p. 606\)](#)
- [Amazon EC2 和 Amazon VPC \(p. 572\)](#)

存储

- [Amazon EBS \(p. 638\)](#)
- [实例存储 \(p. 701\)](#)

使用 Windows 实例

- [Windows Server 与 Amazon EC2 Windows 实例之间的区别 \(p. 10\)](#)
- [设计您的应用程序以在 Amazon EC2 Windows 实例上运行 \(p. 11\)](#)
- [Getting Started with AWS: 托管一个 .NET Web 应用程序](#)

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

相关服务

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

- [Auto Scaling 用户指南](#)

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

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

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

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](#)。

访问 Amazon EC2

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

如果倾向于使用命令行界面，您可使用以下选项：

AWS 命令行界面 (CLI)

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

适用于 Windows PowerShell 的 AWS 工具

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

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

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

Amazon EC2 定价

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

Amazon EC2 为实例提供以下购买选项：

按需实例

您只需要按小时支付使用实例的费用，无需长期购买或预付款。

预留实例

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

竞价型实例

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

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

要计算示例设置环境的成本，请参阅 [AWS 成本中心](#)。

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

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

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

PCI DSS 合规性

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

适用于 Windows 的 Amazon EC2 基本基础设施

Abstract

了解适用于 Windows 的 Amazon EC2 实例的基础设施。

开始使用 Amazon EC2 后，如果了解其基础设施组件以及它们与您自己的数据中心的比较或对比情况，会非常有用。

概念

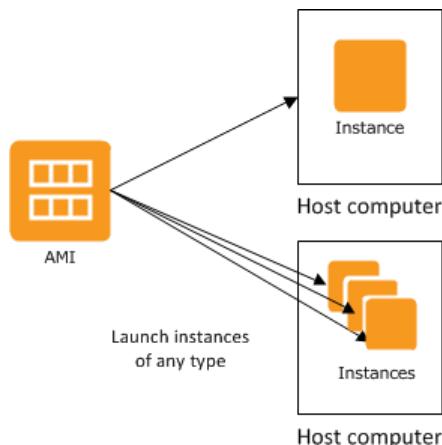
- [Amazon 系统映像和实例 \(p. 5\)](#)
- [地区和可用区域 \(p. 6\)](#)
- [存储 \(p. 6\)](#)
- [根设备卷 \(p. 8\)](#)
- [网络和安全性 \(p. 10\)](#)
- [AWS Identity and Access Management \(p. 10\)](#)
- [Windows Server 与 Amazon EC2 Windows 实例之间的区别 \(p. 10\)](#)
- [设计您的应用程序以在 Amazon EC2 Windows 实例上运行 \(p. 11\)](#)

Amazon 系统映像和实例

*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，这是作为云中虚拟服务器运行的 AMI 副本。

Amazon 发布了许多供公众使用的包含常见软件配置的 AMI。此外，AWS 开发人员社区的会员也发布了他们的定制 AMI。您也可以创建一个或多个定制 AMI；这样能让您快速轻松地启动能满足您一切需求的新实例。例如，如果您的应用程序是网站或 Web 服务，您的 AMI 可能会包含 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。

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。每个实例类型提供不同的计算和存储能力。根据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，选择一种实例类型。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](#)。您也可以从一个 AMI 启动多个实例，如下图所示。



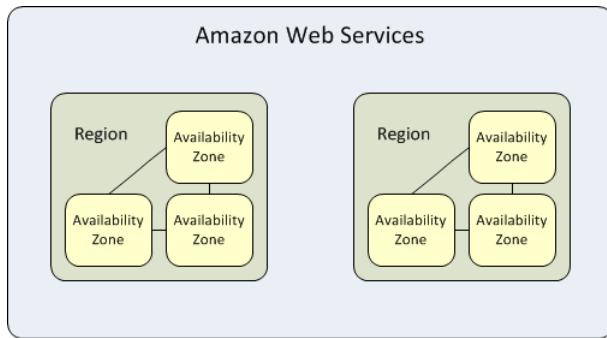
您的 Windows 实例会一直运行，直到您停止或终止运行或者实例失败为止。如果实例失败了，您可以从 AMI 启动一个新实例。

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](#)。

地区和可用区域

Amazon 在世界不同地区有数据中心（例如，北美、欧洲和亚洲）。与此相应，Amazon EC2 可用于不同地区。通过在不同地区启动实例，您可以将您的应用程序设计地更接近特定客户的要求，或满足不同地区的法律或其他要求。Amazon EC2 使用定价因区域而异（有关根据区域定价的更多信息，请参阅 [Amazon EC2 定价](#)）。

每个区域包含许多不同的称为“可用区域”(Availability Zones)的位置。每个可用区都被设计成不受其他可用区故障的影响，并提供低价、低延迟的网络连接，以连接到同一地区其他可用区。通过启动独立可用区内实例，您可以保护您的应用程序不受单一位置故障的影响。



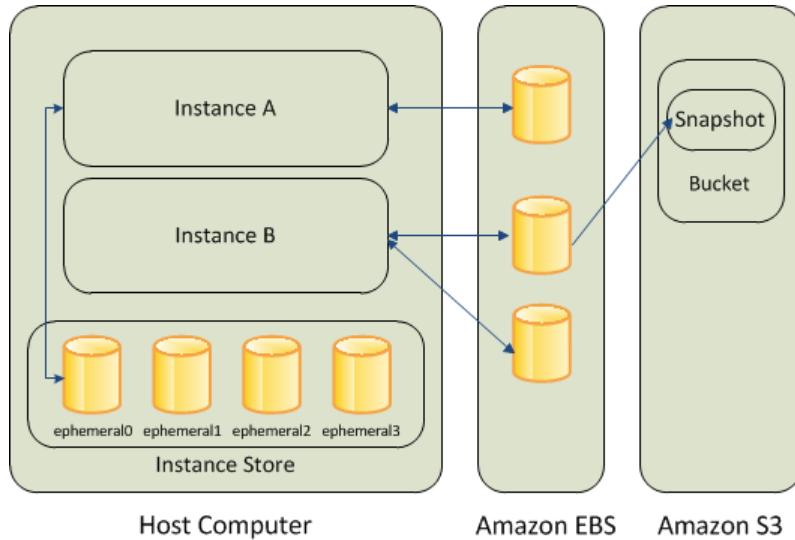
有关区域和可用区的更多信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的[使用区域和可用区](#)。

存储

使用 Amazon EC2 时，您可能会有需要存储的数据。Amazon EC2 为您提供以下存储选择：

- [Amazon Elastic Block Store \(Amazon EBS\)](#)
- [Amazon EC2 实例存储 \(p. 701\)](#)
- [Amazon Simple Storage Service \(Amazon S3\)](#)

下图显示了这些不同存储类型之间的关系。

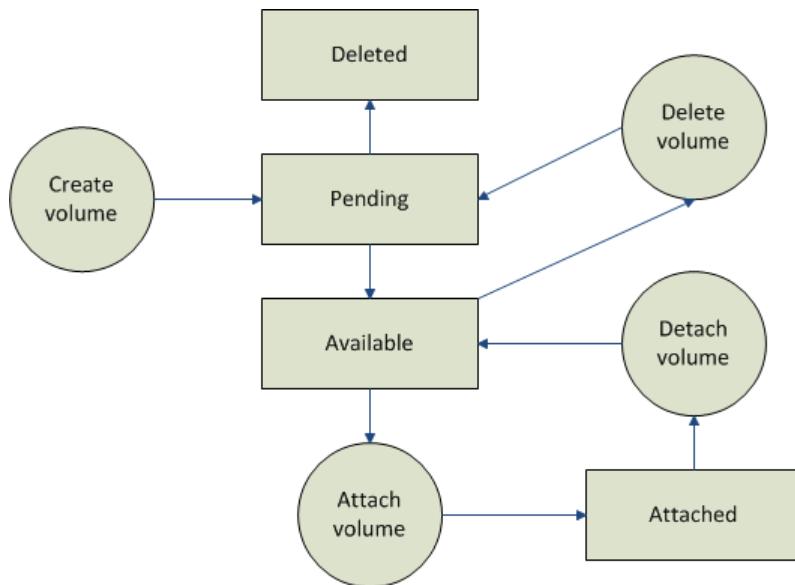


Amazon EBS 卷

对于大多数使用案例，我们推荐使用 Amazon EBS 存储类型。Amazon EBS 为您的实例提供持久的数据块级存储。Amazon EBS 实质上是您可以连接到一个正在运行的实例的硬盘。

对于那些需要建立数据库、文件系统或可访问原始数据块级存储的应用程序来说，Amazon EBS 是特别合适的。

正如上图所示，您可以将多个卷连接到一个实例。同时，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。您可以从该快照创建一个新的 Amazon EBS 卷，并把它连接到另一个实例。您也可以从实例中分离出一个卷，并把它连接到另一个实例。下图显示了一个 EBS 卷的生命周期。



有关 Amazon EBS 卷的更多信息，请参阅 [Amazon Elastic Block Store\(Amazon EBS\) \(p. 638\)](#)。

实例存储

所有的实例类型（Micro 实例外）都提供实例存储，为您的实例提供短暂的数据块级存储。这是一种通过物理方式连接到主机的存储方法。当连接的实例被停止或终止时，实例存储卷上的数据不再保留。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。

实例存储是一种低价的暂时存储选择。如果您对数据持久性没有要求，您可以使用实例存储卷。

Amazon S3

Amazon S3 是一种面向 Internet 的存储服务。它提供了一个简单的 Web 服务接口，使您能够在网络上的任何地方存储和检索任意数量的数据。有关 Amazon S3 的更多信息，请参阅 [Amazon S3 产品页](#)。

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。您可以使用实例存储支持的或 Amazon Elastic Block Store (Amazon EBS) 支持的 AMI 来启动 Amazon EC2 Windows 实例。

- 从 Amazon EBS 支持的 AMI 启动的实例使用 Amazon EBS 卷作为根设备。Amazon EBS 支持的 AMI 的根设备卷是 Amazon EBS 快照。使用 Amazon EBS 支持的 AMI 启动实例时，系统会从 EBS 快照创建根 EBS 卷并将其附加到实例。然后，系统会使用根设备卷启动实例。
- 从实例存储支持的 AMI 启动的实例使用实例存储卷作为根设备。实例存储支持的 AMI 的根设备卷的映像最初会存储在 Amazon S3 中。使用实例存储支持的 AMI 启动实例时，其根设备的映像将从 Amazon S3 复制到实例的根分区。然后，系统会使用根设备卷启动实例。



Important

实例存储唯一支持的 Windows AMI 是用于 Windows Server 2003 的 AMI。实例存储支持的实例不具有 Windows Server 的较高版本所需的可用磁盘空间。

有关实例存储支持的 AMI 与 Amazon EBS 支持的 AMI 之间的区别的汇总，请参阅 [根设备存储 \(p. 63\)](#)。

确定 AMI 的根设备类型

您可以使用控制台或命令行来确定 AMI 的根设备类型。

使用控制台确定 AMI 的根设备类型

- 打开 Amazon EC2 控制台。
- 在导航窗格中，单击 AMI，然后选择 AMI。
- 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)

确定实例的根设备类型

您可以使用控制台或命令行来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，单击 Instances，然后选择实例。
3. 检查说明选项卡上根设备类型的值，如下所示：
 - 如果值为 ebs，那么这是一个由 Amazon EBS 支持的实例。
 - 如果值为 instance store，则表示这是由实例存储提供支持的实例。

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

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

使用控制台在启动时将实例的根设备卷更改为持久保留

1. 打开 Amazon EC2 控制台。
2. 从 Amazon EC2 控制台控制面板中，单击 Launch Instance (启动实例)。
3. 在 Choose an Amazon Machine Image (AMI) (选择一个Amazon 系统映像 (AMI)) 页面上，选择要使用的 AMI 并单击 Select (选择)。
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，然后单击 Launch (启动)。

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

使用命令行将实例的根设备卷更改为持久保留

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)

网络和安全性

您可以在以下两个平台之一中启动实例：EC2-Classic 和 EC2-VPC。在 EC2-Classic 中启动的实例会分配得一个公有 IP 地址。默认情况下，启动到 EC2-VPC 中的实例只有在启动到默认 VPC 中时才会分配到公有 IP 地址。启动到非默认 VPC 中的实例必须在启动时特别分配一个公有 IP 地址，否则您必须修改您的子网的默认公有 IP 地址行为。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅 [支持的平台 \(p. 577\)](#)。

实例可能会因为您不可控的原因失败或终止。如果一个实例失败了，您又启动了一个替代实例，这个替代实例的公用 IP 地址和原来那个不同。然而，如果您的应用程序需要一个静态 IP 地址，Amazon EC2 可为您提供弹性 IP 地址。有关更多信息，请参阅 [Amazon EC2 实例 IP 寻址 \(p. 597\)](#)。

您可以使用安全组来控制您的实例的访问权限。这些安全组类似于一个传入网络防火墙，使您可以指定允许访问您的实例的协议、端口和源 IP 范围。您可以创建多个安全组，并给每个安全组指定不同的规则。然后您可以给每个实例分配一个或多个安全组，我们将按照这些规则确定允许哪些流量可访问实例。您可以配置一个安全组，以便只有特定的 IP 地址或特定的安全组可以访问实例。有关更多信息，请参阅 [Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。

AWS Identity and Access Management

使用 AWS Identity and Access Management (IAM) 可以执行以下操作：

- 在您的 AWS 账户下创建用户和组
- 为您的 AWS 账户下的每个用户分配唯一的安全证书
- 控制每个用户使用 AWS 资源执行任务的权限
- 允许另一 AWS 账户的用户共享 AWS 资源
- 创建 AWS 账户角色并定义可以担任这些角色的用户或服务
- 借助企业的现有身份验证，授予使用 AWS 资源执行任务的权限

通过将 IAM 与 Amazon EC2 配合使用，您可以控制组织中的用户能否使用特定的 Amazon EC2 API 操作执行任务，以及他们能否使用特定的 AWS 资源。

有关 IAM 的更多信息，请参阅下文：

- [创建 IAM 组和用户 \(p. 524\)](#)
- [Amazon EC2 的 IAM 策略 \(p. 525\)](#)
- [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)
- [Identity and Access Management \(IAM\)](#)
- [IAM 用户指南](#)

Windows Server 与 Amazon EC2 Windows 实例之间的区别

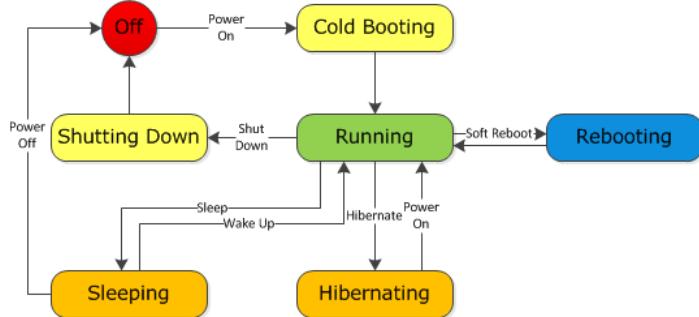
启动 Amazon EC2 Windows 实例之后，该实例的行为非常类似于运行 Windows Server 的传统服务器。例如，Windows Server 和 Amazon EC2 实例都可用于运行您的 Web 应用程序，执行批处理或管理需要大量计算的应用程序。然而，服务器硬件模型和云计算模型之间有重要区别。Amazon EC2 实例与运行 Windows Server 的传统服务器的运行方式是不同的。

在开始启动 Amazon EC2 Windows 实例之前，您应该清楚云服务器上运行的应用程序的架构与硬件上运行的传统应用程序模型会有显著区别。要在云服务器上实现应用程序，需要在设计过程中进行转变。

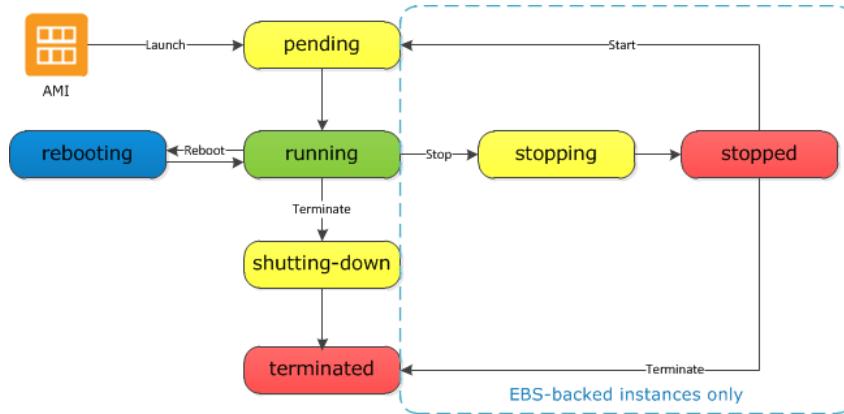
下表介绍了 Windows Server 与 Amazon EC2 Windows 实例之间的一些主要区别。

Windows Server	Amazon EC2 Windows 实例
资源和容量在物理上是受到限制的。	资源和容量是可扩展的。
不管您使用与否，均需要为基础设施付费。	您需要为基础设施的使用付费。只要您停止或终止实例，我们就会停止收费。
占用物理空间，必须定期维护。	不占用物理空间，不需要定期维护。
通过按下电源按钮来启动（称为 冷启动）。	通过启动实例来启动。
您可以保持服务器运行状态直至需要关机，或保持其处于睡眠或休眠状态（服务器在此期间断电）。	您可以保持服务器运行，或者停止或重启它（实例在此期间移至新主机）。
关闭服务器后，所有资源会保持完整，并保持关闭时所处的状态。您在硬盘上存储的信息会保留，并且您可以根据需要随时访问这些信息。您可以通过开启服务器将其还原为运行状态。	终止实例后，将无法再使用其基础设施。在您终止之后，您将无法连接至或重新启动实例。但是，您可以在实例处于运行状态时从实例创建映像，并随时从该映像启动新实例。

运行 Windows Server 的传统服务器会经过下图所示的状态。



将下图与前面的 Windows Server 图进行对比之后，您会发现 Amazon EC2 Windows 实例与传统 Windows Server 之间存在许多相似之处。在您启动实例后，实例在注册时会暂时处于待处理状态，然后进入运行状态。实例会一直处于活动状态，直到您停止或终止它。在您终止实例之后，将无法重新启动它。您可以在实例处于运行状态时从实例创建备份映像，并从备份映像启动新实例。



设计您的应用程序以在 Amazon EC2 Windows 实例上运行

设计您的应用程序以在 Amazon EC2 Windows 实例上运行时，考虑上面部分提到的区别是非常重要的。

为 Amazon EC2 构建的应用程序会按需使用底层的计算基础设施。为了执行任务并在任务完成后舍弃资源，应用程序会按需利用必要资源（例如存储和计算资源）。此外，任务完成之后，它们通常还会对自身进行处理。处理过程中，应用程序会根据资源要求进行灵活扩展和缩小。基础设施出现故障时，在 Amazon EC2 实例上运行的应用程序可终止并随意重新创建各种组件。

设计您的 Windows 应用程序以在 Amazon EC2 上运行时，您可以根据自己不断变化的需求规划计算和存储资源的快速部署和快速缩减。

和 Windows Server 不同，当您运行 Amazon EC2 Windows 实例时，无需设置硬件、软件和存储的准确系统包。取而代之，您需要重点使用各种云资源，以便提高 Windows 应用程序的可扩展性和整体性能。

对于 Amazon EC2，对故障和断电的设计是架构的重要组成部分。与任何可扩展的冗余系统一样，您系统的架构应该考虑计算、网络和存储故障。您必须在自己的应用程序内构建可处理各种故障的机制。关键是构建具有独立组件的模块化系统，这些组件并非紧密结合，可以异步互动并且将彼此视为可独立扩展的黑盒。因此，如果您的某个组件出现故障或很繁忙，您可以启动该组件的更多实例，而无需破坏当前系统。

针对故障进行设计的另一重要元素是按地理位置分配您的应用程序。在不同地理分布区域复制您的应用程序可提高您系统的可用性。

Amazon EC2 基础设施是可编程的，您可以使用脚本自动处理部署流程、安装和配置软件及应用程序，以及引导您的虚拟服务器。

您应该在 Amazon EC2 Windows 实例上运行的应用程序架构的各层中实施安全性。如果您不放心在 Amazon EC2 环境内存储敏感性和机密性数据，则应该在上传之前对这些数据加密。

Amazon EC2 的设置

Abstract

完成这些步骤为首次使用 Amazon EC2 做好准备。

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

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

1. [注册 AWS \(p. 13\)](#)
2. [创建 IAM 用户 \(p. 14\)](#)
3. [创建密钥对 \(p. 15\)](#)
4. [创建 Virtual Private Cloud \(VPC\) \(p. 16\)](#)
5. [创建安全组 \(p. 17\)](#)

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 <http://www.amazonaws.cn/> , 然后选择 Create an AWS Account。
2. 按照屏幕上的说明进行操作。

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

请记住您的 AWS 账户 , 因为进行下一个任务时需要用到该账户。

创建 IAM 用户

AWS 中的服务（例如 Amazon EC2）要求您在访问时提供证书，以便服务可以确定您是否有权限访问其资源。控制台要求您的密码。您可以为您的 AWS 账户创建访问密钥以访问命令行界面或 API。但是，我们不建议您使用 AWS 账户的证书访问 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 用户的证书访问 AWS。

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

为管理员创建组

1. 登录到 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
3. 对于 Group Name，请为您的组键入一个名称（如 **Administrators**），然后选择 Next Step。
4. 在策略列表中，选中 AdministratorAccess 策略旁边的复选框。您可以使用 Filter 菜单和 Search 框来筛选策略列表。
5. 选择 Next Step，然后选择 Create Group。

您的新组列在 Group Name 下方。

要为您自己创建 IAM 用户，请将用户添加到 Administrators 组中，并为该用户创建密码

1. 在导航窗格中选择 Users，然后选择 Create New Users。
2. 在框 1 中，键入用户名。
3. 清除 Generate an access key for each user 旁的复选框。
4. 选择 Create。
5. 在用户列表中，选择您刚创建的用户的名称（而不是复选框）。可以使用 Search 框搜索该用户名。
6. 选择 Groups 选项卡，然后选择 Add User to Groups。
7. 选中 Administrators 组旁的复选框。然后选择 Add to Groups。
8. 选择 Security Credentials 选项卡。在 Sign-In Credentials 下，选择 Manage Password。
9. 选择 Assign a custom password。然后在 Password 和 Confirm Password 框中键入密码。完成后，请选择 Apply。

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

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

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

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

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

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

有关 IAM 的更多信息，请参阅 [IAM 和 Amazon EC2 \(p. 523\)](#)。

创建密钥对

AWS 使用公共密钥密码术来保护您实例的登录信息。您可以在启动实例时指定密钥对的名称，然后提供私有密钥 获取 Windows 实例的管理员密码，以便可以使用 RDP 登录。

如果您尚未创建密钥对，则可以通过 Amazon EC2 控制台自行创建。请注意，如果您计划在多个区域启动实例，则需要在每个区域中创建密钥对。有关区域的更多信息，请参阅 [地区和可用区域 \(p. 6\)](#)。

创建密钥对

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



4. 在导航窗格中的 NETWORK & SECURITY 下，单击 Key Pairs。



Tip

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

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs 

Network Interfaces

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



Important

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

有关更多信息，请参阅 [Amazon EC2 密钥对和 Windows 实例 \(p. 510\)](#)。

创建 Virtual Private Cloud (VPC)

Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。如果您有默认 VPC，则可以跳过此部分并进入下一个任务，即 [创建安全组 \(p. 17\)](#)。若要确定您是否有默认的 VPC，请参阅[在 Amazon EC2 控制台中的所支持的平台 \(p. 578\)](#)。否则，您可以使用以下步骤在账户中创建非默认 VPC。



Important

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

创建非默认 VPC

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

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

创建安全组

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须在安全组中添加规则，以便能够使用 RDP 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[区域和可用区 \(p. 6\)](#)。

先决条件

您需要本地计算机的公有 IP 地址，可以使用服务获得该地址。例如，我们提供以下服务：<http://checkip.amazonaws.com/>。要查找另一项可提供您的 IP 地址的服务，请使用搜索短语“what is my IP address”。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

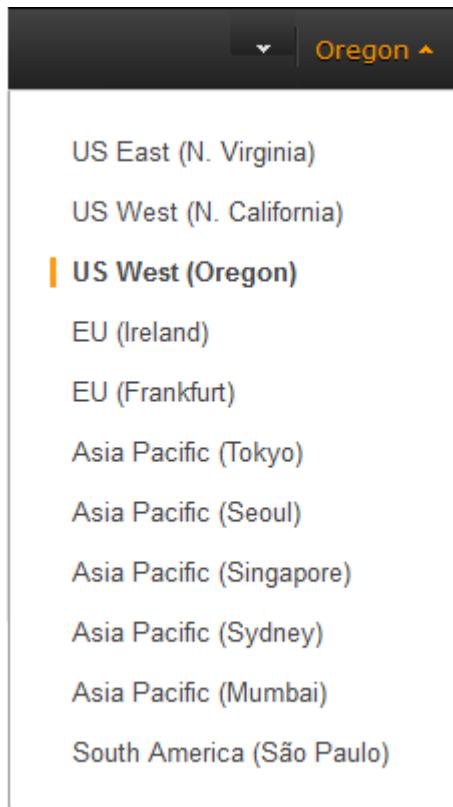
1. 打开 Amazon EC2 控制台。



Tip

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

2. 从导航栏中选择安全组的区域。安全组特定于某一区域，因此您应选择已创建密钥对的区域。



3. 单击导航窗格中的 Security Groups (安全组)。
4. 单击 Create Security Group (创建安全组)。
5. 输入新安全组的名称和描述。选择一个容易记住的名称，例如，您的 IAM 用户名称，后跟 _SG_ 加区域名称。例如，me_SG_uswest2。
6. 在 VPC 列表中选择您的 VPC。如果您有默认 VPC，则该 VPC 会带有星号 (*) 标记。



Note

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

7. 在 Inbound (入站) 选项卡上，创建以下规则（为每个新规则单击 Add Rule (添加规则)），然后单击 Create (创建)：

- 从 Type (类型) 列表中选择 HTTP，确保 Source (源) 设置为 Anywhere (任何位置) (0.0.0.0/0)。
- 从 Type (类型) 列表中选择 HTTPS，确保 Source (源) 设置为 Anywhere (任何位置) (0.0.0.0/0)。
- 从 Type (类型) 列表中选择 RDP。在 Source (源) 框中，确保选择 Custom (自定义 IP)，然后采用 CIDR 表示法指定您计算机或网络的公有 IP 地址。要采用 CIDR 表示法指定单个 IP 地址，请添加路由前缀 /32。例如，如果您的 IP 地址是 203.0.113.25，请指定 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。



Caution

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

有关更多信息，请参阅 [Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。

Amazon EC2 Windows 实例入门

Abstract

通过启动、连接以及使用 Linux 实例实现 Amazon EC2 入门。

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

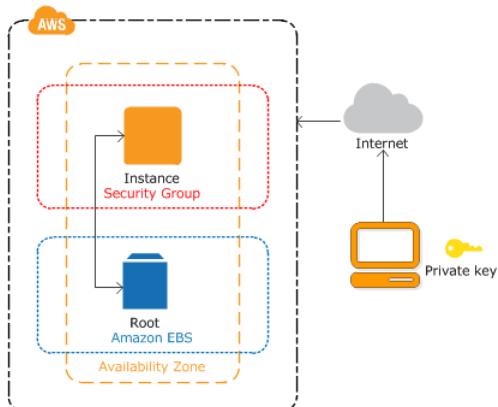
注册 AWS 后，您可以通过 [AWS 免费套餐](#)开始免费使用 Amazon EC2。如果您在过去 12 个月内创建过 AWS 账户，并且还没有超出 Amazon EC2 的免费套餐权益范围，则学完本教程不需要任何费用，因为我们会帮助您选择免费套餐权益范围内的选项。否则，您将从启动实例的那一刻开始承担标准的 Amazon EC2 使用费，直至终止实例（本教程最后一项任务），即使实例处于闲置状态也要计费。

内容

- [概述 \(p. 19\)](#)
- [先决条件 \(p. 20\)](#)
- [步骤 1：启动实例 \(p. 20\)](#)
- [步骤 2：连接到您的实例 \(p. 21\)](#)
- [步骤 3：清除您的实例 \(p. 23\)](#)
- [后续步骤 \(p. 23\)](#)

概述

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



任务

要完成本教程，请执行以下任务：

1. 启动实例 (p. 20)
2. 连接到您的实例 (p. 21)
3. 清除您的实例 (p. 23)

相关教程

- 如果您希望启动 Linux 实例，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的以下教程：[Amazon EC2 Linux 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 \(p. 13\)](#)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 Windows 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

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从控制台控制面板中，选择 Launch Instance。
3. 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。选择适用于 Microsoft Windows Server 2012 R2 Base 或 Microsoft Windows Server 2008 R2 Base 的 AMI。请注意，这些 AMI 标记为“符合条件的免费套餐。”
4. 在 Choose an Instance Type (选择实例类型) 页面上，您可以选择实例的硬件配置。选择 t2.micro 类型（默认情况下的选择）。请注意，此实例类型适用免费套餐。



Note

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

5. 选择 Review and Launch 让向导为您完成其他配置设置。
 6. 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：
 - a. 选择 Edit security groups。
 - b. 在 Configure Security Group 页面上，确保 Select an existing security group 处于选中状态。
 - c. 从现有安全组列表中选择您的安全组，然后选择 Review and Launch。
 7. 在 Review Instance Launch 页面上，选择 Launch。
 8. 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。



Caution

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

准备好后，选中确认复选框，然后选择 Launch Instances。

- 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 列已隐藏，请选择页面右上角的“Show/Hide”图标，然后选择 Public DNS。）
 - 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

要连接到 Windows 实例，必须获取初始管理员密码，然后在使用远程桌面连接到实例时指定该密码。



Note

如果您已将实例加入域，则可以使用您在 AWS Directory Service 中定义的域证书连接实例。有关连接域中实例的更多信息，请参阅[使用域证书连接到实例 \(p. 305\)](#)。

管理员账户的名称取决于操作系统语言。例如，在英语中是 Administrator，在法语中是 Administrateur，在葡萄牙语中是 Administrador。有关更多信息，请参阅 Microsoft TechNet Wiki 中的 [Localized Names for Administrator Account in Windows](#)。

借助适用于 Windows Server 操作系统 (OS) 的许可证，可以同时进行两个远程连接以进行管理。适用于 Windows Server 的许可证包含在您的 EC2 实例的价格中。如果您需要同时进行两个以上的远程连接，则必须购买远程桌面服务 (RDS) 许可证。如果尝试第三个连接，将产生错误。有关更多信息，请参阅 [Configure the Number of Simultaneous Remote Connections Allowed for a Connection](#)。

使用 RDP 客户端连接到 Windows 实例

1. 在 Amazon EC2 控制台中，选择实例，然后选择 Connect。
2. 在 Connect To Your Instance 对话框中，选择 Get Password (密码在实例启动几分钟之后才可用)。
3. 选择 Browse 并导航至您启动实例时所创建的私有密钥文件。选择该文件并选择 Open，将文件的全部内容复制到内容框中。
4. 选择 Decrypt Password。控制台将在 Connect To Your Instance (连接到您的实例) 对话框中显示实例的默认管理员密码，会将先前显示的 Get Password (获取密码) 链接替换为实际密码。
5. 记录下默认管理员密码，或将其复制到剪贴板。需要使用此密码连接实例。
6. 选择 Download Remote Desktop File。您的浏览器会提示您打开或保存 .rdp 文件。两种选择都可以。完成后，可选择 Close 以关闭 Connect To Your Instance 对话框。
 - 如果已打开 .rdp 文件，您将看到 Remote Desktop Connection (远程桌面连接) 对话框。
 - 如果已保存 .rdp 文件，请导航至下载目录，然后打开 .rdp 文件以显示该对话框。
7. 您可能看到一条警告，指出远程连接发布者未知。如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 Connect 以连接到您的实例。如果您正在 Mac 上使用 Microsoft Remote Desktop (Microsoft 远程桌面)，请跳过下一步。
8. 当收到系统提示时，使用操作系统的管理员账户和您在之前记录或复制的密码登录该实例。如果您的 Remote Desktop Connection 已设置了管理员账户，您可能需要选择 Use another account 选项并手动输入用户名和密码。



Note

有时复制和粘贴内容可能会损坏数据。如果您在登录时遇到“Password Failed (密码失败)”错误，请尝试手动键入密码。

9. 由于自签名证书的固有特性，您可能会看到一条警告，指出无法验证该安全证书。请使用以下步骤验证远程计算机的标识；或者，如果您信任该证书，则直接选择 Yes 或 Continue 以继续操作。
 - a. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 View certificate。如果您正在 Mac 上使用 Microsoft Remote Desktop，请选择 Show Certificate。
 - b. 选择 Details 选项卡，并向下滚动到 Thumbprint 条目（在 Windows PC 上）或 SHA1 Fingerprints 条目（在 Mac 上）。这是远程计算机的安全证书的唯一标识符。
 - c. 在 Amazon EC2 控制台中，选择该实例，选择 Actions，然后选择 Get System Log。
 - d. 在系统日志输出中，查找标记为 RDPCERTIFICATE-THUMBPRINT 的条目。如果此值与证书指纹匹配，则表示您已验证了远程计算机的标识。
 - e. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请返回到 Certificate 对话框并选择 OK。如果您正在 Mac 上使用 Microsoft Remote Desktop，请返回到 Verify Certificate 并选择 Continue。
 - f. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 Remote Desktop Connection 窗口中的 Yes 以连接到您的实例。如果您正在 Mac 上使用 Microsoft Remote Desktop (Microsoft 远程桌面)，请使用默认 Administrator 账户和您先前记录或复制的默认管理员密码按提示登录实例。



Note

在 Mac 上，您可能需要切换空间才能看到 Microsoft Remote Desktop (Microsoft 远程桌面) 登录屏幕。有关空间的更多信息，请参阅 <http://support.apple.com/kb/PH14155>。

步骤 3：清除您的实例

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



Important

终止实例可有效地删除实例；无法在终止实例后重新连接到实例。

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

终止您的实例

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

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

后续步骤

启动实例后，您可能想尝试以下的一些练习：

- 配置 CloudWatch 警报以便在您的使用量超出免费套餐时向您发出通知。有关更多信息，请参阅 [AWS Billing and Cost Management 用户指南](#) 中的[创建账单警报](#)。
- 添加 EBS 卷。有关更多信息，请参阅 [创建 Amazon EBS 卷 \(p. 652\)](#) 和 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。
- 安装 WAMP 或 WIMP 堆栈。有关更多信息，请参阅 [教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WAMP 服务器 \(p. 30\)](#) 和 [教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WIMP 服务器 \(p. 33\)](#)。

针对 Amazon EC2 的最佳实践

Abstract

使用此核对清单可评估您对 Amazon EC2 的使用。

此核对清单旨在帮助您从 Amazon EC2 获得最大好处和满意度。

安全与网络

- 使用联合身份验证、IAM 用户和 IAM 角色可管理对 AWS 资源和 API 的访问。建立证书管理策略和过程，以便创建、分配、轮换和撤销 AWS 访问证书。有关更多信息，请参阅 [IAM 用户指南](#) 中的 [IAM 最佳实践](#)。
- 为安全组实现最严格的规则。有关更多信息，请参阅 [安全组规则 \(p. 516\)](#)。
- 定期修补、更新和保护实例上的操作系统和应用程序。有关更新 Amazon Linux 的更多信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [管理 Linux 实例上的软件](#)。有关更新您的 Windows 实例的更多信息，请参阅 [更新 Windows 实例](#)。
- 在 VPC (而不是 EC2-Classic) 中启动您的实例。请注意，如果您在 2013-12-04 后创建 AWS 账户，我们会自动将实例启动到 VPC。有关所获好处的更多信息，请参阅 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 572\)](#)。

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 \(p. 63\)](#)。
- 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 \(p. 235\)](#)。
- 使用您的实例可用的实例存储来存储临时数据。请注意，当您停止或终止您的实例时，会删除存储在实例存储中的数据。如果将实例存储用于数据库存储，请确保您拥有一个具有重复因子的群集，从而确保容错。

资源管理

- 使用实例元数据和自定义资源标签跟踪并确定您的 AWS 资源。有关更多信息，请参阅 [实例元数据和用户数据 \(p. 239\)](#) 和 [标记 Amazon EC2 资源 \(p. 737\)](#)。
- 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 \(p. 746\)](#)。

备份和恢复

- 使用 [Amazon EBS 快照 \(p. 676\)](#)或备份工具定期备份实例。
- 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 \(p. 597\)](#)。
- 监控和响应事件。有关更多信息，请参阅 [监控 Amazon EC2 \(p. 440\)](#)。
- 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 \(ENI\) \(p. 612\)](#)。对于自动解决方案，您可以使用 Auto Scaling。有关更多信息，请参阅 [Auto Scaling 用户指南](#)。
- 定期测试在您实例和 Amazon EBS 卷发生故障时恢复它们的过程。

运行 Windows Server 的 Amazon EC2 实例的相关教程

Abstract

运行 Windows Server 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 Windows Server 的 EC2 实例执行常见任务。

教程

- 教程：在运行 Windows Server 的 Amazon EC2 实例上部署 WordPress 博客 (p. 26)
- 教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WAMP 服务器 (p. 30)
- 教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WIMP 服务器 (p. 33)
- 教程：提高应用程序在 Amazon EC2 上的可用性 (p. 36)
- 教程：远程管理您的 Amazon EC2 实例 (p. 40)
- 教程：在 Amazon EC2 上设置 Windows HPC 集群 (p. 43)

教程：在运行 Windows Server 的 Amazon EC2 实例上部署 WordPress 博客

Abstract

在您的 Windows 实例上部署 WordPress 博客。

本教程将帮助您在运行 Microsoft Windows Server 的 Amazon EC2 实例上安装和部署 WordPress 博客。

如果您希望在 Linux 实例上托管您的 WordPress 博客，请参阅 *Amazon EC2 用户指南 (适用于 Linux 实例)* 中的 [教程：使用 Amazon EC2 托管 WordPress 博客](#)。

先决条件

在开始之前，请务必执行以下操作：

1. 从 Microsoft Windows Server 2008 R2 基础 AMI 启动 Amazon EC2 实例。有关信息，请参阅 [Amazon EC2 Windows 实例入门 \(p. 19\)](#)。
2. 利用 AWS 免费使用套餐（如有资格）来启动并使用免费 Windows *t2.micro* 实例 12 个月。您可以使用 AWS 免费使用套餐来启动新的应用程序、测试现有应用程序或直接获取 AWS 实践经验。有关资格和重点的更多信息，请参阅 [AWS 免费使用套餐](#) 产品页。



Important

如果您已经启动常规实例并且将其用于部署 WordPress 网站，则在终止之前您需要支付针对该实例的标准 Amazon EC2 使用费用。有关 Amazon EC2 使用费率的更多信息，请转到 [Amazon EC2 产品页](#)。

3. 确保您在其中启动实例的安全组已为入站流量打开端口 80 (HTTP)、443 (HTTPS) 和 3389 (RDP)。端口 80 和 443 允许实例外部的计算机通过 HTTP 和 HTTPS 进行连接。如果这些端口未打开，则无法从实例外部访问 WordPress 站点。端口 3389 允许通过远程桌面协议连接到实例。
4. 连接到您的实例。

安装 Microsoft Web 平台安装程序

可以使用 Microsoft Web 平台安装程序在您的服务器上安装和配置 WordPress。此工具简化了 Web 应用程序和网站到 IIS 服务器的部署。有关更多信息，请参阅 [Microsoft Web 平台安装程序](#)。

1. 确认您已满足 [先决条件 \(p. 26\)](#) 中的条件。
2. 禁用 Internet Explorer 增强的安全配置。
3. 下载并安装最新版本的 [Microsoft Web 平台安装程序](#)。

安装 WordPress

现在 Web 平台安装程序已安装，可以用它在您的服务器上安装和配置 WordPress。

安装 WordPress

1. 打开 Web Platform Installer (Web 平台安装程序) 并单击 Applications (应用程序)。
2. 选择 WordPress，单击 Add (添加)，然后单击 Install (安装)。
3. 在 Prerequisites (先决条件) 页面上，选择 MySQL 作为要使用的数据库。在 Password (密码) 和 Re-type Password (再次键入密码) 框中输入所需的 MySQL 数据库管理员密码，然后单击 Continue (继续)。



Note

有关创建安全密码的更多信息，请参阅 <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. 对于第三方应用程序软件、Microsoft 产品（包括 IIS Web 服务器）和组件的列表，请单击 I Accept (我接受)。Web Platform Installer 安装完软件之后，系统会提示您配置新网站。
5. 在 Configure (配置) 页上，清除 'WordPress' application name: ("WordPress" 应用程序名称:) 框中的默认应用程序名称并将其保留为空白，保留其他框中的默认信息，然后单击 Continue (继续)。
6. 单击 Yes (是) 接受将文件夹内容覆盖。

配置安全密钥

通过 WordPress，您可以为站点生成和输入唯一身份验证密钥和加密盐。这些密钥和加密盐值为 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。

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

配置安全密钥

1. 请访问 <https://api.wordpress.org/secret-key/1.1/salt/> 随机生成一组密钥值，您可以将这些值复制并粘贴到安装向导中。以下步骤说明如何在记事本中修改这些值以进行 Windows 安装。
2. 将该页上的所有文本复制到剪贴板。它看上去类似于下面的示例。



Note

以下值仅用作示例；请勿使用以下值进行安装。

```
define('AUTH_KEY',         '3#U$$+[RXN8:b^-L_0(WU_+ c+WFkI~c]o]-  
bHw+/Aj[wTwSiZ<Qb[mghEXcRh-');  
define('SECURE_AUTH_KEY',  'Zsz._P=1//y.Lq)Xj1kwS1y5NJ76E6EJ.AV0pCKZZB,*~*r  
?6OP$eJT@;+(ndLg');  
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWF?{L1GsQ]Ye@2Jh^,8x>)Y  
/;(^[Iw]Pi+LG#A4R?7N`YB3');  
define('NONCE_KEY',        'P(g62HeZxEes/LnT^i=H,[XwK9T&[2s/:?ON}VJM%?;v2v]v+;+^9eXUahg@::Cj');  
define('AUTH_SALT',         'C$DpB4Hj[JK:{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%-  
Bx*M4(qc[Qg%JT!h');  
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M%&%@~gL>U>NV<zpD-  
@2-Es7Q10-bp28EKv');  
define('LOGGED_IN_SALT',   'j{00P*owZf)kVD+FVLn--  
>.Y%Ug4#I^*LvD9QeZ^&XmK/e(76miC+&W&+^0P/');  
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;/_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

3. 通过单击 Start (开始)、All Programs (所有程序)、Accessories (附件) 和 Notepad (记事本) 打开记事本窗口。
4. 将复制的文本粘贴到记事本窗口中。
5. 在 Windows 中安装 WordPress 时，不能在密钥和加密盐值中使用美元符号 (\$)，因此，需要用其他字符（如 S）来替换这些美元符号。在记事本窗口中，依次单击 Edit (编辑)、Replace (替换)。
6. 在 Find what (查找内容) 框中，键入 \$。
7. 在 Replace with (替换为) 框中，键入 S。
8. 单击 Replace All (全部替换) 将所有美元符号替换为 S 字符。
9. 关闭 Replace (替换) 窗口。
10. 将修改后的密钥和加密盐值从记事本窗口粘贴到安装向导中的相应框中。例如，应将记事本窗口中的 AUTH_KEY 值粘贴到向导中的 Authentication Key (身份验证密钥) 框中。

请勿包含值两边的单引号或其他文本，仅包含下面所示的示例中的实际值。

记事本窗口中修改后的 AUTH_KEY 行：

```
define('AUTH_KEY',         '3#USS+[RXN8:b^-L_0(WU_+ c+WFkI~c]o]-  
bHw+/Aj[wTwSiZ<Qb[mghEXcRh-');
```

将此文本粘贴到向导的 Authentication Key (身份验证密钥) 框中：

3#USS+[RXN8:b^-L_0(WU_+ c+WFKI~c)o]-bHw+)/Aj[wTwSiZ<Qb[mghEXcRh-

11. 单击 Continue (继续) 和 Finish (完成) 完成 Web 平台安装程序向导。

配置网站标题和管理员

完成 Web 平台安装程序向导后，安装在 <http://localhost/wp-admin/install.php> 处的 WordPress 会打开一个浏览器窗口。在此页上，您可以配置站点名称和管理用户以调整您的博客。

完成安装

1. 在 WordPress Welcome (欢迎) 页面上，输入以下信息并单击 Install WordPress (安装 WordPress)。

字段	值
Site Title (网站标题)	为您的 WordPress 网站输入名称。
Username	为您的 WordPress 管理员输入名称。出于安全原因，您应为此用户选择唯一的名称，因为相对于默认用户名 admin，这个名称更难破解。
密码	输入强密码，然后再次输入进行确认。请勿重复使用现有密码，并确保将密码保存在安全的位置。
Your E-mail (您的电子邮件)	输入您用于接收通知的电子邮件地址。
隐私	选中此项将允许搜索引擎对您的网站建立索引。

2. 单击 Log In (登录)。
3. 在 Log In (登录) 页上的 Username (用户名) 中输入您的用户名，在 Password (密码) 中输入您之前输入的网站密码。

公开您的 WordPress 网站

您现在可以在自己的本地主机上看到您的 WordPress 博客，可在实例上将该网站发布为默认站点，使其他人也可以看到您的博客。接下来的过程将演示如何修改 WordPress 设置以指向实例的公有 DNS 名称而非您的本地主机。

配置 WordPress 网站的默认设置

1. 打开 WordPress 控制面板，方法是在实例上打开浏览器并转到 <http://localhost/wp-admin>。如果系统提示输入证书，请在 Username (用户名) 中输入您的用户名，在 Password (密码) 中输入您的网站密码。
2. 在 Dashboard (控制面板) 窗格中，单击 Settings (设置)。
3. 在 General Settings (一般设置) 页面上，输入以下信息并单击 Save Changes (保存更改)。
 - WordPress address (URL) (WordPress 地址 (URL)) - 您的实例的公有 DNS 地址。例如，您的 URL 可能看起来类似于 <http://ec2-203-0-113-25.compute-1.amazonaws.com>。

您可以使用 Amazon EC2 控制台获取实例的公有 DNS (选择实例并选中 Public DNS (公有 DNS) 列 ; 如果此列处于隐藏状态 , 请单击 Show/Hide(显示/隐藏) 图标并选择 Public DNS (公有 DNS)) 。

- Site address (URL) - 您在 WordPress address (URL) 中设置的实例的同一公有 DNS 地址。

4. 要查看新网站 , 请在计算机 (不是托管 WordPress 的实例) 上打开一个浏览器 , 然后在 Web 地址字段中键入实例的公有 DNS 地址。系统会显示您的 WordPress 网站。

恭喜您 ! 您刚刚在 Windows 实例上成功部署了一个 WordPress 网站。

后续步骤

如果您不再需要此实例 , 则可以删除它以避免产生费用。有关更多信息 , 请参阅 [清除您的实例 \(p. 23\)](#)。

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

- 对实例扩展存储空间。有关更多信息 , 请参阅 [在 Windows 上扩展 EBS 卷的存储空间 \(p. 671\)](#)。
- 将您的 MySQL 数据库移动到 [Amazon RDS](#) 以利用服务的自动扩展功能。
- 迁移到更大的实例类型。有关更多信息 , 请参阅 [调整您的实例大小 \(p. 133\)](#)。
- 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 \(p. 36\)](#)。

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 , 请参阅 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 , 请参阅 http://codex.wordpress.org/Hardening_WordPress。有关如何让您的 WordPress 博客保持最新的信息 , 请参阅 http://codex.wordpress.org/Updating_WordPress。

教程 : 在运行 Windows Server 的 Amazon EC2 实例上安装 WAMP 服务器

Abstract

在运行 Microsoft Windows Server 的 EC2 实例上安装带有 PHP 和 MySQL 的 Apache Web 服务器。

本教程介绍如何在运行 Microsoft Windows Server 的 EC2 实例上安装带有 PHP 和 MySQL 的 Apache Web 服务器。此软件配置有时称为 WAMP 服务器或 WAMP (Windows、Apache、MySQL、PHP) 堆栈。有关如何在 Linux 上创建类似服务器的信息 , 请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [教程 : 安装 LAMP Web 服务器](#)。

WAMP 堆栈可使安装变得简便 , 以帮助开发人员快速启动并运行。它不适用于在生产环境内使用 , 原因如下 :

- 其默认配置不能满足大多数生产环境的安全要求。
- 在单一的生产服务器上更新和修补不同的软件组件会影响服务器的可用性。
- WAMP 单键安装程序不会将文件放在标准位置 , 这很找到位重要的配置文件。

不过 , 通过在 EC2 实例上创建 WAMP 堆栈 , 您可以在受控测试环境中进行 Web 项目原型设计。例如 , 您可以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。

有很多可用来安装 WAMP 堆栈的第三方解决方案 ; 本教程使用的是 Bitnami WAMP 堆栈。有关更多信息 , 请参阅 [Review: WAMP stacks for Web developers](#)。

先决条件

开始之前，请：

- 配置 Microsoft Windows Server 2008 R2 或 2012 R2 基本实例。必须使用可从 Internet 访问的公共域名系统 (DNS) 名称配置基本实例。有关更多信息，请参阅 [Amazon EC2 Windows 实例入门 \(p. 19\)](#)。或者，您可能有资格使用 AWS 免费套餐配置基本实例。免费套餐专为想要体验 AWS 的新 AWS 账户用户而设计。有关该免费套餐以及使用资格要求的更多信息，请参阅 [AWS 免费套餐](#)。



Important

如果您启动非免费套餐实例并使用它来部署堆栈，则在终止该实例之前，您需要为其支付标准 Amazon EC2 使用费用。有关更多信息，请参阅 [Amazon EC2 定价](#)。

- 确认您的实例的安全组打开了以下端口：
 - 80 (HTTP 入站和出站) - 端口 80 允许实例外部的计算机使用 HTTP 进行连接。
 - 443 (HTTPS 入站和出站) - 端口 443 允许实例外部的计算机使用 HTTPS 进行连接。
 - 3389 (仅 RDP 入站) - 端口 3389 允许通过远程桌面协议 (RDP) 连接到实例。作为最佳安全做法，请将 RDP 访问限制为您组织中的一个特定的 IP 地址范围。

有关这些先决条件的更多信息，请参阅 [Amazon EC2 的设置 \(p. 13\)](#)。

安装 WAMP 服务器

- 使用 Microsoft 远程桌面连接到您的实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
- 禁用 Internet Explorer 增强的安全配置，以便您可以从 Web 下载并安装必需的软件。
 - 在 Microsoft Windows Server 2008 或 2012 的实例中，打开服务器管理器。
 - 在 Windows Server 2008 R2 上，在服务器摘要下的安全信息部分，单击配置 IE ESC。
 - 在 Windows Server 2012 R2 上，在左侧窗格中单击本地服务器。在属性窗格中，找到 IE 增强的安全配置。单击开。
 - 在管理员下，单击关，然后单击确定。
 - 关闭服务器管理器。



Note

请记下原来的配置，以便从 Web 安装完软件后重新启用 Internet Explorer 增强的安全配置。

- 安装软件更新以确保实例有最新的安全更新和错误修复。
 - EC2Config - 下载并安装最新版本的 [Amazon Windows EC2Config 服务](#)。
 - Windows Update - 运行 Windows Update，以确保实例上安装了最新的安全和软件更新。在控制面板中单击系统和安全。在 Windows Update 部分，单击检查更新。
- 下载并安装 WAMP 堆栈。在本教程中，建议您下载并安装[此 WAMP 堆栈](#)。但您也可以下载并安装[其他 Bitnami WAMP 堆栈](#)。无论您安装哪个堆栈，Bitnami 站点都会提示您创建一个免费 Bitnami 账户或使用社交媒体账户登录。登录后，请运行 Bitnami 安装向导。
- 安装完成后，请通过浏览测试页验证 Apache Web 服务器是否正确配置并正常运行。在另一台计算机上打开 Web 浏览器，输入 WAMP 服务器的公有 DNS 地址或公有 IP 地址。您实例的公有 DNS 地

址列在 Amazon EC2 控制台的 Public DNS 列中。如果此列隐藏，请单击 Show/Hide 图标并选择 Public DNS。



Important

如果没有看到 Bitnami 测试页，请使用高级安全 Windows 防火墙创建自定义规则，以允许端口 80 上的 HTTP 协议和端口 443 上的 HTTPS 协议。有关更多信息，请参阅 Microsoft TechNet 上的[高级安全 Windows 防火墙概述](#)。还请确认您所使用的安全组包含允许 HTTP（端口 80）连接的规则。有关向安全组添加 HTTP 规则的信息，请参阅[向安全组添加规则](#)。

6. 通过从 Web 查看 PHP 文件测试 WAMP 服务器。您必须以管理员身份登录实例才能执行以下步骤。

- a. 创建包含以下代码的 phpinfo.php 文件并将此文件放在 Apache 根目录中。默认情况下，路径为：`C:\Bitnami\wampstack-version_number\apache2\htdocs`。

```
<?php phpinfo(); ?>
```

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

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

- c. 验证 PHP 信息页是否显示。如果未显示该页，请验证您输入的公有 DNS 地址是否正确。还请验证 Windows 文件夹选项是否配置为显示已知文件扩展名。默认情况下，文件夹选项会隐藏已知文件扩展名。如果您在记事本中创建 phpinfo.php 文件并将其保存在根目录中，该文件可能会错误保存为 phpinfo.php.txt。

- d. 作为最佳安全做法，请在完成 WAMP 服务器测试后删除 phpinfo.php 文件。

7. 通过禁用默认功能和设置根密码增强 MySQL 安全性。`mysql_secure_installation` Perl 脚本可为您执行这些任务。要运行该脚本，必须安装 Perl。

- a. 从[Perl Programming Language](#) 网站下载并安装 Perl。
- b. 在 `C:\Bitnami\wampstack-version_number\mysql\bin` 目录中，双击 `mysql_secure_installation`。
- c. 在系统提示时，输入您在运行 Bitnami WAMP 堆栈安装程序时输入的 MySQL 根账户密码，然后按 Enter。
- d. 键入 n 跳过密码更改。
- e. 键入 Y 删除匿名用户账户。
- f. 键入 Y 禁用远程 root 登录。
- g. 键入 Y 删除测试数据库。
- h. 键入 Y 重新加载权限表并保存您的更改。

如果成功完成了本教程中的步骤，您的 WAMP 服务器就可以正常工作。要继续测试，您可以向 `C:\Bitnami\wampstack-version_number\apache2\htdocs` 文件夹添加更多内容，并使用实例的公有 DNS 地址查看这些内容。



Important

如果不打算立即使用 MySQL 服务器，建议您最好停止它。您可以在需要时再次重新启动该服务器。

教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WIMP 服务器

Abstract

在运行 Microsoft Windows Server 的 EC2 实例上安装 IIS Web 服务器及 PHP 和 MySQL。

本教程介绍如何在运行 Microsoft Windows Server 的 EC2 实例上安装 Microsoft Internet 信息服务 (IIS) Web 服务器及 PHP 和 MySQL。此软件配置有时称为 WIMP 服务器或 WIMP (Windows、IIS、MySQL、PHP) 堆栈。

WIMP 堆栈可使安装变得简便，以帮助开发人员快速启动并运行。它不适用于在生产环境内使用，原因如下：

- 其默认配置不能满足大多数生产环境的安全要求。
- 在单一的生产服务器上更新和修补不同的软件组件会影响服务器的可用性。
- WAMP 单键安装程序不会将文件放在标准位置，这很找到位重要的配置文件。

但您可以通过在 EC2 实例上创建 WIMP 堆栈，在受控测试环境中进行 Web 项目原型设计。例如，您可以托管静态网站或部署能对数据库中的信息执行读写操作的动态 PHP 应用程序。

先决条件

开始之前，请：

- 配置 Microsoft Windows Server 2008 R2 或 2012 R2 基本实例。必须使用可从 Internet 访问的公共域名系统 (DNS) 名称配置基本实例。有关更多信息，请参阅 [Amazon EC2 Windows 实例入门 \(p. 19\)](#)。或者，您可能有资格使用 AWS 免费套餐配置基本实例。免费套餐专为想要体验 AWS 的新 AWS 账户用户而设计。有关该免费套餐以及使用资格要求的更多信息，请参阅 [AWS 免费套餐](#)。



Important

如果您启动非免费套餐实例并使用它来部署堆栈，则在终止该实例之前，您需要为其支付标准 Amazon EC2 使用费用。有关更多信息，请参阅 [Amazon EC2 定价](#)。

- 确认您的实例的安全组打开了以下端口：
 - 80 (HTTP 入站和出站) - 端口 80 允许实例外部的计算机使用 HTTP 进行连接。
 - 443 (HTTPS 入站和出站) - 端口 443 允许实例外部的计算机使用 HTTPS 进行连接。
 - 3389 (仅 RDP 入站) - 端口 3389 允许通过远程桌面协议 (RDP) 连接到实例。作为最佳安全做法，请将 RDP 访问限制为您组织中的一个特定的 IP 地址范围。

- 有关这些先决条件的更多信息，请参阅 [Amazon EC2 的设置 \(p. 13\)](#)。
- 阅读在 [Microsoft Web 平台](#) 上安装 PHP 的最佳实践。

安装 WIMP 服务器

1. 使用 Microsoft 远程桌面连接到您的实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
2. 禁用 Internet Explorer 增强的安全配置，以便您可以从 Web 下载并安装必需的软件。



Note

请记下原来的配置，以便从 Web 安装完软件后重新启用 Internet Explorer 增强的安全配置。

3. 安装软件更新以确保实例有最新的安全更新和错误修复。
 - a. EC2Config - 下载并安装最新版本的 [Amazon Windows EC2Config 服务](#)。
 - b. Windows Update - 运行 Windows Update，以确保实例上安装了最新的安全和软件更新。在控制面板中单击系统和安全。在 Windows Update 部分，单击检查更新。

安装 IIS Web 服务器

IIS 是 Windows Server 的一个功能，通过“服务器管理器”安装。本节介绍在 Windows Server 2008 或 2012 上安装 IIS 的流程。

在 Windows Server 2012 上安装 IIS

1. 在服务器管理器中，单击添加角色和功能。
2. 在 Before you begin 页面上，单击 Next。
3. 在 Select installation type (选择安装类型) 页面上选择 Role-based or feature-based installation (基于角色或基于功能的安装)，然后单击 Next (下一步)。
4. 在 Select destination server (选择目标服务器) 页面上，从服务器池中选择您的实例，然后单击 Next (下一步)。
5. 在 Select server roles (选择服务器角色) 页面上，选择 Web Server (IIS) (Web 服务器 (IIS))，单击 Add features (添加功能)，然后单击 Next (下一步)。
6. 在选择功能页面上，保持默认功能不变并展开 .NET Framework 4.5 功能，选择 ASP.NET 4.5，然后单击下一步。
7. 在 Web Server Role (IIS) (Web 服务器角色(IIS)) 页面上，单击 Next (下一步)。
8. 在选择角色服务页面上，保持默认服务不变并选择应用程序开发。
9. 展开应用程序开发，然后选择以下功能。在选择这些功能时，如果系统给予提示，请单击添加功能：
 - a. .NET Extensibility 3.5
 - b. .NET Extensibility 4.5
 - c. 应用程序初始化
 - d. ASP.NET 3.5
 - e. ASP.NET 4.5
 - f. CGI
10. 单击 Next (下一步)。
11. 在 Confirm installation selections (确认安装选项) 页面上，选择 Restart the destination server automatically if required (必要时自动重新启动目标服务器)。当系统提示进行确认时，单击 Yes (是)。
12. 单击安装，待安装完成后，单击关闭。
13. 再次运行 Windows 更新。

在 Windows Server 2008 上安装 IIS

1. 在“Server Manager”中，单击“Roles”。
2. 单击添加角色。
3. 在 Before You Begin 页面上，单击 Next。
4. 在选择服务器角色页面上，单击 Web 服务器(IIS)。
5. 在选择角色服务页面的应用程序开发下面，单击 ASP.NET。
 - a. 系统给予提示时，单击添加必需的角色服务。

- b. 单击 CGI。
 - c. 单击 Next (下一步)。
6. 在确认安装选择页面上，单击安装。
 7. 再次运行 Windows 更新。

验证 Web 服务器是否正在运行

安装完成后，请前往 IIS 欢迎页面验证 IIS Web 服务器是否正确配置并正常运行。在另一台计算机上打开 Web 浏览器，输入 WIMP 服务器的公有 DNS 地址或公有 IP 地址。您实例的公有 DNS 地址列在 Amazon EC2 控制台的 Public DNS 列中。如果此列隐藏，请单击 Show/Hide 图标并选择 Public DNS。



Important

如果没有看到 IIS 欢迎页面，请使用高级安全 Windows 防火墙创建自定义规则，以允许端口 80 上的 HTTP 协议和端口 443 上的 HTTPS 协议。有关更多信息，请参阅 Microsoft TechNet 上的 [高级安全 Windows 防火墙概述](#)。还请确认您所使用的安全组包含允许 HTTP (端口 80) 连接的规则。有关向安全组添加 HTTP 规则的信息，请参阅[向安全组添加规则](#)。

安装 MySQL 和 PHP

您可以使用 Microsoft Web 平台安装程序下载并安装 MySQL 和 PHP，如本节所述。

安装 MySQL 和 PHP

1. 在 Microsoft Windows Server 实例中，下载并安装最新版本的 [Microsoft Web 平台安装程序 5.0](#)。
2. 在 Microsoft Web 平台安装程序中，单击产品选项卡。
3. 选择 MySQL Windows 5.5，然后单击添加。
4. 选择 PHP 5.6.0，然后单击添加。
5. 单击 Install (安装)。
6. 在先决条件页面上，为 MySQL 默认数据库管理员账户输入一个密码，然后单击继续。
7. 待安装完成后，单击完成，然后单击退出以关闭 Web 平台安装程序。

测试 WIMP 服务器

通过从 Web 查看 PHP 文件测试 WIMP 服务器。您必须以管理员身份登录实例才能执行以下步骤。

测试 WIMP 服务器

1. 下载并安装 [Visual C++ Redistributable for Visual Studio 2012 Update 4 x86 包](#)。即使服务器是 64 位的，也必须安装 x86 包。
2. 创建包含以下代码的 phpinfo.php 文件并将此文件放在 IIS 根目录中。默认情况下，该路径为：
C:\inetpub\wwwroot。

```
<?php phpinfo(); ?>
```

3. 在 Web 浏览器中，输入您刚刚创建的文件的 URL。此 URL 是实例的公有 DNS 地址，后接正斜杠和文件名，如下例所示：

`http://my.public.dns.amazonaws.com/phpinfo.php`
4. 验证 PHP 信息页是否显示。如果未显示该页，请验证您输入的公有 DNS 地址是否正确。还请验证 Windows 文件夹选项是否配置为显示已知文件扩展名。默认情况下，文件夹选项会隐藏已知文件扩

展名。如果您在记事本中创建 `phpinfo.php` 文件并将其保存在根目录中，该文件可能会错误保存为 `phpinfo.php.txt`。

5. 作为最佳安全做法，请在完成 WAMP 服务器测试后删除 `phpinfo.php` 文件。
6. 通过禁用默认功能和设置根密码增强 MySQL 安全性。`mysql_secure_installation` Perl 脚本可为您执行这些任务。要运行该脚本，必须安装 Perl。
 - a. 从 [Perl Programming Language](#) 网站下载并安装 Perl。
 - b. 在 C:\Program Files\MySQL\MySQL Server 5.5\bin 目录中，双击 `mysql_secure_installation`。
 - c. 系统给予提示时，输入当前根密码并按 Enter。
 - d. 键入 n 跳过密码更改。
 - e. 键入 Y 删除匿名用户账户。
 - f. 键入 Y 禁用远程 root 登录。
 - g. 键入 Y 删除测试数据库。
 - h. 键入 Y 重新加载权限表并保存您的更改。

现在，您应该有了一个功能完善的 WIMP Web 服务器。如果您将内容添加到 IIS 文档根目录（位于 C:\inetpub\wwwroot），您能够在您实例的公有 DNS 地址中看到该内容。



Important

如果不打算立即使用 MySQL 服务器，建议您最好停止它。您可以在需要时再次重新启动该服务器。

教程：提高应用程序在 Amazon EC2 上的可用性

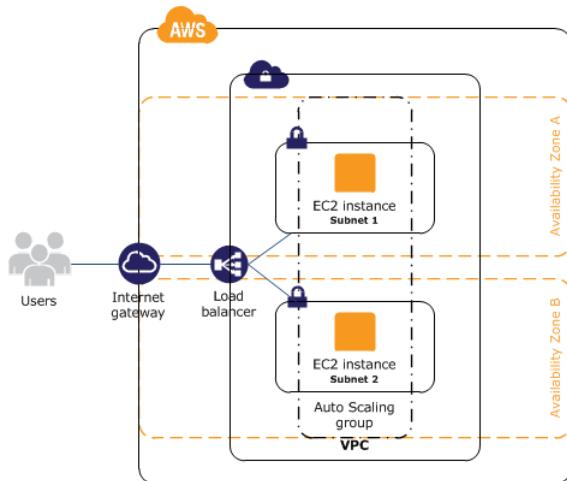
Abstract

了解如何使用 Auto Scaling 和 Elastic Load Balancing 提高应用程序在 Amazon EC2 上的可用性。

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

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

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



内容

- [先决条件 \(p. 37\)](#)
- [对应用程序进行扩展和负载均衡 \(p. 37\)](#)
- [测试负载均衡器 \(p. 39\)](#)

先决条件

本教程假定您已执行以下操作：

1. 如果您没有默认的 Virtual Private Cloud (VPC)，请在两个或更多可用区中利用公有子网创建一个 VPC。有关更多信息，请参阅 [创建 Virtual Private Cloud \(VPC\) \(p. 16\)](#)。
2. 在 VPC 中启动实例。
3. 连接到实例并对其进行自定义。例如，您可以安装软件和应用程序、复制数据和连接更多的 EBS 卷。有关在实例上设置 Web 服务器的信息，请参阅 [教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WAMP 服务器 \(p. 30\)](#) 或 [教程：在运行 Windows Server 的 Amazon EC2 实例上安装 WIMP 服务器 \(p. 33\)](#)。
4. 测试您的实例上的应用程序以确保您的实例配置正确。
5. 从您的实例创建自定义 Amazon 系统映像 (AMI)。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。
6. (可选) 如果您不再需要实例，请终止它。
7. 创建一个 IAM 角色，该角色将为您的应用程序授予对所需的 AWS 的访问权限。有关更多信息，请参阅 [使用控制台创建 IAM 角色 \(p. 567\)](#)。

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

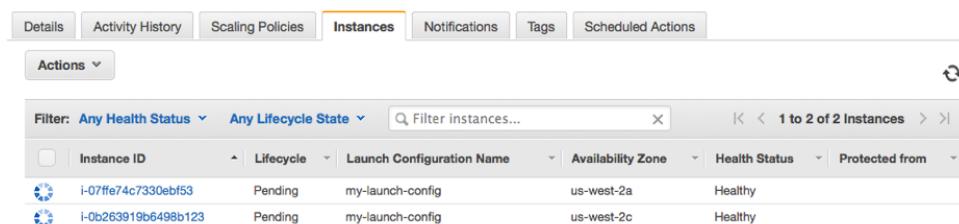
1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中的 LOAD BALANCING 下，单击 Load Balancers。
3. 单击 Create Load Balancer (创建负载均衡器)。
4. 在 Define Load Balancer (定义负载均衡器) 页面上，执行以下操作：

- a. 在 Load Balancer name 中输入负载均衡器的名称。例如，`my-lb`。
 - b. 从 Create LB Inside 中选择您的 VPC。
 - c. 保留 Listener Configuration 的默认值，它是一个 HTTP 侦听器。
 - d. 如果您选择了非默认 VPC，则系统会提示您在 Select Subnets 下选择子网。分别单击您的两个公有子网的 Action 列中的图标。
 - e. 单击 Next: Assign Security Groups。
5. 在 Assign Security Groups 页面上，执行以下操作：
- a. 单击 Create a new security group (创建新安全组)。
 - b. 为您的安全组输入名称和说明。这个新的安全组包含一个规则，该规则允许流量流入 HTTP 侦听器的端口。
 - c. 单击 Next: Configure Security Settings。
6. 在 Configure Security Settings 页面上，单击 Next: Configure Health Check 以前进到下一页，因为我们不创建 HTTPS 负载均衡器。
7. 在 Configure Health Check (配置运行状况检查) 页面上，执行以下操作：
- a. 将 Ping Protocol (Ping 协议) 和 Ping Port (Ping 端口) 保留为默认值。
 - b. 将 Ping Path (Ping 路径) 设置为 `/`。这会向默认页面发送查询，而不管该页面的名称是 `index.html` 还是其他名称。
 - c. 单击 Next: Add EC2 Instances。
8. 在 Add EC2 Instances 页面上，单击 Next: Add Tags 以前进到下一页，因为我们将使用 Auto Scaling 来将 EC2 实例添加到负载均衡器。
9. 在 Add Tags 页面上，添加所需的任何标签，然后单击 Review and Create。
10. 在 Review 页面上，检查您的设置，然后单击 Create。创建负载均衡器后，单击 Close (关闭)。
11. 在导航窗格中的 AUTO SCALING 下，单击 Launch Configurations。
 - 如果您是首次接触 Auto Scaling，您将看到欢迎页面。单击 Create Auto Scaling group 以启动“Create Auto Scaling Group”向导，然后单击 Create launch configuration。
 - 否则，请单击 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. 37) 中创建的 AMI。
13. 在 Choose Instance Type 页面上，选择实例类型，然后单击 Next: Configure details。
14. 在 Configure details 页面上，执行以下操作：
- a. 在 Name 中，为您的启动配置输入一个名称（例如，`my-launch-config`）。
 - b. 从 IAM role 中，选择您在先决条件 (p. 37) 中创建的 IAM 角色。
 - c. (可选) 如果您需要运行一个启动脚本，请展开 Advanced Details 并在 User data 中输入该脚本。
 - d. 单击 Skip to review (跳到审核)。
15. 在 Review (审核) 页面上，单击 Edit security groups (编辑安全组)。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 RDP 流量（前提是您需要连接到该实例）。完成后，单击 Review。
16. 在 Review 页面上，单击 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。单击确认复选框，然后单击 Create launch configuration (创建启动配置)。
18. 创建启动配置后，您必须创建 Auto Scaling 组。

- 如果您是初次使用 Auto Scaling 并且正在使用“Create Auto Scaling group”向导，则会自动进入下一步。
 - 否则，请单击 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：
- 输入 Auto Scaling 组的名称。例如，my-asg。
 - 在 Group size 中，在文本框中输入实例的数量（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。
 - 从 Network 中选择您的 VPC，然后从 Subnet 中选择您的两个公有子网。
 - 展开 Advanced Details (高级详细信息)。选择 Receive traffic from Elastic Load Balancer(s) (从 Elastic Load Balancer 接收流量)。从文本字段选择负载均衡器。
 - 单击 Next: Configure scaling policies (下一步：配置扩展策略)。
20. 在 Configure scaling policies 页面上，单击 Review，因为我们只打算让 Auto Scaling 将组保持在指定大小。请注意，您稍后可以手动扩展此 Auto Scaling 组、根据计划配置要扩展的组或根据需求配置要扩展的组。
21. 在 Review (审核) 页面上，单击 Create Auto Scaling group (创建 Auto Scaling 组)。
22. 创建组后，单击 Close。

测试负载均衡器

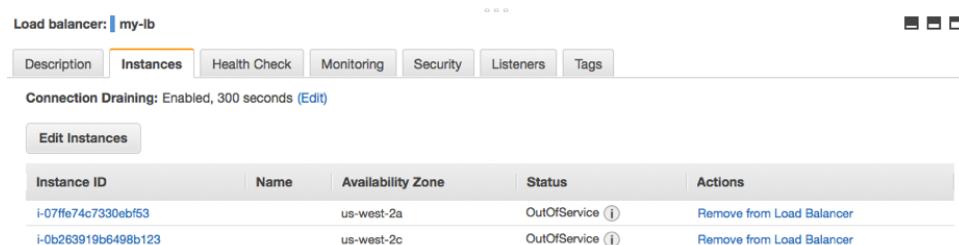
首先，验证 Auto Scaling 是否已启动您的实例并且这些实例已就绪。在 Auto Scaling Groups 页面中，选择您的 Auto Scaling 组，然后选择 Instances 选项卡。



Actions	Instance ID	Lifecycle	Launch Configuration Name	Availability Zone	Health Status	Protected from
	i-07ffe74c7330ebf53	Pending	my-launch-config	us-west-2a	Healthy	
	i-0b263919b6498b123	Pending	my-launch-config	us-west-2c	Healthy	

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。

然后，验证您的实例是否已注册到负载均衡器并准备好接收来自负载均衡器的流量。在 Load Balancers 页面中，选择您的负载均衡器，然后选择 Instances 选项卡。



Instances	Description	Health Check	Monitoring	Security	Listeners	Tags
Connection Draining: Enabled, 300 seconds (Edit)						
Edit Instances						
Instance ID	Name	Availability Zone	Status	Actions		
i-07ffe74c7330ebf53		us-west-2a	OutOfService	Remove from Load Balancer		
i-0b263919b6498b123		us-west-2c	OutOfService	Remove from Load Balancer		

如果实例的状态是 OutOfService，可能表示它们仍在注册过程中。如果状态为 InService，则表示相应实例已就绪。实例就绪后，您可通过以下步骤测试负载均衡器。

测试负载均衡器

- 从 Load Balancers (负载均衡器) 页面选择您的负载均衡器。

2. 在 Description (描述) 选项卡上，找到 DNS 名称。此名称具有以下形式：

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

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

教程：远程管理您的 Amazon EC2 实例

Abstract

了解如何使用 Amazon EC2 Run Command 快速执行命令。

本教程介绍如何从您的本地计算机使用 Amazon Elastic Compute Cloud (Amazon EC2) Run Command 远程管理 Amazon EC2 实例。在此教程中，您将学习如何完成以下任务：

- 启动已为 Run Command 配置的新实例。
- 为 Run Command 配置您的用户账户。
- 使用 Run Command 从您的本地计算机发送一条命令，并检索在实例上运行的服务列表。

本教程包含使用 Amazon EC2 控制台或适用于 Windows PowerShell 的 AWS 工具执行命令的过程。



Note

借助 Run Command，您还可以在本地环境或其他云提供商提供的环境中管理您的服务器和虚拟机 (VM)。有关更多信息，请参阅 [设置托管实例 \(p. 335\)](#)。

启动新实例

实例要求使用允许该实例与 Amazon EC2 Simple Systems Manager (SSM) 进行通信的 AWS Identity and Access Management (IAM) 角色。您必须在创建新实例时分配 IAM 角色。无法将角色分配给已在运行的实例。对于现有实例，您必须创建实例的映像，从该映像启动一个实例，然后在启动实例时分配 IAM 角色。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

创建使用由 SSM 提供支持的角色的实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择支持的区域。
3. 选择 Launch Instance，然后选择 Windows Server Amazon 系统映像 (AMI)。
4. 选择实例类型，然后选择 Next: Configure Instance Details。
5. 在 Auto-assign Public IP 中，选择 Enable。
6. 在 IAM role 旁边，选择 Create new IAM role。IAM 控制台会在新选项卡中打开。
 - a. 选择 Create New Role。
 - b. 在 Step 1: Set Role Name 中，输入用于将此角色标识为 Run Command 角色的名称。
 - c. 在 Step 2: Select Role Type 中，选择 Amazon EC2 Role for Simple Systems Manager。系统会跳过 Step 3: Establish Trust，因为这是一个托管策略。
 - d. 在 Step 4: Attach Policy 中，选择 AmazonEC2RoleforSSM。
 - e. 选择 Next Step，然后选择 Create Role。
 - f. 关闭带有 IAM 控制台的选项卡。

7. 在 Amazon EC2 控制台中，选择 Create New IAM role 旁边的 Refresh 按钮。
8. 从 IAM role 中选择您刚创建的角色。
9. 完成向导以启动新实例。记下实例 ID。您将需要在本教程后面指定此 ID。

向您的用户账户授予对 SSM 的访问权限

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

为您的用户账户创建 IAM 策略

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Policies。（如果这是您首次使用 IAM，请选择 Get Started，然后选择 Create Policy。）
3. 在 Filter 字段中，键入 `AmazonSSMFullAccess` 并按 Enter。
4. 选中 `AmazonSSMFullAccess` 旁边的复选框，然后依次选择 Policy Actions 和 Attach。
5. 在 Attach Policy 页面上，选择您的用户账户，然后选择 Attach Policy。

使用 EC2 控制台发送命令

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

从控制台使用 Run Command 执行命令

1. 在 [Amazon EC2 控制台](#) 的导航窗格中，选择 Command History，然后选择 Run a Command。
2. 在 Command document 列表中，选择 AWS-RunPowerShellScript。
3. 选择 Select instances，然后选择您刚创建的实例。如果您没有看到该实例，请确保您当前位于创建实例时使用的区域。另外，按照本主题中的前文所述，确保您已配置 IAM 角色和信任策略。
4. 在 Commands 字段中，键入 `Get-Service`。如果需要，您可以指定 Working Directory 和 Execution Timeout。Execution Timeout 是 EC2Config 服务在被视为已失败前将尝试运行命令的秒数。建议您在 Comments 字段中输入注释。注释将帮助您识别待处理命令列表中的命令并让查看输出变得轻松。
5. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。
6. 选择 Run 执行命令。Run Command 将显示一个状态屏幕。
7. 选择 View results。
8. 为您刚运行的命令选择命令调用。选择 Output 选项卡，然后选择 View Output。

The screenshot shows the AWS Lambda console interface. At the top, there are two tabs: 'Run a command' (selected) and 'Actions'. Below this is a search bar labeled 'Filter by attributes'. A table lists several command executions:

	Command ID	Instance ID	Document name	Status	Requested date	Comments
<input checked="" type="checkbox"/>	65555b90-ee60-45...	i-8fd6aa30	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	65555b90-ee60-45...	i-d583f76a	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	65555b90-ee60-45...	i-8ed6aa31	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	ca4b10c6-cee1-437...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	getting
<input type="checkbox"/>	561e5f4a-27d2-419...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	ipconfi

Below the table, a message displays the Command ID and Instance ID: 'Command ID: 65555b90-ee60-4520-9dc3-e42e94445469 Instance ID: i-8fd6aa30'. Under the 'Output' tab, details about the command are shown:

Parameter	Value	Instance	State	Comments
Command ID	65555b90-ee60-4520-9dc3-e42e94445469			
Document name	AWS-RunPowerShellScript			
Date requested	October 21, 2015 at 3:56:59 PM UTC-7			
Output S3 bucket	run-command-test			Document parameters

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

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

执行命令

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

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

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

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

4. 执行以下命令来检索在实例上运行的服务。

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

命令将返回一个命令 ID，您将使用该 ID 来查看结果。

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

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

有关如何在 Windows PowerShell 工具 和 AWS 管理控制台中使用 Run Command 执行命令的更多示例，请参阅 [Amazon EC2 Run Command 演练 \(p. 379\)](#)。有关 Run Command 的更多信息，请参阅[远程管理您的实例 \(p. 331\)](#)。

教程：在 Amazon EC2 上设置 Windows HPC 集群

Abstract

在 Amazon EC2 上设置并启动可扩展 Windows HPC 集群。

您可以使用 Amazon EC2 实例启动可扩展 Microsoft Windows 高性能计算 (HPC) 集群。Windows HPC 集群需要 Active Directory 域控制器、DNS 服务器、头节点以及一个或多个计算节点。

要在 Amazon EC2 上设置 Windows HPC 集群，请完成以下任务：

- 步骤 1：设置您的 Active Directory 域控制器 (p. 43)
- 步骤 2：配置头节点 (p. 46)
- 步骤 3：设置计算节点 (p. 48)
- 步骤 4：扩展您的 HPC 计算节点（可选）(p. 49)

有关高性能计算的更多信息，请参阅 [AWS 上的高性能计算 \(HPC\)](#)。

先决条件

- 安装 AWS Command Line Interface 工具，并设置要用作默认区域的区域。有关更多信息，请参阅 [AWS Command Line Interface 用户指南](#) 中的 [安装 AWS 命令行界面](#)。
- 这些步骤假定您具有要在其中启动实例的 VPC。您可以使用默认的 VPC，也可以配置非默认的 VPC。有关更多信息，请参阅 [什么是 Amazon VPC？](#)（在 [Amazon VPC 用户指南](#) 中）。

步骤 1：设置您的 Active Directory 域控制器

Active Directory 域控制器提供身份验证以及针对 HPC 环境的集中式资源管理，而且是安装所必需的。要设置 Active Directory，请完成以下步骤：

1. 创建 Active Directory 所需的安全组。
2. 创建用作 HPC 集群的域控制器的实例。
3. 为您的 HPC 集群配置该域控制器。

为 Active Directory 创建安全组

使用 AWS CLI 为域控制器和域成员创建安全组。

为 Active Directory 创建所需的安全组

1. 在 VPC 中为域控制器创建安全组。记下输出中的安全组 ID。

```
aws ec2 create-security-group --vpc-id vpc-id --group-name "SG - Domain Controller" --description "Active Directory Domain Controller"

{
    "GroupId": "dc-security-group-id"
}
```

2. 在 VPC 中为域成员创建安全组。记下输出中的安全组 ID。

```
aws ec2 create-security-group --vpc-id vpc-id --group-name "SG - Domain Member" --description "Active Directory Domain Member"

{
    "GroupId": "dm-security-group-id"
}
```

3. 将 [Active Directory 安全组的 IP 权限 \(p. 50\)](#) 中的第一个文件的内容复制到文本编辑器。将 *dm-security-group-id* 值替换为您的域成员安全组的 ID。使用文件名 *dc-sg-rules.json* 保存文件。
4. 将规则添加到域控制器安全组。

```
aws ec2 authorize-security-group-ingress --group-id dc-security-group-id --ip-permissions file:///dc-sg-rules.json
```



Note

如果 JSON 文件不在您所使用的目录中，则必须在 *file://* 后面包括此文件的路径。

5. 将 [Active Directory 安全组的 IP 权限 \(p. 50\)](#) 中的第二个文件的内容复制到文本编辑器。将 *dc-security-group-id* 值替换为您的域控制器安全组的 ID。使用文件名 *dm-sg-rules.json* 保存文件。
6. 将规则添加到域成员安全组。

```
aws ec2 authorize-security-group-ingress --group-id dm-security-group-id --ip-permissions file:///dm-sg-rules.json
```

7. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
8. 在导航窗格中，选择 Security Groups。确认以下安全组显示在列表中且填充有所需的规则：

- SG - Domain Controller
- SG - Domain Member

或者，手动设置防火墙以允许所需端口上的流量。有关更多信息，请转到 Microsoft 网站上的[如何为域和信任关系配置防火墙](#)。

为您的 HPC 集群创建域控制器

启动将用作 HPC 集群域控制器的实例。

为您的 HPC 集群创建域控制器

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 选择您创建了安全组的同一个区域。
2. 在控制台控制面板中，选择 Launch Instance。
3. 在 Choose an AMI 页上，为 Windows Server 选择一个 AMI，然后选择 Select。
4. 在向导的下一页上，选择一种实例类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details 页上，从 Network 中选择 VPC，从 Subnet 中选择子网。在向导的下一页上，您可以为实例指定额外的存储。
6. 在 Tag Instance 页上，输入 Domain Controller 作为 Name 标签的值，然后选择 Next: Configure Security Group。
7. 在 Configure Security Group 页上，选择 Select an existing security group，从安全组列表中选择 SG - Domain Controller，然后选择 Review and Launch。
8. 选择 Launch。

启动实例后，请关联弹性 IP 和实例。

要关联弹性 IP 地址和实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate New Address。
4. 根据提示选择 Yes, Allocate，然后关闭确认对话框。



Note

如果您的账户支持 EC2-Classic，请首先从列表中选择 VPC。

5. 选择您创建的弹性 IP 地址，选择 Actions，然后选择 Associate Address。
6. 在 Instance 列表中，选择 Domain Controller 实例，然后选择 Associate。

为您的 HPC 集群配置域控制器

连接到您创建的实例，并将服务器配置为 HPC 集群的域控制器。

将实例配置为域控制器

1. 连接到您的 Domain Controller 实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
2. 打开 Server Manager (服务器管理器)，然后添加“Active Directory Domain Services (Active Directory 域服务)”角色。
3. 通过“服务器管理器”或运行 DCPromo.exe，将服务器升级为域控制器。
4. 在新林中创建新域。
5. 输入 hpc.local 作为完全限定域名 (FQDN)。
6. 选择林功能级别 Windows Server 2008 R2。
7. 确保 DNS Server 选项已选中，然后选择 Next。

8. 选择 Yes, the computer will use an IP address automatically assigned by a DHCP server (not recommended) (是，该计算机将使用 DHCP 服务器自动分配的 IP 地址(不推荐))。
9. 在警告框中，选择 Yes 以继续操作。
10. 完成向导，然后选择 Reboot on Completion (完成后重新启动)。
11. 以 `hpc.local\administrator` 身份连接到实例。
12. 创建域用户 `hpc.local\hpcuser`。

步骤 2：配置头节点

一个 HPC 客户端连接到头节点。头节点会促进相关预定的任务。您可通过完成以下步骤来配置头节点：

1. 为您的 HPC 集群创建安全组。
2. 启动头节点实例。
3. 安装 HPC 包。
4. 配置您的 HPC 集群。

为您的 HPC 集群创建安全组

使用 AWS CLI 为 HPC 集群创建安全组。

为您的 HPC 集群创建安全组

1. 在 VPC 中为 HPC 集群创建安全组。记下输出中的安全组 ID。

```
aws ec2 create-security-group --vpc-id vpc-id --group-name "SG - Windows HPC Cluster" --description "Windows HPC Server 2008 R2 Cluster Nodes"

{
    "GroupId": "hpc-security-group-id"
}
```

2. 将 [HPC 集群安全组的 IP 权限 \(p. 54\)](#) 中的 JSON 文件的内容复制到文本编辑器。将 `hpc-security-group-id` 值替换为您的 HPC 安全组的 ID。使用文件名 `hpc-sg-rules.json` 保存文件。
3. 将规则添加到 HPC 集群安全组。

```
aws ec2 authorize-security-group-ingress --group-id hpc-security-group-id --ip-permissions file://hpc-sg-rules.json
```

4. 打开 Amazon EC2 控制台，从导航窗格中选择 Security Groups，并确认 SG - Windows HPC Cluster 安全组显示在列表中且填充有所需的安全组规则。

或者，为要进行通信的 HPC 集群成员手动配置具有端口要求的防火墙。有关更多信息，请参阅 Microsoft 网站上的 [Windows 防火墙配置](#)。

启动 HPC 头节点实例

启动一个实例，然后将其配置为具有必要用户账户的 `hpc.local` 域成员。

将实例配置为头节点

1. 启动一个实例，将其命名为 HPC-Head。当您启动该实例时，请选择以下两个安全组：

- SG - Windows HPC Cluster
- SG - Domain Member

2. 连接到实例，并使用以下命令从 HPC-Head 获取现有 DNS 服务器地址：

```
C:\> IPConfig /all
```

3. 更新 HPC-Head NIC 的 TCP/IPv4 属性以包括 Domain Controller 实例的弹性 IP 地址作为主 DNS，然后添加上一步中的附加 DNS IP 地址。
4. 使用 hpc.local (域管理员账户) 的证书将计算机加入到 hpc.local\administrator 域。
5. 以本地管理员身份添加 hpc.local\hpcuser。出现提供证书的提示时，使用 hpc.local\administrator，然后重新启动实例。
6. 以 hpc.local\hpcuser 身份连接到 HPC-Head。

安装 HPC 包

安装 HPC 包

1. 使用账户连接到您的 HPC-Head hpc.local\hpcuser 实例。
2. 通过 Server Manager (服务器管理器)，关闭针对管理员的 Internet Explorer 增强的安全配置 (IE ESC)。
 - a. 在 Server Manager 中的 Security Information 下，选择 Configure IE ESC。
 - b. 关闭针对管理员的 IE ESC。
3. 在 HPC-Head 上安装 HPC 包。
 - a. 将 HPC 包从 HPC-Head Microsoft 下载中心[下载到](#)。选择适用于 HPC-Head 上的 Windows Server 版本的 HPC 包。
 - b. 将相关文件提取到一个文件夹中，打开该文件夹并双击 setup.exe。
 - c. 在 Installation 页上，选择 Create a new HPC cluster by creating a head node，然后选择 Next。
 - d. 接受默认设置以在头节点上安装所有数据库，然后选择 Next。
 - e. 完成向导。

在头节点上配置您的 HPC 集群

在头节点上配置您的 HPC 集群

1. 启动 HPC Cluster Manager。
2. 在 Deployment To-Do List (部署待办事项列表) 中，选择 Configure your network (配置您的网络)。
 - a. 在向导中，选择默认选项 (5)，然后选择 Next。
 - b. 接受所有屏幕上的默认值以结束向导，然后选择您想如何更新服务器和参与客户反馈。
 - c. 选择 Configure。

3. 选择 Provide Network Credentials (提供网络证书) , 然后提供 hpc.local\hpcuser 证书。
4. 选择 Configure the naming of new nodes , 然后选择 OK。
5. 选择 Create a node template (创建节点模板)。
 - a. 选择 Compute node template , 然后选择 Next。
 - b. 选择 Without operating system (不使用操作系统) , 然后使用默认设置继续。
 - c. 选择 Create。

步骤 3：设置计算节点

设置计算节点涉及以下步骤：

1. 启动计算节点实例。
2. 在实例上安装 HPC 包。
3. 将计算节点添加到您的集群。

启动 HPC 计算节点实例

配置您的计算节点，方法是启动一个实例，然后使用必要的用户账户将该实例配置为 hpc.local 域的成员。

配置计算节点实例

1. 启动一个实例，将其命名为 HPC-Compute。当您启动实例时，选择以下安全组：SG - Windows HPC Cluster (SG - Windows HPC 集群) 和 SG - Domain Member (SG - 域成员)。
2. 使用以下命令登录该实例，并从 HPC-Compute 获取现有 DNS 服务器地址：

```
C:\> IPConfig /all
```

3. 更新 HPC-Compute NIC 的 TCP/IPv4 属性以包括 Domain Controller 实例的弹性 IP 地址作为主 DNS。然后从上一步开始添加其他 DNS IP 地址。
4. 使用 hpc.local (域管理员账户) 的证书将计算机加入到 hpc.local\administrator 域。
5. 以本地管理员身份添加 hpc.local\hpcuser。当系统提示您提供证书时，使用 hpc.local\administrator，然后重新启动。
6. 以 hpc.local\hpcuser 身份连接到 HPC-Compute。

在计算节点上安装 HPC 包

在计算节点上安装 HPC 包

1. 使用 HPC-Compute 账户连接到您的 hpc.local\hpcuser 实例。
2. 通过 Server Manager (服务器管理器)，关闭针对管理员的 Internet Explorer 增强的安全配置 (IE ESC)。
 - a. 在 Server Manager 中的 Security Information 下，选择 Configure IE ESC。
 - b. 关闭针对管理员的 IE ESC。

3. 在 HPC-Compute 上安装 HPC 包。
 - a. 将 HPC 包从 HPC-Compute Microsoft 下载中心[下载到](#)。选择适用于 HPC-Compute 上的 Windows Server 版本的 HPC 包。
 - b. 将相关文件提取到一个文件夹中，打开该文件夹并双击 setup.exe。
 - c. 在 Installation 页上，选择 Join an existing HPC cluster by creating a new compute node，然后选择 Next。
 - d. 指定 HPC-Head 实例的完全限定名称，然后选择默认设置。
 - e. 完成向导。

将计算节点添加到您的 HPC 集群

要完成您的集群配置，请从头节点中将计算节点添加到您的集群。

将计算节点添加到您的集群

1. 以 HPC-Head 身份连接到 hpc.local\hpcuser 实例。
2. 打开 HPC Cluster Manager。
3. 选择 Node Management (节点管理)。
4. 如果 Unapproved (未批准) 存储桶中显示了计算节点，请右键单击列出的节点，然后选择 Add Node (添加节点)。
 - a. 选择 Add compute nodes or broker nodes that have already been configured (添加已经配置的计算节点或代理节点)。
 - b. 选中节点旁边的复选框并选择 Add。
5. 右键单击节点并选择 Bring Online。

步骤 4：扩展您的 HPC 计算节点（可选）

扩展您的计算节点

1. 以 HPC-Compute 身份连接到 hpc.local\hpcuser 实例。
2. 删除您从 HP Pack 安装包下载到本地的所有文件。（由于您已运行安装程序并在自己的映像中创建了这些文件，因此无需再为 AMI 复制这些文件。）
3. 从 C:\Program Files\Amazon\Ec2ConfigService 打开文件 sysprep2008.xml。
4. 在 <settings pass="specialize"> 底部，添加以下部分。确保替换 hpc.local、password 和 hpcuser 以匹配您的环境。

```
<component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Identification>
        <UnsecureJoin>false</UnsecureJoin>
    <Credentials>
        <Domain>hpc.local</Domain>
        <Password>password</Password>
```

```
        <Username>hpcuser</Username>
    </Credentials>
    <JoinDomain>hpc.local</JoinDomain>
</Identification>
</component>
```

5. 保存 sysprep2008.xml。
 6. 依次选择 Start、All Programs 和 EC2ConfigService Settings。
 - a. 选择 General 选项卡，并清除 Set Computer Name 复选框。
 - b. 选择 Bundle 选项卡，然后选择 Run Sysprep and Shutdown Now。
 7. 打开 Amazon EC2 控制台。
 8. 在导航窗格中，选择 Instances。
 9. 等待实例状态显示为 stopped (停止)。
 10. 选择实例，再依次选择 Actions、Image 和 Create Image。
 11. 指定映像名称和映像描述，然后选择 Create Image 以便从实例创建 AMI。
 12. 启动已关闭的原始 HPC-Compute 实例。
 13. 使用 hpc.local\hpcuser 账户连接到头节点。
 14. 在 HPC Cluster Manager 中，删除现在以错误状态显示的旧节点。
 15. 在 Amazon EC2 控制台的导航窗格中，选择 AMIs。
 16. 使用您创建的 AMI 向集群添加附加节点。

您可以从已创建的 AMI 启动附加计算节点。这些节点会自动加入域，但是您必须使用头节点将它们作为已在 HPC Cluster Manager 配置的节点添加到集群，然后将这些节点联机。

运行 Lizard 性能测量应用程序

您可以选择性地运行 Lizard 应用程序，测量 HPC 集群可实现的计算性能和效率。请转到 <http://www.microsoft.com/download/en/details.aspx?id=8433>，下载 lizard_x64.msi 安装程序，然后以 hpc.local\hpcuser 身份直接在头节点上运行安装程序。

Active Directory 安全组的 IP 权限

下面的 JSON 包含 Active Directory 环境的安全组的 IP 权限结构：一个组用于 Active Directory 域控制器，另一个组用于 Active Directory 域成员服务器。

有关这些安全组规则的更多信息，请转到以下 Microsoft 文章：<http://support.microsoft.com/kb/179442>。

1. 域控制器安全组的安全组规则

以下规则适用于域控制器安全组。将 `dm-security-group-id` 值替换为您的域成员安全组的 ID。将 `cidr_block` 值替换为本地网络的 CIDR 块。

```
    "Protocol": "UDP",  
    "FromPort": 123,  
    "ToPort": 123,  
    "UserIdGroupPairs": [  
        {
```

```
        "GroupId": "dm-security-group-id"
    }
]
},
{
    "IpProtocol": "TCP",
    "FromPort": 135,
    "ToPort": 135,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "UDP",
    "FromPort": 138,
    "ToPort": 138,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 49152,
    "ToPort": 65535,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 389,
    "ToPort": 389,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "UDP",
    "FromPort": 389,
    "ToPort": 389,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 636,
    "ToPort": 636,
```

```
"UserIdGroupPairs": [
    {
        "GroupId": "dm-security-group-id"
    }
]
},
{
    "IpProtocol": "TCP",
    "FromPort": 3268,
    "ToPort": 3269,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 53,
    "ToPort": 53,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "UDP",
    "FromPort": 53,
    "ToPort": 53,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "UDP",
    "FromPort": 88,
    "ToPort": 88,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 88,
    "ToPort": 88,
    "UserIdGroupPairs": [
        {
            "GroupId": "dm-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
```

```
"FromPort": 445,  
"ToPort": 445,  
"UserIdGroupPairs": [  
    {  
        "GroupId": "dm-security-group-id"  
    }  
],  
,  
{  
    "IpProtocol": "UDP",  
    "FromPort": 445,  
    "ToPort": 445,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "dm-security-group-id"  
        }  
    ]  
},  
,  
{  
    "IpProtocol": "ICMP",  
    "FromPort": -1,  
    "ToPort": -1,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "dm-security-group-id"  
        }  
    ]  
},  
,  
{  
    "IpProtocol": "UDP",  
    "FromPort": 53,  
    "ToPort": 53,  
    "IpRanges": [  
        {  
            "CidrIp": "cidr_block"  
        }  
    ]  
},  
,  
{  
    "IpProtocol": "TCP",  
    "FromPort": 3389,  
    "ToPort": 3389,  
    "IpRanges": [  
        {  
            "CidrIp": "cidr_block"  
        }  
    ]  
}  
]
```

2. 域成员安全组的安全组规则

以下规则适用于域成员安全组。将 dc-security-group-id 值替换为您的域控制器安全组的 ID。

```
[  
{
```

```
"IpProtocol": "TCP",
"FromPort": 49152,
"ToPort": 65535,
"UserIdGroupPairs": [
    {
        "GroupId": "dc-security-group-id"
    }
]
},
{
    "IpProtocol": "UDP",
    "FromPort": 49152,
    "ToPort": 65535,
    "UserIdGroupPairs": [
        {
            "GroupId": "dc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 53,
    "ToPort": 53,
    "UserIdGroupPairs": [
        {
            "GroupId": "dc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "UDP",
    "FromPort": 53,
    "ToPort": 53,
    "UserIdGroupPairs": [
        {
            "GroupId": "dc-security-group-id"
        }
    ]
}
]
```

HPC 集群安全组的 IP 权限

下面的 JSON 文件包含为 HPC 集群节点创建安全组所需的 IP 权限。将 hpc-security-group-id 值替换为 SG - Windows HPC Cluster 安全组的 ID。最后一个规则使您可以通过 RDP 连接实例。将 cidr_block 值替换为您网络的 CIDR 块。

有关这些安全组规则的更多信息，请转到以下 Microsoft 文章：http://technet.microsoft.com/en-us/library/ff919486.aspx#BKMK_Firewall

```
[
{
    "IpProtocol": "TCP",
    "FromPort": 80,
    "ToPort": 80,
    "UserIdGroupPairs": [
```

```
{  
    "GroupId": "hpc-security-group-id"  
}  
]  
}  
,  
{  
    "IpProtocol": "TCP",  
    "FromPort": 443,  
    "ToPort": 443,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "hpc-security-group-id"  
        }  
    ]  
},  
{  
    "IpProtocol": "TCP",  
    "FromPort": 1856,  
    "ToPort": 1856,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "hpc-security-group-id"  
        }  
    ]  
},  
{  
    "IpProtocol": "TCP",  
    "FromPort": 5800,  
    "ToPort": 5801,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "hpc-security-group-id"  
        }  
    ]  
},  
{  
    "IpProtocol": "TCP",  
    "FromPort": 5801,  
    "ToPort": 5801,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "hpc-security-group-id"  
        }  
    ]  
},  
{  
    "IpProtocol": "TCP",  
    "FromPort": 5969,  
    "ToPort": 5969,  
    "UserIdGroupPairs": [  
        {  
            "GroupId": "hpc-security-group-id"  
        }  
    ]  
},  
{  
    "IpProtocol": "TCP",  
    "FromPort": 5970,
```

```
"ToPort": 5970,
"UserIdGroupPairs": [
    {
        "GroupId": "hpc-security-group-id"
    }
],
{
    "IpProtocol": "TCP",
    "FromPort": 5974,
    "ToPort": 5974,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 5999,
    "ToPort": 5999,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 6729,
    "ToPort": 6730,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 7997,
    "ToPort": 7997,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 8677,
    "ToPort": 8677,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
```

```
"IpProtocol": "TCP",
"FromPort": 9087,
"ToPort": 9087,
"UserIdGroupPairs": [
    {
        "GroupId": "hpc-security-group-id"
    }
]
},
{
    "IpProtocol": "TCP",
    "FromPort": 9090,
    "ToPort": 9092,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 9100,
    "ToPort": 9163,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 9200,
    "ToPort": 9263,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 9794,
    "ToPort": 9794,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
},
{
    "IpProtocol": "TCP",
    "FromPort": 9892,
    "ToPort": 9893,
    "UserIdGroupPairs": [
        {
            "GroupId": "hpc-security-group-id"
        }
    ]
}
```

```
        },
        {
            "IpProtocol": "UDP",
            "FromPort": 9893,
            "ToPort": 9893,
            "UserIdGroupPairs": [
                {
                    "GroupId": "hpc-security-group-id"
                }
            ]
        },
        {
            "IpProtocol": "TCP",
            "FromPort": 6498,
            "ToPort": 6498,
            "UserIdGroupPairs": [
                {
                    "GroupId": "hpc-security-group-id"
                }
            ]
        },
        {
            "IpProtocol": "TCP",
            "FromPort": 7998,
            "ToPort": 7998,
            "UserIdGroupPairs": [
                {
                    "GroupId": "hpc-security-group-id"
                }
            ]
        },
        {
            "IpProtocol": "TCP",
            "FromPort": 8050,
            "ToPort": 8050,
            "UserIdGroupPairs": [
                {
                    "GroupId": "hpc-security-group-id"
                }
            ]
        },
        {
            "IpProtocol": "TCP",
            "FromPort": 5051,
            "ToPort": 5051,
            "UserIdGroupPairs": [
                {
                    "GroupId": "hpc-security-group-id"
                }
            ]
        },
        {
            "IpProtocol": "TCP",
            "FromPort": 3389,
            "ToPort": 3389,
            "IpRanges": [
                {
                    "CidrIp": "cidr_block"
                }
            ]
        }
    ]
}
```

```
        }  
    ]  
}
```

Amazon 系统映像 (AMI)

Abstract

AMI 为实例提供软件配置。

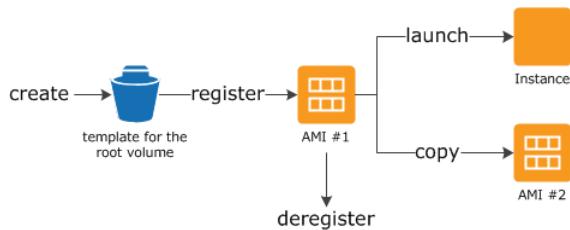
Amazon 系统映像 (AMI) 提供启动实例 (云中的虚拟服务器) 所需的信息。您在启动实例时指定 AMI , 可以从该 AMI 启动所需任意数量的实例。您还可以根据需要从任意多个不同 AMI 启动实例。

AMI 包括以下内容 :

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

使用 AMI

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



您可以搜索符合您实例条件的 AMI。您可以搜索 AWS 提供的 AMI 或社区提供的 AMI。有关更多信息 , 请参阅 [AMI 类型 \(p. 62\)](#) 和 [查找 Windows AMI \(p. 65\)](#)。

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 \(p. 110\)](#)。

创建您自己的 AMI

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

实例的根存储设备确定创建 AMI 所遵循的过程。实例的根卷是 Amazon EBS 卷或实例存储卷。有关信息，请参阅 [根设备卷 \(p. 8\)](#)。

要创建由 Amazon EBS 支持的 AMI，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。要创建由实例存储支持的 AMI，请参阅[创建实例存储支持的 Windows AMI \(p. 78\)](#)。

您可以为 AMI 分配自定义标签，以帮助您对 AMI 进行分类和管理。有关更多信息，请参阅[标记 Amazon EC2 资源 \(p. 737\)](#)。

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 \(p. 67\)](#)。

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

取消注册您的 AMI

使用完 AMI 之后，可以取消注册它。取消注册 AMI 之后，便无法将其用于启动新实例。有关更多信息，请参阅[取消注册您的 AMI \(p. 89\)](#)。

AWS Windows AMI

AWS 提供了一组公开可用的 AMI，其中包含特定于 Windows 平台的软件配置。借助这些 AMI，您可以使用 Amazon EC2 快速开始生成和部署应用程序。首先选择满足您的特定要求的 AMI，然后使用该 AMI 启动实例。检索管理员账户的密码，然后使用远程桌面连接登录实例，就如同使用任何其他 Windows 服务器一样。管理员账户的名称取决于操作系统语言。例如，在英语中是 Administrator，在法语中是 Administrateur，在葡萄牙语中是 Administrador。有关更多信息，请参阅 Microsoft TechNet Wiki 中的 [Localized Names for Administrator Account in Windows](#)。

选择初始 Windows AMI

要使用 Amazon EC2 控制台查看 AWS 提供的 Windows AMI，请单击此链接以筛选公用 AMI 的列表：[Windows AMI](#)。如果您使用 Amazon EC2 控制台启动实例，则向导的第一页包括 Quick Start (快速启动) 选项卡，其中列出了 AWS 提供的一些最常用的 AMI，包括符合免费套餐要求的 AMI。

AWS 目前针对以下版本的 Windows 提供 AMI：

- Microsoft Windows Server 2012 R2 (64 位)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)

- Microsoft Windows Server 2008 (64-bit)
- Microsoft Windows Server 2008 (32-bit)
- Microsoft Windows Server 2003 R2 (64 位)
- Microsoft Windows Server 2003 R2 (32 位)

其中一些 AMI 还包括 Microsoft SQL Server (SQL Enterprise Edition、SQL Server Standard、SQL Server Express 或 SQL Server Web) 的版本。从包含 Microsoft SQL Server 的 AWS Windows AMI 启动实例，您可以像使用数据库服务器那样运行实例。此外，您可以从任意 Windows AMI 启动实例，然后在实例上安装您需要的数据库软件。要查看包含 SQL Server 的 Windows Server AMI，请参阅 AWS Marketplace 上的 [Windows AMI](#)。

一些 AMI 附带了互联网信息服务 (IIS) 并且已配置了 ASP.NET，以帮助您快速入门。此外，您可以从任意 Windows AMI 启动实例，然后安装 IIS 和 ASP.NET。如需分步指导，请参阅 *Getting Started with AWS: 托管一个 .NET Web 应用程序 中的配置您的 EC2 实例*。

除 AWS 提供的公用 AMI 之外，您还可以使用 AWS 开发人员社区发布的 AMI。我们强烈建议您只使用 AWS 或其他可靠来源提供的 Windows AMI。要了解如何查找 Amazon 批准的 Microsoft Windows AMI 的列表，请参阅 [查找 Windows AMI \(p. 65\)](#)。

您也可以从您的 Windows 计算机创建 AMI。有关更多信息，请参阅 [导入和导出虚拟机 \(p. 401\)](#)。

保持您的 AMI 为最新

AWS 在 Microsoft 的修补程序星期二（每个月的第二个星期二）后的五个工作日内提供更新的、完整修补的 Windows AMI。有关更多信息，请参阅 [AWS Windows AMI 版本 \(p. 93\)](#)。

初始启动之后，您的 Windows 实例即包含所有最新的安全更新。我们建议您在启动 Windows 之后，首先运行 Windows 更新服务，然后再创建 AMI。在您启动实例或创建 AMI 之后，您将负责确保其最新。您可以使用 Windows 更新服务或实例上的 Automatic Updates 工具来将 Microsoft 更新部署到您的实例。您还必须通过适用于部署到您的实例上的任何其他软件的机制，确保该软件为最新。在您更新 Windows 实例之后，您可以创建 AMI，替换任何以前创建的 AMI。有关更多信息，请参阅 [更新您的 Windows 实例 \(p. 92\)](#)。

AMI 类型

Abstract

基于区域、操作系统、架构和根卷类型选择 AMI。

可以基于以下特性选择要使用的 AMI：

- 区域（请参阅 [地区和可用区域 \(p. 6\)](#)）
- 操作系统
- 架构（32 位或 64 位）
- [启动许可 \(p. 62\)](#)
- [根设备存储 \(p. 63\)](#)

启动许可

AMI 的拥有者通过指定启动许可来确定其可用性。启动许可分为以下类别。

启动许可	说明
公有	拥有者向所有 AWS 账户授予启动许可。
显式	拥有者向特定 AWS 账户授予启动许可。
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 \(p. 67\)](#)。开发人员可以为其 AMI 收费。有关更多信息，请参阅 [付费 AMI \(p. 72\)](#)。

根设备存储

所有 AMI 均可归类为由 Amazon EBS 支持或由实例存储支持。前者是指从 AMI 启动的实例的根设备是从 Amazon EBS 快照创建的 Amazon EBS 卷。后者是指从 AMI 启动的实例的根设备是从存储在 Amazon S3 中的模板创建的实例存储卷。有关更多信息，请参阅 [根设备卷 \(p. 8\)](#)。

本节总结了两种类型的 AMI 之间的重要区别。下表简要总结了这些区别。

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

* 默认情况下，Amazon EBS 支持的实例根卷的 `DeleteOnTermination` 标志设置为 `true`。有关如何更改此标志以便卷在终止之后保留的信息，请参阅 [根设备卷 \(p. 8\)](#)。

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

大小限制

由 Amazon EC2 实例存储支持的 AMI 仅限于 10 GiB 存储大小的根设备，而由 Amazon EBS 支持的 AMI 的上限为 1 TiB。许多 Windows AMI 的大小都接近 10 GiB 的上限，因此您会发现 Windows AMI 大多由 Amazon EBS 卷支持。



Note

默认情况下，所有 Windows Server 2008、Windows Server 2008 R2 和 Windows Server 2012 AMI 都由 Amazon EBS 卷支持，因为这些 AMI 比较大。

停止状态

您可以停止由 Amazon EBS 支持的实例，但不能停止由 Amazon EC2 实例存储支持的实例。停止操作会导致实例停止运行（它的状态会由 running 变成 stopping 再到 stopped）。停止的实例保留在 Amazon EBS 中，这样就可重新启动。停止与终止不同；您无法重新启动一个已终止的实例。因为由 Amazon EC2 实例存储支持的 AMI 不能被停止，所以这些 AMI 要么在运行要么已经终止。有关实例停止可能会发生情况及您可以执行哪些操作的更多信息，请参阅 [停止和启动您的实例 \(p. 227\)](#)。

默认数据存储和持久性

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

使用 Amazon EBS 作为根设备的实例自动附加 Amazon EBS 卷。该卷像其他卷一样显示在您的卷列表中。默认情况下，实例不使用任何可用的实例存储卷。您可以使用块储存设备映射添加实例存储或其他 Amazon EBS 卷。有关更多信息，请参阅 [块储存设备映射 \(p. 712\)](#)。有关停止实例时实例存储卷可能发生的状况的信息，请参阅 [停止和启动您的实例 \(p. 227\)](#)。

启动时间

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

AMI 创建

若要创建由实例存储支持的 Windows AMI，您可以通过一个 API 操作来创建 AMI，通过另一个 API 操作来注册 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 Windows AMI \(p. 76\)](#)。

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

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

当由 Amazon EBS 支持的实例停止时，您无需再为实例使用付费；但是，您仍需为卷存储付费。每次从停止状态转换到运行状态，即使您在一小时内进行多次状态转换，我们都按一个完整实例小时收费。例如，假设您的实例每小时的实例收费为 0.10 USD。如果您要运行该实例一小时，中途不停止，您将被收取 0.10 USD。如果您在一小时内停止并重新启动该实例两次，您将因该使用小时被收取 0.30 USD（最初 0.10 USD，加上 2 x 每次重新启动 0.10 USD）。

查找 Windows AMI

Abstract

搜索符合您的要求的 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（请参阅[AWS Windows AMI \(p. 61\)](#)）
- 架构：32 位 (i386) 或 64 位 (x86_64)
- 根设备类型：Amazon EBS 或实例存储
- 提供商：Amazon Web Services、Oracle、IBM、Microsoft 或社区

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

内容

- 使用 Amazon EC2 控制台查找 Windows AMI (p. 65)
- 使用 AWS CLI 查找 AMI (p. 66)
- 使用适用于 Windows PowerShell 的 AWS 工具 查找 AMI (p. 66)
- 查找 Windows Server 2003 AMI (p. 67)

使用 Amazon EC2 控制台查找 Windows AMI

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

使用“Images (映像)”页面查找 Windows AMI

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中选择区域。您可以选择向您提供的任何区域，无需理会您身处的位置。这是您将在其中启动实例的区域。
3. 在导航窗格中，选择 AMIs。
4. (可选) 使用 Filter (筛选条件) 选项将显示的 AMI 列表范围确定为仅限您关注的 AMI。例如，要列出 AWS 提供的所有 Windows 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. 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 \(p. 218\)](#)。如果您没有准备好立即启动实例，请记下 AMI ID (ami-xxxxxxx) 以供将来使用。

在您启动实例时查找 Windows AMI

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

使用 AWS CLI 查找 AMI

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

```
C:\> aws ec2 describe-images --owners self amazon
```

在上一个命令中添加以下筛选条件以便仅显示 Windows AMI：

```
--filters "Name=platform,Values=windows"
```

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

使用适用于 Windows PowerShell 的 AWS 工具 查找 AMI

您可以使用命令行参数仅列出您感兴趣的 AMI 类型。有关更多信息，请参阅 *适用于 Windows PowerShell 的 AWS 工具 用户指南* 中的[使用 Windows PowerShell 查找 AMI](#)。

找到满足您需要的 AMI 之后，记下其 ID (ami-xxxxxxx)。您可以使用此 AMI 启动实例。有关更多信息，请参阅 *适用于 Windows PowerShell 的 AWS 工具 用户指南* 中的[使用 Windows PowerShell 启动实例](#)。

查找 Windows Server 2003 AMI

自 2015 年 7 月 14 日起，Microsoft 不再支持 Windows Server 2003。如果您的企业或组织目前正在运行 Windows Server 2003 EC2 实例，建议您将这些实例升级到 Windows Server 2008。有关更多信息，请参阅[将 Windows Server EC2 实例升级到新版本 Windows Server](#)。

查找 Windows Server 2003 AMI

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 AMIs。
3. 选择 Owned by me，然后选择 Public images。
4. 在 Search 字段中，添加以下筛选条件。
 - a. Owner : Amazon images
 - b. AMI Name : Windows_Server-2003



Note

Search 字段区分大小写。

共享 AMI

Abstract

查找或共享公用 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，对其进行适当的功能调查。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 的公用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 Windows AMI](#) 或 [创建 Amazon EBS 支持的 Windows AMI](#)。有关在 AWS Marketplace 中构建、交付和维护应用程序的更多信息，请参阅[AWS Marketplace 用户指南](#)和[AWS Marketplace 卖方指南](#)。

内容

- [查找共享 AMI \(p. 68\)](#)
- [将 AMI 设为公用 \(p. 69\)](#)
- [将 AMI 与特定 AWS 账户共享 \(p. 70\)](#)
- [使用书签 \(p. 71\)](#)
- [共享 Windows AMI 指导原则 \(p. 71\)](#)

查找共享 AMI

Abstract

查找共享 AMI。

可以使用 Amazon EC2 控制台或命令行查找共享 AMI。

查找共享 AMI (控制台)

使用控制台查找共享的私有 AMI

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

使用控制台查找共享的公用 AMI

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

查找共享 AMI (命令行)

使用命令行工具查找共享的公用 AMI

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

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

```
C:\> aws ec2 describe-images --executable-users all
```

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

```
C:\> aws ec2 describe-images --executable-users self
```

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

```
C:\> aws ec2 describe-images --owners amazon
```

以下命令列出指定 AWS 账户拥有的 AMI。

```
C:\> aws ec2 describe-images --owners 123456789012
```

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

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

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

将 AMI 设为公用

Abstract

与所有 Amazon EC2 用户共享您的 AMI。

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 \(p. 70\)](#)）。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。



Note

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

与所有 AWS 账户分享 AMI（控制台）

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

使用控制台共享公用 AMI

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

与所有 AWS 账户共享 AMI（命令行）

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

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

将 AMI 设为公用

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

```
C:\> aws ec2 modify-image-attribute --image-id ami-2bb65342 --launch-permission "[{"Add": [{"Group": "all"}]}]"
```

要验证 AMI 的启动许可，请使用以下 `describe-image-attribute` 命令。

```
C:\> aws ec2 describe-image-attribute --image-id ami-2bb65342 --attribute launchPermission
```

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

```
C:\> aws ec2 modify-image-attribute --image-id ami-2bb65342 --launch-permission "{\"Remove\":[{\"Group\": \"all\"}]}"
```

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

将 AMI 与特定 AWS 账户共享

Abstract

将 AMI 与特定 Amazon EC2 用户共享。

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。

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.amazonaws.cn/ec2/>。
2. 在导航窗格中 , 选择 AMIs。
3. 在列表中选择您的 AMI , 然后选择 Actions、Modify Image Permissions。
4. 在 AWS Account Number 字段中指定您想与之共享 AMI 的用户的 AWS 账号 , 然后选择 Add Permission。

要与多个用户共享此 AMI , 请重复上述步骤 , 直至您添加完所需全部用户。

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



Note

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

6. 完成后选择 Save。

共享 AMI (命令行)

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

要授予显式启动许可

以下命令向指定 AWS 账户授予指定 AMI 的启动许可。

```
C:\> aws ec2 modify-image-attribute --image-id ami-2bb65342 --launch-permission "{\"Add\":[{\"UserId\":\"123456789012\"}]}"
```

要删除账户的启动许可

以下命令从指定 AWS 账户中删除指定 AMI 的启动许可：

```
C:\> aws ec2 modify-image-attribute --image-id ami-2bb65342 --launch-permission  
">{"Remove": [{"UserId": "123456789012"}]}
```

要删除所有的启动许可

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

```
C:\> aws ec2 reset-image-attribute --image-id ami-2bb65342 --attribute launch  
Permission
```

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

使用书签

Abstract

允许其他 Amazon EC2 用户访问和使用您的共享 AMI。

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

请注意，您的 AMI 必须为公用，否则必须与您要向其发送书签的用户共享它。

为您的 AMI 创建书签

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

```
https://console.www.amazonaws.cn/ec2/v2/home?region=<region>#LaunchInstanceWiz  
ard:ami=<ami_id>
```

举例来说，该 URL 从 cn-north-1 区域的 ami-2bb65342 AMI 启动实例：

```
https://console.www.amazonaws.cn/ec2/v2/home?region=cn-north-1#LaunchIn  
stanceWizard:ami=ami-2bb65342
```

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 Windows AMI 指导原则

Abstract

创建共享 Windows AMI 的指南。

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。

- 制定一个用于构建、更新和重新发布 AMI 的可重复过程。
- 使用最新的操作系统、程序包和软件构建 AMI。
- 下载并安装最新版本的 [Amazon Windows Ec2Config 服务](#)。
- 验证 Ec2SetPassword、Ec2WindowsActivate 和 Ec2HandleUserData 是否已启用。
- 验证客户账户或远程桌面用户账户是否存在。
- 禁用或删除不必要的服务和程序，以缩小您的 AMI 的攻击面。
- 从 AMI 中删除实例凭证，如密钥对（如果您已将实例凭证保存到 AMI 上）。在安全的位置存储凭证。
- 确保管理员密码和任何其他账户上的密码均已设为利于共享的合适值。任何启动您的共享 AMI 的人均可获得这些密码。
- 在共享 AMI 之前测试 AMI。

付费 AMI

Abstract

购买或出售自定义 AMI（称为付费 AMI）。

付费 AMI 是可以从开发人员处购买的 AMI。

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

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

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



Important

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

主题

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

出售 AMI

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

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

查找付费 AMI

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

使用控制台查找付费 AMI

使用控制台查找付费 AMI

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

使用 AWS Marketplace 查找付费 AMI

使用 AWS Marketplace 查找付费 AMI

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

使用命令行查找付费 AMI

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

```
C:\> aws ec2 describe-images --owners aws-marketplace
```

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

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

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

购买付费 AMI

必须先注册（购买）付费 AMI，然后才能使用该 AMI 启动实例。

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

使用控制台购买付费 AMI

可以使用 Amazon EC2 启动向导购买付费 AMI。有关更多信息，请参阅 [启动 AWS Marketplace 实例 \(p. 223\)](#)。

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 1-Click 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 \(p. 223\)](#)。

从开发人员处购买付费 AMI

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

获取实例的产品代码

可以使用实例元数据检索实例的 AWS Marketplace 产品代码。有关检索元数据的更多信息，请参阅 [实例元数据和用户数据 \(p. 239\)](#)。

要检索产品代码，请使用以下查询：

```
C:\> GET http://169.254.169.254/latest/meta-data/product-codes
```

如果实例具有产品代码，则 Amazon EC2 将返回产品代码。例如：

```
774F4FF8
```

使用付费支持

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



Important

不能将支持产品用于预留实例。通常情况下，您需按支持产品卖方指定的价格付费。

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

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

```
C:\> aws ec2 modify-image-attribute --image-id ami_id --product-codes  
"product_code"
```

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

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

您设置产品代码属性后，该属性不能被更改或删除。

付费和支持 AMI 的账单

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

管理 AWS Marketplace 订阅

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

检查订阅详细信息

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

取消 AWS Marketplace 订阅

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



Note

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

创建 Amazon EBS 支持的 Windows AMI

Abstract

为自定义 Windows 实例创建 Amazon EBS 支持的 Windows AMI。

要创建 Amazon EBS 支持的 Windows AMI，需启动并自定义 Windows 实例，然后创建 AMI。

如果您需要创建 Amazon EBS 支持的 Linux AMI，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的 [创建 Amazon EBS 支持的 Linux AMI](#)。

用于由实例存储支持的 AMI 的 AMI 创建过程有些不同。有关 Amazon EBS 支持的实例和实例存储支持的实例之间的差别以及如何确定实例的根设备类型的更多信息，请参阅 [根设备卷 \(p. 8\)](#)。如果您需要创建实例存储支持的 Windows AMI，请参阅 [创建实例存储支持的 Windows AMI \(p. 78\)](#)。

创建 Amazon EBS 支持的 AMI 的概述

首先，从类似于您要创建的 AMI 的 AMI 启动实例。您可以连接到您的实例并进行自定义。按照您的需求创建实例后，通过在创建 AMI 和映像之前停止该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。

在 AMI 创建过程中，Amazon EC2 会创建您实例的根卷和附加到您实例的任何其他 EBS 卷的快照。如果有任何附加到实例的卷进行了加密，则新 AMI 只会在支持 Amazon EBS 加密的实例上成功启动。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 686\)](#)。

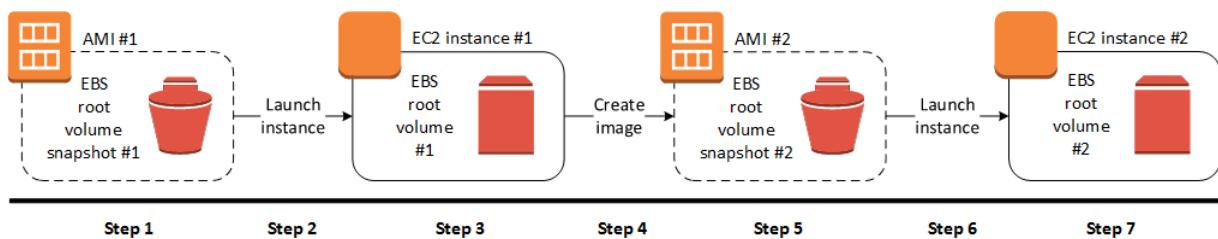
根据卷的大小，可能需要几分钟才能完成 AMI 创建过程（有时长达 24 小时）。您可能发现在创建 AMI 之前创建卷快照更有效。这样，创建 AMI 时就只需创建小的增量快照，且创建过程完成得更快（快照创建的总时间保持不变）。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 677\)](#)。

该过程完成之后，您便具有从实例的根卷创建的新 AMI 和快照。当您使用新 AMI 启动实例时，我们会使用快照为其根卷创建新 EBS 卷。AMI 和快照都会对您的账户产生费用，直至您删除它们。有关更多信息，请参阅 [取消注册您的 AMI \(p. 89\)](#)。

如果除了根设备卷之外，您还向实例添加了实例存储卷或 Amazon 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 \(p. 712\)](#)。

从正在运行的实例创建 Windows 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。如果您已有正在运行的基于 Amazon EBS 的实例，则可以直接执行第 4 步操作。



使用控制台从实例创建 AMI

1. 选择适当的由 EBS 支持的 AMI 作为新 AMI 的起始点。要查看 EBS 支持的 Windows AMI，请从 Filter 列表中选择以下选项：Public images、EBS images 和 Windows。

您可以选择任何与您的 AMI 使用相同版本的 Windows Server 的公用 AMI。然而，您必须先选择 EBS 支持的 AMI，而不是实例存储支持的 AMI。

2. 选择 Launch 以启动您选择的由 EBS 支持的 AMI 实例。接受默认值，以按向导逐步操作。有关更多信息，请参阅 [启动实例 \(p. 216\)](#)。
3. 在实例运行时连接到该实例。

您可以对您的实例执行以下任何操作，以便根据您的需求自定义该实例：

- 安装软件和应用程序
- 复制数据
- 通过删除临时文件、对您的硬盘进行碎片整理以及将可用空间清零来缩短启动时间
- 连接其他 EBS 卷
- 创建新用户账户并将其添加到 Administrators 组



Tip

如果您要共享 AMI，则可以提供用于 RDP 访问的这些凭证而不公开您的默认管理员密码。

- 使用 EC2Config 配置设置。如果您希望 AMI 在启动时生成随机密码，则需要启用 Ec2SetPassword 插件；否则会使用当前管理员密码。有关更多信息，请参阅 [使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)。
- 如果实例使用 RedHat 驱动程序访问 Xen 虚拟化硬件，请先升级为 Citrix 驱动程序，然后创建 AMI。有关更多信息，请参阅在 [Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。

(可选) 正确配置实例后，最好在创建 AMI 之前停止实例，以确保数据完整性。您可以使用 EC2Config 停止实例或在 Amazon EC2 控制台中选择实例，然后依次选择 Actions、Instance State 和 Stop。

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



Tip

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

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

名称

图像的唯一名称。

说明

(可选) 图像的描述 (最多 255 个字符)。

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



Warning

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

您可以修改根卷、Amazon EBS 卷和实例存储卷，方法如下：

- 要更改根卷的大小，请在 Type (类型) 列中找到 Root (根) 卷，然后填写 Size (大小) 字段。
 - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的 Amazon EBS 卷，请在列表中找到该 EBS 卷，然后选择 Delete。
 - 要添加 Amazon EBS 卷，请依次选择 Add New Volume、Type 和 EBS，然后填写字段。然后，当您从新 AMI 启动实例时，这些额外的卷会自动附加到该实例。您必须格式化并安装空卷。您必须安装基于快照的卷。
 - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的实例存储卷，请在列表中找到卷，然后选择 Delete。
 - 要添加实例存储卷，请依次选择 Add New Volume、Type 和 Instance Store，然后从 Device 列表中选择设备名称。当您从新 AMI 启动实例时，这些额外的卷会自动初始化并挂载。这些卷不包含您的 AMI 所基于的运行实例的实例存储卷上的数据。
5. 在创建 AMI 时，您可以选择导航窗格中的 AMIs 以查看其状态。最初，状态为 pending。几分钟后，状态应更改为 available。
(可选) 选择导航窗格中的 Snapshots 以查看为新 AMI 创建的快照。您从此 AMI 启动实例时，我们使用此快照创建其根设备卷。
6. 从新 AMI 启动实例。有关更多信息，请参阅 [启动实例 \(p. 216\)](#)。正在运行的新实例包含您在之前的步骤中应用的所有自定义项。



Note

您可指定脚本在实例启动时执行。在实例配置向导的 User data 部分中输入脚本。例如，您可指定 PowerShell 脚本以在实例启动时对实例进行重命名。有关更多信息，请参阅 [使用用户数据配置实例 \(p. 241\)](#)。

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)

创建实例存储支持的 Windows AMI

Abstract

通过启动并自定义 Windows 实例来创建实例存储支持的 Windows AMI，然后捆绑并注册该 AMI。

要创建实例存储支持的 Windows AMI，请首先启动并自定义 Windows 实例，然后捆绑该实例，并从捆绑过程中创建的清单注册 AMI。



Important

实例存储唯一支持的 Windows AMI 是用于 Windows Server 2003 的 AMI。实例存储支持的实例不具有 Windows Server 的较高版本所需的可用磁盘空间。

使用此步骤只能捆绑由实例存储支持的 Windows 实例。如果您需要创建实例存储支持的 Linux AMI，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [创建实例存储支持的 Linux AMI](#)。

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，请参阅根设备卷 (p. 8)。如果您需要创建 Amazon EBS 支持的 Windows AMI，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

内容

- [实例存储支持的 Windows AMI \(p. 79\)](#)
- [准备创建实例存储支持的 Windows AMI \(p. 79\)](#)
- [捆绑实例存储支持的 Windows 实例 \(p. 80\)](#)
- [注册实例存储支持的 Windows AMI \(p. 81\)](#)

实例存储支持的 Windows AMI

从实例存储支持的 AMI 启动的实例会使用实例存储卷作为根设备卷。实例存储支持的 AMI 的根设备卷的映像最初会存储在 Amazon S3 中。使用实例存储支持的 AMI 启动实例时，其根设备卷的映像会从 Amazon S3 复制到实例的根分区。然后，系统会使用根设备卷启动实例。

当您创建实例存储支持的 AMI 时，必须将其上传到 Amazon S3。Amazon S3 会将数据对象存储在概念类似于目录的存储段中。存储桶具有全球唯一的名称，并且属于唯一 AWS 账户。

捆绑过程

捆绑过程包含以下任务：

- 压缩映像以最小化带宽使用和存储要求。
- 对压缩映像加密并进行签名以确保保密性，并且根据映像创建者对其进行身份验证。
- 将加密映像划分成可管理的部分以进行上传。
- 运行 `Sysprep` 将计算机特定信息（例如 MAC 地址和计算机名称）从 Windows AMI 分离，准备将其虚拟化。
- 创建一个包含映像各部分及其校验和的清单文件。
- 将 AMI 的所有组件放在您在发出捆绑请求时指定的 Amazon S3 存储桶中。

存储卷

创建实例存储支持的 AMI 时，请务必记住以下有关实例存储的详情：

- 从您的新 AMI 启动新实例时，根设备卷 (C:) 会自动附加。系统捆绑实例后，会删除任何其他实例存储卷上的数据。
- 根设备卷（例如 D:）之外的实例存储卷是临时性的，只能用于短期存储。
- 您可以将 Amazon EBS 卷添加到实例存储支持的实例。Amazon EBS 卷会存储在 Amazon S3 存储桶内，并且在实例被捆绑时仍保持完整。因此，我们建议您在 Amazon EBS 卷（而不是实例存储卷）上保存所有必须持久保留的数据。

有关 Amazon EC2 存储选项的更多信息，请参阅[存储 \(p. 637\)](#)。

准备创建实例存储支持的 Windows AMI

当您创建 AMI 时，必须首先以某个实例为其基础。您可以自定义该实例以包含您所需的数据和软件。如此一来，您从自己的 AMI 启动的所有实例都会包含您所需的全部内容。

启动实例存储支持的 Windows 实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，单击 AMIs。选择与您想创建的 AMI 类似的实例存储支持的 AMI。要查看实例存储支持的 Windows AMI，请从 Filter (筛选) 列表中依次选择以下选项：Public images (公有映像)、Instance store images (实例存储映像) 和 Windows。

您可以选择任何与您的 AMI 使用相同版本的 Windows Server 的公用 AMI。然而，您必须先选择实例存储支持的 AMI，而不是 Amazon EBS 支持的 AMI。

3. 单击 Launch (启动) 启动所选的实例存储支持的 AMI。接受默认值，以按向导逐步操作。
4. 实例在运行时，请连接到该实例并对其进行自定义。例如，您可以在自己的实例上执行以下任何操作：
 - 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。
 - 创建新用户账户并将其添加到 Administrators 组。



Tip

如果您要共享 AMI，则可以提供用于 RDP 访问的这些证书，而不用公开您的默认管理员密码。

- 使用 EC2Config 配置设置。例如，若要在从此 AMI 启动实例时为实例生成随机密码，请启用 Ec2SetPassword 插件；否则使用当前管理员密码。有关更多信息，请参阅 [使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)。
5. 如果实例使用 RedHat 驱动程序访问 Xen 虚拟化硬件，请先升级为 Citrix 驱动程序，然后创建 AMI。有关更多信息，请参阅 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。

捆绑实例存储支持的 Windows 实例

既然您已自定义实例，就可以使用 AWS 管理控制台或命令行捆绑该实例以创建 AMI。

使用控制台捆绑实例存储支持的 Windows 实例

1. 确定您是要为自己的新 AMI 使用一个现有 Amazon S3 存储桶，还是要新建一个存储桶。要创建新 Amazon S3 存储桶，请执行以下步骤：
 - a. 打开 Amazon S3 控制台。
 - b. 单击 Create Bucket (创建存储桶)。
 - c. 为该存储桶指定一个名称，然后单击 Create。
2. 打开 Amazon EC2 控制台。
3. 在导航窗格中，单击 Instances。右键单击在上一步骤中设置的实例，然后选择 Bundle Instance (instance store AMI)(捆绑实例 (实例存储 AMI))。
4. 在 Bundle Instance (捆绑实例) 对话框中，填写所需信息，然后单击 OK (确定)：
 - Amazon S3 bucket name (Amazon S3 存储桶名称)：指定您所拥有的 S3 存储桶的名称。捆绑文件和清单将存储在此存储桶中。
 - Amazon S3 key name (Amazon S3 密钥名称)：为捆绑过程生成的文件指定前缀。

Bundle Instance (捆绑实例) 对话框会确认捆绑实例的请求已成功，并且提供捆绑任务的 ID。单击 Close (关闭)。

若要查看捆绑任务的状态，请单击导航窗格中的 Bundle Tasks (捆绑任务)。捆绑任务会经过几个状态，包括 waiting-for-shutdown、bundling 和 storing。如果捆绑任务无法成功完成，则状态应该为 failed。

使用命令行捆绑实例存储支持的 Windows 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 \(p. 3\)](#)。

- [bundle-instance](#) (AWS CLI)
- [New-EC2InstanceBundle](#) (适用于 Windows PowerShell 的 AWS 工具)

注册实例存储支持的 Windows AMI

最后，您必须注册自己的 AMI，这样 Amazon EC2 才可以找到它并从中启动实例。

您的新 AMI 存储在 Amazon S3 中。取消注册 AMI 并在 Amazon S3 中删除捆绑之前，您将承担这种存储的费用。

如果您对存储在 Amazon S3 中的源 AMI 进行任何更改，则必须将其取消注册，然后再重新注册 AMI，更改才会生效。

从控制台中的 AMI 页注册实例存储支持的 Windows AMI

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，单击 AMIs。默认情况下，控制台会显示您所拥有的 AMI。
3. 单击 Actions (操作)，然后选择 Register new AMI (注册新 AMI)。
4. 在 Register Image (注册映像) 对话框中，提供 AMI Manifest Path (AMI 清单路径)，然后单击 Register (注册)。

从控制台中的“Bundle Tasks (捆绑任务)”页注册实例存储支持的 Windows AMI

1. 在导航窗格中，单击 Bundle Tasks (捆绑任务)。
2. 选择捆绑任务，然后单击 Register as an AMI (注册为 AMI)。
3. 对话框显示 AMI 清单路径。单击 Register (注册)，然后在确认对话框内单击 Close (关闭)。

使用命令行注册实例存储支持的 Windows 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)

若要查看新 AMI，请在导航窗格中单击 AMI，然后确保选中 Owned by me (我拥有的) 筛选条件选项。

带加密快照的 AMI

Abstract

在各种配置中将 EBS 加密与 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。

带加密卷的 EC2 实例从 AMI 中启动的方式与其他实例的相同。

CopyImage 操作可用于从带未加密快照的 AMI 创建带加密快照的 AMI。默认情况下，在创建目标副本时，CopyImage 会保留源快照的加密状态。但是，您也可以配置复制过程的参数来加密目标快照。

可使用您的默认 AWS Key Management Service 客户主密钥 (CMK)，或您指定的自定义密钥加密快照。在所有情况下，您都必须拥有使用所选密钥的权限。如果您拥有带加密快照的 AMI，则可以选择使用其他加密密钥对其进行重新加密以作为 CopyImage 操作的一部分。CopyImage 一次只接受一个密钥并且会将映像的所有快照（无论是根还是数据）加密到该密钥。但是，无法使用加密到多个密钥的快照手动构建 AMI。

对创建带加密快照的 AMI 的支持可通过 Amazon EC2 控制台、Amazon EC2 API 或 AWS CLI 获得。

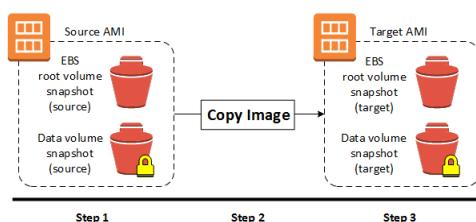
CopyImage 的加密参数在 AWS KMS 可用的所有区域中都可用。

涉及加密的 EBS 快照的 AMI 情景

您可以使用 AWS 管理控制台或命令行复制 AMI 并同时对与其关联的 EBS 快照进行加密。

复制带加密数据快照的 AMI

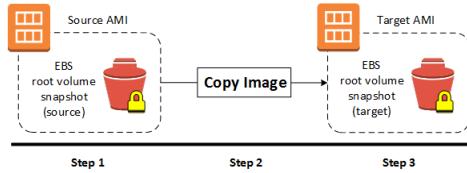
在此方案中，EBS 支持的 AMI 拥有未加密的根快照和加密的数据快照，如步骤 1 所示。在步骤 2 中，CopyImage 操作在没有加密参数的情况下调用。因此，将保留每个快照的加密状态，以便让目标 AMI（如步骤 3 所示）也由未加密的根快照和加密的数据快照提供支持。尽管这两种快照包含相同的数据，但两者是截然不同的，两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。



您可以使用 Amazon EC2 控制台或命令行执行简单复制（如上述复制）。有关更多信息，请参阅 [复制 AMI \(p. 84\)](#)。

复制由加密的根快照支持的 AMI

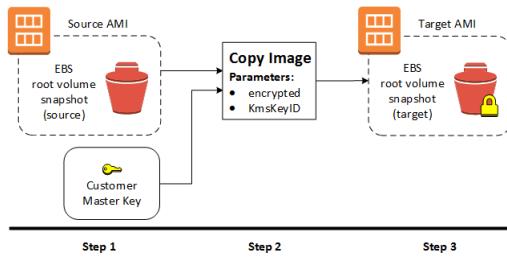
在此方案中，Amazon EBS 支持的 AMI 拥有加密的根快照，如步骤 1 所示。在步骤 2 中，CopyImage 操作在没有加密参数的情况下调用。因此，将保留快照的加密状态，以便让目标 AMI（如步骤 3 所示）也由加密的根快照支持。尽管这两种根快照包含相同的系统数据，但两者是截然不同的，两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。



您可以使用 Amazon EC2 控制台或命令行执行简单复制（如上述复制）。有关更多信息，请参阅 [复制 AMI \(p. 84\)](#)。

从未加密的 AMI 创建带加密的根快照的 AMI

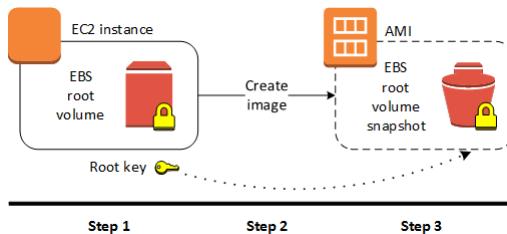
在此方案中，Amazon EBS 支持的 AMI 拥有未加密的根快照（如步骤 1 所示），将创建带加密的根快照的 AMI（如步骤 3 所示）。步骤 2 中的 `CopyImage` 操作将通过两个加密参数（包括选择 CMK）调用。因此，根快照的加密状态将更改，以便让目标 AMI 由包含与源快照相同的数据但使用指定密钥进行加密的根快照提供支持。两个 AMI 中的快照都将产生存储费用，从任一 AMI 启动的任何实例也将产生费用。



您可以使用 Amazon EC2 控制台或命令行执行复制和加密操作（如上述操作）。有关更多信息，请参阅 [复制 AMI \(p. 84\)](#)。

从正在运行的实例创建带加密的根快照的 AMI

在此方案中，将从正在运行的 EC2 实例创建 AMI。步骤 1 中的正在运行的实例拥有加密的根卷，步骤 3 中创建的 AMI 拥有加密到与源卷相同的密钥的根快照。无论加密是否存在，`CreateImage` 操作都具有完全相同的行为。



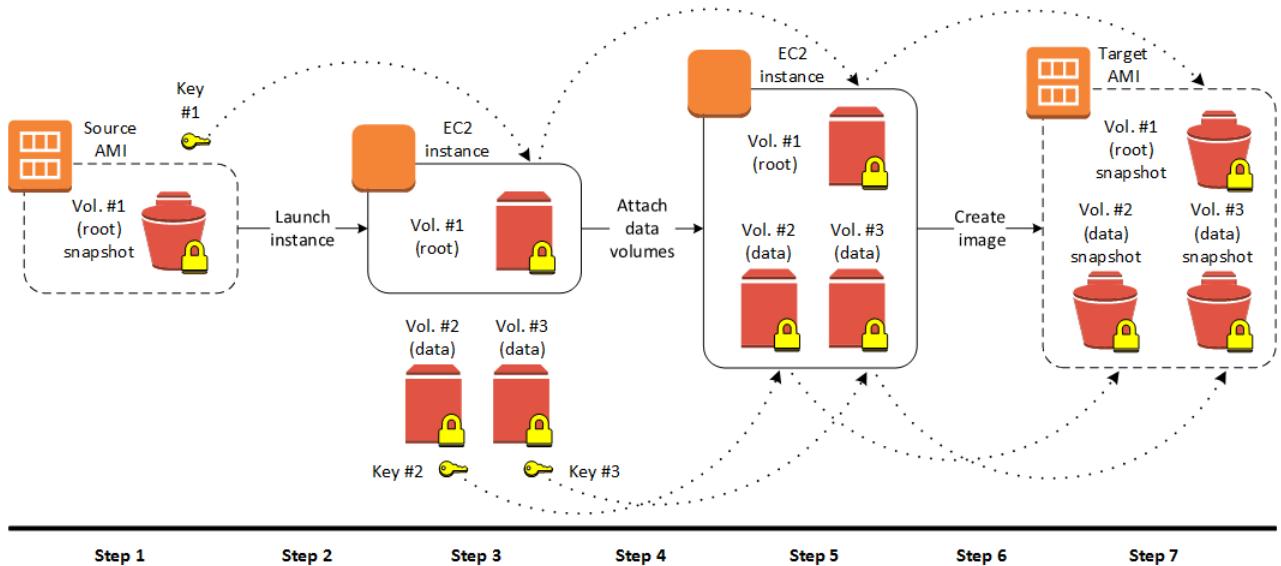
您可以使用 Amazon EC2 控制台或命令行从正在运行的 Amazon EC2 实例（带或不带加密卷）创建 AMI。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

使用每个加密快照的唯一 CMK 创建 AMI

此方案最初有一个由根卷快照（加密到密钥 #1）支持的 AMI，最终得到一个附加了 2 个额外数据卷快照（加密到密钥 #2 和密钥 #3）的 AMI。`CopyImage` 操作无法将多个加密密钥应用于单个操作。但是，您可以从拥有加密到不同密钥的多个附加卷的实例创建 AMI。生成的 AMI 拥有加密到这些密钥的快照，且从此新 AMI 启动的任何实例也拥有加密到这些密钥的卷。

本示例过程的步骤对应于下图。

1. 从 vol. #1 (根) 快照支持的源 AMI 开始 , 该快照使用密钥 #1 进行加密。
2. 从源 AMI 启动 EC2 实例。
3. 创建 EBS 卷 vol.#2 (数据) 和 vol.#3 (数据) , 它们分别加密到密钥 #2 和密钥 #3。
4. 将加密的数据卷附加到 EC2 实例。
5. EC2 实例现在拥有 1 个加密的根卷以及 2 个加密的数据卷 , 这些卷都使用不同的密钥。
6. 对 EC2 实例执行 CreateImage 操作。
7. 生成的目标 AMI 包含三个 EBS 卷的加密快照 , 这些卷都使用不同的密钥。



您可以使用 Amazon EC2 控制台或命令行执行此过程。有关更多信息 , 请参阅以下主题 :

- [启动实例 \(p. 216\)](#)
- [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)。](#)
- [Amazon EBS 卷 \(p. 640\)](#)
- [AWS Key Management Service Developer Guide 中的 AWS 密钥管理](#)

复制 AMI

Abstract

将 AMI 复制到另一个区域 , 或创建加密 Amazon EBS 快照支持的版本。

您可以使用 AWS 管理控制台、命令行或 Amazon EC2 API (三者均支持 CopyImage 操作) 在 AWS 区域内或跨 AWS 区域复制 Amazon 系统映像 (AMI)。Amazon EBS 支持的 AMI 和实例存储支持的 AMI 均可复制。

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。(唯一的例外是您选择加密快照时 , 如下所述。) 源 AMI 可更改或取消注册 , 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。

复制您拥有的 AMI

可使用 `CopyImage` 操作复制属于 AWS 账户的任何 AMI。这包括带加密的快照的 AMI 和已加密的 AMI。

跨 AWS 账户复制 AMI

您可以跨 AWS 账户复制 AMI。这包括带加密的快照的 AMI，但不包括已加密的 AMI。

账户的所有者必须授予对支持该 AMI 的存储的读取许可，无论它是关联的 EBS 快照（对于 Amazon EBS 支持的 AMI）还是关联的 Amazon S3 存储桶（对于实例存储支持的 AMI）。要允许其他账户复制您的 AMI，您必须使用 Amazon EBS 或 Amazon S3 访问管理工具授予对您的关联快照或存储桶的读取许可。

复制 AMI 后，源 AMI 的所有者需要支付标准 Amazon EBS 或 Amazon S3 传输费，目标 AMI 的所有者需要支付目标区域的存储费用。

限制

- 您无法在账户之间复制加密的 AMI。您可以改为将基础加密快照复制到另一个账户，然后将它注册为新的 AMI。
- 无法直接复制具有关联的 `billingProduct` 代码的 AMI。这包括 Windows AMI 和来自 AWS Marketplace 由另一个 AWS 账户拥有和共享的其他 AMI。要创建已具有关联的 `billingProduct` 代码的 AMI 的私有副本，我们推荐以下步骤：

1. 使用共享 AMI 在目标账户中启动 EC2 实例。
2. 从新实例创建映像。

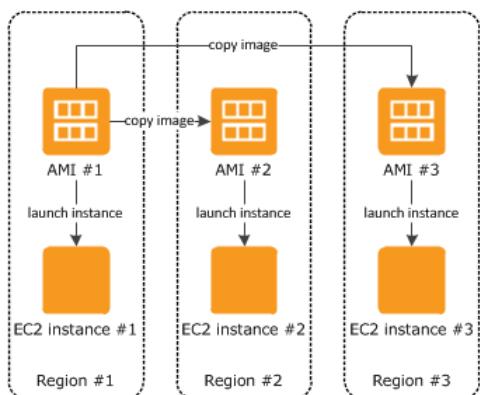
这将生成您拥有的私有 AMI，并且可以像您拥有的任何其他 AMI 一样对其进行自定义。例如，如果您已创建由 EBS 支持的 AMI 的私有副本，则可使用 `CopyImage` 创建具有加密的根卷的 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

跨区域复制 AMI

跨不同地理位置复制 AMI 具有以下优势：

- 一致的全球部署：通过将 AMI 从一个区域复制到另一个区域，使您能够在不同的区域启动基于相同 AMI 的一致实例。
- 可扩展性：无论用户身处何处，您都可以更轻松地设计和构建能满足他们需求的全球范围应用程序。
- 性能：您可以通过分发您的应用程序以及找到较接近您用户的应用程序的关键组件来提高性能。您还可以利用区域特定的功能，例如实例类型或其他 AWS 服务。
- 高可用性：您可以跨 AWS 区域设计和部署应用程序以提高可用性。

下图显示源 AMI 和不同区域中的两个复制 AMI 以及从三者启动的 EC2 实例之间的关系。当您从 AMI 启动一个实例时，该实例将驻留在 AMI 所在的区域。如果您更改源 AMI，并希望这些更改反映到目标区域的 AMI 中，则必须将源 AMI 重新复制到目标区域。



当您首次将实例存储支持的 AMI 复制到一个区域时，我们会为复制到该区域的 AMI 创建一个 Amazon S3 存储桶。复制到该区域的所有实例存储支持的 AMI 都将存储在此存储桶中。这些存储桶的名称具有以下格式：`amis-for-account-in-region-hash`。例如：
`amis-for-123456789012-in-us-west-2-yhjmxvp6`。



Note

目标区域限制为一次 50 个并发 AMI 副本，并且来自一个源区域的不能超过 25 个。要请求提高此限制，请参阅 [Amazon EC2 服务限制 \(p. 746\)](#)。

复制 AMI 前，您必须确保源 AMI 的内容得到更新，以支持在另一个区域运行。例如，您应更新任何数据库连接字符串或相似的应用程序配置数据，以指向适当的资源。否则，从目标区域的新 AMI 启动的实例可能会继续使用来自源区域的资源，这可能会影响性能和成本。

复制到加密

在复制期间加密仅适用于 Amazon EBS 支持的 AMI。由于实例存储支持的 AMI 不依赖快照，因此无法使用 CopyImage 操作来更改其加密状态。

CopyImage 操作还可以用于创建加密 Amazon EBS 快照支持的新 AMI。如果您在复制 AMI 时调用加密，将使用您指定的密钥对为其关联的 Amazon EBS 卷（包括根卷）拍摄的每个快照进行加密。有关使用具有加密快照的 AMI 的更多信息，请参阅 [带加密快照的 AMI \(p. 82\)](#)。

默认情况下，将复制 AMI 的备份快照并保持其原始加密状态。复制未加密快照支持的 AMI 将生成完全相同、也未加密的目标快照。如果源 AMI 受加密快照支持，则复制它将生成一个加密到指定密钥的目标快照。复制多个快照支持的 AMI 将保留其在每个目标快照中的源加密状态。有关复制具有多个快照的 AMI 的更多信息，请参阅 [带加密快照的 AMI \(p. 82\)](#)。

下表显示了各种场景的加密支持。请注意，尽管可以复制未加密快照来生成加密快照，但是不能复制加密快照来生成未加密快照。

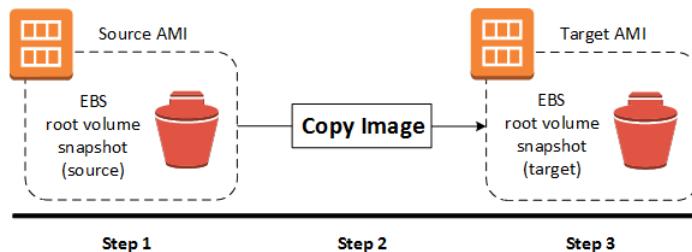
场景	说明	支持服务
1	未加密到未加密	是
2	加密到加密	是
3	未加密到加密	是
4	加密到未加密	否

AMI 复制方案

本部分将介绍复制 AMI 的基本场景并提供使用 Amazon EC2 控制台和命令行进行复制的过程。

将未加密的源 AMI 复制到未加密的目标 AMI

在最简单的情况下，具有单个未加密支持快照的 AMI 副本是在指定地理区域（未显示）中创建的。

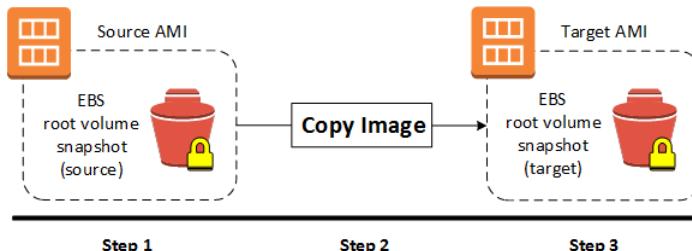


Note

尽管上图显示了具有单个支持快照的 AMI，**CopyImage** 操作也适用于具有多个快照的 AMI。将保留每个快照的加密状态。这意味着源 AMI 中的未加密快照将导致在目标 AMI 中创建未加密快照，源 AMI 中的加密快照将导致在目标 AMI 中创建加密快照。

将加密源 AMI 复制到加密目标 AMI

尽管此场景涉及加密快照，但它在功能上等效于前一场景。

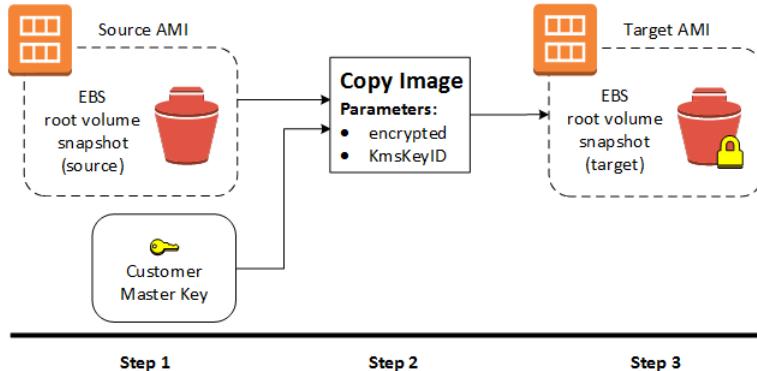


Note

如果您在复制多快照 AMI 时应用加密，则将使用指定密钥（如果未指定密钥，则使用默认密钥）来加密所有目标快照。有关利用加密到多个密钥的多个快照创建 AMI 的信息，请参阅[带加密快照的 AMI \(p. 82\)](#)。

将未加密的源 AMI 复制到加密目标 AMI

在此最后一个场景中，**CopyImage** 操作将更改目标映像的加密状态，例如，对未加密快照进行加密，或使用不同密钥对加密快照进行重新加密。要在复制期间应用加密，您必须提供加密参数：一个加密标志和一个密钥。仅当您提供此密钥时，从目标快照创建的卷才可访问。有关 AMI 的支持加密场景的更多信息，请参阅[带加密快照的 AMI \(p. 82\)](#)。



使用控制台或命令行复制 AMI

以下过程中的步骤对应于每副场景图中的三个步骤。除加密选项的配置外，所有案例中执行 CopyImage 操作的过程完全相同。

使用控制台复制 AMI

1. 创建或获取 Amazon EBS 快照支持的 AMI。有关更多信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。许多 AWS 提供的 AMI 可通过 Amazon EC2 控制台使用。

从控制台导航栏中，选择包含您要复制的 AMI 的区域。在导航窗格中，展开 Images 并选择 AMIs 以显示所选区域中可供您使用的 AMI 的列表。

2. 选择要复制的 AMI，然后选择 Actions 和 Copy AMI。

在 AMI Copy 页中，设置以下字段并选择 Copy AMI：

- Destination region：选择要将 AMI 复制到的区域。
- Name：为新 AMI 提供名称。
- 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 Amazon EBS 快照，或使用不同的密钥对它们进行重新加密。
- Master Key：将用于加密目标 Amazon EBS 快照的 KMS 密钥（如果选择了 Encryption）。

3. 我们将显示一个确认页面，以告知您复制操作已启动，并为您提供新 AMI 的 ID。

若要立即查看复制操作的进度，请访问提供的链接。若要稍后查看进度，请选择 Done，然后在您准备就绪时使用导航栏切换到目标区域（如果适用）并在 AMI 列表中找到您的 AMI。

目标 AMI 的初始状态为 pending，当状态为 available 时，此操作完成。

使用命令行复制 AMI

使用命令行复制 AMI 需要您同时指定源区域和目标区域。可使用 `--source-region` 参数指定源区域。对于目标区域，您有两种选择：

- 使用 `--region` 参数。
- 设置环境变量。有关更多信息，请参阅[配置 AWS 命令行界面](#)。

在复制期间加密目标快照时，您需要提供两个额外参数：

- 一个布尔值，`--encrypted`
- 一个字符串，`--kms-key-id`，提供主加密密钥 ID

您可以使用以下命令之一复制 AMI。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

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

停止待处理的 AMI 复制操作

您可以使用 AWS 管理控制台或命令行停止待处理的 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.amazonaws.cn/ec2/>。
2. 从导航栏中，在区域选择器中选择目标区域。
3. 在导航窗格中，选择 AMIs。
4. 选择要停止复制的 AMI 并选择 Actions 和 Deregister。
5. 当系统要求确认时，请选择 Continue。

使用命令行停止 AMI 复制操作

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

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

取消注册您的 AMI

Abstract

使用后取消注册您的 AMI。

使用完 AMI 之后，可以取消注册它。取消注册 AMI 之后，便无法将其用于启动新实例。

取消注册某个 AMI 时，不会影响您已从该 AMI 启动的任何实例。这些实例将继续对您产生使用费用。因此，如果您使用完这些实例，应终止它们。

用于清除 AMI 的过程取决于它是由 Amazon EBS 还是由实例存储支持。（请注意，只有用于 Windows Server 2003 的 Windows AMI 可由实例存储支持。）

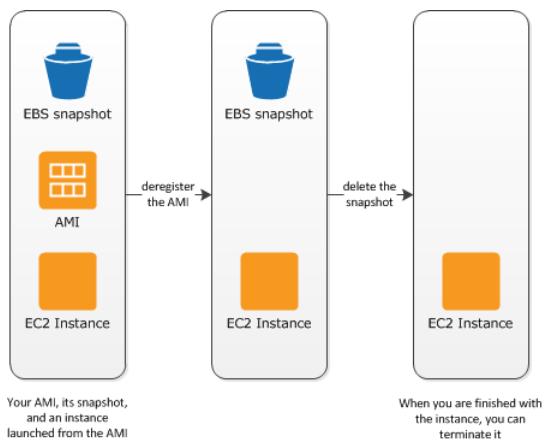
内容

- [清除由 Amazon EBS 支持的 AMI \(p. 89\)](#)
- [清除由实例存储支持的 AMI \(p. 90\)](#)

清除由 Amazon EBS 支持的 AMI

在取消注册 Amazon EBS 支持的 AMI 时，不会影响在创建 AMI 的过程中为实例的根卷创建的快照。此快照将继续对您产生存储费用。因此，如果您使用完该快照，应删除它。

下图说明清除由 Amazon EBS 支持的 AMI 的过程。



清除由 Amazon EBS 支持的 AMI

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 AMIs。选择 AMI 并记下其 ID — 这可帮助您在下一步骤中找到正确的快照。选择 Actions，然后选择 Deregister。当系统提示进行确认时，请选择 Continue。

AMI 状态现在变为 unavailable。



Note

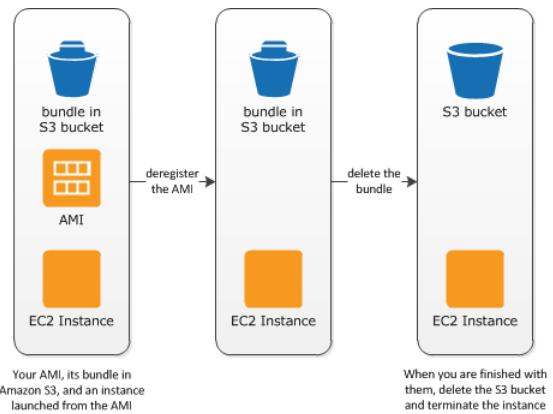
可能要用几分钟时间，控制台才会将状态 available 变为 unavailable 或者从列表中完全删除该 AMI。选择 Refresh 以刷新状态。

3. 在导航窗格中，选择 Snapshots，然后选择快照（在 Description 列中查找 AMI ID）。选择 Actions，然后选择 Delete Snapshot。当系统提示进行确认时，选择 Yes, Delete。
4. (可选) 如果您使用完从 AMI 启动的实例，请终止该实例。在导航窗格中，选择 Instances。选择实例，然后依次选择 Actions、Instance State 和 Terminate。当系统提示您确认时，选择 Yes, Terminate。

清除由实例存储支持的 AMI

取消注册某个由实例存储支持的 AMI 时，不会影响您在创建该 AMI 时上传到 Amazon S3 的文件。这些文件将继续在 Amazon S3 中对您产生使用费用。因此，如果您使用完这些文件，应删除它们。

下图说明清除由实例存储支持的 AMI 的过程。



清除由实例存储支持的 AMI

1. 使用 `ec2-deregister` 命令取消注册 AMI，如下所示。

```
ec2-deregister ami_id
```

AMI 状态现在变为 unavailable。

2. 使用 `ec2-delete-bundle` 命令删除捆绑，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 `ec2-terminate-instances` 命令终止该实例，如下所示。

```
ec2-terminate-instances 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。

AWS Windows AMI 版本历史

Abstract

了解 AWS Windows AMI 的发行日期和更改历史。

AWS 提供包含 Microsoft Windows Server 版本的 Amazon 系统映像 (AMI)，称为 *AWS Windows AMI*。某些 AWS Windows AMI 还配置了 Microsoft SQL Server 或 Internet Information Services (IIS)。您可以使用已配置 Microsoft SQL Server 和 IIS 的 AMI，也可以从一个基础 Windows AMI 开始使用，然后在实例上安装 Microsoft SQL Server 并启用 IIS。有关更多信息，请参阅 [AWS Windows AMI \(p. 61\)](#)。

内容

- [配置设置和驱动程序 \(p. 92\)](#)
- [更新您的 Windows 实例 \(p. 92\)](#)
- [确定实例版本 \(p. 92\)](#)
- [AWS Windows AMI 版本 \(p. 93\)](#)
- [映像更改 \(p. 103\)](#)

- 订阅 Windows AMI 通知 (p. 104)
- 升级或迁移 Windows Server 实例 (p. 105)

配置设置和驱动程序

AWS Windows AMI 的配置方法与您从 Microsoft 发布的媒介安装 Windows Server 的方法大致相同。然而，在安装默认设置方面，两者之间存在一些区别。

AWS Windows AMI 安装有一个附加服务，即 EC2Config 服务。EC2Config 服务会在本地系统账户中运行并主要在初始设置期间使用。有关 EC2Config 执行的任务的信息，请参阅 [EC2Config 任务概述 \(p. 250\)](#)。

使用初始配置启动 Windows 实例后，您可以在自定义和创建自己的 AMI 时使用 EC2Config 服务来更改配置设置。系统会使用新配置从您的自定义 AMI 中启动实例。

AWS Windows AMI 包含一系列驱动程序，以允许访问 Xen 虚拟化硬件。Amazon EC2 会使用这些驱动程序将实例存储和 Amazon EBS 卷映射到其设备。有关更多信息，请参阅 [半虚拟化驱动程序 \(p. 272\)](#)。

更新您的 Windows 实例

启动 Windows 实例后，您需要在上面安装更新。您可以仅手动安装您感兴趣的更新，也可以从当前的 AWS Windows AMI 启动并构建一个新的 Windows 实例。有关查找当前 AWS Windows AMI 的信息，请参阅 [查找 Windows AMI \(p. 65\)](#)。

对于 Windows 实例，您可以将更新安装到以下服务或应用程序：

- Windows
- Microsoft SQL Server
- Windows PowerShell
- EC2Config 服务 (p. 258)
- 半虚拟化驱动程序 (p. 275)
- 适用于 Windows PowerShell 的 AWS 工具
- AWS CloudFormation 帮助程序脚本

您可以在安装更新之后重启 Windows 实例。有关更多信息，请参阅 [重启您的实例 \(p. 230\)](#)。

确定实例版本

AWS 管理控制台提供了有关用于创建 Amazon EC2 实例的 AMI 的详细信息。Description 选项卡上的 AMI ID 字段含有一些信息，包括 Windows Server SKU、架构（32 位或 64 位）、创建 AMI 的日期以及 AMI ID。

Description		Status Checks	Monitoring	Tags	Public DNS	Public IP	Elastic IP	Availability zone	us-west-2a	Security groups	Scheduled events	AMI ID	Windows_Server-2012-R2_RTM-English	Platform	windows
Instance ID															
Instance state	stopped														
Instance type	t2.micro														
Private DNS															
Private IPs															
Secondary private IPs															
VPC ID															
Subnet ID															

如果 AMI 已被设为私有或被更高版本替代，并且不再在目录中列出，则 AMI ID 字段将指明“Cannot load detail for ami-xxxxx. You may not be permitted to view it.”要确定用于创建实例的 AMI，您必须打开系统日

志。在 EC2 控制台中，选择一个实例，从上下文菜单（右键单击）中选择 Instance Settings，然后选择 Get System Log。AMI 创建日期和 SKU 将在 AMI Origin Version 和 AMI Origin Name 字段中列出。

```
2015/04/23 17:19:17Z: EC2ConfigMonitorState: 0
2015/04/23 17:19:18Z: AMI Origin Version: 2015.04.15
2015/04/23 17:19:18Z: AMI Origin Name: Windows Server-2003-R2 SP2-English-32Bit-Base
2015/04/23 17:19:18Z: OS: Microsoft Windows NT 5.2.3790
2015/04/23 17:19:18Z: OsVersion: 5.2
2015/04/23 17:19:18Z: OsProductName: Microsoft Windows Server 2003 R2
2015/04/23 17:19:18Z: OsBuildLabEx: NotFound
2015/04/23 17:19:18Z: Language: en-US
2015/04/23 17:19:18Z: EC2 Agent: Ec2Config service v3.3.174
2015/04/23 17:19:19Z: Message: Waiting for meta-data accessibility...
2015/04/23 17:19:20Z: Message: Meta-data is now available.
2015/04/23 17:19:20Z: Driver: Citrix PV Ethernet Adapter v5.9.960.49119
2015/04/23 17:19:20Z: Driver: Citrix PV SCSI Host Adapter v6.0.2.56921
2015/04/23 17:19:33Z: AMI-ID: ami-a3c9e393
```



Note

仅当 EC2Config 服务运行的是版本 2.1.19 或更高版本并且 AMI 是在 2013 年 11 月 13 日之后创建的情况下，AMI Origin Version 和 AMI Origin Name 才会显示在系统日志中。

AWS Windows AMI 版本

AWS 在 Microsoft 的修补程序星期二（每个月的第二个星期二）后的五个工作日内提供更新的、完整修补的 Windows AMI。新的 AMI 将通过 Amazon EC2 控制台的 Images 页面立即提供。在新的 AMI 发行后的几天内，即可在 AWS Marketplace 中和启动实例向导的 Quick Start 选项卡中找到这些 AMI。在发布 Windows AMI 更新版本后的 10 个工作日内，AWS 会将以前发布的 Windows AMI 版本设为私有，确保客户默认拥有最新的安全更新。

各个版本的 Windows AMI 均拥有新的 AMI ID。因此，我们建议您编写脚本，以便按名称而非 ID 查找最新的 AWS Windows AMI。有关更多信息，请参阅适用于 Windows PowerShell 的 AWS 工具 用户指南中的 [Get-EC2ImageByName](#)。您还可以创建 Lambda 函数以使用 Amazon EC2 以及其他服务（例如 AWS CloudFormation）执行此任务。有关更多信息，请参阅 [创建 Lambda 函数](#)。

下表总结了对每个 AWS Windows AMI 版本所做的更改。请注意，有些更改适用于所有 AWS Windows AMI，而有些只适用于一部分 AMI。

发布	更改
2016.7.13	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2016 年 7 月最新 适用于 Windows PowerShell 的 AWS 工具更新了 AWS 半虚拟化驱动程序 7.4.2.0适用于 Windows Server 2008 R2 的 AWS 半虚拟化驱动程序
2016.6.16	<ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2016 年 6 月最新 适用于 Windows PowerShell 的 AWS 工具EC2Config 服务，版本 3.17.1032发布了 10 个包含 64 位版本 Microsoft SQL Server 2016 的新 AMI。您可以通过 EC2 控制台、CLI 或 API 从其中一个 AMI 启动实例。如果使用控制台，请导航到 EC2 > Images > AMIs，选择 Public Images，然后在搜索栏中输入“Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_Standard”。有关 SQL Server 2016 的更多信息，请参阅 MSDN 上的 SQL Server 2016 的新增功能。

发布	更改
2016.5.11	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2016 年 5 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.16.930• 安装了 MS15-011 Active Directory 补丁• 适用于基于 Windows Server 2012 R2 的 AMI 的 Intel SRIOV 驱动程序。版本 1.0.16.1 (2014/03/04)
2016.4.13	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2016 年 4 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.15.880
2016.3.9	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2016 年 3 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.14.786
2016.2.10	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2016 年 2 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.13.727
2016.1.25	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2016 年 1 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.12.649
2016.1.5	<p>所有 AMI</p> <ul style="list-style-type: none">• 最新 适用于 Windows PowerShell 的 AWS 工具
2015.12.15	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 12 月• 最新 适用于 Windows PowerShell 的 AWS 工具

发布	更改
2015.11.11	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 11 月• 最新 适用于 Windows PowerShell 的 AWS 工具• EC2Config 服务，版本 3.11.521• CFN 代理已更新到最新版本
2015.10.26	已将基础 AMI 的启动卷大小更正为 30GB (而不是 35GB)
2015.10.14	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 10 月• EC2Config 服务，版本 3.10.442• 最新 适用于 Windows PowerShell 的 AWS 工具• 已为所有 SQL 变体将 SQL Service Pack 更新为最新版本• 删除了事件日志中的旧条目• 已更改 AMI 名称以反映最新的 Service Pack。例如，Server 2012 和 SQL 2014 Standard 的最新 AMI 名为“Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP1_Standard-2015.10.26”，而不是“Windows_Server-2012-RTM-English-64Bit-SQL_2014_RTM_Standard-2015.10.26”。
2015.9.9	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 9 月• EC2Config 服务，版本 3.9.359• 最新 适用于 Windows PowerShell 的 AWS 工具• 最新 AWS CloudFormation 帮助程序脚本
2015.8.18	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 8 月• EC2Config 服务，版本 3.8.294• 最新 适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Windows Server 2012 和 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">• AWS 半虚拟化驱动程序 7.3.2
2015.7.21	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 7 月• EC2Config 服务，版本 3.7.308• 最新 适用于 Windows PowerShell 的 AWS 工具• 修改了 SQL 映像的 AMI 描述以实现一致性

发布	更改
2015.6.10	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 6 月• EC2Config 服务，版本 3.6.269• 最新 适用于 Windows PowerShell 的 AWS 工具• 最新 AWS CloudFormation 帮助程序脚本 <p>仅使用 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">• AWS 半虚拟化驱动程序 7.3.1
2015.5.13	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 5 月• EC2Config 服务，版本 3.5.228• 最新 适用于 Windows PowerShell 的 AWS 工具
2015.04.15	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 4 月• EC2Config 服务，版本 3.3.174• 最新 适用于 Windows PowerShell 的 AWS 工具
2015.03.11	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 3 月• EC2Config 服务，版本 3.2.97• 最新 适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">• AWS 半虚拟化驱动程序 7.3.0
2015 年 2 月 11 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2015 年 2 月• EC2Config 服务，版本 3.0.54• 最新 适用于 Windows PowerShell 的 AWS 工具• 最新 AWS CloudFormation 帮助程序脚本

发布	更改
2015 年 1 月 14 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2015 年 1 月EC2Config 服务，版本 2.3.313最新适用于 Windows PowerShell 的 AWS 工具最新 AWS CloudFormation 帮助程序脚本
2014 年 12 月 10 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2014 年 12 月EC2Config 服务，版本 2.2.12最新适用于 Windows PowerShell 的 AWS 工具
2014 年 11 月 19 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2014 年 11 月EC2Config 服务，版本 2.2.11最新适用于 Windows PowerShell 的 AWS 工具
2014 年 10 月 15 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2014 年 10 月EC2Config 服务，版本 2.2.10最新适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">AWS 半虚拟化驱动程序 7.2.4.1 (解决了即插即用清理功能的问题，该功能现已默认启用)
2014 年 9 月 10 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2014 年 9 月EC2Config 服务，版本 2.2.8最新适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">禁用即插即用清理功能 (请参阅重要信息)AWS 半虚拟化驱动程序 7.2.2.1 (解决了卸载程序的问题)

发布	更改
2014 年 8 月 13 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 8 月• EC2Config 服务，版本 2.2.7• 最新 适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Windows Server 2012 R2 的 AMI</p> <ul style="list-style-type: none">• AWS 半虚拟化驱动程序 7.2.2.1 (提高磁盘性能，解决了重新连接多个网络接口和丢失网络设置的问题)
2014 年 7 月 10 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 7 月• EC2Config 服务，版本 2.2.5• 最新 适用于 Windows PowerShell 的 AWS 工具
2014 年 6 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 6 月• EC2Config 服务，版本 2.2.4• 删除了 NVIDIA 驱动程序 (Windows Server 2012 R2 AMI 除外)• 最新 适用于 Windows PowerShell 的 AWS 工具
2014 年 5 月 14 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 5 月• EC2Config 服务，版本 2.2.2• 最新 适用于 Windows PowerShell 的 AWS 工具• AWS CloudFormation 帮助程序脚本，版本 1.4.0
2014 年 4 月 9 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 4 月• 最新 适用于 Windows PowerShell 的 AWS 工具• 最新 AWS CloudFormation 帮助程序脚本
2014 年 3 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2014 年 3 月

发布	更改
2014 年 2 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2014 年 2 月EC2Config 服务，版本 2.2.1最新适用于 Windows PowerShell 的 AWS 工具KB2634328删除 BCDEdit useplatformclock 值 <p>仅使用 Microsoft SQL Server 的 AMI</p> <ul style="list-style-type: none">Microsoft SQL Server 2012 SP1 累积更新程序包 8Microsoft SQL Server 2008 R2 累积更新程序包 10
2013 年 11 月 13 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2013 年 11 月EC2Config 服务，版本 2.1.19最新适用于 Windows PowerShell 的 AWS 工具将 NTP 配置为每天同步一次时间（默认为每七天同步） <p>仅使用 Windows Server 2012 的 AMI</p> <ul style="list-style-type: none">使用以下命令清理 WinSXS 文件夹：dism /online /cleanup-image /StartComponentCleanup
2013 年 9 月 11 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2013 年 9 月EC2Config 服务，版本 2.1.18最新适用于 Windows PowerShell 的 AWS 工具AWS CloudFormation 帮助程序脚本，版本 1.3.15
2013 年 7 月 10 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2013 年 7 月EC2Config 服务，版本 2.1.16已将根卷扩展为 50 GB将页面文件设置为 512 MB，可根据需要扩展到 8 GB最新适用于 Windows PowerShell 的 AWS 工具

发布	更改
2013 年 6 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2013 年 6 月• 最新 适用于 Windows PowerShell 的 AWS 工具 <p>仅使用 Microsoft SQL Server 的 AMI</p> <ul style="list-style-type: none">• Microsoft SQL Server 2012 SP1 (含累积更新程序包 4)
2013 年 5 月 15 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2013 年 5 月• EC2Config 服务，版本 2.1.15• 默认附加所有实例存储卷• 默认启用远程 PowerShell• 最新 适用于 Windows PowerShell 的 AWS 工具
2013 年 4 月 14 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2013 年 4 月• 最新 适用于 Windows PowerShell 的 AWS 工具• AWS CloudFormation 帮助程序脚本，版本 1.3.14
2013 年 3 月 14 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2013 年 3 月• EC2Config 服务，版本 2.1.14• 锁定 CPU 检测信号的 Citrix 代理• 最新 适用于 Windows PowerShell 的 AWS 工具• AWS CloudFormation 帮助程序脚本，版本 1.3.11

发布	更改
2013 年 2 月 22 日	<p>所有 AMI</p> <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2013 年 2 月KB2800213Windows PowerShell 3.0 升级EC2Config 服务，版本 2.1.13限定时间的 Citrix 代理Citrix 半虚拟化驱动程序，日期为 2011 年 7 月 19 日最新适用于 Windows PowerShell 的 AWS 工具AWS CloudFormation 帮助程序脚本，版本 1.3.8 <p>仅使用 Microsoft SQL Server 的 AMI</p> <ul style="list-style-type: none">Microsoft SQL Server 2012 累积更新程序包 5
2012 年 12 月 12 日	所有 AMI <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2012 年 12 月将 ActiveTimeBias 注册表值设为 0禁用网络适配器的 IPv6EC2Config 服务，版本 2.1.9添加适用于 Windows PowerShell 的 AWS 工具 并将策略设置为允许导入模块
2012 年 11 月 15 日	所有 AMI <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2012 年 11 月EC2Config 服务，版本 2.1.7
2012 年 10 月 10 日	所有 AMI <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2012 年 10 月
2012 年 8 月 15 日	所有 AMI <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2012 年 8 月EC2Config 服务，版本 2.1.2KB2545227
2012 年 7 月 11 日	所有 AMI <ul style="list-style-type: none">Microsoft 安全更新，最新日期为 2012 年 7 月

发布	更改
2012 年 6 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 6 月• 将页面文件设置为 4 GB• 删除已安装的语言包• 将性能选项设置为“Adjust for best performance”• 将屏幕程序保护设置为恢复时不再显示登录屏幕• 使用 pnputil 删除以前的 RedHat 驱动程序版本• 使用 bcdedit 删除重复的启动加载程序，并将 bootstatuspolicy 设置为 ignoreallfailures
2012 年 5 月 10 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 5 月• EC2Config 服务，版本 2.1.0
2012 年 4 月 11 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 4 月• KB2582281• EC2Config 最新版本• 系统时间使用 UTC 而非 GMT
2012 年 3 月 13 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 3 月
2012 年 2 月 24 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 2 月• 标准化 AMI 名称和描述
2012 年 1 月 12 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2012 年 1 月• RedHat 半虚拟化驱动程序，版本 1.3.10
2011 年 9 月 11 日	<p>所有 AMI</p> <ul style="list-style-type: none">• Microsoft 安全更新，最新日期为 2011 年 9 月

发布	更改
1.04	所有 AMI <ul style="list-style-type: none">• 最新 Microsoft 安全更新• 更新网络驱动程序• 解决在更改实例时区时丢失连接的 VPC 中的实例问题
1.02	所有 AMI <ul style="list-style-type: none">• 最新 Microsoft 安全更新• 更新网络驱动程序• 为 VPC 的实例添加许可激活支持
1.01	所有 AMI <ul style="list-style-type: none">• 最新 Microsoft 安全更新• 解决在等待网络可用性时错误生成密码的问题
1.0	所有 AMI <ul style="list-style-type: none">• 首次发布

映像更改

以下更改适用于 Amazon 提供的每个映像。

- 允许 Internet 控制消息协议 (ICMP) 流量通过防火墙
- 设置性能选项以获得最佳性能
- 将电源设置设为高性能
- 禁用保护屏幕程序密码
- 禁用休眠
- 在关闭时禁用清除页面
- 添加指向桌面 EC2 Microsoft Windows 指南 (<http://docs.amazonaws.cn/AWSEC2/latest/WindowsGuide/concepts.html>) 和指向 EC2 反馈的链接 (https://aws.qualtrics.com/se/?sid=sv_e5mofjhv18gtayw)
- 将时区设置为 UTC
- 配置页面文件 (512 MB 至 8 GB)
- 安装 PowerShell 工具 (<http://www.amazonaws.cn/powershell>)
- 安装最新版本的 EC2Config 服务
- 禁用 Windows 网络位置配置文件选择提示
- 安装 Cloud Formation 工具 (<http://www.amazonaws.cn/developertools/aws-cloudformation/4026240853893296>)
- 在网络适配器中禁用 IPv6
- 在网络适配器中禁用 NetBIOS

- 为版本低于 Windows Server 2012 的映像安装 PowerShell 3.0
- 启用远程 PowerShell
- 启用文件和打印机共享
- 为包含 SQL Server 的映像打开端口 1433
- 启用 Windows 更新的通知
- 通过 NTP 每天同步时间
- 禁用 Windows Internet Explorer RunOnce
- 为 Windows Server 2008 或 Server 2008 R2 映像应用以下修补程序：
 - GARP (<http://support.microsoft.com/kb/2582281>)
 - Microsoft DST (<http://support.microsoft.com/kb/2800213>)
 - Microsoft RTIU 时钟同步 (<http://support.microsoft.com/kb/2922223>)
 - ELB (<http://support.microsoft.com/kb/2634328>)
 - TCP 缩放 (<http://support.microsoft.com/kb/2780879>)
 - SMB2 (<http://support.microsoft.com/kb/2394911>)
- 将实例存储卷挂载到扩展挂载点 (25)
- 安装最新的 Microsoft Windows 更新

订阅 Windows AMI 通知

如果您希望在新 AMI 发布时或在以前的 AMI 设为私有时接收相关通知，可以使用 Amazon SNS 订阅这些通知。

订阅 Windows AMI 通知

1. 打开 Amazon SNS 控制台。
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）。您必须选择此区域，因为您订阅的 SNS 通知是在此区域中创建的。
3. 在导航窗格中，单击 Subscriptions。
4. 单击 Create Subscription (创建订阅)。
5. 在 Create Subscription (创建事件订阅) 对话框中，请执行以下操作：
 - a. 在 TopicARN 中，输入以下任意一个 Amazon 资源名称 (ARN)：
 - `arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-update`
 - `arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-private`
 - b. 在 Protocol 中，选择 Email。
 - c. 在 Endpoint 中，输入用于接收通知的电子邮件地址。
 - d. 单击 Subscribe (订阅)。
6. 您将收到一封包含主题行 AWS Notification - Subscription Confirmation 的确认电子邮件。打开电子邮件，然后单击 Confirm subscription 以完成订阅。

每当发布新的 Windows AMI 时，我们都会向订阅 `ec2-windows-ami-update` 主题的用户发送通知。每当有新的 Windows AMI 被设为私有时，我们都会向订阅 `ec2-windows-ami-private` 主题的用户发送通知。如果您不希望再收到这些通知，请通过以下步骤取消订阅。

取消订阅 Windows AMI 通知

1. 打开 Amazon SNS 控制台。
2. 在导航窗格中，单击 Subscriptions。
3. 选择订阅内容，然后单击 Delete Subscriptions。当系统提示您进行确认时，单击 Yes, Delete。

升级或迁移 Windows Server 实例

有关如何将实例升级或迁移到较新版本的 Windows 的信息，请参阅[将 Windows Server EC2 实例升级到较新版本的 Windows Server](#)。

使用 Sysprep 创建标准 Amazon 系统映像 (AMI)

Abstract

使用 Sysprep 创建标准 Amazon 系统映像 (AMI)。

Microsoft 系统准备 (Sysprep) 工具可简化复制 Microsoft Windows 自定义安装的过程。我们建议您使用 Sysprep 创建标准化 Amazon 系统映像(AMI)。随后可以通过此标准化映像为 Windows 创建新的 Amazon EC2 实例，并在组织中部署这些实例。

我们还建议您将 Sysprep 与 EC2Config 服务一起运行，这样可使用应答文件自动执行并保护针对 AMI 的映像准备过程。默认情况下，该文件位于以下目录中：C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml

重要提示：请勿使用 Sysprep 创建实例备份。Sysprep 会删除特定于系统的信息；删除这些信息可能会对实例备份导致意外结果。

内容

- [在您开始之前 \(p. 105\)](#)
- [将 Sysprep 与 EC2Config 服务结合使用 \(p. 105\)](#)
- [将 Sysprep 与 EC2Config 服务一起运行 \(p. 108\)](#)
- [使用 EC2Config 对 Sysprep 进行故障排除 \(p. 109\)](#)

在您开始之前

- 在 Microsoft TechNet 上了解有关 [Sysprep](#) 的更多信息。
- 了解 [Sysprep 支持的服务器角色](#)。

将 Sysprep 与 EC2Config 服务结合使用

了解准备映像时的不同 Sysprep 执行阶段以及 EC2Config 服务执行的任务的详细信息。

Sysprep 阶段

Sysprep 会经历以下阶段：

1. 一般化：该工具删除特定于映像的信息和配置。例如，Sysprep 会删除安全标识符 (SID)、计算机名称、事件日志和特定驱动程序等等。完成这一阶段后，操作系统 (OS) 即准备就绪，可以创建 AMI。



Note

将 Sysprep 与 EC2Config 服务一起运行时，系统会防止删除驱动程序，因为 PersistAllDeviceInstalls 在默认情况下设置为 true。

2. 专门化：即插即用功能会扫描计算机并为检测到的所有设备安装驱动程序。该工具生成 OS 要求（如计算机名称和 SID）。您可以选择在这一阶段执行命令。
3. 全新体验 (OOBE)：系统运行 Windows 安装程序的一个简化版本并要求用户输入信息（如系统语言、时区和注册组织）。如果配合使用 Sysprep 与 EC2Config，应答文件会自动执行这一阶段。

Sysprep 操作

准备映像时，Sysprep 和 EC2Config 服务执行以下操作。

1. 在 EC2 Service Properties 对话框中选择 Shutdown with Sysprep 时，系统运行 ec2config.exe –sysprep 命令。
2. EC2Config 服务读取 BundleConfig.xml 文件的内容。默认情况下，此文件位于以下目录中：C:\Program Files\Amazon\Ec2ConfigService\Settings。

BundleConfig.xml 文件包含以下设置。您可以更改这些设置：

- AutoSysprep：指明是否自动使用 Sysprep。如果从 EC2 Service Properties 对话框运行 Sysprep，则无需更改此值。默认值为 No。
 - SetRDPCertificate：为 Windows Server 2003 上运行的远程桌面服务器设置自签名证书。这样，您可以安全地使用远程桌面协议 (RDP) 连接到实例。如果新实例应使用证书，请将该值更改为 Yes。此设置不适用于 Windows Server 2008 或 Windows Server 2012 实例，因为这些操作系统会生成自己的证书。默认值为 No。
 - SetPasswordAfterSysprep：在新启动的实例上设置随机密码，使用用户启动密钥对其进行加密，并将加密密码输出到控制台。如果新实例不应设置为随机加密密码，请将该值更改为 No。默认值是 Yes。
 - PreSysprepRunCmd：要运行的命令的位置。默认情况下，该命令位于以下目录中：C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd
3. 系统执行 BeforeSysprep.cmd。此命令创建以下注册表项：

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f"
```

该注册表项禁用 RDP 连接，直到它们重新启用。禁用 RDP 连接是必需的安全措施，因为在 Sysprep 运行之后的第一个启动会话过程中，在短时间内，RDP 允许连接并且管理员密码为空。

4. EC2Config 服务通过执行以下命令来调用 sysprep.exe：

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /oobe /generalize /shutdown
```

一般化阶段

1. 该工具删除特定于映像的信息和配置（如计算机名称和 SID）。如果实例是域的成员，则会从域中将其移除。sysprep2008.xml 应答文件包含影响这一阶段的以下设置：
 - PersistAllDeviceInstalls：此设置防止 Windows 安装程序删除和重新配置设备，这可加快映像准备过程，因为 Amazon AMI 需要运行特定驱动程序，而这些驱动程序的重新检测需要花费一些时间。
 - DoNotCleanUpNonPresentDevices：此设置为当前不存在的设备保留即插即用信息。
2. Sysprep.exe 在准备创建 AMI 时会关闭 OS。系统会启动新实例或启动原始实例。

专门化阶段

系统生成特定于 OS 的要求（如计算机名称和 SID）。系统还根据您在 sysprep2008.xml 应答文件中指定的配置来执行以下操作。

- CopyProfile：Sysprep 可以配置为删除所有用户配置文件，包括内置管理员配置文件。此设置保留内置管理员账户，这样，您对该账户进行的所有自定义都可转移到新映像。默认值是 True。

如果您没有要转移到新映像的特定用户配置文件自定义设置，请将此设置更改为 False。Sysprep 会删除所有用户配置文件；这可以节省时间和磁盘空间。

- TimeZone：默认情况下，时区设置为协调世界时 (UTC)。
- 顺序 1 同步命令：系统执行以下命令，以启用管理员账户并指定密码要求。

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER  
/PASSWORDREQ:YES
```

- 顺序 2 同步命令：系统加密管理员密码。如果未启用 ec2setpassword 设置，则此安全措施可防止在 Sysprep 完成之后实例处于可访问状态。

```
C:\Program Files\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator
```

- 顺序 3 同步命令：系统执行以下命令：

```
C:\Program Files\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd
```

此命令添加以下注册表项，用于重新启用 RDP：

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 0 /f
```

OOBE 阶段

1. 通过使用 EC2Config 服务应答文件，系统指定以下配置：

- <InputLocale>en-US</InputLocale>
- <SystemLocale>en-US</SystemLocale>
- <UILanguage>en-US</UILanguage>
- <UserLocale>en-US</UserLocale>
- <HideEULAPage>true</HideEULAPage>
- <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
- <NetworkLocation>Other</NetworkLocation>
- <ProtectYourPC>3</ProtectYourPC>
- <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
- <TimeZone>UTC</TimeZone>
- <RegisteredOrganization>Amazon.com</RegisteredOrganization>
- <RegisteredOwner>Amazon</RegisteredOwner>



Note

在一般化和专门化阶段期间，EC2Config 服务监控 OS 的状态。如果 EC2Config 检测到 OS 处于 Sysprep 阶段，则会向系统日志发布以下消息：

```
"EC2ConfigMonitorState: 0 Windows is being configured.  
SysprepState=IMAGE_STATE_UNDEPLOYABLE"
```

2. 在 OOBE 阶段完成之后，系统从以下位置执行 SetupComplete.cmd：

C:\Windows\Setup\Scripts\SetupComplete.cmd。在 2015 年 4 月之前的 Amazon 公用 AMI 中，此文

件为空，不对映像执行任何操作。在 2015 年 4 月之后的公用 AMI 中，此文件包含以下值：call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd"。

3. 系统执行 PostSysprep.cmd，后者执行以下操作：

- 将本地管理员密码设置为不过期。如果密码已过期，管理员可能无法登录。
- 设置 MSSQLServer 机器名称（如果已安装），以便该名称与 AMI 同步。

Sysprep 之后

Sysprep 完成之后，EC2Config 服务将以下消息发送到控制台输出：

"Windows sysprep configuration complete. Message: Sysprep Start Message: Sysprep End"

EC2Config 随后执行以下操作：

1. 读取 config.xml 文件的内容并列出所有已启用的插件。

2. 同时执行所有“Windows 就绪之前”插件。

- Ec2SetPassword
- Ec2SetComputerName
- Ec2InitializeDrives
- Ec2EventLog
- Ec2ConfigureRDP
- Ec2OutputRDPCert
- Ec2SetDriveLetter
- Ec2WindowsActivate
- Ec2DynamicBootVolumeSize

3. 完成之后，将“Windows 准备就绪”消息发送到实例系统日志。

4. 同时运行所有“Windows 就绪之后”插件。

- AWS CloudWatch 日志
- UserData
- Simple Systems Manager (SSM)

有关 Windows 插件的更多信息，请参阅[使用 EC2Config 服务配置 Windows 实例](#)。

将 Sysprep 与 EC2Config 服务一起运行

通过以下过程可使用 Sysprep 和 EC2Config 服务创建标准化 AMI。

1. 在 Amazon EC2 控制台中，查找或[创建](#)要复制的 AMI。

2. 启动并连接到您的 Windows 实例。

3. 对它进行自定义。

4. 在 EC2Config 服务应答文件中指定配置设置：

C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml

5. 在 Windows 开始菜单中，选择所有程序，然后选择 EC2ConfigService Settings。

6. 在 Ec2 Service Properties 对话框中选择 Image 选项卡。有关 Ec2 Service Properties 对话框中的选项和设置的更多信息，请参阅[Ec2 服务属性](#)。

7. 选择管理员密码选项，然后单击 Shutdown with Sysprep 或 Shutdown without Sysprep。EC2Config 会根据您选择的密码选项编辑设置文件。

- Random：EC2Config 生成一个密码，使用用户的密钥加密，并向控制台显示加密的密码。我们会在首次启动后禁用此设置，以便在重启或停止再启动实例后该密码仍然存在。

- Specify : 密码以非加密格式（明文）存储在 Sysprep 应答文件中。下一次运行 Sysprep 时，它将设置管理员密码。如果现在就关闭，则会立即设置密码。服务再次启动时，则会删除管理员密码。务必要记住此密码，因为以后无法将其取回。
- Keep Existing : 运行 Sysprep 或重新启动 EC2Config 时，管理员账户的现有密码不变。务必要记住此密码，因为以后无法将其取回。

8. 选择 OK。

如果系统询问您是否想运行 Sysprep 并关闭该实例，请单击 Yes。您会看到 EC2Config 运行 Sysprep。然后，您会退出实例并且实例会关闭。如果您在 Amazon EC2 控制台中查看 Instances 页面，实例状态会从 running 变为 stopping，然后最终变为 stopped。此时，从该实例创建一个 AMI 是安全的。

您可以使用以下命令从命令行中手动调用 Sysprep 工具：

```
C:\> %ProgramFiles%\Amazon\Ec2ConfigService\ec2config.exe -sysprep
```

但是，请务必确保 Ec2ConfigService\Settings 文件夹中指定的 XML 文件选项正确无误，否则您可能无法连接到实例。有关设置文件的更多信息，请参阅 [EC2Config 设置文件 \(p. 253\)](#)。有关配置 Sysprep 并从命令行中运行它的示例，请参阅 Ec2ConfigService\Scripts\InstallUpdates.ps1。

使用 EC2Config 对 Sysprep 进行故障排除

如果在映像准备过程中遇到问题或收到错误消息，请查看以下日志：

- %WINDIR%\Panther\Unattendgc
- %WINDIR%\System32\Sysprep\Panther
- "C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt"

如果在使用 Sysprep 进行映像准备的过程中收到错误消息，则 OS 可能无法访问。要查看日志文件，您必须停止实例，将其根卷作为辅助卷挂载到另一个运行状况良好的实例，然后在辅助卷上查看前述日志。

如果在 Unattendgc 日志文件中找到错误，请使用 [Microsoft 错误查找工具](#) 获取有关错误的更多详细信息。以下在 Unattendgc 日志文件中报告的问题通常是实例上一个或多个损坏的用户配置文件造成的：
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]

有两个选项可用于解决此问题：

选项 1：在实例上使用 Regedit 搜索以下项。验证已删除用户是否没有配置文件注册表项：

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\]
```

选项 2：编辑 EC2Config 应答文件 (C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml) 并将 <CopyProfile>true</CopyProfile> 更改为 <CopyProfile>false</CopyProfile>。再次运行 Sysprep。请注意，此配置更改会在 Sysprep 完成之后删除内置管理员用户配置文件。

Amazon EC2 实例

Abstract

配置、启动、连接和管理您的实例。

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 \(p. 13\)](#)
- [Amazon EC2 Windows 实例入门 \(p. 19\)](#)
- [实例生命周期 \(p. 213\)](#)

您需先回答以下问题，然后才能启动生产环境。

Q. 什么样的实例类型最能满足我的需求？

Amazon EC2 提供不同的实例类型，以便您可以选择需要的 CPU、内存、存储和网络容量来运行您的应用程序。有关更多信息，请参阅 [实例类型 \(p. 110\)](#)。

Q. 什么样的购买选项最能满足我的需求？

Amazon EC2 支持按需实例（默认设置）、竞价型实例和预留实例。有关更多信息，请参阅 [实例购买选项 \(p. 136\)](#)。

Q. 哪种类型的根卷能满足我的需求？

由 Amazon EBS 或实例存储支持的每一个实例。根据您需要的根卷类型选择 AMI。有关更多信息，请参阅 [根设备存储 \(p. 63\)](#)。

Q. 我能否从使用 Virtual Private Cloud 中获益？

如果您可以在 EC2-Classic 或 EC2-VPC 中启动实例，您将需要确定哪个平台能满足您的需求。有关更多信息，请参阅 [支持的平台 \(p. 577\)](#) 和 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 572\)](#)。

实例类型

Abstract

Amazon EC2 提供了具有不同计算、内存、存储和网络功能的各种实例类型。

启动实例时，您指定的实例类型决定了用于您的实例的主机硬件。每个实例类型提供不同的计算、内存和存储功能，并按照这些功能分组到实例系列。选择一种基于您打算在实例上运行的应用程序或软件的需求的实例类型。

Amazon EC2 为每个实例提供一致且可预计的 CPU 容量，无论实际的底层硬件是什么。

CPU、内存和实例存储这类主机资源是 Amazon EC2 专用的。但 Amazon EC2 也会在实例间共享主机的另一些资源，例如网络和磁盘子系统。如果一台主机上的每个实例都试图尽可能多地使用这些共享的资源，那么每个实例都将获得该资源相等份额。然而，当某个资源未被充分利用时，实例往往可以在它可用时获取该资源的更高份额。

每种实例类型均从共享资源提供更高或更低的起始性能。例如，高 I/O 性能的实例类型能获取共享资源的更高份额。分配更大份额的共享资源也降低了 I/O 性能的方差。对于大多数应用程序，中等 I/O 是绰绰有余的。然而，对于需要更大或一致性更高的 I/O 性能的应用程序，可考虑使用更高 I/O 性能的实例类型。

内容

- [可用实例类型 \(p. 111\)](#)
- [硬件规格 \(p. 112\)](#)
- [联网和存储功能 \(p. 112\)](#)
- [实例限量 \(p. 113\)](#)

可用实例类型

Amazon EC2 提供了以下各表中列出的实例类型。

当前一代实例

为获得最佳性能，我们建议您在启动新实例时使用当前一代实例类型。有关当前一代实例类型的更多信息，请参阅 [Amazon EC2 实例](#)。

实例系列	当前一代实例类型
通用型	t2.nano t2.micro t2.small t2.medium t2.large m3.medium m3.large m3.xlarge m3.2xlarge
计算优化	c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge
内存优化	r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge x1.32xlarge
存储优化	i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge
GPU 实例	g2.2xlarge

上一代实例

Amazon Web Services 为根据上一代实例优化了应用程序，但尚未升级的用户提供了上一代实例。我们鼓励您使用最新一代的实例以获得最佳性能，但我们将继续支持这些上一代数据库实例。如果您目前使用的是上一代实例，您可以查看哪个当前一代实例是合适的升级。有关更多信息，请参阅 [上一代实例](#)。

实例系列	上一代实例类型
通用型	m1.small m1.medium m1.large m1.xlarge
计算优化	c1.medium c1.xlarge cc2.8xlarge
内存优化	m2.xlarge m2.2xlarge m2.4xlarge cr1.8xlarge
存储优化	hi1.4xlarge hs1.8xlarge
GPU 实例	cg1.4xlarge
微型实例	t1.micro

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

要确定最适合您需求的实例类型，我们建议启动一个实例，并使用自己的基准测试应用程序。由于是按实例小时数付费，因而您能够在做出决策前方便而经济地测试不同的实例类型。

在做出决策后，如果您的需求有变化，则可以在稍后调整您的实例的大小。有关更多信息，请参阅 [调整您的实例大小 \(p. 133\)](#)。

联网和存储功能

在选择实例类型时，这将决定以下哪些联网和存储功能可用：

- 某些实例类型在 EC2-Classic 中不可用，因此您必须在 VPC 中启动它们。通过在 VPC 中启动某个实例，您可以利用在 EC2-Classic 中不可用的功能，如增强联网、将多个私有 IP 地址分配给实例和更改分配给您的实例的安全组。有关更多信息，请参阅 [实例类型仅在 VPC 中可用 \(p. 576\)](#)。
- 一些实例类型支持 EBS 卷和实例存储卷，而另一些实例类型仅支持 EBS 卷。某些支持实例存储卷的实例使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。有关更多信息，请参阅 [存储 \(p. 637\)](#)。
- 若要获得 Amazon EBS I/O 的额外专用容量，您可以将某些实例类型作为 EBS 优化实例启动。某些实例类型在默认情况下会进行 EBS 优化。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。
- 若要为高性能计算 (HPC) 应用程序优化实例，您可以启动某个置放群组中的某些实例类型。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。
- 若要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，您可以为某些当前一代实例类型启用增强联网。有关更多信息，请参阅 [Windows 上的增强联网 \(p. 630\)](#)。
- 支持的最大 MTU 因实例类型而异。所有 Amazon EC2 实例类型都支持标准以太网 V2 1500 MTU 框架。所有当前一代实例都支持 9001 MTU（超大框架），某些上一代实例也支持它们。有关更多信息，请参阅 [EC2 实例的网络最大传输单位 \(MTU\) \(p. 627\)](#)。

下表总结了当前一代实例类型支持的联网和存储功能。

	仅限 VPC	仅限于 EBS	SSD 卷	置放群组	仅限 HVM	增强联网
C3			是	是		Intel 82599 VF
C4	是	是		是	是	Intel 82599 VF
D2				是	是	Intel 82599 VF
G2			是	是	是	

	仅限 VPC	仅限于 EBS	SSD 卷	置放群组	仅限 HVM	增强联网
I2			是	是	是	Intel 82599 VF
M3			是			
M4	是	是		是	是	Intel 82599 VF
R3			是	是	是	Intel 82599 VF
T2	是	是			是	
X 1	是		是	是	是	ENI

实例限量

在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。

有关默认限制的更多信息，请参阅[我可以在 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 \(p. 746\)](#)。

T2 实例

Abstract

使用 T2 实例提供适度的基准性能，并能够根据您工作负载的需要实现性能的显著突增。

T2 实例旨在提供适度的基准性能，并能够根据您工作负载的需要实现性能的显著突增。它们旨在用于不经常或不持续使用完整 CPU、但偶尔需要突增性能的工作负载。T2 实例非常适合于通用工作负载，如 Web 服务器、开发人员环境和小型数据库。有关 T2 实例定价的更多信息和其他硬件详细信息，请参阅[Amazon EC2 实例](#)。

如果您的账户不到 12 个月，您可以在特定使用限制下免费使用 t2.micro 实例。有关更多信息，请参阅[AWS 免费套餐](#)。

内容

- [硬件规格 \(p. 113\)](#)
- [T2 实例要求 \(p. 113\)](#)
- [CPU 积分 \(p. 114\)](#)
- [监控 CPU 积分 \(p. 115\)](#)

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅[Amazon EC2 实例](#)。

T2 实例要求

以下是 T2 实例的要求：

- 必须在 Virtual Private Cloud (VPC) 中启动 T2 实例；EC2-Classic 平台不支持 T2 实例。Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。您无法将 EC2-Classic 中的现有实例的实例类型更改为 T2 实例类型。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 577\)](#)。有关启动仅限 VPC 的实例的更多信息，请参阅[实例类型仅在 VPC 中可用 \(p. 576\)](#)。

- T2 实例可用作按需实例和预留实例，但它们不能用作竞价型实例、计划实例或专用实例。此外，它们在专用主机上不受支持。有关这些选项的详细信息，请参阅 [实例购买选项 \(p. 136\)](#)。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。默认情况下，您最多可同时运行 20 个 T2 实例。如果您需要更多 T2 实例，可以使用 [Amazon EC2 实例请求表](#) 请求实例。
- 确保您选择的 T2 实例大小达到您的操作系统和应用程序的最低内存要求。在许多使用案例中，带有消耗大量内存和 CPU 资源的图形用户界面的操作系统（例如，Microsoft Windows）可能需要 t2.micro 或更大的实例大小。随着您的工作负载对内存和 CPU 的需求随着时间增加，您可以扩展到更大的 T2 实例或其他 EC2 实例类型。

CPU 积分

一个 CPU 积分可以持续一分钟提供完整的 CPU 核心性能。传统 Amazon EC2 实例类型提供固定性能，而 T2 实例提供基准水平的 CPU 性能并能够突增到基准水平之上。基准性能和突增能力由 CPU 积分控制。

什么是 CPU 积分？

一个 CPU 积分等于一个 vCPU 按 100% 使用率运行一分钟。vCPU、利用率和时间的其他组合也等于一个 CPU 积分；例如，一个 vCPU 按 50% 利用率运行两分钟，或是两个 vCPU 按 25% 利用率运行两分钟。

如何赢取 CPU 积分？

每个 T2 实例开始都附带适量的初始 CPU 积分余额，随后每小时都以固定的数额持续（以毫秒级精度）接收 CPU 积分（具体取决于实例大小）。用于加减积分的核算过程也以毫秒级精度进行，因此您不必担心 CPU 积分超支；CPU 的短时间突增只消耗少部分的 CPU 积分。

当 T2 实例使用的 CPU 资源少于其基本性能水平资源限量时（如空闲时），未使用的 CPU 积分（或积分赢取与花费之间的差异）将存入积分余额且最多保留 24 小时，从而积累 CPU 积分以应对性能突增。当您的 T2 实例需要的 CPU 资源超过其基本性能水平资源限量时，它将占用 CPU 积分余额中的积分突增到最大 100% 的使用率。T2 实例拥有的 CPU 资源积分越多，它在需要更佳性能时可以超过其基本性能水平的突增时间就越长。

下表列出启动时收到的初始 CPU 积分分配、收到 CPU 积分的速率、采用完整核心性能百分比形式的基本性能水平，以及实例可以累积的获得的最大 CPU 积分余额。

实例类型	初始 CPU 积分 *	每小时获得的 CPU 积分	基本性能 (CPU 使用率)	获得的最大 CPU 积分余额***
t2.nano	3	5%	72	
t2.micro	6	10%	144	
t2.small	12	20%	288	
t2.medium	24	40%**	576	
t2.large	36	60%**	864	

* 可使用初始 CPU 积分启动的 T2 实例数量存在限制；默认情况下，该限制被设置为每个区域中每个账户的任何 T2 实例每 24 小时可启动 100 次。如果您要提高此限制，则可以使用[基于 Amazon EC2 积分的实例启动积分表](#)提出客户支持限制提高请求。如果您的账户在 24 小时内不会启动 100 个以上 T2 实例，则此限制对您没有影响。

** t2.medium 和 t2.large 实例有两个 vCPU。基本性能是两个 vCPU 的聚合。例如，如果您完全使用了一个 vCPU 并少量使用了其他 vCPU，则您的 CloudWatch 指标将显示利用率超过 50%。

*** 此最大值不包括初始 CPU 积分，初始积分将最先使用，并且不会过期。例如，启动后保持空闲长达 24 小时以上的 t2.micro 实例可达到高达 174 个积分余额（30 个初始 CPU 积分 + 获得的 144 个积分）。但是，在此实例使用初始 30 个 CPU 积分后，积分余额绝对不会超过 144 个，除非停止并再次启动此实例产生了新的初始 CPU 积分余额。

此初始积分余额旨在提供良好的启动体验。实例的获得的最大积分余额等于每小时收到的 CPU 积分数乘以 24 小时。例如，一个 t2.micro 实例每小时获得 6 个 CPU 积分，可以积累获得的最大 CPU 积分余额为 144 个 CPU 积分。

CPU 积分是否会过期？

初始 CPU 积分不会过期，但将在实例使用 CPU 积分时最先使用它们。以指定的 5 分钟时间为间隔，未使用的获得的积分将在获得后 24 小时过期，届时，在添加任何新获得的积分之前，将从 CPU 积分余额中删除过期的任何积分。此外，实例的 CPU 积分余额不会在实例停止与启动之间保留；停止实例会导致它丢失其全部积分余额，但是当它重新启动时会再次收到初始积分余额。

例如，如果 t2.small 实例在某个小时的 CPU 使用率为 5%，则它会使用 3 个 CPU 积分（60 分钟的 5%），但它在该小时赢得 12 个 CPU 积分，因此相差的 9 个 CPU 积分会添加到 CPU 积分余额。若在这个小时内，余额中有任何 CPU 积分达到其 24 小时的过期时间，这些积分（如果实例在 24 小时前完全空闲，则会有多达 12 个积分）也会从余额中扣除。如果过期的积分量大于赢得的积分量，则积分余额会减少；相反，如果过期的积分量小于赢得的积分量，则积分余额会增多。

如果我用掉了所有积分，会发生什么情况？

如果您的实例使用其所有 CPU 积分余额，则性能会保持在基准性能水平。如果您的实例在积分较少的情况下运行，则实例的 CPU 积分消耗（因此还有 CPU 性能）会在 15 分钟间隔内逐渐降低到基本性能水平，因此您在 CPU 积分耗尽时不会遇到急剧的性能下降。如果您的实例经常用完所有 CPU 积分余额，建议您使用更大的 T2 大小，或使用固定性能实例类型（如 M3 或 C3）。

监控 CPU 积分

您可以查看 CloudWatch 控制台 Amazon EC2 每个实例的指标中提供的每个 T2 实例积分余额。T2 实例有两个指标：CPUCreditUsage 和 CPUCreditBalance。CPUCreditUsage 指标指示在测量期内使用的 CPU 积分数。CPUCreditBalance 指标指示 T2 实例获得的未使用 CPU 积分数。此余额会在突增期间耗尽，因为花费 CPU 积分的速度比获得积分的速度更快。

下表介绍可以使用的新 CloudWatch 指标；有关在 CloudWatch 中使用这些指标的信息，请参阅[列出实例的可用 CloudWatch 指标 \(p. 453\)](#)。

指标	说明
CPUCreditUsage	<p>(仅对 T2 实例有效) 在指定时段内消耗的 CPU 积分数量。</p> <p>这项指标标识了物理 CPU 在处理虚拟 CPU 分配给实例的指令时所花费的时间。</p> <p> Note</p> <p>CPU 积分指标每 5 分钟可用一次。</p> <p>单位 : 计数</p>
CPUCreditBalance	<p>(仅对 T2 实例有效) 实例累积的 CPU 积分数量。</p> <p>该指标用于确定实例在给定的速率下可以突增至超出基准性能水平的时长。</p> <p> Note</p> <p>CPU 积分指标每 5 分钟可用一次。</p> <p>单位 : 计数</p>

C4 实例

Abstract

使用 C4 实例可提供高性能计算和高级优化功能。

C4 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。C4 实例也适用于以下应用程序：

- 批处理工作负载
- 媒体转码
- 高流量 Web 服务器、大型多人联机 (MMO) 游戏服务器和广告服务引擎
- 高性能计算 (HPC) 以及其他计算密集型应用程序

内容

- [硬件规格 \(p. 116\)](#)
- [C4 实例功能 \(p. 117\)](#)
- [C4 实例要求 \(p. 117\)](#)

硬件规格

C4 实例基于定制的 2.9 GHz Intel Xeon E5-2666 v3 (Haswell) 处理器，专门针对 Amazon EC2 进行了优化。借助 Intel 睿频加速技术，在 c4.8xlarge 实例中的单核或双核经睿频加速后，C4 实例的处理器时钟频率可高达 3.5Ghz。

下表突出显示了 Intel Xeon E5-2666 v3 处理器的功能集。有关更多信息，请参阅 [Intel 和 Amazon Web Services](#)。

功能	规范
处理器编号	E5-2666 v3
Intel 智能缓存	25 MiB
指令集	64 位
指令集扩展	AVX 2.0
平版印刷	22 nm
处理器基础频率	2.9 GHz
所有核心最大睿频	3.2 GHz
最大睿频	3.5 GHz (用于 c4.8xlarge 上)
Intel 睿频加速技术	2.0
Intel vPro 技术	是
Intel 超线程技术	是
Intel 64	是
空闲状态	是
增强的 Intel SpeedStep 技术	是
热量监控技术	是
AES 新指令	是
安全密钥	是
执行禁用位	是

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](#)。

C4 实例功能

以下是 C4 实例功能的摘要：

- 默认情况下，C4 实例为 EBS 优化实例，可为 Amazon EBS 提供从 500 Mbps 到 4000 Mbps 的专用数据块存储吞吐量，无需其他费用。通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 C4 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。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。
- 您可以启用增强联网功能。通过增强联网功能，您可以显著提高每秒数据包数 (PPS) 性能，降低网络抖动，并减少延迟。有关更多信息，请参阅 [Windows 上的增强联网 \(p. 630\)](#)。
- 您可以在置放群组中集中放置 C4 实例。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

C4 实例要求

以下是 C4 实例的要求：

- C4 实例需要 64 位 HVM AMI。它们具有大容量内存（RAM 最高可达 60 GiB），需要 64 位操作系统才能充分利用该容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- 必须在 Virtual Private Cloud (VPC) 中启动 C4 实例；EC2-Classic 平台不支持 C4 实例。Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅 [支持的平台 \(p. 577\)](#)。有关启动仅限 VPC 的实例的更多信息，请参阅 [实例类型仅在 VPC 中可用 \(p. 576\)](#)。
- 在一个区域中可以启动的实例总数存在限制，某些 C4 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？](#)

如果您需要更多 C4 实例，可以使用 [Amazon EC2 实例请求表](#) 请求实例。

Windows GPU 实例

Abstract

GPU 实例专用于图形和一般用途的 GPU 计算应用程序。

如果您需要较高的并行处理能力，则使用 GPU 实例会使您受益，通过这些实例可以访问具有多达 1536 个 CUDA 核心和 4 GB 视频内存的 NVIDIA GPU。可以通过 GPU 实例来利用统一计算设备架构 (CUDA) 或 OpenCL 并行计算框架，从而为很多科学、工程和绘制应用加速。还可以将这些实例用于图形应用程序，包括游戏流式处理、3-D 应用流式处理和其他图形工作负载。

GPU 实例作为基于 HVM 的实例来运行。硬件虚拟机 (HVM) 虚拟化使用 AWS 平台提供的硬件辅助技术。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提高性能之外。这使 Amazon EC2 可以在每个 GPU 实例中提供对一个或多个离散 GPU 的专用访问。

您可以在置放群组中对 GPU 实例进行群集化。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

内容

- [硬件规格 \(p. 118\)](#)
- [GPU 实例限制 \(p. 118\)](#)
- [GPU 实例的 AMI \(p. 119\)](#)
- [在 Windows 上安装 NVIDIA 驱动程序 \(p. 119\)](#)

有关 Linux GPU 实例的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Linux GPU 实例](#)。

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](#)。

GPU 实例限制

GPU 实例具有以下限制：

- 您必须使用 HVM AMI 启动实例。
- 除非安装了 NVIDIA 驱动程序，否则它们无法访问 GPU。
- 您可运行的实例数存在限制。有关更多信息，请参阅 Amazon EC2 常见问题中的 [我可以在 Amazon EC2 中运行多少个实例？](#)。要请求增大这些限制，请使用以下表格：[增大 Amazon EC2 实例限制请求](#)。

GPU 实例的 AMI

为了帮助您开始使用，NVIDIA 提供了适用于 GPU 实例的 AMI。这些参考 AMI 包含 NVIDIA 驱动程序，可实现 NVIDIA GPU 的完整功能和性能。有关具有 NVIDIA 驱动程序的 AMI 的列表，请参阅 [AWS Marketplace \(NVIDIA GRID\)](#)。

您可以使用任何 HVM AMI 启动 CG1 和 G2 实例。

在 Windows 上安装 NVIDIA 驱动程序

要在 Windows 实例上安装 NVIDIA 驱动程序，请使用远程桌面以管理员身份登录您的 Windows 实例。您可以从 <http://www.nvidia.com/Download/Find.aspx> 下载 NVIDIA 驱动程序。选择适用于 Windows Server 版本的 NVIDIA GRID K520 (G2 实例) 或 Tesla M-Class M2050 (CG1 实例) 的驱动程序。打开在其中下载驱动程序的文件夹，然后双击安装文件以启动它。按照说明安装驱动程序并根据需要重启实例。要验证 GPU 是否正常工作，请检查设备管理器。



Note

如果使用在 g2.2xlarge 实例 (包含 1 个 GPU) 上创建的 Windows AMI 启动 g2.8xlarge 实例 (包含 4 个 GPU)，则 Windows 不会自动在所有 4 个 GPU 上安装 NVIDIA 驱动程序。您必须授权新 GPU 硬件的驱动程序安装。

您可以通过打开 Other 设备类别 (非活动 GPU 不显示在 Display Adapters 下) 手动更正此问题，然后针对每个非活动 GPU，右键单击并选择 Update Driver Software，然后选择默认 Automatic Update 选项。

使用远程桌面时，使用 WDDM 驱动程序模型的 GPU 会替换为非加速的远程桌面显示驱动程序。要访问 GPU 硬件，您必须使用不同的远程访问工具，如 VNC。还可以使用 AWS Marketplace 中的 GPU AMI 之一，因为它们提供支持 3D 加速的远程访问工具。

I2 实例

Abstract

I2 实例提供非常快速的 SSD 支持型实例存储，它经过优化，具有极高的随机 I/O 性能和较低的每 IOPS 成本。

I2 实例经过了优化，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)。它们非常适合用于下列情况：

- NoSQL 数据库 (例如，Cassandra 和 MongoDB)
- 群集化数据库
- 联机事务处理 (OLTP) 系统

内容

- [硬件规格 \(p. 119\)](#)
- [I2 实例功能 \(p. 120\)](#)
- [I2 实例要求 \(p. 120\)](#)
- [SSD I/O 性能 \(p. 120\)](#)

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](#)。

I2 实例功能

以下是 I2 实例功能的摘要：

- 主要数据存储是基于 SSD 的实例存储。与所有实例存储一样，这些卷只在实例生命周期内存在。当您停止或终止实例时，将擦除其实例存储中的应用程序和数据。我们建议您定期备份或复制您存储在实例存储中的数据。有关更多信息，请参阅 [SSD 实例存储卷 \(p. 707\)](#)。
- 您可以启用增强联网功能。通过增强联网功能，您可以显著提高每秒数据包数 (PPS) 性能，降低网络抖动，并减少延迟。有关更多信息，请参阅 [Windows 上的增强联网 \(p. 630\)](#)。
- 您可以在置放群组中集中放置 I2 实例。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。
- 您可以启用 EBS 优化来为 Amazon EBS I/O 获取额外的专用容量。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。

I2 实例要求

以下是 I2 实例的要求：

- 您必须使用 HVM AMI 启动 I2 实例。
- 在一个区域中可以启动的实例总数存在限制，某些 I2 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？](#)

如果您需要更多 I2 实例，可以使用 [Amazon EC2 实例请求表](#) 请求实例。

SSD I/O 性能

如果您使用内核版本为 3.8 或更高版本的 Linux AMI 并使用可用于该实例的、基于 SSD 的所有实例存储卷，则您可以获取下表所列的最低随机 IOPS (4096 字节的数据块大小)。否则，您获得的 IOPS 性能将低于下表所示数值。

实例大小	读取 IOPS	首次写入 IOPS
i2.xlarge	35000	35000
i2.2xlarge	75000	75000
i2.4xlarge	175000	155000
i2.8xlarge	365000	315000

随着您不断在您的实例的基于 SSD 的实例存储中填充数据，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 I2 实例提供的基于 SSD 的实例存储卷不会为超额配置预留空间。要减少写入放大问题造成的影响，您应留出 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。这会减少您可使用的存储空间，但会提升性能。

I2 实例存储支持的卷支持 TRIM。如果不再需要已写入的数据，可以使用 TRIM 命令通知 SSD 控制器。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 \(p. 707\)](#)。

D2 实例

Abstract

使用 D2 实例可提供高计算性能和高级优化功能。

D2 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。D2 实例也适用于以下应用程序：

- 大规模并行处理 (MPP) 数据仓库
- MapReduce 和 Hadoop 分布式计算
- 日志或数据处理应用程序

内容

- [硬件规格 \(p. 121\)](#)
- [D2 实例功能 \(p. 121\)](#)
- [D2 实例要求 \(p. 121\)](#)

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](#)。

D2 实例功能

以下是 D2 实例的功能的摘要：

- D2 实例的主要数据存储是基于 HDD 的实例存储。与所有实例存储一样，这些卷只在实例生命周期内存在。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。
- 默认情况下，D2 实例为 EBS 优化实例，可为 Amazon EBS 提供从 750 Mbps 到 4000 Mbps 的专用数据块存储吞吐量，无需其他费用。通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 D2 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。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。
- 您可以启用增强联网功能。通过增强联网功能，您可以显著提高每秒数据包数 (PPS) 性能，降低网络抖动，并减少延迟。有关更多信息，请参阅 [Windows 上的增强联网 \(p. 630\)](#)。
- 您可以在置放群组中集中群集 D2 实例。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

D2 实例要求

以下是 D2 实例的要求：

- D2 实例需要 64 位 HVM AMI。它们具有大容量内存（RAM 最高可达 244 GiB），需要 64 位操作系统才能充分利用该容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- 在一个区域中可以启动的实例总数存在限制，某些 D2 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？](#)

如果您需要更多 D2 实例，可以使用 [Amazon EC2 实例请求表](#) 请求实例。

- 您的 d2.8xlarge 实例能够通过 2 MiB 的数据块大小实现 3.5 GB/s 的读性能和 3.1 GB/s 的写性能。

HI1 实例

Abstract

HI1 实例提供非常快速的 SSD 支持型实例存储，它经过优化，具有极高的随机 I/O 性能和较低的每 IOPS 成本。

HI1 实例 (hi1.4xlarge) 可以向应用程序提供每秒上万次低延迟随机 I/O 操作 (IOPS)。它们非常适合用于下列情况：

- NoSQL 数据库（例如，Cassandra 和 MongoDB）
- 群集化数据库
- 联机事务处理 (OLTP) 系统

您可以在置放群组中集中放置 HI1 实例。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

默认情况下，您最多可运行两个 hi1.4xlarge 实例。如果您需要两个以上 hi1.4xlarge 实例，请联系 <http://www.amazonaws.cn/support-plans/>。

内容

- [硬件规格 \(p. 122\)](#)
- [磁盘 I/O 性能 \(p. 122\)](#)
- [SSD 存储 \(p. 122\)](#)

硬件规格

hi1.4xlarge 实例类型是以固态硬盘 (SSD) 技术为基础的。

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](#)。

磁盘 I/O 性能

使用 Linux 半虚拟化 (PV) AMI 时，HI1 实例可以跨两个 SSD 数据卷向应用程序提供高于 120000 4 KB 的随机读取 IOPS，以及介于 10000 与 85000 之间的 4 KB 随机写入 IOPS（具体取决于活动逻辑数据块寻址范围）。使用硬件虚拟机 (HVM) AMI，性能大约是 90 000 4 KB 的随机读取 IOPS 和 9 000 到 75 000 4 KB 的随机写入 IOPS。

HI1 Windows 实例提供约 90 000 4 KB 的随机读取 IOPS，以及 9 000 到 75 000 4 KB 的随机写入 IOPS。

最大顺序吞吐量大约为每秒读取 2 GB，每秒写入 1.1 GB。

SSD 存储

在 HI1 实例上采用 SSD 存储：

- 原始数据源是采用 SSD 存储的实例存储。
- 读取性能始终如一，写入性能可能会有所波动。
- 可能会发生写入放大问题。
- 目前不支持 TRIM 命令。

采用 SSD 存储的实例存储

hi1.4xlarge 实例使用由 Amazon EBS 支持的根设备。但是，它们的原始数据存储由实例存储中的 SSD 卷提供。像其他实例存储卷一样，这些实例存储卷只在实例生命周期内存在。由于 hi1.4xlarge 实例的根设备由 Amazon EBS 支持，因此您仍然可以启动和停止实例。当您停止实例时，应用程序仍会存留，但是实例存储中的生产数据则不会保留。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。

可变动的写入性能

写入性能受应用程序利用逻辑块寻址 (LBA) 空间的方式的影响。如果您的应用程序使用总 LBA 空间，则写入性能可能会下降约 90%。测试您的应用程序并监控队列长度（卷的待处理 I/O 请求数量）和 I/O 大小。

写入放大

写入放大是指与闪存和 SSD 相关的不良情况，在这种情况下，实际写入的物理信息量是计划写入的符合逻辑的信息量的几倍。因为对闪存执行重新写入操作前，必须先执行擦除操作，而执行这些操作的过程会导致用户数据和元数据遭到多次移动（或覆盖）。放大影响会在 SSD 的使用期限内增加必须写入次数，而这会缩短稳定运行的时间。hi1.4xlarge 实例的设计自带调配模式，以用于最大程度上减少写入放大问题的影响。

比起顺序写入操作，随机写入在写入放大方面的影响更为严重。如果您担心写入放大问题，可为您的应用程序分配少于 1 TiB 的存储（也称为预留空间）。

TRIM 命令

TRIM 命令支持操作系统通知 SSD，之前保存的数据块被认为已废止。TRIM 限制写入放大的影响。

HI1 实例不提供 TRIM 支持。有关支持 TRIM 的实例的信息，请参阅 [实例存储卷 TRIM 支持 \(p. 707\)](#)。

HS1 实例

Abstract

HS1 实例具有很高的存储密度、较低的存储成本和较高的顺序 I/O 性能。

HS1 实例 (hs1.8xlarge) 为每个实例提供非常高的存储密度以及高连续读取和写入性能。它们非常适合用于下列情况：

- 数据仓库
- Hadoop/MapReduce
- 并行文件系统

您可以在置放群组中集中放置 HS1 实例。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

默认情况下，您最多可运行两个 HS1 实例。如果您需要两个以上的 HS1 实例，可以使用 [Amazon EC2 实例请求表](#) 申请更多实例。

内容

- [硬件规格 \(p. 124\)](#)
- [实例存储 \(p. 124\)](#)
- [磁盘初始化 \(p. 124\)](#)

硬件规格

HS1 实例同时支持由 Amazon Elastic Block Store (Amazon EBS) 支持的和由实例存储支持的Amazon 系统映像 (AMI)。HS1 实例同时支持半虚拟化 (PV) 和硬件虚拟机 (HVM) AMI。

HS1 实例提供高带宽联网，也可用于 provisioned IOPS (io1) 卷以提高一致性和性能。

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](#)。

实例存储

HS1 实例同时支持实例存储和 Amazon EBS 根设备卷。但是，即使在使用由 Amazon EBS 支持的实例时，主要数据存储也是由实例存储中的硬盘驱动器提供的。像其他实例存储卷一样，这些实例存储卷只在实例生命周期内存在。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。

磁盘初始化

如果计划在稳定状态下长时间运行 HS1 实例，我们建议您首先对硬盘清零以提高性能。此过程需要长达六小时的时间来完成。

T1 微型实例

Abstract

T1 微型实例是一种低成本选择，可提供少量的计算资源。

T1 微型实例 (`t1.micro`) 提供了少量一致性 CPU 资源，可在存在更多周期时在短时间内突增 CPU 容量。这种实例非常适合需要定期增加计算周期的低吞吐量应用程序和网站。



Note

`t1.micro` 是上一代实例，已被 `t2.micro` 取代，后者具有更好的性能配置。我们建议使用 `t2.micro` 实例类型而不是 `t1.micro`。有关更多信息，请参阅 [T2 实例 \(p. 113\)](#)。

`t1.micro` 实例只可作为 Amazon EBS 支持的实例使用。

本文档介绍了 `t1.micro` 实例的运行方式，以便您了解如何对其进行应用。我们的目的不在于指定确切的行为，而是让您了解实例的工作行为，从而了解其性能。

主题

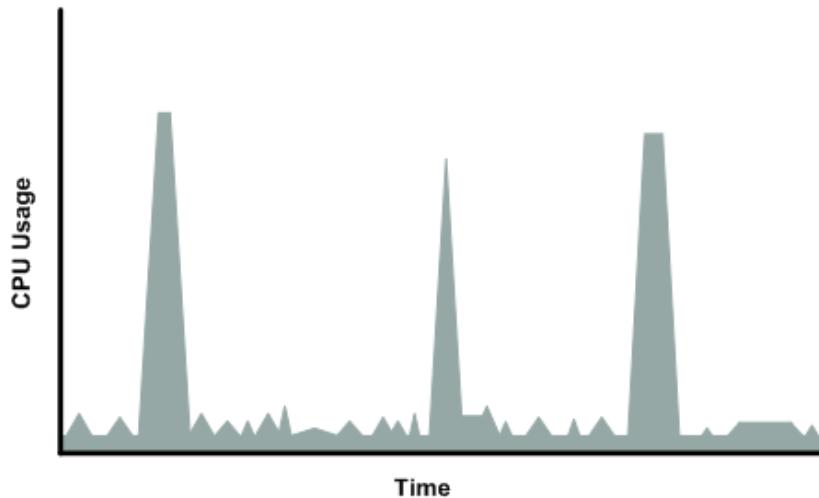
- [硬件规格 \(p. 124\)](#)
- [T1 微型实例的最佳应用程序 \(p. 125\)](#)
- [峰值期间的可用 CPU 资源 \(p. 126\)](#)
- [当实例用其分配到的资源时 \(p. 126\)](#)
- [与 m1.small 实例类型的比较 \(p. 128\)](#)
- [微型实例的 AMI 优化 \(p. 130\)](#)

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

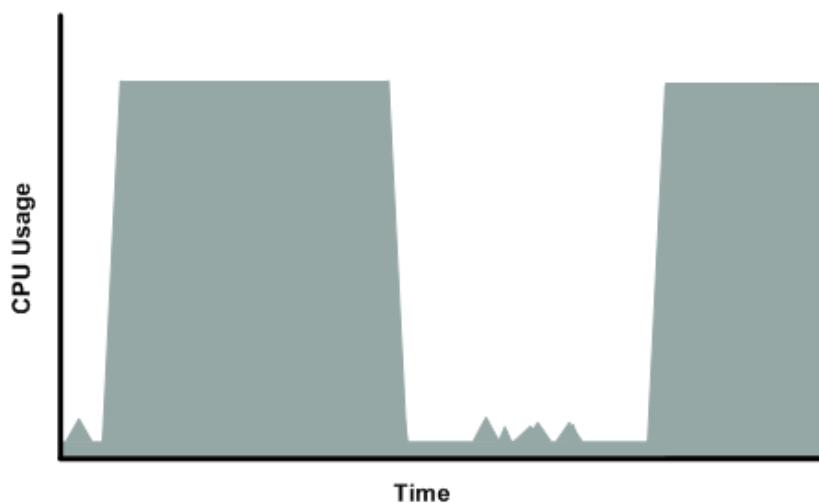
T1 微型实例的最佳应用程序

针对 CPU 占用状态与下图所示类似的工作负荷，t1.micro 实例可为其在短时间内突增 CPU 资源。

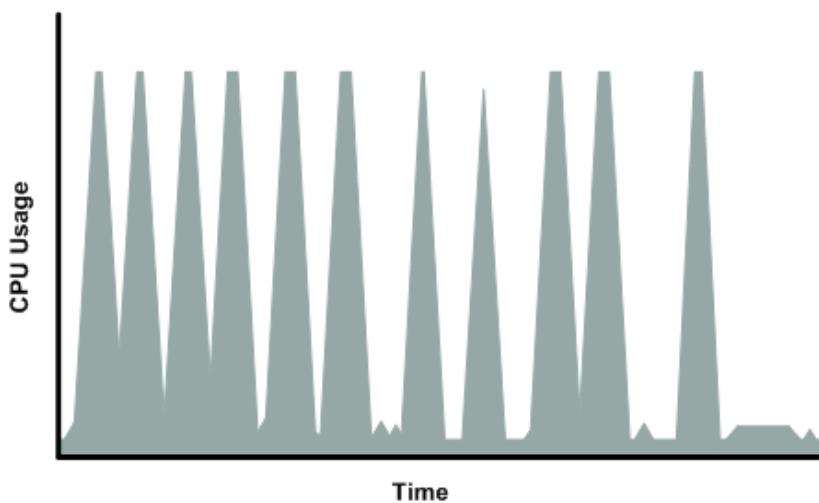


该实例设计为基本只在两个水平上用其 CPU 占用进行运行：普通的低背景水平和比背景水平高的简短峰值水平。我们允许实例在最高为 2 个 EC2 计算单位 (ECU) 的情况下运行（一个 ECU 提供相当于一个 1.0-1.2 GHz 2007 Opteron 或 2007 Xeon 处理器的 CPU 容量）。最大层面与背景层面之间的比率被设定为大值。我们对 t1.micro 实例的设计使其可以支持您的应用程序上每分钟产生的数十个请求。但是，根据您的应用程序上的每个请求所需 CPU 资源量的不同，实际性能也会大有不同。

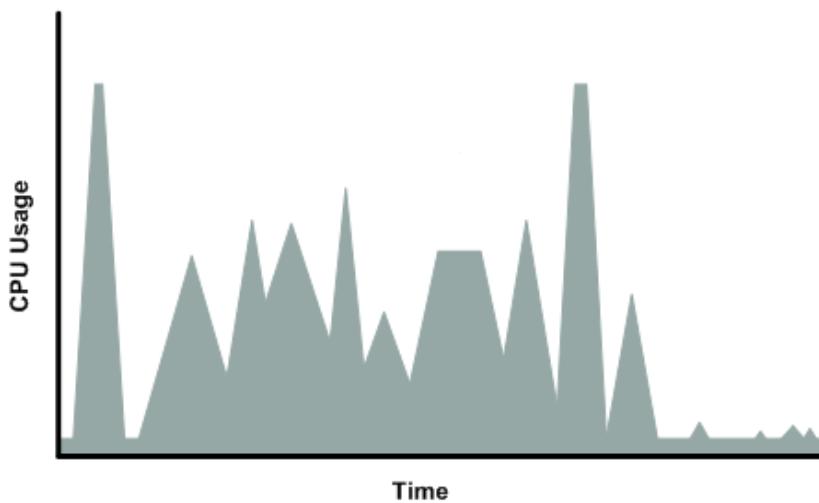
您的应用程序 CPU 占用状态可能会不同于前述章节中的描述。下图显示了一个不适合使用 t1.micro 实例的应用程序的 CPU 占用状态。该应用程序针对每个请求都需要连续的数据处理 CPU 资源，从而带来 t1.micro 实例无法处理的 CPU 占用停滞期。



下图显示了另一个不适合使用 t1.micro 实例的 CPU 占用情况。此处的 CPU 占用峰值简短，但它们的产生频率太高，以使微型实例不能处理。



下图显示了另一个不适合使用 `t1.micro` 实例的 CPU 占用情况。此图中峰值的产生频率不高，但峰值之间的背景水平太高，导致 `t1.micro` 实例不能处理。



在上述每一个不适合使用 `t1.micro` 实例的工作负载案例中，我们建议您考虑使用其他实例类型。有关实例类型的更多信息，请参阅 [实例类型 \(p. 110\)](#)。

峰值期间的可用 CPU 资源

当您的实例 *bursts* 按需调节峰值以计算资源时，该实例会使用主机上的未用资源。可用量的多少取决于峰值产生时争用量的多少。无论主机上的其他实例是否处于峰值状态，实例的可用 CPU 资源永远不会为零。

当实例用其分配到的资源时

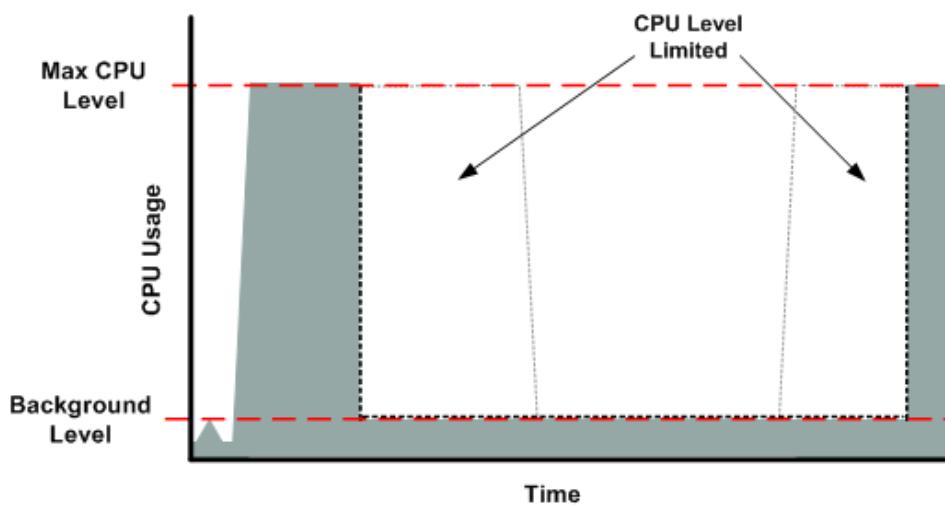
我们希望您的应用程序在一段时间内只消耗一定量的 CPU 资源。如果应用程序消耗的资源超过您的实例分配到的资源，则我们会暂时限制实例，以使其在较低的 CPU 水平下运行。如果您的实例继续使用其分

配到的所有资源，则其性能会下降。我们会增加对其 CPU 水平的限制时间，从而延长实例被允许再次进行突增前的等待时间。

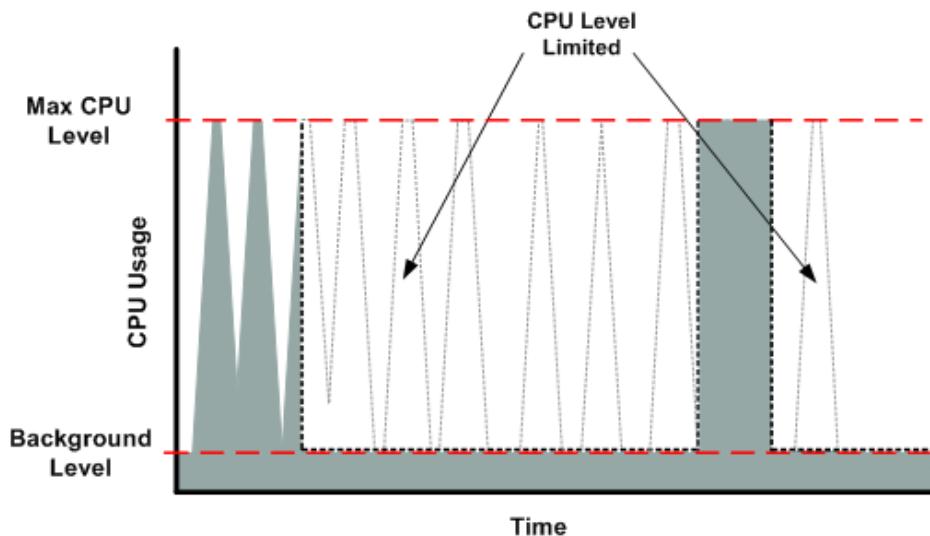
如果您针对您的 t1.micro 实例启用 CloudWatch 监控，则您可以使用 AWS 管理控制台中的“Avg CPU Utilization (CPU 平均利用率)”图表来判断您的实例是否在定期使用其分配到的所有 CPU 资源。我们建议您在每个给定的期间查看达到的最大值。如果最大值为 100%，我们建议您使用 Auto Scaling 来横向扩展（使用其他 t1.micro 实例和负载均衡器），或迁移到更大的实例类型。有关更多信息，请参阅 [Auto Scaling 用户指南](#)。

下图显示了前述章节中所述的三个非最优配置文件，以及它在实例消耗所分配到的资源且我们不得不限制实例 CPU 水平时可能出现的样子。如果实例消耗了其分配到的资源，我们会将其限制到低背景水平。

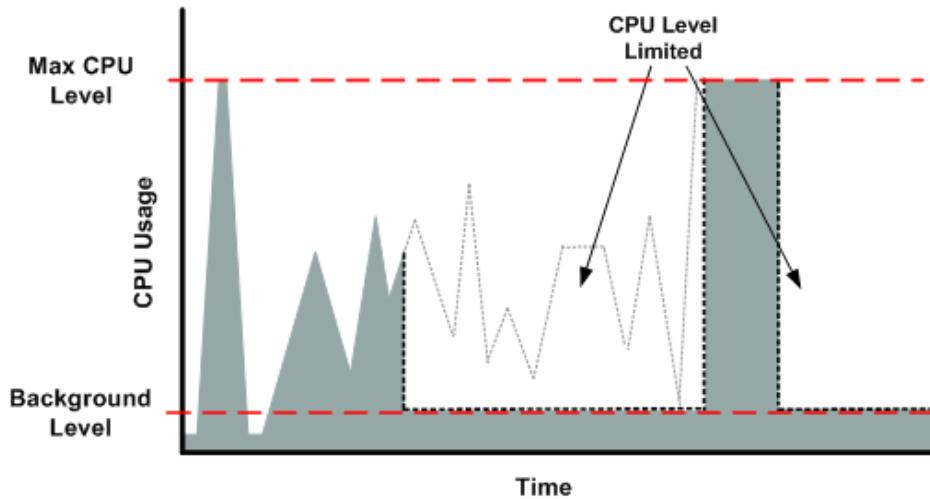
下图显示了数据处理 CPU 占用长时间停滞的状况。CPU 达到最大允许水平，且在实例所分配到的资源在此期间消耗完之前停留在此水平。此时，我们限制实例在低背景水平下运行，且在我们允许其在该水平之上再次进发之前都到在此水平运行。在分配到的资源被消耗完与我们再次对其进行限制之前，实例会再次停留在此水平（图形中未予显示）。



下图显示了请求太频繁的状况。实例在仅有几个请求后使用其分配到的资源，所以我们对其进行限制。我们取消限制后，实例的 CPU 占用达到了最高限制并试图紧跟请求，我们对其进行再次限制。

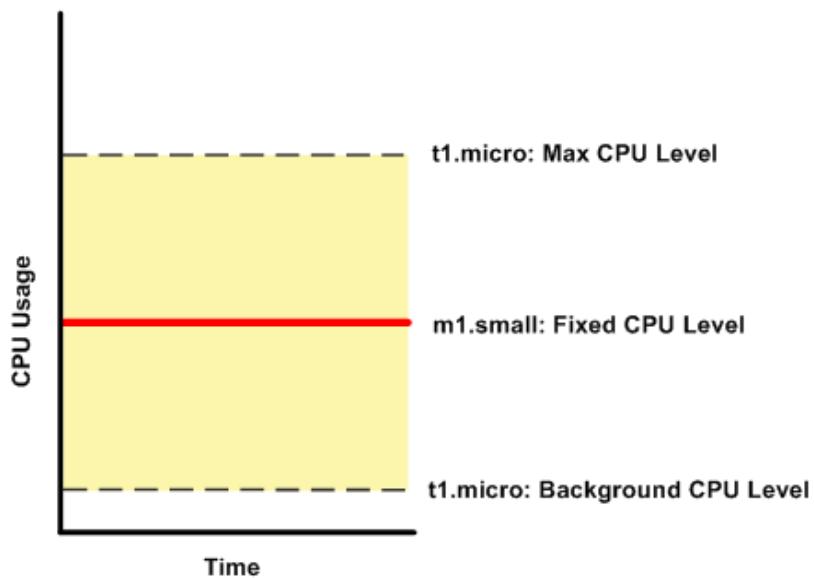


下图显示了背景水平太高的情况。请注意，实例不必在最大的 CPU 水平下运行，因为我们会对其进行限制。当实例在正常背景水平之上运行且在给定期间消耗完了分配给其的资源时，我们会对实例进行限制。在此情况下（与前述情况相同），实例无法跟进工作，所有我们会再次对其进行限制。



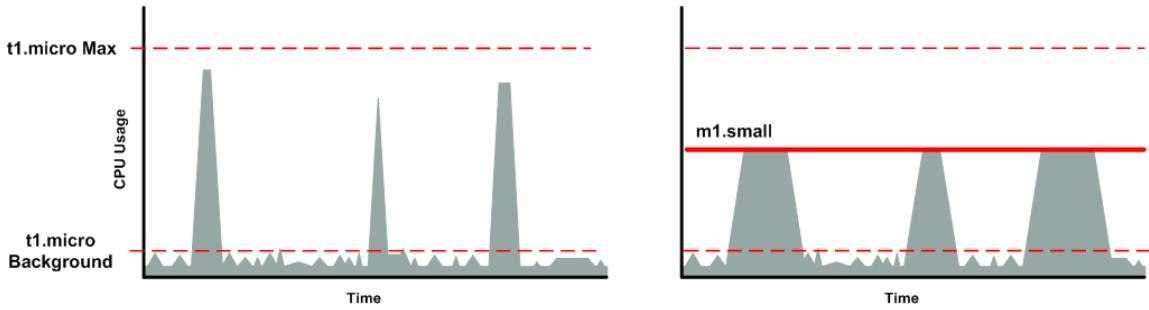
与 m1.small 实例类型的比较

t1.micro 实例在不同时间提供不同水平的 CPU 资源（最高为 2 个 ECU）。相比而言，m1.small 实例类型始终提供 1 个 ECU 的 CPU 资源。下图阐明了两者间的不同。

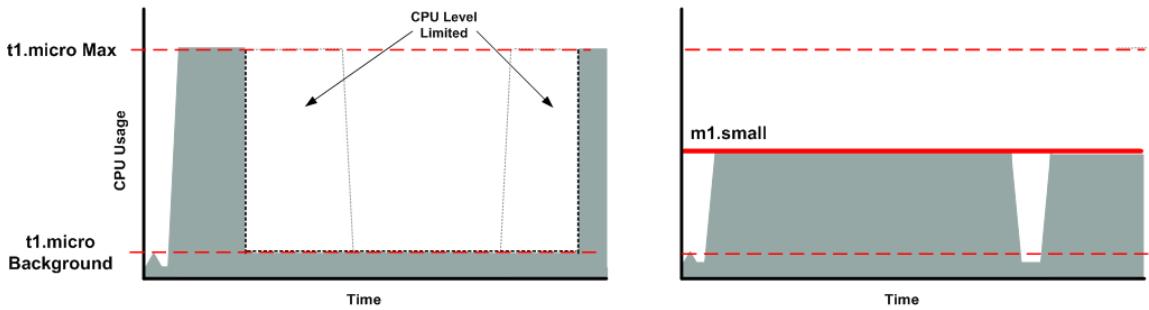


下列各图所示为前述章节所讨论的各种情况下，`t1.micro` 实例与 `m1.small` 实例的 CPU 占用情况对比。

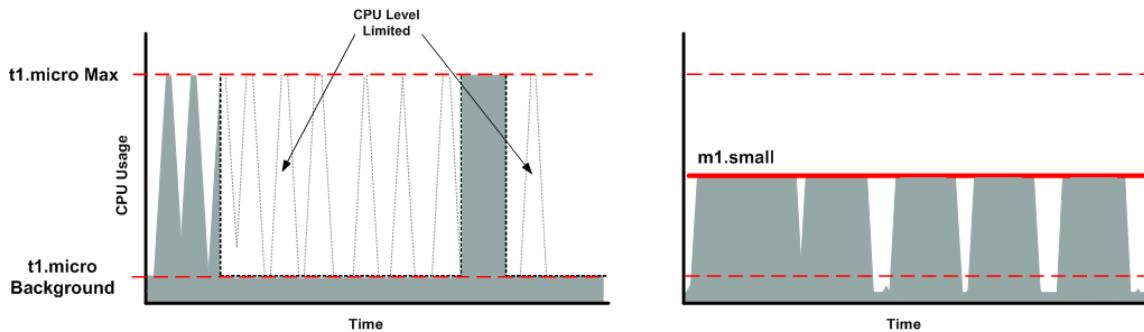
以下第一幅图显示了对 `t1.micro` 实例而言的最佳情况（左图），并且显示了 `m1.small` 实例的可能情况（右图）。在此情况下，我们不需要限制 `t1.micro` 实例。与 `m1.small` 实例相比，`t1.micro` 实例对每次 CPU 需求峰值的处理时间要更长。



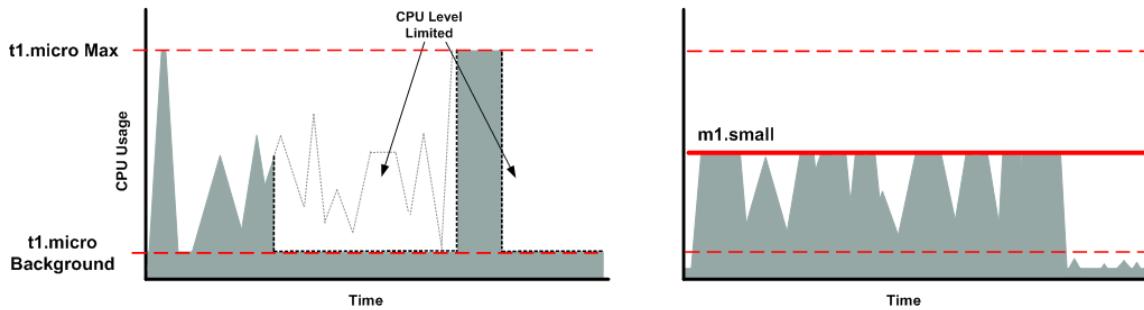
下一幅图所示为数据处理请求用尽了 `t1.micro` 实例所分配到的资源的情况，并且显示了使用 `m1.small` 实例时的可能情况。



下一幅图所示为频繁的请求用尽了 t1.micro 实例所分配到的资源的情况，并且显示了使用 m1.small 实例时的可能情况。



下一幅图所示为背景水平用尽了 t1.micro 实例分配到的资源的情况，并且显示了使用 m1.small 实例时的可能情况。



微型实例的 AMI 优化

在为 t1.micro 实例类型优化 AMI 时，我们建议您遵循以下最佳做法：

- 将 AMI 设计为在 600 MB 的 RAM 上运行
- 限制使用 CPU 时间的重复出现的进程（例如，Cron 作业、守护程序）的数量

当您进行重大的 AMI 或实例配置更改时（例如，启用服务器角色或安装大型应用程序），您可能会发现实例性能受到限制，因为这些更改可能需要使用大量内存且要求 CPU 资源长时间运行。我们建议您先使用较大的实例类型来对 AMI 进行这些更改，然后再在 t1.micro 实例上运行 AMI 以执行常规操作。

X1 实例

Abstract

使用 X1 实例实现大型内存工作负载的快速性能。

X1 实例旨在为处理内存中的大型数据集的工作负载交付快速性能。X1 实例也适用于以下应用程序：

- 内存数据库，如 SAP HANA，包含针对 Business Suite S/4HANA、Business Suite on HANA (SoH)、Business Warehouse on HANA (BW) 和 Data Mart Solutions on HANA 的 SAP 认证支持。有关更多信息，请参阅 [AWS 云上的 SAP HANA](#)。
- 大数据处理引擎（如 Apache Spark 或 Presto）。

- 高性能计算 (HPC) 应用程序。

硬件规格

有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 [Amazon EC2 实例](#)。

内存性能

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。

计算性能

X1 实例具备高达 128 的 vCPU 并且由 4 个 Intel Xeon E7-8880 v3 处理器（具备内存增强型带宽和更大的 L3 缓存）提供动力来提升内存应用程序的性能。X1 实例还通过最新的 Intel AES-NI 功能实现加密性能提高，支持 Intel Transactional Synchronization Extensions (TSX) 以提升内存事务性数据处理的性能以及支持高级矢量扩展 2 (Intel AVX2) 处理器指令以将大部分整数命令扩展为 256 位。

下表突出显示了 Intel Xeon E7-8880 v3 处理器的功能集。有关更多信息，请参阅 [Intel 和 Amazon Web Services](#)。

功能	规范
处理器编号	E7-8880 v3
末级缓存	45 MB
Intel QPI 速度	9.6 GT/s
QPI 链接数量	3
指令集	64 位
指令集扩展	AVX 2.0
平版印刷	22 nm
处理器基础频率	2.3 GHz
最大睿频	3.1 GHz
Intel 睿频加速技术	2.0
Intel 超线程技术	是
Intel TSX-NI	是
Intel 64	是
空闲状态	是
增强的 Intel SpeedStep 技术	是
热量监控技术	是
Intel AES 新指令	是

X1 实例功能

以下是 X1 实例功能的摘要：

- 默认情况下对 X1 实例进行了 EBS 优化，从而可利用 Amazon EBS 卷提供高达 10 Gbps 的专用存储带宽。通过 EBS 优化实例，您可以消除存储 I/O 与来自 X1 实例的其他网络流量之间的争用，从而持续获得高性能。有关更多信息，请参阅 [Amazon EBS 优化实例](#)。
- X1 实例支持基于 SSD 的实例存储。与所有实例存储一样，这些卷只在实例生命周期内存在。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储](#)。
- 您可以在置放群组中集中放置 X1 实例。置放群组可在单个可用区域内实现实例间的低延迟和高带宽连接。有关更多信息，请参阅 [置放群组](#)。
- x1.32xlarge 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 [EC2 实例的处理器状态控制](#)。
- X1 实例可用作按需实例、预留实例或计划的预留实例，但它们不能用作竞价型实例或专用实例。此外，它们在专用主机上也受支持。有关更多信息，请参阅 [实例购买选项](#)。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。默认情况下，最多可同时运行两个 X1 实例。如果您需要更多 X1 实例，可以使用 [Amazon EC2 实例请求表](#) 请求实例。

X1 实例要求

以下是 X1 实例的要求：

- x1.32xlarge 实例类型提供了 128 个虚拟 CPU，这在虚拟 CPU 数量限制低于 128 个的某些 Linux 操作系统中可能会造成启动问题。有关更多信息，请参阅 [支持 128 个 vCPU \(p. 133\)](#)。
- x1.32xlarge 的实例存储能够提供高达 126000 的随机读取 IOPS（数据块大小为 4KiB）。为确保 Linux 上的 X1 实例实现最佳磁盘 I/O 性能，建议使用 Amazon Linux AMI 的最新版本，或者内核版本为 3.8 或更高版本的其他 Linux AMI。如果使用支持持久授予（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，X1 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 项目博客上的通过持久授予提高数据块协议可扩展性](#)。
- X1 实例具有增强型内存（高达 1952 GiB 的 RAM），需要 64 位 HVM AMI 才能利用其容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。有关更多信息，请参阅 [Linux AMI 虚拟化类型](#)。
- 您必须在 Virtual Private Cloud (VPC) 中启动 X1 实例；EC2-Classic 平台不受支持。EC2-VPC 允许您将 AWS 资源启动到您已定义的虚拟网络中。您无法将 EC2-Classic 中的现有实例的实例类型更改为 X1 实例类型。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅 [支持的平台](#)。有关启动仅 VPC 支持的实例的更多信息，请参阅 [仅在 VPC 中可用的实例类型](#)。

高可用性和可靠性

X1 实例支持可检测和校准多位错误的单设备数据校准 (SDDC +1)。SDDC +1 利用错误检查和校准代码来识别和禁用失败的单一 DRAM 设备。

此外，您可以利用 [Amazon CloudFormation](#) 和 [Amazon EC2 Auto Recovery](#)，实施高可用性 (HA) 和灾难恢复 (DR) 解决方案来实现恢复点目标 (RPO)、恢复时间目标 (RTO) 和成本要求。有关实现 HA 和 DR 解决方案的更多信息，请参阅 [使用 AWS 实现灾难恢复白皮书](#)。

如果您运行 SAP HANA 生产环境，则还可以选择在 X1 实例上使用 HANA 系统复制 (HSR)。有关在 X1 实例上设计 HA 和 DR 解决方案的更多信息，请参阅 [Amazon Web 服务云上的 SAP HANA：快速入门参考部署](#)。

支持 128 个 vCPU

`x1.32xlarge` 实例类型提供了 128 个虚拟 CPU，这在虚拟 CPU 数量限制低于 128 个的某些 Linux 操作系统中可能会造成启动问题。强烈建议您在启动 `x1.32xlarge` 实例时，使用最新的 AMI。

以下 Linux AMI 支持启动具有 128 个虚拟 CPU 的 `x1.32xlarge` 实例：

- Amazon Linux AMI 2016.03 (HVM)
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 (HVM)

调整您的实例大小

Abstract

调整您的实例的大小，使之与其工作负载相匹配。

随着您的需求变化，您可能会发现您的实例过度使用（实例类型过小）或利用不足（实例类型过大）。如果出现这种情况，您可更改您的实例大小。例如，如果您的 `t2.micro` 实例对于其工作负载过小，您可将其更改为 `m3.medium` 实例。

如果实例的根设备是 EBS 卷，您可以通过更改其实例类型来更改实例的大小，这称为 调整大小。如果实例的根设备是实例存储卷，则必须将应用程序迁移到实例类型为您所需的新实例。有关根设备卷的更多信息，请参阅 [根设备存储 \(p. 63\)](#)。

在调整实例大小时，您必须选择与实例的配置兼容的实例类型。如果您所需的实例类型与您具有的实例配置不兼容，则必须将应用程序迁移到实例类型为您所需的新实例。



Important

在调整实例大小时，已调整大小的实例通常具有您在启动原始实例时指定的相同实例存储卷数。如果您要添加实例存储卷，则必须将应用程序迁移到实例类型和实例存储卷为您所需的全新实例。此规则的一个例外是：调整为存储密集型的实例类型时，默认包含更多数量的卷。有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。

内容

- [调整大小的实例的兼容性 \(p. 133\)](#)
- [调整 Amazon EBS 支持实例的大小 \(p. 134\)](#)
- [迁移实例存储支持的实例 \(p. 135\)](#)
- [迁移到新的实例配置 \(p. 135\)](#)

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：

- 网络。EC2-Classic 中不支持某些实例类型，这些类型必须在 VPC 中启动。因此，您不能将 EC2-Classic 中的实例的大小调整为仅在 VPC 中可用的实例类型的大小，除非您有非默认 VPC。有关更多信息，请参阅 [实例类型仅在 VPC 中可用 \(p. 576\)](#)。
- 平台。所有 Amazon EC2 实例类型都支持 64 位 AMI，但只有以下实例类型支持 32 位 AMI：`t2.nano`、`t2.micro`、`t2.small`、`t2.medium`、`c3.large`、`t1.micro`、`m1.small`、`m1.medium` 和 `c1.medium`。如果您要调整 32 位实例的大小，将限于这些实例类型。

例如，EC2-Classic 中不支持 T2 实例，这些实例仅限 HVM。因此，您不能将 T1 实例的大小调整为 T2 实例的大小，因为 T1 实例不支持 HVM 且必须从 PV AMI 启动。如果您要将 T2 实例的大小调整到更大的实例类型的大小，则可以选择任何当代实例类型（如 M3），因为所有当代实例类型都支持 HVM AMI。有关更多信息，请参阅 [可用实例类型 \(p. 111\)](#)。

调整 Amazon EBS 支持实例的大小

您必须先停止 Amazon EBS 支持实例，然后才能更改其实例类型。当您停止和启动实例时，需要注意以下事项：

- 我们将实例迁移到新硬件；但是，实例 ID 不会更改。
- 如果您的实例在 VPC 中运行并具有公有 IP 地址，则我们会释放该地址并向它提供新的公有 IP 地址。实例会保留其私有 IP 地址以及任何弹性 IP 地址。
- 如果实例在 EC2-Classic 中运行，则我们会为其提供新的公有和私有 IP 地址，并取消该实例与任何弹性 IP 地址的关联。因此，为确保您的用户可不间断地继续使用托管在您的实例上的应用程序，在重启实例后，您必须重新关联所有弹性 IP 地址。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。为防止出现此情况，您可以在调整实例大小时，为组暂停 Auto Scaling 流程。有关更多信息，请参阅 [Auto Scaling 用户指南](#) 中的 [暂停和恢复 Auto Scaling 流程](#)。

有关更多信息，请参阅 [停止和启动您的实例 \(p. 227\)](#)。

使用 AWS 管理控制台，通过以下过程调整 Amazon EBS 支持实例的大小。

调整 Amazon EBS 支持实例的大小

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. [EC2-Classic] 如果实例具有关联的弹性 IP 地址，则记录下详细信息窗格中显示的弹性 IP 地址和实例 ID。
4. 依次选择 Actions、Instance State 和 Stop。
5. 在确认对话框中，选择 Yes, Stop。停止实例可能需要几分钟时间。

[EC2-Classic] 当实例状态变为 stopped 时，详细信息窗格中的 Elastic IP (弹性 IP)、Public DNS (公有 DNS)、Private DNS (私有 DNS) 和 Private IPs (私有 IP) 字段为空，表明旧值不再与实例关联。

6. 在实例仍处于选中状态的情况下，依次选择 Actions、Instance Settings 和 Change Instance Type。请注意，如果实例状态不是 stopped，则禁用此操作。
7. 在 Change Instance Type 对话框中，执行以下操作：
 - a. 从 Instance Type 中，选择您所需的实例类型。如果列表中未显示您所需的实例类型，则说明它与您的实例配置不兼容（例如，由于虚拟化类型）。
 - b. （可选）如果您选择的实例类型支持 EBS 优化，则选择 EBS-optimized 以启用 EBS 优化或取消选择 EBS-optimized 以禁用 EBS 优化。请注意，如果您选择的实例类型默认情况下已经过 EBS 优化，则 EBS-optimized 已选中，您无法取消选择。
 - c. 选择 Apply 以接受新设置。

8. 要重启已停止的实例，请选择该实例，然后依次选择 Actions、Instance State 和 Start。
9. 在确认对话框中，选择 Yes, Start。实例进入 running 状态可能需要几分钟时间。
10. [EC2-Classic] 当实例状态为 running 时，详细信息窗格中的 Public DNS (公有 DNS)、Private DNS (私有 DNS) 和 Private IPs (私有 IP) 字段包含我们分配给实例的新值。如果您的实例具有关联的弹性 IP 地址，则必须按以下方式对其进行重新关联：
 - a. 在导航窗格中，选择 Elastic IPs。

- b. 选择您在停止实例前所记下的弹性 IP 地址。
- c. 依次选择 Actions 和 Associate Address。
- d. 从 Instance 中，选择您在停止实例前所记下的实例 ID，然后选择 Associate。

迁移实例存储支持的实例

如果您要将应用程序从一个实例存储支持的实例移至另一个不同实例类型的实例存储支持的实例，则必须通过从您的实例创建映像来迁移它，然后从此映像启动实例类型为您所需的新实例。要确保您的用户可不间断地继续使用托管在您的实例上的应用程序，您必须使用已与您的原始实例关联的任何弹性 IP 地址，并将其与新实例关联。之后您可以终止原始实例。

迁移实例存储支持的实例

1. [EC2-Classic] 如果您迁移的实例具有关联的弹性 IP 地址，请立即记录该弹性 IP 地址，以便之后可将其与新实例关联。
2. 备份实例存储卷上所有您需要保留在持久性存储中的数据。要迁移 EBS 卷上您需要保留的数据，请拍摄这些卷的快照（请参阅 [创建 Amazon EBS 快照 \(p. 677\)](#)）或从实例中分离卷，以便您之后可以将其连接到新的实例（请参阅 [从实例断开 Amazon EBS 卷 \(p. 670\)](#)）。
3. 通过满足先决条件并按照 [创建实例存储支持的 Windows AMI \(p. 78\)](#) 中的过程操作，从实例存储支持的实例创建 AMI。当您通过您的实例创建完 AMI 后，请返回到此过程。
4. 打开 Amazon EC2 控制台，在导航窗格中选择 AMIs。从筛选条件列表中，选择 Owned by me，然后选择您在上一步中创建的映像。请注意，AMI Name (AMI 名称) 是您在注册映像时指定的名称，而 Source (源) 是您的 Amazon S3 存储桶。



Note

如果您没有看到在上一步中创建的 AMI，请确保您已选择在其中创建了 AMI 的区域。

5. 选择 Launch。在您为实例指定选项时，务必选择您所需的新实例类型。如果无法选择您所需的实例类型，则说明它与您创建的 AMI 的配置不兼容（例如，由于虚拟化类型）。您还可以指定从原始实例中分离的任何 EBS 卷。

请注意，实例进入 running 状态可能需要几分钟时间。

6. [EC2-Classic] 如果您启动的实例具有关联的弹性 IP 地址，则必须将该地址与新实例关联，如下所示：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择您在此过程开始时记录的弹性 IP 地址。
 - c. 依次选择 Actions 和 Associate Address。
 - d. 从 Instance 中，选择新实例，然后选择 Associate。
7. （可选）如果不再需要用以创建映像的原有实例，则您可将其终止。选择实例并确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间）。依次选择 Actions、Instance State 和 Terminate。

迁移到新的实例配置

如果您的实例的当前配置与您所需的新实例类型不兼容，则不能将该实例的大小调整为新实例类型的小。您可以将应用程序迁移到其配置与您所需的新实例类型兼容的新实例。

如果您要将从 PV AMI 启动的实例变为仅限 HVM 的实例类型，一般过程如下：

1. 备份实例存储卷上所有您需要保留在持久性存储中的数据。要迁移 EBS 卷上您需要保留的数据，请创建这些卷的快照（请参阅 [创建 Amazon EBS 快照 \(p. 677\)](#)）或从实例中分离卷，以便您之后可以将其挂载到新实例（请参阅 [从实例断开 Amazon EBS 卷 \(p. 670\)](#)）。
2. 启动新实例，选择下列内容：
 - HVM AMI。
 - 仅限 HVM 的实例类型。
 - [EC2-VPC] 如果您正在使用弹性 IP 地址，请选择原始实例当前正在其中运行的 VPC。
 - 您从原始实例中分离并且要挂载到新实例的任何 EBS 卷，或者基于您创建的快照的新的 EBS 卷。
 - 如果您要允许相同的流量到达新实例，请选择与原始实例关联的安全组。
3. 在实例上安装应用程序和所有必需软件。
4. 还原您在原始实例的实例存储卷中备份的所有数据。
5. 如果您正在使用弹性 IP 地址，请按如下所示将其分配给新启动的实例：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择与原始实例关联的弹性 IP 地址，然后依次选择 Actions 和 Disassociate Address。当系统提示进行确认时，选择 Yes, Disassociate。
 - c. 在弹性 IP 地址仍处于选中状态的情况下，依次选择 Actions 和 Associate Address。
 - d. 从 Instance 中，选择新实例，然后选择 Associate。
6. （可选）如果不再需要原始实例，您可以将其终止。选择实例并确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间）。依次选择 Actions、Instance State 和 Terminate。

有关将应用程序从 EC2-Classic 中的实例迁移到 VPC 中的实例的信息，请参阅 [从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例 \(p. 588\)](#)。

实例购买选项

Abstract

Amazon EC2 提供了帮助您优化成本的各种购买选项。

Amazon EC2 提供了以下让您根据需求优化成本的购买选项：

- 按需实例 - 按小时为您启动的实例付费。
- 预留实例 - 以大幅折扣购买一年期到三年期的始终可用的实例。
- 计划实例 - 以一年为期限购买按指定重复计划始终可用的实例。
- 竞价型实例 - 对未使用的实例竞价，只要这些实例可用且您的出价高于现货价格，就可以以大幅折扣运行这些实例。
- 专用主机 - 为完全专用于运行您的实例的物理主机付费，通过您现有的按套接字、按内核或按 VM 的软件许可证来降低成本。
- 专用实例 - 按小时付费的在单一租户硬件上运行的实例。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [专用实例](#)。

如果您需要容量预留，请考虑预留实例或计划实例。如果您能灵活控制应用程序的运行时间并且应用程序可以中断，那么竞价型实例将是您的经济实惠之选。使用专用主机，既能在满足合规要求上助您一臂之力，又能通过使用现有服务器端绑定软件许可来节省费用。有关更多信息，请参阅 [Amazon EC2 实例购买选项](#)。

内容

- [实例生命周期 \(p. 137\)](#)
- [预留实例 \(p. 138\)](#)
- [计划的预留实例 \(p. 157\)](#)
- [竞价型实例 \(p. 160\)](#)
- [专用主机 \(p. 201\)](#)

实例生命周期

实例的生命周期在运行时开始，在停止时结束。您所选择的购买选项会影响实例的生命周期。例如，按需实例，当您启动并结束，在您终止实例。只要竞价型实例的容量可用，并且您的出价高于现货价格，便可运行。在计划的时间周期内，您可以启动计划内的实例；Amazon EC2 会启动实例并在时间周期结束的前三分钟终止它们。

使用以下程序来确定实例的生命周期。

使用控制台确定实例的生命周期

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 在描述选项卡上，查找租期。如果值为host，表示实例正在专用主机上运行。如果值为dedicated，表示是实例专用实例。
5. 在 Description 选项卡上，查找 生命周期。如果值为spot，表示实例是竞价型实例。如果值为scheduled，表示实例是计划内的实例。如果值为normal，此实例或者是按需实例，或者是预留实例。
6. (可选)，如果您购买了预留实例并要验证它是应用，您就可以检查Amazon EC2的使用报告。有关更多信息，请参阅 [预留实例使用率报告 \(p. 753\)](#)。

使用AWS CLI来确定实例的生命周期。

使用以下[描述实例](#)口令：

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

如果实例在专用主机上运行，那么输出内容包含以下信息：

```
"Tenancy": "host"
```

如果实例为专用实例，那么输出内容包含以下信息：

```
"Tenancy": "dedicated"
```

如果实例为竞价型实例，那么输出内容包含以下信息：

```
"InstanceLifecycle": "spot"
```

如果实例为计划内的实例，那么输出内容包含以下信息：

```
"InstanceLifecycle": "scheduled"
```

否则，输出内容包含以下信息：

```
"InstanceLifecycle": "normal"
```

预留实例

Abstract

通过预留实例可为 EC2 实例预留容量并降低平均实例使用成本。

预留实例是应用于实例的账单折扣和容量预留，可降低每小时运行成本。预留实例不是物理实例。打折使用价格在您拥有预留实例期间是固定的，使您可以预测预留期内的计算成本。与拥有您自己的硬件或仅运行按需实例相比，预留实例的长期大量使用能够实现大幅的节约。有关更多信息，请参阅 [选择预留实例付款选项 \(p. 140\)](#)。

当您购买预留实例时，预留会自动应用到与您指定的参数匹配的运行实例。或者，您也可以启动与所购预订容量配置相同的按需 EC2 实例。无预付和部分预付的预留实例将根据使用情况按小时计费，无论这些实例是否正在被使用。全部预付的预留实例无额外的按小时计算的费用。

预留实例不会自动更新；您可以继续使用 EC2 实例而不会中断，但要支付按需费率。新的预留实例可以具有与过期实例相同的参数，或者，您也可以购买具有不同参数的预留实例。

您可以使用 Auto Scaling 或其他 AWS 服务来启动使用预留实例优惠的按需实例。有关启动按需实例的信息，请参阅 [启动实例](#)。有关使用 Auto Scaling 启动实例的信息，请参阅 [Auto Scaling 用户指南](#)。

有关产品定价信息，请参阅以下页面：

- [AWS 服务定价概述](#)
- [Amazon EC2 按需实例定价](#)
- [Amazon EC2 预留实例定价](#)
- 有关预留实例定价套餐的信息，请参阅 [了解预留实例折扣定价套餐 \(p. 142\)](#)。



Note

低、中、高使用率预留实例无法再购买。有关预留实例定价模型变更对这些选项所产生的影响的更多信息，请参阅 [预留实例常见问题](#)。

主题

- [预留实例如何运行 \(p. 139\)](#)
- [账单优惠和付款选项 \(p. 140\)](#)
- [购买预留实例 \(p. 144\)](#)
- [在预留实例市场中出售实例 \(p. 147\)](#)
- [修改您的预留实例 \(p. 152\)](#)
- [修改请求故障排除 \(p. 157\)](#)

预留实例如何运行

Abstract

查看预留实例和预留实例市场的使用要求与限制核查表。

Amazon EC2 预留实例和预留实例市场可为您的业务运行提供强大且节省成本的战略。但是，在您使用预留实例或预留实例市场之前，请确保满足购买和出售的要求。您还必须了解预留实例和预留实例市场中某些元素的详细信息和限制 - 包括卖家注册、银行、使用 AWS 免费套餐、处理取消的实例等。使用本主题作为购买和出售预留实例以及在预留实例市场中购买和出售的核对清单。



Note

要购买并修改预留实例，请确保您的 IAM 用户账户具有适当的权限，例如描述可用区的能力。有关信息，请参阅[使用 AWS CLI 或 AWS SDK 的策略示例](#)和[用于 Amazon EC2 控制台的策略示例](#)。

入门

- AWS 账户 - 您需要拥有 AWS 账户才能购买预留实例。如果您没有 AWS 账户，请阅读[Amazon EC2 的设置 \(p. 13\)](#)中所述的说明（其中包含注册 Amazon EC2 账户和凭证的相关信息）并完成相应操作。
- AWS 免费套餐 - AWS 免费使用套餐可供新 AWS 账户使用。如果您正在用 AWS 免费使用套餐运行 Amazon EC2 实例，然后您购买了一个预留实例，那么您将按照标准定价指南付费。有关免费套餐、适用服务及使用量的信息，请参阅[AWS 免费套餐](#)。

购买预留实例

- 使用费 - 使用预留实例时，无论您是否使用，您都需为整个期限付费。
- 购买时的套餐折扣 - 预留实例定价套餐折扣仅适用于通过 AWS 进行的购买。这些折扣不适用于第三方预留实例购买。有关信息，请参阅[了解预留实例折扣定价套餐 \(p. 142\)](#)。
- 取消购买 - 在您确认购买前，请检查您计划购买的预留实例的详细信息，并确保所有参数都是准确的。在您购买预留实例（无论是从预留实例市场中的第三方卖家购买还是从 AWS 购买）之后，将无法取消您的购买。但是，如果您需要更改，则可出售预留实例。有关信息，请参阅[列示您的预留实例 \(p. 149\)](#)。

预留实例出售与预留实例市场

- 卖方要求 - 要成为 预留实例市场 中的卖方，必须注册为卖方。有关信息，请参阅[列示您的预留实例 \(p. 149\)](#)。
- 银行要求 - 为了在您出售预留实例时支付收取的资金，AWS 必须获得您的银行信息。您指定的银行必须有一个美国地址。有关更多信息，请参阅[银行账户 \(p. 148\)](#)。
- 税务要求 - 出于税务原因，交易次数达到 50 次或以上的卖方或是计划出售价值 20 000 USD 或以上预留实例的卖方必须提供关于他们业务的额外信息。有关信息，请参阅[税务信息 \(p. 149\)](#)。
- 最低售价 - 预留实例市场中允许的最低价格为 \$0.00。
- 何时可以出售预留实例 - 只有在 AWS 收到预付款款且预留实例已激活（您已拥有）达到 30 天之后，预留实例才能出售。此外，您列出的预留实例的剩余期限必须至少为一个月。
- 修改您的列示 - 无法直接修改您在预留实例市场中的列示。然而，您可通过先取消它然后再用新参数创建另一个列示来更改您的列示。有关信息，请参阅[给您的预留实例定价 \(p. 152\)](#)。您也可在列出您的预留实例之前更改它们。有关信息，请参阅[修改您的预留实例 \(p. 152\)](#)。
- 出售折扣预留实例 - 通过某个套餐折扣以较低成本购买的 Amazon EC2 预留实例不能在预留实例市场中出售。有关更多信息，请参阅[预留实例市场 \(p. 140\)](#)。
- 服务费 - AWS 会向您收取您在预留实例市场中出售的每个预留实例的总预付价格 12% 的服务费。（预付价格是卖方对预留实例收取的费用。）

- 其他 AWS 预留实例 - 只有 Amazon EC2 预留实例可在预留实例市场中出售。其他 AWS 预留实例（如 Amazon Relational Database Service (Amazon RDS) 和 Amazon ElastiCache 预留实例）不能在预留实例市场中出售。

在 Amazon VPC 中使用预留实例

您可以将实例启动进入Amazon Virtual Private Cloud (Amazon VPC) 并从您的预留实例中获益。有关更多信息，请参阅[Amazon VPC 是什么？](#)（在 *Amazon VPC 用户指南* 中）。

如果您有 EC2 经典账户，则可购买预留实例，通过选择名称内含有 *Amazon VPC* 的平台将其应用于启动进入非默认 VPC 的实例。有关更多信息，请参阅[检测支持的平台以及是否具有默认 VPC](#)。

如果您的账户仅限于 EC2-VPC，由于所有平台都有默认子网，因此可用平台列表的名称中不包含 *Amazon VPC*。如果您启动与预留的容量具有相同配置的实例，则会在您的默认或非默认的 VPC 中启动该实例，并且容量预留和账单优惠也会自动应用于该实例。有关默认 VPC 的信息，请参阅 *Amazon VPC 用户指南* 中的[您的默认 VPC 和子网](#)。

您还可以通过将专用指定为实例租赁，选择购买在主机硬件级别被物理隔离的预留实例。有关专用实例的更多信息，请参阅[专用实例](#)在 *Amazon VPC 用户指南*。

预留实例市场



Note

仅 Amazon EC2 预留实例可在预留实例市场出售。其他类型实例，如 Amazon RDS 和 Amazon ElastiCache 预留实例，不能在预留实例市场上出售。

预留实例市场是一个支持销售第三方和 AWS 客户的未使用的预留实例的平台，这些实例的期限时间和定价选项各不相同。例如，某位 AWS 客户可能希望在将实例迁移到新的 AWS 区域、更换为新的实例类型或结束项目之后，出售实例到期之前的容量。预留实例市场允许您满足您的特定业务需求并搜索与您理想的实例类型、区域及持续时间组合最相匹配的预留实例，从而提供更多的选择和灵活性。Amazon EC2 实例（通过预留实例市场购买）与从 AWS 上直接购买的预留实例具有相同的容量预留。

账单优惠和付款选项

Abstract

了解预留实例账单优惠和付款选项。

预留实例的账单优惠将自动应用于匹配的正在运行的实例。您也可购买预留实例，然后启动具有匹配规范的按需实例 - 定价优惠将自动应用于这些实例。容量预留确保了您将始终能够启动具有这些规范的实例。您也可以在 预留实例市场 中出售未使用的预留实例，只要您满足特定要求即可。

选择预留实例付款选项

Abstract

选择合适的预留实例付款选项。

预留实例有三种付款选项：

- 无预付 - 无论是否使用，您都将按照期限内的小时数，采用打折小时费率进行付费，无需任何预付款。此选项仅用作一年期预留。



Note

在整个预留期限内，“无预付”预留实例需要根据合同义务每月支付费用。因此，在某个账户能够购买“无预付”预留实例前，该账户需要具有成功的账单历史记录。

- 部分预付 - 必须预付部分费用，期限内剩余的小时数无论是否使用，都将按照打折小时费率计费。
- 全部预付 - 所有款项于期限开始时支付，无论使用了多少小时数，剩余期限不会再产生其他任何费用。

了解按小时计费

在您选择的预留实例期限内，无论实例是否正在运行，预留实例均按小时进行计费。请务必了解实例状态之间的差异以及这些差异对计费小时数的影响。有关更多信息，请参阅 [实例生命周期 \(p. 213\)](#)。

预留实例的计费优惠仅适用于每小时内的一一个实例小时。实例小时从实例启动之时开始计时，持续 60 分钟或持续到实例停止或终止时，以时间较早者为准。将从午夜至次日午夜的标准 24 小时均分为 24 个小时，其中一个小时前定义为一个实例小时（例如，1:00: 00 到 1:59:59 为一小时）。

当实例持续运行 60 分钟时，或者实例停止又重新启动时，一个新的实例小时则开始计时。重启实例将不会重置运行实例小时。

例如，如果实例在一个小时内停止后重新启动，并持续运行了两个多小时，则第一个实例小时（重启前）按折扣后的预留实例费率收费。下一个实例小时（重启后）以按需费率收费，下两个实例小时按折扣后的预留实例费率收费。

[预留实例使用率报告 \(p. 753\)](#) 部分包括示例报告，说明了针对正在运行的按需实例的节省费用。[预留实例常见问题](#)包括示例标价计算。

如何将预留实例应用于正在运行的实例

要将预留加入正在运行的实例，您可以修改现有预留实例，或者通过选择可用区（如 us-east-1b）、实例类型（如 m3.large）、平台（如 Amazon Linux VPC）和租赁（如默认）购买预留实例，以便与正在运行的实例的配置相匹配。

以下为客户已购买以下按需实例的示例方案：

- 可用区 us-east-1a 中的 4 个 m1.small 实例
- 可用区 us-east-1b 中的 4 个 c1.medium 实例
- 可用区 us-east-1b 中的 2 个 c1.xlarge 实例

然后，客户购买以下预留：

- 可用区 us-east-1a 中的 2 个 m1.small
- 可用区 us-east-1a 中的 3 个 c1.medium
- 可用区 us-east-1b 中的 1 个 c1.xlarge

采用以下方式应用定价优惠：

- 适用于两个 m1.small 预留的折扣将应用于可用区 us-east-1a 中四个正在运行的 m1.small 实例中的两个。

可用区 us-east-1a 中的另外两个实例将继续按照当前的按需费率收费。

- 三个 c1.medium 预留与正在运行的 c1.medium 实例的可用区不匹配。四个正在运行的 c1.medium 实例将继续按照当前的按需费率收费。

如果客户在可用区 us-east-1a 中启动 c1.medium 实例，则打折使用费率将应用于该实例。

- 将适用于一个 c1.xlarge 预留的折扣使用费率应用于可用区 us-east-1b 中的两个正在运行的 c1.xlarge 实例中的一个。

可用区 us-east-1b 中的另一个 c1.xlarge 实例将继续按照当前的按需费率收费。

在本示例中，立即将小时使用费折扣应用于已在运行的两个 m1.small 和一个 c1.xlarge 按需实例的小时费用；同时确保客户拥有在需要剩余的四个实例时运行这些实例的容量。

了解预留实例折扣定价套餐

Abstract

了解 Amazon EC2 预留实例的定价套餐折扣。

如果您的账户有资格获得折扣定价套餐，那么自您取得该资格时起，您在该套餐等级内购买的所有预留实例的预付费和每小时使用费均自动享受折扣。要取得折扣资格，您在该区域内的预留实例的标价必须达到 500000 美元或更高。

主题

- [计算预留实例定价折扣 \(p. 142\)](#)
- [定价套餐的整合账单 \(p. 142\)](#)
- [以折扣套餐价格购买 \(p. 143\)](#)
- [当前定价套餐限制 \(p. 143\)](#)
- [跨越定价套餐 \(p. 143\)](#)

计算预留实例定价折扣

通过计算您在区域中的所有预留实例的标价，可以确定您的账户所适用的定价套餐。将每个预留实例的每小时费用乘以每个期限的剩余小时数，加上购买时 [AWS 营销网站](#) 所列的未打折预付价格（称为固定价格）。由于标价基于未打折（公开）定价，您是否有资格获得总量折扣或者您购买预留实例后是否降价均不影响标价。

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

使用 AWS 管理控制台查看预留实例的固定价格

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 通过选择右上角的 Show/Hide，打开 Fixed Price 列的显示。

使用命令行查看预留实例的固定价格

- 使用 AWS CLI，请参阅 [describe-reserved-instances](#)
- 使用适用于 Windows PowerShell 的 AWS 工具，请参阅 [Get-EC2ReservedInstance](#)
- 使用 Amazon EC2 API，请参阅 [DescribeReservedInstances](#)

定价套餐的整合账单

整合账单账户汇总了某个区域内所有成员账户的标价。当整合账单账户的所有活动预留实例的标价达到折扣定价套餐时，整合账单账户的任何账户成员在此后购买任何预留实例都将享受折扣费率（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 \(p. 143\)](#)。

以折扣套餐价格购买

当您购买预留实例时，Amazon EC2 会自动将所有折扣应用于购买中处于折扣定价套餐范围内的部分。您无需执行任何其他操作，而且可以使用任何 Amazon EC2 工具进行购买。有关更多信息，请参阅 [在预留实例市场中购买 \(p. 146\)](#)。



Note

预留实例购买是确定您的折扣定价套餐的唯一购买行为，这些折扣也仅适用于购买 Amazon EC2 预留实例。

您在某区域的活动预留实例的标价达到某一折扣定价套餐范围后，未来在该区域中购买任何预留实例都将按打折费率收费。如果在某区域的预留实例单项购买额超过了折扣套餐阈值，那么此项购买超出价格阈值的部分将按打折费率收费。有关在购买过程中创建的临时预留实例 ID 的更多信息，请参阅 [跨越定价套餐 \(p. 143\)](#)。

如果您的标价降至低于折扣定价套餐价格点（例如，如果部分预留实例到期），之后在该区域购买预留实例将不享受折扣。但是，原来在折扣定价套餐范围内购买的所有预留实例都将继续享受折扣。

当您购买预留实例时，可能出现以下四种情况之一：

- 没有折扣 - 您在某区域内的购买仍然低于折扣阈值。
- 部分折扣 - 您在某区域内的购买跨越了第一折扣套餐的阈值。没有折扣将应用于一个或多个预留，而折扣费率将应用于剩余的预留。
- 全部折扣 - 您在某区域内的购买全部在一个折扣套餐之内并且获得了相应的折扣。
- 两种折扣率 - 您在某区域内的购买从较低折扣套餐跨入较高的折扣套餐。您将按两种费率付费：一个或多个预留采用较低的折扣费率，剩余的预留采用较高的折扣费率。

当前定价套餐限制

以下限制当前适用于预留实例定价套餐：

- 预留实例定价套餐和相关折扣仅适用于购买Amazon EC2预留实例。
- 预留实例定价套餐不适用于带有 SQL Server Standard 的 Windows 或带有 SQL Server Web 的 Windows 的预留实例。
- 作为套餐折扣的一部分购买的 预留实例无法在预留实例市场上出售。有关更多信息，请参阅 [预留实例市场 \(p. 140\)](#) 页面。

跨越定价套餐

如果您的购买跨入某个折扣定价套餐范围，您将看到该项购买有多个条目：一个条目显示购买中将按常规价格收费的部分，另一个条目显示购买中将按适用的打折费率收费的部分。

预留实例服务会生成多个预留实例 ID，因为您的购买从未打折套餐跨入到打折套餐，或从一个打折套餐跨入到另一个打折套餐。套餐中的每组预留都有一个 ID。因此，由您的购买 CLI 命令或 API 操作返回的 ID 将不同于新预留实例的实际 ID。

预留实例和整合账单

Abstract

当购买账户属于一个整合账单付款人账户的一部分时，共享预留实例的定价优惠。

当购买账户属于在一个整合账单付款人账户之下开具账单的一套账户的一部分时，预留实例的定价优惠可以共享。将所有子账户的小时使用量每月聚合到付款人账户。这通常对具有不同职能团队或团体的公司很

有用；然后，将应用正常的预留实例逻辑来计算账单。有关更多信息，请参阅 [AWS Billing and Cost Management 用户指南](#) 中的整合账单。

有关预留实例定价套餐的折扣如何应用于整合账单账户的更多信息，请参阅 [Amazon EC2 预留实例](#)。

阅读您的声明（发票）

Abstract

通过在 AWS 管理控制台中查看您的报表，查明您的账户的支出和费用状况。

您可通过查看 AWS 管理控制台中的 Billing & Cost Management 页面来查明您的账户的支出和费用状况。选择账户名旁的箭头可访问它。

- Dashboard 页面将显示您的账户的所有支出 - 例如预付费用、一次性费用及周期性费用。您可获得关于您的开支的汇总或详细清单。
- 您在预留实例市场中购买第三方预留实例而产生的预付费用将在 AWS Marketplace Charges 部分中列出，并在旁边显示卖方名称。这些预留实例的所有经常性费用或使用费将在 AWS Service Charges 部分列出。
- Detail 部分包含关于预留实例的信息 - 例如可用区域、实例类型、成本及实例的数量。

您可在线上查看开支，而且您还能下载一个关于开支信息 PDF 文件。

购买预留实例

Abstract

使用 AWS 管理控制台、命令行工具或 Amazon EC2 API 按照此程序从第三方或 AWS 购买 Amazon EC2 预留实例。

您可搜索要购买的特定类型的预留实例，从而在找到您所寻找的完全匹配的实例之前调整参数。

购买任何预留实例时，一定要注意以下内容：

- 使用费 - 使用预留实例时，无论您是否实际使用了整个期限，都需要为该期限付费。
- 购买的套餐折扣 - 定价套餐折扣仅适用于 AWS 购买。这些折扣不适用于第三方预留实例购买。有关更多信息，请参阅 [了解预留实例折扣定价套餐 \(p. 142\)](#)。
- 取消购买 - 确认购买之后便无法取消。在确认之前，请检查您计划购买的预留实例的详细信息，并确保所有参数都是准确的。但是，如果您的需求发生更改并且您符合相应要求，则可以出售预留实例。有关更多信息，请参阅 [在预留实例市场中出售实例 \(p. 147\)](#)。

在选择要购买的预留实例后，您将收到一个关于您选择的实例的总成本报价。当您决定继续购买后，AWS 将自动对购买价格设定一个限定价格，这样您的预留实例的总成本将不会超过对您报价的金额。

如果价格因任何原因而上升或发生变化，您将会返回至前一屏幕，并且购买将不会完成。如果在购买之时有与您的选择类似的低价位产品，AWS 将为您提供价格更低的产品。

使用 AWS 管理控制台购买预留实例

使用 AWS 管理控制台购买预留实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Navigation 窗格中，选择 Reserved Instances。
3. 在 Reserved Instances 页面上，选择 Purchase Reserved Instances。
4. 为要购买的预留实例指定详细信息，然后选择 Search。



Note

搜索结果中的 Seller 列指示卖方是否是第三方。如果是，则 Term 列会显示非标准期限。

5. 选择您希望的预留实例，输入数量，然后选择 Add to Cart。
6. 要查看已选择的预留实例的汇总，请选择 View Cart。
7. 要完成订单，请选择 Purchase。



Note

如果在购买之时有与您的选择类似的低价位产品，AWS 将为您提供价格更低的产品。

要应用您的预留实例，请启动按需实例，确保匹配您已为您的预留实例指定的相同标准。AWS 将自动按较低的小时价格对您收费。您不必重启您的实例。

使用 AWS 管理控制台查看交易状态

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择预留实例页面。您的购买状态将在 State 列中列出。当您的订单完成时，State 值将从 payment-pending 变为 active。

使用命令行界面或 API 购买预留实例

使用命令行或 API 购买预留实例

1. 使用 AWS CLI，请参阅 [purchase-reserved-instances-offering](#)
2. 使用适用于 Windows PowerShell 的 AWS 工具，请参阅 [New-EC2ReservedInstance](#)
3. 使用 Amazon EC2 API，请参阅 [PurchaseReservedInstancesOffering](#)

使用命令行或 API 查看交易状态

1. 使用 AWS CLI，请参阅 [describe-reserved-instances](#)
2. 使用适用于 Windows PowerShell 的 AWS 工具，请参阅 [Get-EC2ReservedInstance](#)
3. 使用 Amazon EC2 API，请参阅 [DescribeReservedInstances](#)

应用预留实例

预留实例将自动应用于正在运行的或潜在的按需实例（前提是满足规范要求）。您可以使用 AWS 管理控制台、命令行工具或 Amazon EC2 API 执行这些任务。



Note

要购买并修改预留实例，请确保您的 IAM 用户账户具有适当的权限，例如描述可用区的能力。有关信息，请参阅[使用 AWS CLI 或 AWS SDK 的策略示例](#)和[用于 Amazon EC2 控制台的策略示例](#)。

购买 - 确定要预留的容量大小。指定以下条件：

- 平台（例如，Linux）。



Note

要在特定 Linux 平台上运行您的预留实例，您必须在购买预留容量时确定该平台。然后，当您启动实例以使用购买的预留容量时，必须选择运行该特定 Linux 平台的 Amazon 系统映像 (AMI) 以及在购买时确定的任何其他规格。

- 实例类型（例如，`m1.small`）。
- 要在其中运行实例的可用区。
- 您希望预留容量的期限（时间段）。
- 租期。您可为实例预留容量，以便在单租户硬件（`dedicated` 租户，与 `shared` 相反）中运行。您选择的租期必须与正在或计划将预留实例应用于的按需实例的租期匹配。有关更多信息，请参阅[专用实例](#)。
- 服务（无预付、部分预付、全部预付）。

使用 - 要使用您的预留实例，请启动具有与购买的预留相同的规格的按需实例。定价优惠和容量预留自动适用于预留容量中尚未包含的所有匹配实例。

有关更多信息，请参阅[启动实例 \(p. 216\)](#)。

预留实例状态

预留实例可以处于以下某种状态：

- `active`（已激活） – 预留实例可供使用。
- `payment-pending` – AWS 正在处理您的预留实例付款。当状态变为 `active` 时，您可以使用预留实例。
- `retired` – 预留实例由于以下任何原因而终止：
 - AWS 没有收到您的付款。例如，信用卡交易没有完成。
 - 预留实例超出期限。

请务必注意，Reserved Instance 页面中的 State 列显示的状态信息与 My Listings 选项卡中的 Listing State 显示的状态信息不一致。

如果您是预留实例市场中的卖家，Listing State 将显示已在预留实例市场中列出的预留的状态。有关更多信息，请参阅[预留实例列示状态 \(p. 150\)](#)。

在预留实例市场中购买

Abstract

从 Amazon Web Services 购买预留实例或通过预留实例市场从第三方卖方进行购买。

您可以购买 Amazon EC2 预留实例（从 AWS 购买或从拥有其不再需要的预留实例的第三方卖方购买）。

作为买家，预留实例市场允许您搜索与您理想的实例类型、区域及持续时间组合最相匹配的预留实例，它提供了增加的选择性和灵活性。

有关预留实例市场的更多信息，请参阅[在预留实例市场中出售实例 \(p. 147\)](#)。

在预留实例市场中购买的预留实例与直接从 AWS 购买的预留实例有一些区别：

- 期限 - 从第三方卖方购买的预留实例拥有的剩余期限短于完整标准期限。从 AWS 获得的完整标准期限为一年或三年。
- 预付价格 - 第三方预留实例可以不同的预付价格出售。使用费或周期性费用与最初从 AWS 购买预留实例时设定的费用一致。

有关您的基本信息将与卖方进行共享，如您的邮政编码和国家/地区信息。

此信息使卖方能够计算他们必须汇给政府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，则可以[联系 AWS Support](#)。

在预留实例市场中出售实例

Abstract

随着您的需求发生变化，在预留实例市场中出售剩余的预留实例。

在预留实例市场中出售未使用的预留为您提供了灵活性，以便您在您的业务需求发生改变时或当您拥有不再需要的容量时迁移到新配置。

只要您在预留实例市场中列出您的预留实例，便可供潜在的买方找到。所有预留实例将会根据剩余期限及小时价格进行分组。

要满足买方的请求，AWS 首先出售指定群组中预付价格最低的预留实例；然后再出售下一个最低价格的预留实例，直到买方的整个订单完成为止。AWS 随后处理这些交易，并将预留实例的所有权转移给买方。

在您的预留实例出售之前，该实例将归您所有。出售之后，您便放弃了容量预留和打折的周期性费用。如果继续使用您的实例，AWS 将从您的预留实例出售的时间开始以按需价格向您收费。您可购买更多预留容量，或在您的容量预留出售之时终止您的实例。

内容

- [收款 \(p. 147\)](#)
- [注册为卖家 \(p. 148\)](#)
- [列示您的预留实例 \(p. 149\)](#)
- [给您的预留实例定价 \(p. 152\)](#)

收款

AWS 收到来自买家的资金后，系统便会立即向相应电子邮件地址（与注册为已售的预留实例的拥有者的账户关联）发送一封电子邮件。

AWS 将自动清算所 (ACH) 电汇发送至您的指定银行账户。通常，此电汇在您的预留实例已售出后的一天到三天内发生。您可通过查看预留实例支付报告来查看此支付的状态。支付每天只发生一次。请记住，在 AWS 从您的银行那里收到验证之前，您无法接收付款。此期间可能最多需要两个星期。

您售出的预留实例将继续出现在您的 `DescribeReservedInstances` 调用的结果中。

您将直接从您的银行账户通过电汇转账收到您的预留实例的现金付款。AWS 会向您收取您在预留实例市场中出售的每个预留实例的总预付价格 12% 的服务费。



Note

仅 Amazon EC2 预留实例可在预留实例市场中出售。其他类型实例（如 Amazon RDS 和 Amazon ElastiCache 预留实例）不能在预留实例市场中出售。

要注意以下重要限制：

- 预留实例可在 30 天之后出售 - 预留实例只能在您已拥有它们至少 30 天之后进行出售。此外，您列示的预留实例的剩余期限至少为一个月。

- 无法修改列示 - 您无法在预留实例市场中修改您的列示。然而，您可通过先取消它然后再用新参数创建另一个列示来更改您的列示。有关信息，请参阅 [列示您的预留实例 \(p. 149\)](#)。您也可以在列出预留实例之前修改它们。有关信息，请参阅 [修改您的预留实例 \(p. 152\)](#)。
- 无法出售打折的预留实例 - 通过某个套餐折扣以较低价格购买的预留实例不能在预留实例市场中出售。有关更多信息，请参阅 [预留实例市场 \(p. 140\)](#)。

注册为卖家

Abstract

作为卖方进行注册，以便您可在预留实例市场中出售预留实例。

为了能够在 预留实例市场 进行销售，您的第一个任务是注册为卖家。注册期间，您需要提供您的企业名称、关于您的银行的信息以及企业的税务标识号。

在 AWS 收到您已完成的卖家注册后，您将收到对您的注册进行确认并告知您可以开始在预留实例市场中出售实例的电子邮件。

主题

- [银行账户 \(p. 148\)](#)
- [税务信息 \(p. 149\)](#)
- [与买家共享信息 \(p. 149\)](#)

银行账户

为了在您出售您的预存实例时支付收取的资金，AWS 必须获得您的银行信息。您指定的银行必须有一个美国地址。

注册付款的默认银行账户

- 在 [预留实例市场 Seller Registration](#) 页面上登录。如果尚未有 AWS 账户，您也可通过此页面创建一个。
- 在 [Manage Bank Account \(管理银行账户\)](#) 页面上，提供关于您用于接收付款的银行的以下信息：

- 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，您将无法收到付款。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

- 在 [预留实例市场 Seller Registration](#) 页面上，使用您注册时所用的账户登录。
- 在 [Manage Bank Account](#) 页面上，根据需要添加新的银行账户或修改默认银行账户。

税务信息

您出售预留实例可能需要交纳交易税，例如销售税或增值税。您应与您的企业的税务、法律、财务或会计部门沟通，以确定是否适用于基于交易的税种。您负责向相关税务机构收集并交纳基于交易的税款。

作为卖家注册的一部分，您可选择完成税务会见。如果以下事项之任一适用，那么我们鼓励您完成此过程：

- 您要 AWS 生成一个表 1099-K。
- 您期待在一个日历年内进行 50 次或更多次的交易，或者销售价值 20 000 USD 或更多的预留实例。一项交易涉及一个或多个预留实例。如果您在注册时选择跳过此步骤，后来您的交易次数达到 49，那么您将得到一条信息“*You have reached the transaction limit for pre-tax.* 请在[卖方注册门户](#)中完成税务问题表。
- 您是非美国卖家。在这种情况下，您必须以电子手段完成表 W-8BEN。

有关 IRS 要求和表 1099-K 的更多信息，请参阅 [IRS 网站](#)。

根据您的企业是美国法律实体还是非美国法律实体，您输入的作为税务会见的一部分的税务信息将有所不同。当您填写税务会见时，请记住以下事项：

- AWS 提供的信息（包括本主题中的信息）不构成税务、法律或其他专业建议。查明 IRS 报告要求将如何影响您的企业，或者如果您有其他问题，请联系您的税务、法律或其他专业顾问。
- 为了尽可能高效地满足 IRS 报告要求，在会见过程中回答所有的问题并输入所有要求的信息。
- 检查您的回答。避免拼写错误或输入了不正确的税务识别号，它们会导致纳税申报表格无效。

在您完成税务注册过程后，AWS 将表 1099-K 归档。您将在您的税务账户达到阈值水平的年份的后一年的 1 月 31 日收到通过美国邮政发来的 1099-K 副本。例如，如果您的税务账户于 2016 年达到阈值，则您将于 2017 年收到该表。

与买家共享信息

当您在预留实例市场中出售时，AWS 将按照美国的规章在买方声明上分享您的公司法律名称。此外，如果买家因发票或其他税务相关的原因需要联系您而呼叫 AWS 客户支持，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](#)。

列示您的预留实例

Abstract

在预留实例市场中列示和出售您的预留实例。

作为注册卖方，您可选择出售您的一个或多个预留实例，而且可选择将一个列示中的实例全部出售或部分出售。此外，您可以列示任何类型的预留实例 - 包括实例类型、平台、区域和可用区的任何配置。

如果您决定取消您的列示，且列示的一部分已经售出，则取消不会在已售出的部分生效。只有列示中未售出的部分在预留实例市场中将不再可用。

列示的生命周期

既然您已经创建了列示，那么我们就看看在您的列示出售时发生了什么。

当您的列示中的所有实例均已匹配并售出后，My Listings 选项卡将显示您的 Total instance count 与 Sold 下列出的计数相匹配，您的列示没有 Available 的实例，而且它的 Status 为 closed。

当您的列示中只有一部分售出时，AWS 将停用列示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，列示 ID 及其代表的列示（现在具有较少的待售预留）仍处于激活状态。

以此方式处理此列示中任何未来预留实例销售。当列示中的所有预留实例售出后，AWS 会将列示标记为 closed。

例如，让我们假设您创建了一个所列数量为 5 的预留实例列示 ID 5ec28771-05ff-4b9b-aa31-9e57dexample。

您的 AWS 管理控制台的 Reserved Instance 页面中的 My Listings 选项卡将如此显示列示：

预留实例列示 ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 0
- 可用 = 5
- 状态 = 已激活

我们假设某个买家购买了其中两个预留，这使得三个预留的计数依然可供销售。此部分销售的结果是 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。

这是您的列示在您的“My Listings”标签中看起来的样子：

预留实例列示 ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 2
- 可用 = 3
- 状态 = 已激活

如果您决定取消您的列示，且列示的一部分已经售出，取消不会在已售出的部分生效。只有列示中未售出的部分在预留实例市场中将不再可用。

在您的实例出售后

当您的预留实例售出后，AWS 将向您发送一个电子邮件通知。在有任何活动（例如您创建了一个列示；您出售了一个列示或者 AWS 将资金发送到您的账户）的每一天，您将收到一个电子邮件通知，告知您当天的活动。

您可查看 AWS 管理控制台中 Reserved Instance 页面上所选预留实例的 My Listings 选项卡，由此追踪您的预留实例列示的状态。此选项卡包含 Listing State (列示状态)、期限信息、标价以及列示中可用、等待、出售和取消的实例数量明细。您也可以使用 ec2-describe-reserved-instances-listings CLI 命令或 DescribeReservedInstancesListings API 调用，借助合适的筛选器来获取有关您的列示的信息。

预留实例列示状态

Listing State 显示您的列示的当前状态：

Listing State (列示状态) 显示的信息与您在预留实例市场中的列示的状态有关。它与“Reserved Instances”页面中的 State 列显示的状态信息不同。此 State 信息是关于您的预留的。有关更多信息，请参阅 [预留实例状态 \(p. 146\)](#)。

使用 AWS CLI 列出您的预留实例

使用 AWS CLI 列出 预留实例市场 中的预留实例

1. 通过调用`aws ec2 describe-reserved-instances`获得您的预留实例的列表。
2. 指定您要列示的预留实例的 ID 并调用`aws ec2 create-reserved-instances-listing`。您必须指定以下要求的参数：

- 预留实例 ID
- 实例计数
- 月份:价格

要查看您的列示

- 调用`aws ec2 describe-reserved-instances-listings`可得到关于您的列出的详细信息。

取消并更改您的列示

- 运行`aws ec2 cancel-reserved-instances-listings`可取消您的列示。

使用 Amazon EC2 API 列示您的预留实例

使用 Amazon EC2 API 在预留实例市场中列示预留实例

1. 通过调用`DescribeReservedInstances`获得您的预留实例的列表。记下您要在预留实例市场中列示的预留实例的 ID。
2. 使用`CreateReservedInstancesListing` 创建列示。

要查看您的列示

- 1. 调用`DescribeReservedInstancesListings`可得到关于您的列示的详细信息。

要取消您的列示

1. 运行`CancelReservedInstancesListing`。
2. 确认已通过调用`DescribeReservedInstancesListings` 取消列示。

使用 AWS 管理控制台列示您的预留实例

您可通过使用 AWS 管理控制台来列示希望在预留实例市场中出售的预留实例。

若要在预留实例市场中列出预留实例，可使用AWS 管理控制台

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择要列示的预留实例，然后选择 Sell Reserved Instances。
4. 在 Configure Your Reserved Instance Listing 页面上，在相关列中设置要出售的实例数并为剩余期限设定预付价格。通过单击 Months Remaining 列旁边的箭头，您可看见您的预留的价值是如何随着剩余期限的变化而变化的。
5. 如果您是高级用户且想对定价进行自定义，那么您可为后续月输入一个不同的值。要返回默认的线性价格降低，请选择 Reset。
6. 当您完成配置您的列示后，请选择 Continue。

7. 在 Confirm Your Reserved Instance Listing 页面上确认您的列示的详细信息并且对此类信息感到满意 , 请选择 List Reserved Instance。

Listing State 显示您的列示的当前状态 :

- active - 列示可供购买。
- cancelled - 列示已取消而且不能在预留实例市场中购买。
- closed - 预留实例未列示。预留实例可能因列示实例的销售已完成而处于 closed 状态。

给您的预留实例定价

预付费用是您可为正在出售的预留实例指定的唯一费用。预付费用是买方在购买预留实例时支付的一次性费用。您无法指定使用费或周期性费用 ; 买方将支付与最初购买预留时设定的使用费或周期性费用相同的费用。

要注意以下重要限制 :

- 您每年可出售的预留实例价值最多为 50000 美元。如需出售更多 , 请填写[提高 Amazon EC2 预留实例销售限制申请表单](#)。
- 最低价格为 \$0。预留实例市场中允许的最低价格为 \$0.00。

您无法直接修改您的列示。然而 , 您可通过先取消它然后再用新参数创建另一个列示来更改您的列示。

只要您的列示处于 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列示。如果您的列示中的某些实例已匹配且您取消了列示 , 则仅剩余的未匹配的实例将从列示中删除。

设置定价表

由于预留实例的价值随时间的推移而降低 , 因此 , 在默认情况下 , AWS 可设定要以同样的变化量逐月降低的价格。但是 , 您可根据预留实例出售的时间设置不同的预付价格。

例如 , 如果您的预留实例剩余期限为九个月 , 那么如果一个客户要购买这个剩余期限为九个月的预留实例 , 您能指定您愿意接受的金额 , 当剩余期限为五个月时 , 您可设定另外一个价格 , 当剩余期限为一个月时 , 再设定另一个价格。

修改您的预留实例

Abstract

当计算需求改变时 , 可修改预留实例 , 继续利用容量预留的优势。

当计算需求改变时 , 可以修改预留实例 , 继续利用容量预留。

以下主题将引导您完成修改过程 :

主题

- [修改的要求 \(p. 153\)](#)
- [修改预留的实例大小 \(p. 153\)](#)
- [提交修改请求 \(p. 155\)](#)

修改不会更改预留实例的剩余期限 ; 预留实例的结束日期将保持不变。不会产生任何费用 , 因此您不会收到任何新账单或发票。修改与购买无关 , 不会对您使用、购买或出售预留实例产生任何影响。您可通过以下一种或多种方式修改您的整个预留或预留的一部分 :

- 在相同区域内切换可用区

- 在 EC2-VPC 和 EC2-Classic 之间切换
- 在同一实例类型内更改实例的大小

对于所有产品平台类型 (Linux 和 Windows) 均支持可用区和网络平台修改。仅 Linux 平台类型支持实例类型修改。但是，由于许可差异，无法将 Linux 预留实例修改为 RedHat 或 SUSE Linux 预留实例。有关 RedHat 和 SUSE 定价的更多信息，请参阅 [Amazon EC2 预留实例定价](#)。

修改之后，预留实例的定价权益仅适用于与新参数匹配的实例。除非您的账户有其他适用的预留，否则将按照按需费率收费对不再符合新参数的实例收费。

修改的要求

Abstract

了解您的预留实例的修改要求。

Amazon EC2 处理您的修改请求的前提是，对于您的目标配置，有足够的容量，同时满足以下条件。

修改后的预留实例必须：

- 活动
- 没有其他等待处理的修改请求
- 预留实例市场中未列示
- 在同一小时（不是分钟或秒）内终止

您的修改请求必须：

- 是可用区、实例类型和网络平台属性的唯一组合
- 原始预留的实例大小占用空间与目标配置匹配

如果您的预留实例不处于活动状态或无法修改，则 API 调用将返回错误，并且 AWS 管理控制台中的 Modify Reserved Instances 按钮将处于禁用状态。如果您选择多个预留实例进行修改，而其中一个或多个预留实例用于不允许修改实例类型的产品平台，则 Modify Reserved Instances 页面不会显示用于更改任何所选预留实例的实例类型的选项。有关更多信息，请参阅 [修改预留的实例大小 \(p. 153\)](#)。

您可以随时修改您的预留；但是，对于未完成上次修改请求的预留，您不能提交修改请求。在提交修改请求后，您也无法更改或取消等待处理的修改请求。修改成功完成后，您可以提交另一个修改请求，以回滚您所做的任何更改。有关更多信息，请参阅 [确定修改的状态 \(p. 156\)](#)。

要修改预留实例市场中列出的预留实例，请取消列表，请求修改预留实例，然后再次列出这些实例。此外，您无法在购买前或购买时修改产品。有关更多信息，请参阅 [预留实例市场 \(p. 140\)](#)。

修改预留的实例大小

Abstract

更改预留的实例大小，如占用空间中的大小分配或是产品平台。

如果您在具有多个实例大小的实例类型中有 Amazon Linux 预留，则可调整预留实例的实例大小。请记住，仅当其他属性（如区域、使用类型、租期、产品、结束日期和小时）匹配并且容量可用时，才允许修改实例大小。不能修改 Windows 预留实例的实例大小。



Note

实例按照系列（依据存储或 CPU 容量）、类型（为特定的使用案例而设计）和大小分组。例如，c4 实例类型属于计算优化型的实例系列，并且有多个大小可用。当 c3 实例属于同一系列时，您

无法将 c4 实例修改进入 c3 实例，因为它们的硬件规格不同。有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

有关修改过程和步骤的信息，请参阅[提交修改请求 \(p. 155\)](#)。

以下实例无法进行修改，因为没有其他大小：

- t1.micro
- cc1.4xlarge
- cc2.8xlarge
- cg1.8xlarge
- cr1.8xlarge
- hi1.4xlarge
- hs1.8xlarge
- g2.2xlarge

如果容量存在，并且修改未更改预留实例的实例大小占用空间，则您的请求成功。

了解实例大小占用空间

每个预留实例都有实例大小占用空间，占用空间由预留中实例类型的标准化因子和实例数量决定。在 Amazon EC2 控制台中，占用空间是用单位计量的。

标准化因子基于实例类型（例如，m1 实例系列）中的大小，并且只在相同实例类型内有意义；无法将实例类型从一个类型修改为另一个类型。下表说明在实例类型中应用的标准化因子。

实例大小	标准化因子
微型	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
4xlarge	32
8xlarge	64
10xlarge	80

如果目标配置的占用空间与原始配置的大小不匹配，则不会处理修改请求。

要计算预留实例的实例占用空间大小，请将实例数量乘以标准化因子。例如，m1.medium 的标准化因子为 2，因此四个 m1.medium 实例的预留相当于 8 个单位的占用空间。

只要预留的实例大小占用空间保持不变，您就可以将预留分配给相同实例类型中的不同实例大小。例如，您可以将一个 m1.large (1 x 4) 实例的预留划分为四个 m1.small (4 x 1) 实例，也可以将四个 m1.small 实例的预留合并为一个 m1.large 实例。但是，您不能将两个 m1.small (2 x 1) 实例的预留更改为一个 m1.large (1 x 4) 实例，因为当前预留的现有实例大小占用空间小于计划的预留空间。

有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

提交修改请求

Abstract

使用 AWS 管理控制台、命令行工具或 Amazon EC2 API 提交修改您的预留实例的请求。

AWS 提供多种查看和处理修改请求的方法：您可以使用 AWS 管理控制台直接与 Amazon EC2 API 交互，也可以使用命令行界面。

主题

- [AWS 管理控制台 \(p. 155\)](#)
- [命令行界面 \(p. 156\)](#)
- [Amazon EC2 API \(p. 156\)](#)
- [确定修改的状态 \(p. 156\)](#)

AWS 管理控制台

Modify Reserved Instances 页面上的每个目标配置行都记录了当前实例类型的实例数量 (Count)，以及您的预留相对于其实例类型的实例大小占用空间 (Units)。有关更多信息，请参阅 [了解实例大小占用空间 \(p. 154\)](#)。

如果您指定的预留实例数多于或少于可修改的数量，则分配的总额显示为红色。在您为可修改的所有预留实例指定更改之后，总数变为绿色，然后您可以选择 Continue。

修改预留的一部分时，Amazon EC2 会将您的原始预留实例分为两个或更多的新预留实例。例如，如果您在 us-east-1a 中有 10 个实例的预留，并决定将其中 5 个实例移动至 us-east-1b，则修改请求会生成两个新的预留实例 - 一个用于 us-east-1a (原始可用区) 中的 5 个实例，另一个用于 us-east-1b 中的 5 个实例。

使用 AWS 管理控制台修改预留实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Reserved Instances 页面上，选择一个或多个要修改的预留实例，然后选择 Modify Reserved Instances。



Note

修改表中的第一个条目是原始的未修改预留。要修改所有预留的属性，请从菜单中选择新规格。要仅修改或拆分某些预留，请为每个更改添加一行。

3. 对于每个附加属性更改选择 Add，并在 Count 字段中输入要修改的预留的数量。
 - 要更改可用区，请在 Availability Zone 列表中选择值。
 - 要更改网络平台，请在 Network 列表中选择值。
 - 要更改实例类型，请在 Instance Type 列表中选择值。
4. 要删除某个指定的属性，请选择相应行的 X。



Note

如果 Modify Reserved Instances 页面仅包含一个属性更改行，则不能删除该行。要修改多个预留实例属性，请先为新规格添加一行，然后删除原始行。

5. 选择 Continue (继续)。
6. 指定好目标配置之后，若要确认您的修改选择，请选择 Submit Modifications。如果您在任何时候改变了主意，请选择 Cancel 退出向导。

命令行界面

您也可以使用 AWS CLI ([modify-reserved-instances](#))、适用于 Windows PowerShell 的 AWS 工具 ([Edit-EC2ReservedInstance](#))、Amazon EC2 API ([ModifyReservedInstances](#)) 以及[适用于 Java 的 AWS 开发工具包](#)以编程方式完成修改任务。

Amazon EC2 API

您可以使用 [ModifyReservedInstances](#) 操作来修改预留实例。有关更多信息，请参阅 [Amazon EC2 API 参考](#)。

确定修改的状态

您可以通过查看所修改的预留实例的状态 来确定修改请求的状态。返回的状态将请求显示为 `in-progress`、`fulfilled` 或 `failed`。使用以下资源可获取这些信息：

- AWS 管理控制台中的 State 字段
- [DescribeReservedInstancesModifications](#) API 操作
- [-describe-reserved-instances-modifications](#) AWS CLI 命令
- [Get-EC2ReservedInstancesModifications](#) 适用于 Windows PowerShell 的 AWS 工具 命令

下表说明了 AWS 管理控制台中可能的 State 值。

状态	说明
活动(等待修改)	原始预留实例的转换状态。
retired (pending modification)	创建新预留实例时原始预留实例的转换状态。
停用	已成功修改和替换预留实例。
活动	从成功的修改请求创建的新预留实例。 -或者- 修改请求失败后的原始预留实例。



Note

(如果您使用 [DescribeReservedInstancesModifications](#) API 操作，则修改请求的状态应显示为 `processing`、`fulfilled` 或 `failed`。

如果您的修改请求成功：

- 修改的预留会立即生效，并且定价优惠将于进行修改请求时这一小时的开始应用于新实例。例如，如果您在晚上 9:15 成功修改了预留，则定价优惠将在晚上 9:00 转移到新实例。（您可以使用 [DescribeReservedInstances](#) API 操作或 [describe-reserved-instances](#) 命令 (AWS CLI) 获取所修改的预留实例的 `effective date`。）
- 原始预留将停用。其结束日期是新预留的开始日期，而新预留的结束日期与原始预留实例的结束日期相同。如果您修改一个剩余期限为 16 个月的三年期预留，则修改后得到的预留是为期 16 个月的预留，其结束日期与原始预留相同。
- 已修改的预留将列出 0 美元固定价格，而不是原始预留的固定价格。



Note

已修改的预留实例的固定价格不影响您的账户的折扣定价套餐计算，后者基于原始预留的固定价格。

如果您的修改请求失败：

- 您的预留实例将保持原始配置。
- 您的预留实例可立即用于另一个修改请求。

有关无法修改某些预留实例的原因的更多信息，请参阅[修改的要求 \(p. 153\)](#)。

修改请求故障排除

Abstract

排查预留实例修改请求问题。

如果您请求的目标配置设置是唯一的，则您会收到正在处理该请求的消息。此时，Amazon EC2 仅确定了修改请求的参数有效。在处理过程中，您的修改请求仍然可能因无可用容量而失败。

在某些情况下，您可能会收到一个指示修改请求未完成或失败的消息而不是确认。使用此类消息中的信息作为重新提交另一个更改请求的起点。

不是所有选择的预留实例都可以进行修改处理

Amazon EC2 会确定并列出无法修改的预留实例。如果收到与此类似的消息，请转到 AWS 管理控制台中的 Reserved Instances 页面，查看有关这些容量预留的详细信息。

处理修改请求时出错

您提交了一个或多个预留实例进行修改，而且不能处理您的处理请求。根据您修改的预留数量，您可以获取不同版本的消息。

Amazon EC2 会显示无法处理请求的原因。举例来说，您可能已经为正在修改的预留实例的一个或更多子集指定了相同的目标配置 – 可用区和平台的组合。尝试重新提交这些修改请求，但确保预留的实例详细信息是匹配的，并确保修改的所有子集的目标配置是唯一的。

计划的预留实例

Abstract

购买按指定的计划重复的容量预留。

利用计划的预留实例（计划实例），您可以以一年为期限购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的容量预留。您应提前预留容量，以确定其在需要时可用。您需要为计划的实例时间付费，即使您未使用它们也是如此。

对于不持续运行，而是按固定的计划运行的工作负载，计划实例是一个很好的选择。例如，您可以为在工作时间运行的应用程序，或为在周末运行的批处理作业使用计划实例。

如果您需要持续的容量预留，预留实例可能符合您的需求并且可以降低成本。有关更多信息，请参阅[预留实例 \(p. 138\)](#)。如果您的实例运行时间比较灵活，竞价型实例可能符合您的需求并且可以降低成本。有关更多信息，请参阅[竞价型实例 \(p. 160\)](#)。

内容

- [计划实例如何运行 \(p. 158\)](#)

- 购买计划实例 (p. 158)
- 启动计划实例 (p. 159)
- 计划实例限制 (p. 159)

计划实例如何运行

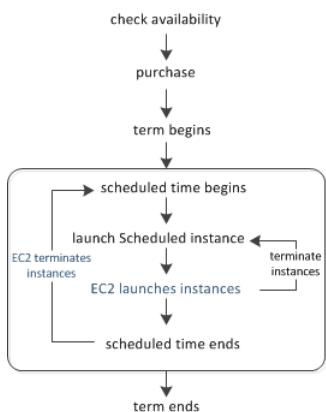
Amazon EC2 在每个可用区内都留下了一些 EC2 实例池以用作计划实例。每个池都支持实例类型、操作系统和网络 (EC2-Classic 或 EC2-VPC) 的一个特定组合。

首先，您必须搜索可用的计划。您可在多个池或单个池中进行搜索。在找到合适的计划后，您购买该计划。

必须在计划实例的计划时间段内启动该实例。当您执行此操作时，Amazon EC2 将根据指定的启动说明代表您启动 EC2 实例。Amazon EC2 必须确保 EC2 实例在当前计划时间段结束时终止，以使容量可用于其为之预留的任何其他计划实例。因此，Amazon EC2 在当前计划时间段结束前三分钟终止 EC2 实例。

您无法停止或重启计划实例，但可以根据需要手动终止它们。如果您在计划实例的当前计划时间段结束前将其终止，可以在几分钟后再次启动它。否则，您必须等到下一个计划时间段。

下图说明了计划实例的生命周期。



购买计划实例

要购买计划实例，可使用计划预留实例预留向导。



Warning

购买计划实例后，您无法取消、修改或转售该购买。

购买计划实例使用控制台

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 在导航窗格中的 INSTANCES 下，选择 Scheduled Instances。
- 选择 Purchase Scheduled Instances。
- 在 Find available schedules 页面中，执行以下操作：
 - 在 Create a schedule 下，从 Starting on 中选择启动日期、从 Recurring 中选择计划重复周期（每日、每周或每月），并从 for duration 中选择最短持续时间。请注意，控制台可确保您为达到计划实例所需的最低利用率（每年 1200 个小时）的最短持续时间指定一个值。

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。

使用 AWS CLI 购买计划实例

使用 [describe-scheduled-instance-availability](#) 命令列出满足您需求的可用计划，然后使用 [purchase-scheduled-instances](#) 命令完成购买。

启动计划实例

在购买计划实例后，可在计划实例的计划时间段内启动该实例。

使用控制台启动计划实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中的 INSTANCES 下，选择 Scheduled Instances。
3. 选择计划实例，然后选择 Launch Scheduled Instances。
4. 在 Configure 页面上，完成您的计划实例的启动说明，然后选择 Review。
5. 在 Review 页面上，验证启动配置并根据需要修改它。完成后，选择 Launch。

使用 AWS CLI 启动计划实例

使用 [describe-scheduled-instances](#) 命令列出计划实例，然后使用 [run-scheduled-instances](#) 命令在每个计划实例的计划时间段内启动实例。

计划实例限制

计划实例受以下限制的约束：

- 以下是仅有的几个受支持的实例类型：C4、C3、M4 和 R3。
- 所需的期限为 365 天（一年）。
- 所需的最低利用率为每年 1200 个小时。
- 您最多可以提前三个月购买计划实例。

竞价型实例

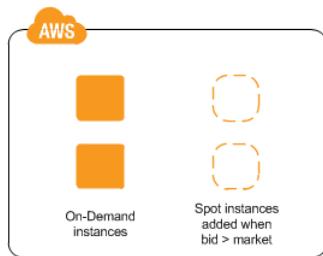
Abstract

了解如何使用竞价型实例降低 Amazon EC2 成本。

竞价型实例使您可以对未使用的 EC2 实例出价，这可以大幅降低您的 Amazon EC2 成本。（每个可用区中的每种实例类型的）竞价型实例的每小时价格由 Amazon EC2 设置，并根据竞价型实例的供求波动。只要您的出价超过当前市场价格，您的竞价型实例就会运行。

如果您能灵活控制应用程序的运行时间并且应用程序可以中断，那么竞价型实例将是您的经济实惠之选。例如，竞价型实例非常适合数据分析、批处理作业、后台处理和可选的任务。有关更多信息，请参阅 [Amazon EC2 竞价型实例](#)。

竞价型实例和按需实例的主要差别在于，竞价型实例可能无法立即启动，竞价型实例每小时价格会根据需求变动，并且 Amazon EC2 可以根据竞价型实例每小时价格或可用情况的变化终止单个竞价型实例。可以采取的一种策略是启动一组核心按需实例，以便为应用程序维护最低级别的保障计算资源，再适机通过竞价型实例来进行补充。



另一项策略是，启动具有要求的时长的竞价型实例（也被称为竞价型限制），这些实例不会因现货价格更改而中断。有关更多信息，请参阅 [指定竞价型实例的持续时间 \(p. 171\)](#)。

概念

在开始使用竞价型实例之前，您应该熟悉以下概念：

- **竞价型实例池** - 一组未使用的 EC2 实例，具有相同的实例类型、操作系统、可用区和网络平台（EC2-Classic 或 EC2-VPC）。
- **现货价格** - 竞价型实例当前的每小时市场价格，该价格由 Amazon EC2 根据执行的最后出价设置。您还可以检索现货价格历史记录。
- **竞价型实例请求（或竞价出价）** - 提供您希望为每个竞价型实例每小时支付的最高价（出价）。当您的出价超过现货价格时，Amazon EC2 会满足您的请求。请注意，竞价型实例请求可以是一次性或持久性请求。Amazon EC2 会在与持久性竞价请求关联的竞价型实例终止之后自动重新提交该请求。您的竞价型实例请求可选择性地为竞价型实例指定一个持续时间。
- **竞价型队列** - 一组基于指定条件启动的竞价型实例。竞价型队列会选择满足您的需要的竞价型实例池，并启动竞价型实例以满足队列的目标容量。默认情况下，在队列中的竞价型实例终止之后，系统会启动替代实例以维持竞价型队列的目标容量。它们也可以作为一次性请求来提交，这种请求在实例终止后不会被保留。
- **竞价型实例中断** - 当现货价格超过您的出价时，或者不再有任何未使用的 EC2 实例时，Amazon EC2 将终止您的竞价型实例。Amazon EC2 将竞价型实例标记为终止并提供竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。
- **出价状态** - 提供有关您的竞价出价最新状态的详细信息。

如何开始

您需要做的第一件事是为使用 Amazon EC2 进行设置。在启动竞价型实例之前，若拥有启动按需实例的经验也会有所帮助。

设置和运行

- [Amazon EC2 的设置 \(p. 13\)](#)
- [Amazon EC2 Windows 实例入门 \(p. 19\)](#)

竞价基本知识

- [竞价型实例运行方式 \(p. 162\)](#)
- [竞价型队列的工作方式 \(p. 165\)](#)

使用竞价型实例

- [准备中断 \(p. 197\)](#)
- [创建竞价型实例请求 \(p. 172\)](#)
- [获取出价状态信息 \(p. 195\)](#)

使用竞价型队列

- [竞价型队列先决条件 \(p. 178\)](#)
- [创建竞价型队列请求 \(p. 179\)](#)

相关服务

您可以直接使用 Amazon EC2 预配竞价型实例。您也可以使用 AWS 中的其他服务预置竞价型实例。有关更多信息，请参阅以下文档。

Auto Scaling 和竞价型实例

您可以通过出价创建启动配置，这样 Auto Scaling 可以启动竞价型实例。有关更多信息，请参阅 [Auto Scaling 用户指南 中的在 Auto Scaling 组中启动竞价型实例](#)。

Amazon EMR 和竞价型实例

有时候，在 Amazon EMR 群集中运行竞价型实例会非常有帮助。有关更多信息，请参阅 [Amazon EMR 开发人员指南 中的通过竞价型实例降低成本](#)。

AWS CloudFormation 模板

AWS CloudFormation 使您能够使用 JSON 格式的模板来创建和管理 AWS 资源集合。AWS CloudFormation 模板可以包含现货价格。有关更多信息，请参阅 [EC2 竞价型实例更新 - Auto Scaling 和 CloudFormation 集成](#)。

AWS SDK for Java

您可以使用 Java 编程语言来管理竞价型实例。有关更多信息，请参阅 [教程：Amazon EC2 竞价型实例](#) 和 [教程：高级 Amazon EC2 竞价请求管理](#)。

适用于 .NET 的 AWS 开发工具包

您可以使用 .NET 编程环境来管理竞价型实例。有关更多信息，请参阅 [教程：Amazon EC2 竞价型实例](#)。

定价

您为竞价型实例支付现货价格，现货价格由 Amazon EC2 设置，并根据竞价型实例的供求周期性波动。如果您的出价超出当前的现货价格，则 Amazon EC2 会满足您的请求，您的竞价型实例将会运行，直到您选择终止它们或现货价格增长到高于您的出价。

在该期间内，每个人支付的现货价格相同，无论他们的出价是否更高。您每小时支付的金额绝不会超过您的出价，并且常常会低于出价。例如，如果您的出价是每小时 0.25 USD，现货价格是每小时 0.20 USD，您只需支付每小时 0.20 USD 即可。如果现货价格下降，您将支付更低的新价格。如果现货价格提高，在现货价格等于或低于您的出价时，您将按照新价格支付。如果现货价格提高并超过您的出价，则会中断您的竞价型实例。

在每一小时实例使用时间开始时，将按照现货价格计费。若因现货价格超过您的出价，导致您的竞价型实例在一小时的实例使用时间内被中断，则您无需为不足一小时的部分付费。如果您自己在一小时的实例使用时间内终止了竞价型实例，则需要为不足一小时的部分付费。

请注意，具有预定义的持续时间的竞价型实例使用的小时固定价格在该实例运行时仍有效。

要查看各个区域和实例类型的当前（每 5 分钟更新一次）最低现货价格，请参阅[竞价型实例定价](#)页面。

要查看过去三个月的现货价格历史记录，请使用 Amazon EC2 控制台或者 `describe-spot-price-history` 命令 (AWS CLI)。有关更多信息，请参阅[竞价型实例定价历史记录 \(p. 169\)](#)。

要查看您的账单，请转至[“AWS 账户活动”页面](#)。您的账单中包含了提供您的账单详情的使用情况报告的链接。有关更多信息，请参阅[AWS Account Billing](#)。

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

竞价型实例运行方式

Abstract

了解竞价型实例的工作方式。

要使用竞价型实例，请创建一个竞价型实例请求或竞价型队列请求。该请求包括您愿意为每个实例每小时支付的最高价（您的出价）以及其他约束（例如，实例类型和可用区）。如果您的出价超过了指定实例当前的现货价格，并且指定的实例可用，将立即满足您的请求。否则，只要现货价格低于您的出价或者指定的实例可用，就会完成您的请求。在您终止竞价型实例或者 Amazon EC2 必须终止竞价型实例（也称为竞价型实例中断）之前，竞价型实例将保持运行。

当您使用竞价型实例时，您必须做好应对中断的准备。随着对竞价型实例需求的增长，或者竞价型实例供应的减少，在现货价格上涨超过了您的出价时，Amazon EC2 可以中断您的竞价型实例。当 Amazon EC2 将竞价型实例标记为终止时，它会提供一个竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。请注意，您无法为竞价型实例启用终止保护。有关更多信息，请参阅[竞价型实例中断 \(p. 197\)](#)。

请注意，如果 Amazon EBS 支持的实例是竞价型实例，那么您无法停止和启动该实例，但可以重新启动或终止它。

在操作系统级别关闭竞价型实例会导致竞价型实例被终止。这种情况无法改变。

内容

- [竞价市场上供应和需求 \(p. 163\)](#)
- [在启动组中启动竞价型实例 \(p. 164\)](#)
- [在可用区组中启动竞价型实例 \(p. 164\)](#)
- [在 VPC 中启动竞价型实例 \(p. 164\)](#)

竞价市场上供应和需求

AWS 持续评估每个竞价型实例池中有多少竞价型实例可用，监视已经为每个池出了什么价，然后将可用竞价型实例预置给最高出价者。池的现货价格设置为该池中执行的最低出价。因此，您的出价必须高于现货价格，才会立即执行针对单个竞价型实例的竞价请求。

例如，假设您创建了竞价型实例请求，对应的竞价型实例池只有五个竞价型实例可供销售。您的出价为 0.10 USD，这也是当前现货价格。下表按照降序排名显示了当前出价。将执行出价 1-5。出价 5（最后执行的出价）将现货价格设置在 0.10 USD。出价 6 未执行。0.10 USD 这一相同出价的出价 3-5 按随机顺序排列。

出价	出价	当前现货价格	备注
1	1.00 USD	0.10 USD	
2	1.00 USD	0.10 USD	
3	0.10 USD	0.10 USD	
4	0.10 USD	0.10 USD	您的出价
5	0.10 USD	0.10 USD	最后执行的出价（设置现货价格）。每个人在相应时段内都会支付相同的现货价格。
-----	-----		竞价容量截止
6	\$0.05		

现在，假设此池的大小下降为 3。将执行出价 1-3。出价 3（最后执行的出价）将现货价格设置在 0.10 USD。出价 4-5（也就是 0.10 USD）未执行。如您所见，尽管现货价格没有变化，但由于竞价供应减少，包括您的出价在内的两个竞价将不再执行。

出价	出价	当前现货价格	备注
1	1.00 USD	0.10 USD	
2	1.00 USD	0.10 USD	
3	0.10 USD	0.10 USD	最后执行的出价（设置现货价格）。每个人在相应时段内都会支付相同的现货价格。
-----	-----		竞价容量截止
4	0.10 USD		您的出价
5	0.10 USD		
6	\$0.05		

要执行此池中单个实例的竞价请求，您的出价必须超过当前的现货价格 0.10 USD。如果您出价 0.101 USD，则将执行您的请求，出价 3 的竞价型实例将中断，现货价格成为 0.101 USD。如果您出价 2.00 USD，则出价 3 的竞价型实例将中断，现货价格成为 1.00 USD（出价 2 的价格）。

请记住，不论您出价多高，您获得的竞价型实例数都不会超过竞价型实例池中可用的竞价型实例数。如果池的大小下降为零，则该池中的所有竞价型实例都将中断。

在启动组中启动竞价型实例

在竞价型实例请求中指定启动组，可以通知 Amazon EC2 只有在可以全部启动一组竞价型实例时才启动。此外，如果竞价型服务必须终止启动组中的一个实例（例如，如果现货价格提高并超过您的出价），则必须终止该组中的所有实例。不过，如果由您终止启动组中的一个或多个实例，Amazon EC2 不会终止该启动组中的剩余实例。

请注意，虽然此选项非常有用，但添加此约束会减少完成您的竞价型实例请求的几率。这还会增加您的竞价型实例被终止的几率。

如果您创建了另一个成功的竞价型实例请求并指定与之前成功请求相同（现有）的启动组，则新实例将添加到该启动组中。以后，在该启动组的一个实例终止时，启动组中的所有实例均会终止，这包括第一次请求和第二次请求启动的实例。

在可用区组中启动竞价型实例

在竞价型实例请求中指定可用区组，可以通知竞价服务在同一可用区中启动一组竞价型实例。请注意，Amazon EC2 不必同时终止某个可用区组中的所有实例。如果 Amazon EC2 必须终止可用区组中的某个实例，剩余的实例仍保持运行。

请注意，虽然此选项非常有用，但添加此约束会减少完成您的竞价型实例请求的几率。

如果您在竞价型实例请求中指定了可用区组，但没有指定可用区，则竞价服务所采取的操作将取决于您指定的是 EC2-Classic 网络、默认 VPC 还是非默认 VPC。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅 [支持的平台 \(p. 577\)](#)。

EC2-Classic

Amazon EC2 查找区域中最低价格的可用区，如果该组的最低出价高于该可用区中当前的现货价格，则在该可用区中启动您的竞价型实例。只要现货价格保持低于该组的最低出价，Amazon EC2 就将等待，直至有足够的容量来同时启动您的竞价型实例。

默认 VPC

Amazon EC2 使用指定子网的可用区，如果您没有指定子网，则竞价服务将选择一个可用区及其默认子网，但这可能不是最低价格的可用区。如果您删除了可用区的默认子网，则必须指定其他子网。

非默认 VPC

Amazon EC2 使用指定子网的可用区。

在 VPC 中启动竞价型实例

如果您想在使用竞价型实例时利用 EC2-VPC 的功能，请在您的竞价请求中将您的竞价型实例指定为在 VPC 中启动。按照您为按需实例指定子网的相同方法，为您的竞价型实例指定子网。

对于在 VPC 中启动竞价型实例的竞价型实例请求，其提交过程与在 EC2-Classic 中启动竞价型实例的竞价型实例请求基本相同，但有以下区别：

- 您应该基于 VPC 中竞价型实例的现货价格历史记录来确定您的出价。
- [默认 VPC] 如果希望在特定的低价格可用区中启动您的竞价型实例，您必须在竞价型实例请求中指定对应的子网。如果您没有指定子网，则 Amazon EC2 将为您选择一个子网，而该子网的可用区中的现货价格不一定是最低的。
- [非默认 VPC] 您必须为您的竞价型实例指定子网。

竞价型队列的工作方式

Abstract

使用单个竞价型队列请求启动几十个、几百个或几千个竞价型实例。

竞价型队列是竞价型实例的集合或队列。竞价型队列会尝试启动适当数量的竞价型实例，以满足在竞价型队列请求中指定的目标容量要求。如果您的竞价型实例由于现货价格或可用容量的变化而中断，则竞价型队列还会尝试维持其目标容量队列。

竞价型实例池是一组未使用的 EC2 实例，具有相同的实例类型、操作系统、可用区和网络平台（EC2-Classic 或 EC2-VPC）。在您发出竞价型队列请求时，您可以指定多个启动说明（因实例类型、AMI、可用区或子网而异）。竞价型队列会基于竞价型队列请求中包含的启动说明以及竞价型队列请求的配置来选择用于执行请求的竞价型实例池。竞价型实例来自所选池。

内容

- 竞价型队列分配策略 (p. 165)
- 现货价格覆盖 (p. 165)
- 竞价型队列实例权重 (p. 166)
- 演练：将竞价型队列与实例权重结合使用 (p. 167)

竞价型队列分配策略

竞价型队列的分配策略决定了如何根据启动说明从可能的竞价型实例池执行竞价型队列请求。以下是您在竞价型队列请求中可以指定的分配策略：

lowestPrice

竞价型实例来自具有最低价格的池。这是默认策略。

diversified

竞价型实例分布在所有池中。

选择分配策略

您可以基于您的使用案例来优化竞价型队列。

如果您的队列较小或只是短时间运行，则您的竞价型实例中断的可能性较低（即使所有实例都在同一个竞价型实例池中）。因此，lowestPrice 策略可能会满足您的需求，同时提供最低的成本。

如果您的队列较大或长时间运行，则您可以通过在多个池间分配竞价型实例来提高队列的可用性。例如，如果您的竞价型队列请求指定 10 个池，且目标容量为 100 个实例，则竞价型队列会在每个池中启动 10 个竞价型实例。如果一个池的现货价格上涨到超过您对该池的出价，则只有队列的 10% 受到影响。使用此策略还可降低您的队列对单个池的现货价格随时间上涨的敏感度。

请注意，使用 diversified 策略时，竞价型队列不在现货价格高于 [按需价格](#) 的任何池中启动竞价型实例。

维持目标容量

在竞价型实例由于竞价型实例池的现货价格或可用容量发生变化而终止之后，竞价型队列会启动替换竞价型实例。如果分配策略是 lowestPrice，则竞价型队列在当前具有最低现货价格的池中启动替换实例。如果分配策略是 diversified，则竞价型队列在其余池间分配替换竞价型实例。

现货价格覆盖

每个竞价型队列请求必须包含一个全局现货价格。默认情况下，竞价型队列使用此价格作为每个启动说明的出价。

您可以选择在一个或多个启动说明中指定现货价格。此出价特定于启动说明。如果启动说明包含特定现货价格，则竞价型队列使用此价格作为该启动说明的出价（覆盖全局现货价格）。请注意，不包含特定现货价格的任何其他启动说明仍使用全局现货价格。

竞价型队列实例权重

当请求竞价型实例队列时，您可以使用 **实例权重** 定义每种实例类型对应用程序性能贡献的容量单位，并相应地为每个竞价型实例池调整出价。

默认情况下，您指定的现货价格表示每实例小时的出价。使用实例权重功能时，您指定的现货价格表示每单位小时的出价。您可以通过将实例类型出价除以它表示的单位数来计算每单位小时出价。竞价型队列通过将目标容量除以实例权重来计算要启动的竞价型实例数。如果结果不是整数，则竞价型队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。

下表中提供了用于为目标容量是 10 的竞价型队列请求确定每单位出价的计算示例。

实例类型	实例权重	每实例小时现货价格	每单位小时现货价格	启动的实例数
r3.xlarge	2	\$0.05	0.025 (0.05 除以 2)	5 (10 除以 2)
r3.8xlarge	8	0.10 USD	0.0125 (0.10 除以 8)	2 (10 除以 8 , 结果向上舍入)

按如下所示使用竞价型队列实例权重，在执行时具有每单位最低价格的池中预置所需的目标容量：

1. 采用实例（默认设置）或采用所选单位（如虚拟 CPU、内存、存储或吞吐量）为竞价型队列设置目标容量。
2. 设置每单位出价。
3. 对于每个启动配置，指定权重，这是实例类型向目标容量提供的单位数。

实例权重示例

考虑一个具有以下配置的竞价型队列请求：

- 目标容量为 24
- 一个实例类型为 r3.2xlarge 且权重为 6 的启动说明
- 一个实例类型为 c3.xlarge 且权重为 5 的启动说明

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动说明提供了最低的每单位现货价格（r3.2xlarge 每实例小时现货价格除以 6），则竞价型队列会启动四个这样的实例（24 除以 6）。

如果第二个启动说明提供了最低的每单位现货价格（c3.xlarge 每实例小时现货价格除以 5），则竞价型队列会启动五个这样的实例（24 除以 5，结果向上舍入）。

实例权重和分配策略

考虑一个具有以下配置的竞价型队列请求：

- 目标容量为 30
- 一个实例类型为 c3.2xlarge 且权重为 8 的启动说明
- 一个实例类型为 m3.xlarge 且权重为 8 的启动说明

- 一个实例类型为 r3.xlarge 且权重为 8 的启动说明

竞价型队列会启动四个实例（30 除以 8，结果向上舍入）。使用 lowestPrice 策略时，所有四个实例都来自提供最低每单位现货价格的池。使用 diversified 策略时，竞价型队列会在所有三个池中各启动 1 个实例，并在三个池中提供最低每单位现货价格的那个池中启动第四个实例。

演练：将竞价型队列与实例权重结合使用

此演练使用一个名为 Example Corp 的虚构公司演示使用实例权重为竞价型队列出价的过程。

目标

Example Corp 是一家医药公司，该公司想要利用 Amazon EC2 的计算功能来筛查可能用于对抗癌症的化学成分。

计划

Example Corp 首先查看[竞价最佳实践](#)。然后，Example Corp 确定了他们的竞价型队列的以下要求。

实例类型

Example Corp 有一个计算和内存密集型应用程序，该应用程序在至少 60 GB 内存和八个虚拟 CPU (vCPU) 的情况下性能最佳。他们希望以尽可能低的价格为该应用程序提供尽可能多的这些资源。Example Corp 认定以下任意 EC2 实例类型都能满足其需求：

实例类型	内存 (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

以单位数表示的目标容量

采用实例权重，目标容量可以等于几个实例（默认）或一些因素（如内核 (vCPU)、内存 (GiB) 和存储 (GB)）的组合。将其应用程序的基本要求（60 GB RAM 和八个 vCPU）作为 1 个单位，Example Corp 决定 20 倍此数量可满足其需求。因此该公司将其竞价型队列请求的目标容量设置为 20。

实例权重

确定目标容量后，Example Corp 计算了实例权重。为了计算每个实例类型的实例权重，他们按如下所示确定每个实例类型需要多少单位才能达到目标容量：

- r3.2xlarge (61.0 GB, 8 vCPUs) = 1 个 20 单位
- r3.4xlarge (122.0 GB, 16 vCPUs) = 2 个 20 单位
- r3.8xlarge (244.0 GB, 32 vCPUs) = 4 个 20 单位

因此，Example Corp 在其竞价型队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时出价

Example Corp 使用每实例小时[按需定价](#)作为其出价的起点。他们也可以使用最近的现货价格或两者的组合。为了计算每单位小时出价，他们用每实例小时的起始出价除以权重。例如：

实例类型	按需价格	实例权重	每单位小时价格
r3.2xLarge	\$0.7	1	\$0.7
r3.4xLarge	1.4 USD	2	\$0.7
r3.8xLarge	\$2.8	4	\$0.7

Example Corp 可以输入一个每单位小时 0.7 USD 的全局出价来对全部三个实例类型竞价。他们还可以输入一个每单位小时 0.7 USD 的全局出价并在 `r3.8xlarge` 启动说明中输入每单位小时 0.9 USD 的特定出价。根据其竞价型队列的预置策略，Example Corp 可以出较低的价格以便进一步降低成本，也可以出较高的价格以便减少可能的中断。

验证权限

在创建竞价型队列请求之前，Example Corp 验证它是否拥有具备所需权限的 IAM 角色。有关更多信息，请参阅 [竞价型队列先决条件 \(p. 178\)](#)。

创建请求

Example Corp 为其竞价型队列请求创建一个具有以下配置的文件 config.json：

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-482e4972",  
            "WeightedCapacity": 1  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.4xlarge",  
            "SubnetId": "subnet-482e4972",  
            "WeightedCapacity": 2  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.8xlarge",  
            "SubnetId": "subnet-482e4972",  
            "SpotPrice": "0.90",  
            "WeightedCapacity": 4  
        }  
    ]  
}
```

Example Corp 使用以下 `request-spot-fleet` 命令创建竞价型队列请求：

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关更多信息，请参阅 [竞价型队列请求 \(p. 176\)](#)。

执行

分配策略确定竞价型实例来自哪个竞价型实例池。

使用 `lowestPrice` 策略（这是默认策略）时，竞价型实例来自在执行时具有最低每单位现货价格的池。为了提供 20 个单位的容量，竞价型队列有三种做法：启动 20 个 `r3.2xlarge` 实例（20 除以 1）、10 个 `r3.4xlarge` 实例（20 除以 2）或 5 个 `r3.8xlarge` 实例（20 除以 4）。

如果 Example Corp 使用 `diversified` 策略，则竞价型实例会来自所有三个池。竞价型队列会启动 6 个 `r3.2xlarge` 实例（提供 6 个单位）、3 个 `r3.4xlarge` 实例（提供 6 个单位）和 2 个 `r3.8xlarge` 实例（提供 8 个单位），总共 20 个单位。

竞价型实例定价历史记录

Abstract

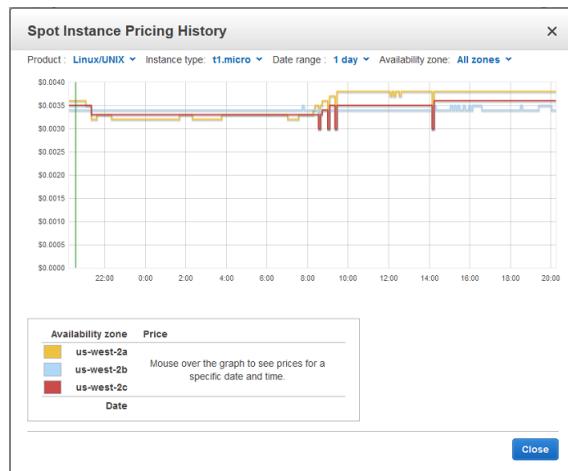
查看竞价型实例的定价历史记录。

您的出价需要高于现货价格以确保单个竞价请求能够完成。当您的出价超过现货价格时，Amazon EC2 会启动您的竞价型实例，当现货价格上涨到超出您的出价，Amazon EC2 会终止您的竞价型实例。您可以出价超过当前现货价格，以便快速完成竞价请求。不过，在您为竞价型实例指定出价前，我们建议您查看现货价格历史记录。您可以查看最近 90 天的现货价格历史记录，并按照实例类型、操作系统和可用区筛选。

以现货价格历史记录为指导，您可以选择在之前能够满足您的需求的出价。例如，您可以确定什么出价在您查看的时间范围内提供了 75% 的正常运行时间。但请注意，历史趋势不能确保以后的结果。现货价格因实时供需情况而异，过去产生特定现货价格模式的情况可能在未来不会出现。

使用控制台查看现货价格历史记录

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 如果您是首次接触竞价型实例，则会看到欢迎页面；请选择 Get started，滚动到屏幕底部，然后选择 Cancel。
4. 选择 Pricing History。默认情况下，页面显示过去一天中所有可用区中的 Linux `t1.micro` 实例的数据图。将鼠标移动到图形上可在图形下方的表中显示特定时间的价格。



5. (可选) 要查看特定可用区的现货价格历史记录，请从列表中选择一个可用区。您还可以选择其他产品、实例类型或日期范围。

使用命令行查看现货价格历史记录

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

- [describe-spot-price-history](#) (AWS CLI)
- [Get-EC2SpotPriceHistory](#) (适用于 Windows PowerShell 的 AWS 工具)

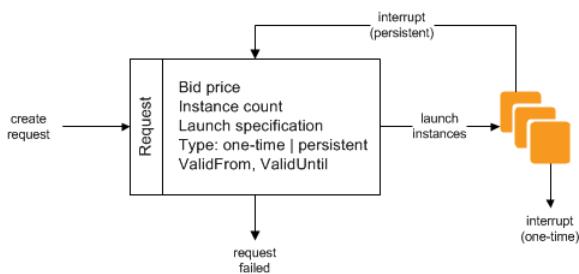
竞价型实例请求

Abstract

创建竞价型实例请求，指定您的竞价型实例，包括您愿意支付的每小时实例使用时间的价格。

要使用竞价型实例，您需要创建竞价型实例请求，其中包括实例数量、实例类型、可用区以及您愿意为每小时实例使用时间支付的最高价格（您的出价）。如果您的出价超过当前现货价格，则 Amazon EC2 将立即执行您的请求。否则，Amazon EC2 将等待直至可以执行您的请求，或者直至您取消请求。

以下演示了竞价请求的运行方式。请注意，为竞价型实例中断采取的操作取决于请求类型（一次性还是持久性）。如果请求是持久性请求，则在竞价型实例终止之后将重新打开请求。



内容

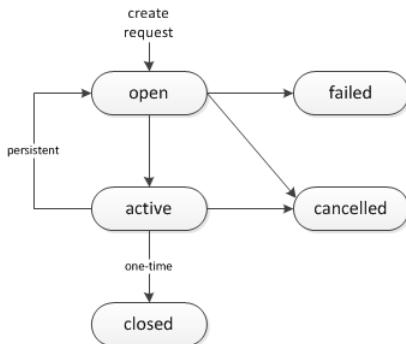
- 竞价型实例请求状态 (p. 170)
- 指定竞价型实例的持续时间 (p. 171)
- 创建竞价型实例请求 (p. 172)
- 查找正在运行的竞价型实例 (p. 173)
- 标记竞价型实例请求 (p. 174)
- 取消竞价型实例请求 (p. 174)
- 竞价请求示例启动说明 (p. 175)

竞价型实例请求状态

竞价型实例请求可以处于以下某种状态：

- `open` - 请求正在等待执行。
- `active` - 请求已执行并有关联的竞价型实例。
- `failed` - 请求的一个或多个参数错误。
- `closed` - 竞价型实例被中断或终止。
- `cancelled` - 您取消了请求，或者请求已过期。

以下显示了请求状态之间的转换。请注意，转换取决于请求类型（一次性还是持久性）。



一次性竞价型实例请求在 Amazon EC2 启动竞价型实例、请求过期前或者您取消请求前保持有效。如果现货价格提高并超过您的出价，您的竞价型实例会终止，竞价型实例请求关闭。

持久性竞价型实例请求在过期或您取消它之前保持有效，即使该请求已完成也如此。例如，如果您在现货价格为 0.25 USD 时为一个实例创建持久性竞价型实例请求，当您的出价超过 0.25 USD 时，Amazon EC2 启动您的竞价型实例。如果现货价格上涨超过了您的出价，您的竞价型实例将终止；不过，竞价型实例请求重新打开，Amazon EC2 将在现货价格低于您的出价时启动新的竞价型实例。

您可以通过出价状态跟踪您的竞价型实例请求状态以及启动的竞价型实例状态。有关更多信息，请参阅 [竞价出价状态 \(p. 193\)](#)。

指定竞价型实例的持续时间

当现货价格发生更改时，Amazon EC2 不会终止带有指定持续时间的竞价型实例（也被称作竞价型限制）。这使得此实例非常适合需在有限时间内完成的任务，如批处理、编码和渲染、建模和分析以及连续集成。

您可将持续时间指定为 1、2、3、4、5 或 6 小时。您支付的价格取决于指定的持续时间。要查看 1 小时持续时间或 6 小时持续时间的当前价格，请参阅 [竞价型实例价格](#)。您可使用这些价格来估计 2、3、4 和 5 小时持续时间的费用。在完成带持续时间的请求时，您的竞价型实例的价格是固定的，而且此价格在实例终止前保持有效。

在您的竞价请求中指定持续时间时，每个竞价型实例的持续时间段将在该实例收到其实例 ID 后立即开始。竞价型实例将运行，直到您终止它或其持续时间段结束。在持续时间段结束后，Amazon EC2 将竞价型实例标记为终止并提供一个竞价型实例终止通知，这将在实例终止前为其提供两分钟时间的警告。

使用控制台启动具有指定持续时间的竞价型实例

选择合适的请求类型。有关更多信息，请参阅 [创建竞价型实例请求 \(p. 172\)](#)。

使用 AWS CLI 启动具有指定持续时间的竞价型实例

要为您的竞价型实例指定持续时间，请将 `--block-duration-minutes` 选项与 `request-spot-instances` 命令包含在一起。例如，以下命令可创建一个竞价请求，启动运行时间为两小时的竞价型实例：

```
aws ec2 request-spot-instances --spot-price "0.050" --instance-count 5 --block-duration-minutes 120 --type "one-time" --launch-specification file://specification.json
```

使用 AWS CLI 检索带指定的持续时间的竞价型实例的费用

使用 `describe-spot-instance-requests` 命令可检索带指定持续时间的竞价型实例的固定费用。该信息位于 `actualBlockHourlyPrice` 字段中。

创建竞价型实例请求

请求竞价型实例的过程与启动按需实例的过程相似。请注意，提交请求之后，您无法更改竞价请求的参数，包括出价。

如果您一次请求了多个竞价型实例，Amazon EC2 将创建单独的竞价型实例请求，这样您可以分别跟踪各个请求的状态。有关跟踪竞价请求的更多信息，请参阅[竞价出价状态 \(p. 193\)](#)。

先决条件

在开始之前，请确定您的出价、需要多少个竞价型实例以及要使用的实例类型。要查看现货价格趋势，请参阅[竞价型实例定价历史记录 \(p. 169\)](#)。

使用控制台创建竞价型实例请求

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 如果您是首次接触竞价型实例，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot Instances。
4. 在 Find instance types 页面中，执行以下操作：
 - a. 对于 Request type，默认值为使用竞价型队列创建的一次性竞价请求。有关更多信息，请参阅[竞价型队列请求 \(p. 176\)](#)。要改为使用竞价型限制，请选择 Reserve for duration。
 - b. 对于 Target capacity，输入要请求的单位数量。您可以选择实例或是对应用程序工作负载十分重要的性能特征（如 vCPU、内存和存储）。
 - c. [竞价型限制] 对于 Reserved duration，请选择完成工作所需的小时数。
 - d. 对于 AMI，选择 AWS 提供的一个基本 Amazon 系统映像 (AMI)，或选择 Use custom AMI 以指定您自己的 AMI。
 - e. 对于 Instance type(s)，请选择 Select。选择具有您所需最低硬件规格的实例类型（虚拟 CPU、内存和存储）。
 - f. [竞价型队列] 对于 Allocation strategy，请选择满足您需求的策略。有关更多信息，请参阅[竞价型队列分配策略 \(p. 165\)](#)。
 - g. 对于 Network，您的账户可能支持 EC2-Classic 和 EC2-VPC 平台，或者仅支持 EC2-VPC 平台。要查明您的账户支持的平台，请参阅[支持的平台 \(p. 577\)](#)。
 - [现有 VPC] 选择 VPC。
 - [新 VPC] 选择 Create new VPC 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。
 - [EC2-Classic] 选择 EC2-Classic。
 - h. (可选) 对于 Availability Zones，默认由 AWS 为您的竞价型实例选择可用区。如果您想使用特定可用区，请执行以下操作：
 - [EC2-VPC] 选择一个或多个可用区。如果您在一个可用区中有多个子网，则请从 Subnet 中选择合适的子网。要添加子网，请选择 Create new subnet 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。
 - [EC2-Classic] 选择 Select specific zone/subnet，然后选择一个或多个可用区。
 - i. [竞价型队列] 对于 Maximum price，您可以使用自动出价，也可以指定一个出价。如果您的出价低于所选实例类型的现货价格，则您的竞价型实例不会启动。
 - j. 选择 Next。
5. 在 Configure (配置实例详细信息) 页面中，执行以下操作：
 - a. (可选) 如果您需要连接到您的实例，请使用 Key pair name 指定您的密钥对。
 - b. (可选) 如果您需要启动带有 IAM 角色的竞价型实例，请使用 IAM instance profile 指定角色。
 - c. (可选) 如果您要运行任何启动脚本，请使用 User data 指定脚本。

- d. 对于 Security groups，选择一个或多个安全组。
 - e. [EC2-VPC] 如果您需要连接到您在 VPC 中的实例，对于 Public IP，请选择 auto-assign at launch。
 - f. 默认情况下，请求在被执行或被您取消之前保持有效。要创建仅在特定时段内有效的请求，请编辑 Request valid from 和 Request valid to。
 - g. [竞价型队列] 默认情况下，我们会在请求过期时终止您的竞价型实例。要维持实例在请求过期之后继续运行，请清除 Terminate instances at expiration。
 - h. 选择 Review。
6. 在 Review 页面上，确认启动配置。要进行更改，请选择 Previous。要下载启动配置的副本以便与 AWS CLI 结合使用，请选择 JSON config。如果准备就绪，请选择 Launch。
7. 在确认页面上，请选择 OK。
- [竞价型队列] 请求类型为 fleet。执行请求后，系统会添加请求类型 instance，此时其状态为 active 和 fulfilled。
- [竞价型限制] 请求类型为 block，且初始状态为 open。执行请求后，状态为 active 和 fulfilled。

使用 AWS CLI 创建竞价型实例请求

使用以下 `request-spot-instances` 命令可创建一次性请求：

```
aws ec2 request-spot-instances --spot-price "0.05" --instance-count 5 --type "one-time" --launch-specification file://specification.json
```

使用以下 `request-spot-instances` 命令可创建持久性请求：

```
aws ec2 request-spot-instances --spot-price "0.05" --instance-count 5 --type "persistent" --launch-specification file://specification.json
```

例如，启动规范文件，请参阅[竞价请求示例启动说明 \(p. 175\)](#)。

当现货价格低于您的出价时，Amazon EC2 将启动您的竞价型实例。竞价型实例将运行，直到它被中断或您自行将它终止。使用以下 `describe-spot-instance-requests` 命令可监控您的竞价型实例请求：

```
aws ec2 describe-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

查找正在运行的竞价型实例

当现货价格低于您的出价时，Amazon EC2 将启动竞价型实例。竞价型实例将会运行，直到出价不再高于现货价格或您自己终止了它。（如果您的出价与现货价格完全一致，那么根据需求情况，您的竞价型实例有机会保持运行。）

使用控制台查找正在运行的竞价型实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。

您可以看到竞价型实例请求和竞价型队列请求。如果竞价型实例请求已执行，那么 Capacity 就是竞价型实例的 ID。对于竞价型队列，Capacity 表示已执行的请求容量。要查看竞价型队列中的实例的 ID，请选择扩展箭头，或者选择队列，然后选择 Instances 选项卡。

3. 或者，在导航窗格中，选择 Instances。在右上角，选择 Show/Hide 图标，然后选择 Lifecycle。对于每个实例，Lifecycle 为 normal、spot 或 scheduled。

使用 AWS CLI 查找正在运行的竞价型实例

要枚举您的竞价型实例，请结合使用 [describe-spot-instance-requests](#) 命令和 --query 选项，如下所示：

```
aws ec2 describe-spot-instance-requests --query SpotInstanceRequests[*].{ID:InstanceId}
```

下面是示例输出：

```
[  
  {  
    "ID": "i-1234567890abcdef0"  
  },  
  {  
    "ID": "i-0598c7d356eba48d7"  
  }  
]
```

或者，您可结合使用 [describe-instances](#) 命令和 --filters 选项来枚举您的竞价型实例，如下所示：

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

标记竞价型实例请求

要对您的竞价型实例请求进行分类和管理，您使用您选择的元数据为它们做标记。您可以使用标记任何其他 Amazon EC2 资源的同样方法来标记您的竞价型实例请求。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 737\)](#)。

您可以在创建请求之后为其分配标签。

您为竞价型实例请求创建的标签只适用于该请求。这些标签不会自动添加到竞价服务为完成请求所启动的竞价型实例中。在竞价型实例启动后，您必须自己将标签添加到竞价型实例。

使用 AWS CLI 向您的竞价型实例请求或竞价型实例添加标签

使用以下 [create-tags](#) 命令标记您的资源：

```
aws ec2 create-tags --resources sir-08b93456 i-1234567890abcdef0 --tags  
Key=purpose,Value=test
```

取消竞价型实例请求

如果您不再需要竞价请求，您可以将其取消。您只能取消处于 open 或 active 状态的竞价型实例请求。当您的请求未执行，且实例没有启动时，您的竞价请求处于 open 状态。当您的请求完成，且竞价型实例已启动时，您的竞价请求处于 active 状态。如果您的竞价请求处于 active 状态，且关联的竞价型实例正在运行，那么取消此请求不会终止该实例；您必须手动终止正在运行的竞价型实例。

如果竞价请求是持久性竞价请求，则会返回 open 状态，这样就可以启动新的竞价型实例。要取消持久性竞价请求并终止其竞价型实例，您必须先取消竞价请求，然后终止竞价型实例。否则，竞价请求可以启动新实例。

使用控制台取消竞价型实例请求

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests，然后选择竞价请求。

3. 选择 Actions，然后选择 Cancel spot request。
4. (可选) 如果您使用完关联的竞价型实例，则可以终止这些实例。在导航窗格中，请选择 Instances 并选择实例，然后依次选择 Actions、Instance State、Terminate。

使用 AWS CLI 取消竞价型实例请求

使用以下 [cancel-spot-instance-requests](#) 命令可取消指定的竞价请求：

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

如果您已完成关联的竞价型实例，则可使用以下 [terminate-instances](#) 命令手动终止这些实例：

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

竞价请求示例启动说明

Abstract

了解如何创建用于 AWS CLI 的启动说明。

以下示例显示了可与 [request-spot-instances](#) 命令结合使用来创建竞价型实例请求的启动配置。有关更多信息，请参阅 [创建竞价型实例请求 \(p. 172\)](#)。

1. [启动竞价型实例 \(p. 175\)](#)
2. [在指定的可用区中启动竞价型实例 \(p. 175\)](#)
3. [在指定的子网中启动竞价型实例 \(p. 176\)](#)

示例 1：启动竞价型实例

以下示例不包括可用区或子网。Amazon EC2 为您选择可用区。如果您的账户仅支持 EC2-VPC，则 Amazon EC2 将在所选可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则 Amazon EC2 将在所选可用区的 EC2-Classic 中启动实例。

```
{
  "ImageId": "ami-1a2b3c4d",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d" ],
  "InstanceType": "m3.medium",
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

请注意，您可按 ID 或名称为 EC2-Classic 指定安全组（使用 `SecurityGroups` 字段）。您必须按 ID 为 EC2-VPC 指定安全组。

示例 2：在指定的可用区中启动竞价型实例

以下示例包括一个可用区。如果您的账户仅支持 EC2-VPC，则 Amazon EC2 将在指定可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则 Amazon EC2 将在指定可用区的 EC2-Classic 中启动实例。

```
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],  
    "InstanceType": "m3.medium",  
    "Placement": {  
        "AvailabilityZone": "us-west-2a"  
    },  
    "IamInstanceProfile": {  
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
    }  
}
```

示例 3：在指定的子网中启动竞价型实例

以下示例包括一个子网。Amazon EC2 在指定的子网中启动实例。如果 VPC 是一个非默认 VPC，则默认情况下该实例不接收公有 IP 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 IP 地址分配给非默认 VPC 中的实例，请指定 `AssociatePublicIpAddress` 字段，如以下示例所示。请注意，在指定一个网络接口时，必须使用该网络接口（而不是使用示例 3 中所示的 `SubnetId` 和 `SecurityGroupIds` 字段）包含子网 ID 和安全组 ID。

```
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "InstanceType": "m3.medium",  
    "NetworkInterfaces": [  
        {  
            "DeviceIndex": 0,  
            "SubnetId": "subnet-1a2b3c4d",  
            "Groups": [ "sg-1a2b3c4d" ],  
            "AssociatePublicIpAddress": true  
        }  
    ],  
    "IamInstanceProfile": {  
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
    }  
}
```

竞价型队列请求

Abstract

创建竞价型队列请求，为您的竞价型实例指定启动配置，包括您愿意支付的每单位小时的价格。

要使用竞价型队列，您需要创建一个竞价型队列请求，该请求包括目标容量、实例的一个或多个启动说明以及您的出价。当出价发生更改时，Amazon EC2 将尝试维护您的竞价型队列的目标容量。有关更多信息，请参阅 [竞价型队列的工作方式 \(p. 165\)](#)。

您可以创建竞价型队列，以针对所需容量提交一次性 `request`，或者要求其随着时间的推移 `maintain` 目标容量。两种请求类型都可以使用竞价型队列的分配策略。

当您 `request` 目标容量时，竞价型队列会根据需要出价，但在容量减少时，不会尝试补充竞价型实例。如果容量不可用，竞价型队列不会在其他竞价池中提交出价。

如果您要 `maintain` 目标容量，竞价型队列会根据需要提交出价以满足目标容量，并自动补充任何中断的实例。默认情况下，竞价型队列设置为 `maintain` 请求的目标容量。

提交一次性 `request` 后，其目标容量则无法修改。要更改目标容量，请取消请求并重新提交新请求。

竞价型队列请求在过期或您取消它之前保持有效。取消竞价型队列请求时，您可以指定取消竞价型队列请求是否会终止您竞价型队列中的竞价型实例。

每个启动说明包括 Amazon EC2 启动实例所需的信息 – 例如 AMI、实例类型、子网或可用区、一个或多个安全组。

内容

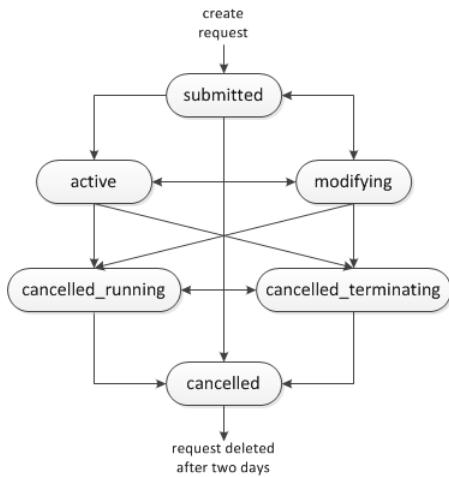
- [竞价型队列请求状态 \(p. 177\)](#)
- [竞价型队列先决条件 \(p. 178\)](#)
- [竞价型队列和 IAM 用户 \(p. 178\)](#)
- [规划竞价型队列请求 \(p. 179\)](#)
- [创建竞价型队列请求 \(p. 179\)](#)
- [监控您的竞价型队列 \(p. 181\)](#)
- [修改竞价型队列请求 \(p. 181\)](#)
- [取消竞价型队列请求 \(p. 182\)](#)
- [竞价型队列示例配置 \(p. 183\)](#)

竞价型队列请求状态

竞价型队列请求可以处于以下某种状态：

- `submitted` - 正在评估竞价型队列请求，并且 Amazon EC2 正准备启动目标数量的竞价型实例。
- `active` - 已验证竞价型队列，并且 Amazon EC2 正在尝试维持目标数量的正在运行的竞价型实例。请求会保持这一状态，直到其被修改或取消。
- `modifying` - 正在修改竞价型队列请求。请求会保持这一状态，直到修改全部完成或竞价型队列被取消。无法修改一次性 `request`，并且这一状态不适用于此类竞价请求。
- `cancelled_running` - 竞价型队列已取消且不会启动其他竞价型实例，但其现有的竞价型实例将继续运行，直到其被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。
- `cancelled_terminating` - 竞价型队列已取消，且其竞价型实例正在终止。请求会保持此状态，直到所有实例都已终止。
- `cancelled` - 竞价型队列已取消，且没有正在运行的竞价型实例。竞价型队列请求将在其实例终止两天后被删除。

以下显示了请求状态之间的转换。请注意，如果您超出了竞价型队列的限制，则请求会被立即取消。



竞价型队列先决条件

如果您使用 AWS 管理控制台创建竞价型队列，则该队列会创建一个命名为 `aws-ec2-spot-fleet-role` 的角色（该角色会授予竞价型队列代表您出价、启动和终止实例的权限），并在您的竞价型队列请求中指定该队列。如果您使用 AWS CLI 或 API 创建竞价型队列，则可以使用该角色（如果存在）或按以下步骤手动创建您自己的角色。

使用 AmazonEC2SpotFleetRole 策略手动创建 IAM 角色

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
 2. 在导航窗格中选择 Roles，然后选择 Create New Role。
 3. 在 Set Role Name 页面上，请键入角色名称，然后选择 Next Step。
 4. 在 Select Role Type 页面上，选择 Amazon EC2 Spot Fleet Role 旁的 Select。
 5. 在 Attach Policy 页面上，选择 AmazonEC2SpotFleetRole 策略，然后选择 Next Step。
 6. 在 Review 页面上，选择 Create Role。

竞价型队列和 IAM 用户

如果 IAM 用户将创建或管理竞价型队列，请确保授予他们所需的权限，如下所示。

授予 IAM 用户竞价型队列的权限

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
 2. 在导航窗格中选择 Policies，然后选择 Create Policy。
 3. 在 Create Policy 页上，选择 Create Your Own Policy 旁的 Select。
 4. 在 Review Policy 页上，输入策略名称并将以下文本复制到 Policy Document 部分。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam:PassRole",  
        "iam>ListRoles",  
        "iam>ListInstanceProfiles"  
    ],  
    "Resource": "*"  
}  
]  
}
```

ec2:* 使 IAM 用户能够调用所有 Amazon EC2 API 操作。要将用户限制到特定 API 操作，请改为指定这些操作。

iam:PassRole 操作使用户能够在竞价型队列请求中指定竞价型实例角色。iam>ListRoles 操作使用户能够枚举现有角色。iam>ListInstanceProfiles 操作使用户能够枚举现有实例配置文件。Amazon EC2 控制台使用 iam>ListRoles 填充 IAM role 列表，使用 iam>ListInstanceProfiles 填充 IAM instance profile 列表。要使用户能够通过控制台来创建角色或实例配置文件，您必须添加以下操作：iam>CreateRole、iam>CreateInstanceProfile 和 iam>AddRoleToInstanceProfile。

5. 选择 Create Policy。
6. 在导航窗格中选择 Users，然后选择将提交竞价型队列请求的用户。
7. 在 Permissions 选项卡上，选择 Attach Policy。
8. 在 Attach Policy 页上，选择您在上面创建的策略，然后选择 Attach Policy。

规划竞价型队列请求

在创建竞价型队列请求前，请查看[竞价最佳实践](#)。使用这些最佳实践规划您的竞价型队列请求，以便以可能的最低价格配置需要的实例类型。还建议执行以下操作：

- 确定您要创建的竞价型队列是针对所需目标容量提交一次性 request，还是随着时间推移 maintain 目标容量。
- 确定满足您的应用程序要求的实例类型。
- 确定您的竞价型队列请求的目标容量。您可以采用实例或自定义单位设置目标容量。有关更多信息，请参阅[竞价型队列实例权重 \(p. 166\)](#)。
- 确定每实例小时出价。出价较低能够进一步降低成本，而出价较高则可以降低中断发生的可能性。
- 如果您在使用实例权重，请确定您的每单位现货价格。要计算每单位出价，请将每实例小时出价除以该实例表示的单位数（或权重）。（如果不使用实例权重，则默认的每单位出价是每实例小时出价。）
- 查看用于您的竞价型队列请求的可能选项。关于更多信息，请参阅 AWS Command Line Interface Reference 中的 request-spot-fleet 命令。有关其他示例，请参阅[竞价型队列示例配置 \(p. 183\)](#)。

创建竞价型队列请求

创建竞价型队列请求时，您必须指定有关要启动的竞价型实例的信息（例如实例类型和现货价格）。

使用控制台创建竞价型队列请求

1. 在 <https://console.amazonaws.cn/ec2spot> 处打开竞价控制台。
2. 如果您是首次接触竞价，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot Instances。
3. 在 Find instance types 页面中，执行以下操作：

- a. 对于 Request type , 请选择 Request 或 Request and Maintain。
 - b. 对于 Target capacity , 输入要请求的单位数量。您可以选择实例或是对应用程序工作负载十分重要的性能特征 (如 vCPU、内存和存储)。
 - c. 对于 AMI , 选择由 AWS 提供的基础 Amazon 系统映像 (AMI) 之一 , 或者选择 Use custom AMI 以使用来自我们用户社区的 AMI、AWS Marketplace 或您自己的 AMI 之一。
 - d. 对于 Instance type(s) , 请选择 Select。选择具有您所需最低硬件规格的实例类型 (虚拟 CPU、内存和存储)。
 - e. 对于 Allocation strategy , 选择满足您的需求的策略。有关更多信息 , 请参阅 [竞价型队列分配策略 \(p. 165\)](#)。
 - f. 对于 Network , 您的账户可能支持 EC2-Classic 和 EC2-VPC 平台 , 或者仅支持 EC2-VPC 平台。要查明您的账户支持的平台 , 请参阅 [支持的平台 \(p. 577\)](#)。
 - [现有 VPC] 选择 VPC。
 - [新 VPC] 选择 Create new VPC 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。
 - [EC2-Classic] 选择 EC2-Classic。
 - g. (可选) 对于 Availability Zones , 默认由 AWS 为您的竞价型实例选择可用区。如果您想使用特定可用区 , 请执行以下操作 :
 - [EC2-VPC] 选择一个或多个可用区。如果您在一个可用区中有多个子网 , 则请从 Subnet 中选择合适的子网。要添加子网 , 请选择 Create new subnet 以前往 Amazon VPC 控制台。完成之后 , 请返回向导并刷新列表。
 - [EC2-Classic] 选择 Select specific zone/subnet , 然后选择一个或多个可用区。
 - h. 对于 Maximum price , 您可以使用自动出价 , 也可以指定一个出价。如果您的出价低于所选实例类型的现货价格 , 则您的竞价型实例不会启动。
 - i. 选择 Next。
4. 在 Configure (配置实例详细信息) 页面中 , 执行以下操作 :
 - a. (可选) 如果您需要连接到您的实例 , 请使用 Key pair name 指定您的密钥对。
 - b. (可选) 如果您需要启动带有 IAM 角色的竞价型实例 , 请使用 IAM instance profile 指定角色。
 - c. (可选) 如果您要运行任何启动脚本 , 请使用 User data 指定脚本。
 - d. 对于 Security groups , 选择一个或多个安全组。
 - e. [EC2-VPC] 如果您需要连接到您在 VPC 中的实例 , 对于 Public IP , 请选择 auto-assign at launch。
 - f. 默认情况下 , 请求在被执行或被您取消之前保持有效。要创建仅在特定时段内有效的请求 , 请编辑 Request valid from 和 Request valid to。
 - g. (可选) 默认情况下 , 我们会在请求过期时终止您的竞价型实例。要维持实例在请求过期之后继续运行 , 请清除 Terminate instances at expiration。
 - h. 选择 Review。
 5. 在 Review 页面上 , 确认启动配置。要进行更改 , 请选择 Previous。要下载启动配置的副本以便与 AWS CLI 结合使用 , 请选择 JSON config。如果准备就绪 , 请选择 Launch。
 6. 在确认页面上 , 请选择 OK。请求类型为 fleet。执行请求后 , 系统会添加请求类型 instance , 此时其状态为 active 和 fulfilled。

使用 AWS CLI 创建竞价型队列请求

使用以下 `request-spot-fleet` 命令可创建竞价型队列请求 :

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关示例配置文件，请参阅 [竞价型队列示例配置 \(p. 183\)](#)。

下面是示例输出：

```
{  
    "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

监控您的竞价型队列

当现货价格低于您的出价时，竞价型队列会启动竞价型实例。竞价型实例将会运行，直到出价不再高于现货价格或您自己终止了它们。

使用控制台监控您的竞价型队列

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的竞价型队列请求。配置详细信息在 Description 选项卡中提供。
4. 要列出竞价型队列的竞价型实例，请选择 Instances 选项卡。
5. 要查看竞价型队列的历史记录，请选择 History 选项卡。

使用 AWS CLI 监控您的竞价型队列

使用以下 [describe-spot-fleet-requests](#) 命令可描述竞价型队列请求：

```
aws ec2 describe-spot-fleet-requests
```

使用以下 [describe-spot-fleet-instances](#) 命令可描述指定竞价型队列的竞价型实例：

```
aws ec2 describe-spot-fleet-instances --spot-fleet-request-id sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE
```

使用以下 [describe-spot-fleet-request-history](#) 命令可描述指定竞价型队列请求的历史记录：

```
aws ec2 describe-spot-fleet-request-history --spot-fleet-request-id sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2015-05-18T00:00:00Z
```

修改竞价型队列请求

您可以修改活动的竞价型队列请求以完成以下任务：

- 提升目标容量
- 减少目标容量



Note

竞价型队列 request 无法修改。

当您提升目标容量时，竞价型队列会根据其竞价型队列请求的分配策略来启动额外的竞价型实例。如果分配策略是 `lowestPrice`，则竞价型队列从竞价型队列请求中价格最低的竞价型实例池启动实例。如果分配策略是 `diversified`，则竞价型队列在竞价型队列请求中的池间分配实例。

当您减少目标容量时，竞价型队列会取消任何超过新目标容量的开放出价。您可以请求竞价型队列终止竞价型实例，直到队列的大小达到新目标容量。如果分配策略是 `lowestPrice`，则竞价型队列会终止每单位价格最高的实例。如果分配策略是 `diversified`，则竞价型队列会在池间终止实例。或者，您可以请求竞价型队列保持当前的队列大小，而不替换已中断或您手动终止的任何竞价型实例。

使用控制台修改竞价型队列请求

1. 在 <https://console.amazonaws.cn/ec2spot/home/fleet> 处打开竞价控制台。
2. 选择您的竞价型队列请求。
3. 选择 Actions，然后选择 Modify target capacity。
4. 在 Modify target capacity 中，执行以下操作：
 - a. 输入新的目标容量。
 - b. (可选) 如果您要减少目标容量，但是要使队列保持其当前大小，请取消选择 Terminate instances。
 - c. 选择 Submit。

使用 AWS CLI 修改竞价型队列请求

使用以下 `modify-spot-fleet-request` 命令可更新指定竞价型队列请求的目标容量：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 20
```

您可以按如下所示修改前面的命令，以减少指定竞价型队列的目标容量而不因此终止任何竞价型实例：

```
aws ec2 modify-spot-fleet-request --spot-fleet-request-id sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity 10 --excess-capacity-termination-policy NoTermination
```

取消竞价型队列请求

在使用完竞价型队列后，可以取消竞价型队列请求。这将取消与竞价型队列关联的所有竞价请求，从而不会为您的竞价型队列启动任何新的竞价型实例。您必须指定竞价型队列是否应终止其竞价型实例。如果您终止实例，则竞价型队列请求会进入 `cancelled_terminating` 状态。否则，竞价型队列请求会进入 `cancelled_running` 状态，并且实例会继续运行，直到它们中断或您手动终止它们。

使用控制台取消竞价型队列请求

1. 在 <https://console.amazonaws.cn/ec2spot/home/fleet> 处打开竞价控制台。
2. 选择您的竞价型队列请求。
3. 选择 Actions，然后选择 Cancel spot request。
4. 在 Cancel spot request 中，确认是否要取消竞价型队列。要使队列保持其当前大小，请取消选择 Terminate instances。如果准备就绪，请选择 Confirm。

使用 AWS CLI 取消竞价型队列请求

使用以下 `cancel-spot-fleet-requests` 命令可取消指定的竞价型队列请求并终止实例：

```
aws ec2 cancel-spot-fleet-requests --spot-fleet-request-ids sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --terminate-instances
```

下面是示例输出：

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE",  
            "CurrentSpotFleetRequestState": "cancelled_terminating",  
            "PreviousSpotFleetRequestState": "active"  
        }  
    ],  
    "UnsuccessfulFleetRequests": []  
}
```

可以按如下所示修改前面的命令，以取消指定的竞价型队列请求而不终止实例：

```
aws ec2 cancel-spot-fleet-requests --spot-fleet-request-ids sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --no-terminate-instances
```

下面是示例输出：

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE",  
            "CurrentSpotFleetRequestState": "cancelled_running",  
            "PreviousSpotFleetRequestState": "active"  
        }  
    ],  
    "UnsuccessfulFleetRequests": []  
}
```

竞价型队列示例配置

Abstract

了解如何为您的竞价型队列请求创建启动配置。

下列示例显示了可与 [request-spot-fleet](#) 命令结合使用以创建竞价型队列请求的启动配置。有关更多信息，请参阅 [创建竞价型队列请求 \(p. 179\)](#)。

1. 使用区域中价格最低的可用区或子网启动竞价型实例 ([p. 183](#))
2. 使用指定列表中价格最低的可用区或子网启动竞价型实例 ([p. 184](#))
3. 使用指定列表中价格最低的实例类型启动竞价型实例 ([p. 185](#))
4. 覆盖请求的现货价格 ([p. 187](#))
5. 使用多样化分配策略启动竞价型队列 ([p. 188](#))
6. 使用实例权重启动竞价型队列 ([p. 189](#))

示例 1：使用区域中价格最低的可用区或子网启动竞价型实例

以下示例指定一个没有可用区或子网的启动说明。如果您的账户仅支持 EC2-VPC，则竞价型队列会在具有默认子网的价格最低的可用区中启动实例。如果您的账户支持 EC2-Classic，则竞价型队列会在价格最低的可用区的 EC2-Classic 中启动实例。请注意，您支付的价格不会超过为请求指定的现货价格。

```
{  
    "SpotPrice": "0.07",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

示例 2：使用指定列表中价格最低的可用区或子网启动竞价型实例

以下示例指定具有的可用区或子网不同但实例类型和 AMI 相同的两种启动说明。

可用区

如果您的账户仅支持 EC2-VPC，则竞价型队列会在您指定的价格最低的可用区的默认子网中启动实例。如果您的账户支持 EC2-Classic，则竞价型队列会在您指定的价格最低的可用区中启动实例。

```
{  
    "SpotPrice": "0.07",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "Placement": {  
                "AvailabilityZone": "us-west-2a, us-west-2b"  
            },  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

Subnets

您可以指定默认子网或非默认子网，并且非默认子网可来自默认 VPC 或非默认 VPC。竞价服务会在位于价格最低的可用区的子网中启动实例。

请注意，您无法在竞价型队列请求中指定来自相同可用区的不同子网。

```
{  
    "SpotPrice": "0.07",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

如果在默认 VPC 中启动实例，则默认情况下它们会收到一个公有 IP 地址。如果在非默认 VPC 中启动实例，则默认情况下它们不会收到一个公有 IP 地址。在启动说明中使用网络接口来将一个公有 IP 地址分配给在非默认 VPC 中启动的实例。请注意，在指定一个网络接口时，您必须使用该网络接口包含子网 ID 和安全组 ID。

```
...  
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "InstanceType": "m3.medium",  
    "NetworkInterfaces": [  
        {  
            "DeviceIndex": 0,  
            "SubnetId": "subnet-1a2b3c4d",  
            "Groups": [ "sg-1a2b3c4d" ],  
            "AssociatePublicIpAddress": true  
        }  
    ],  
    "IamInstanceProfile": {  
        "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"  
    }  
}  
...
```

示例 3：使用指定列表中价格最低的实例类型启动竞价型实例

以下示例指定实例类型不同、但 AMI 和可用区或子网相同的两种启动配置。竞价型队列使用价格最低的指定实例类型启动实例。

可用区域

```
{  
    "SpotPrice": "2.80",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        }  
    ]  
}
```

子网

```
{  
    "SpotPrice": "2.80",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

```
        "SubnetId": "subnet-1a2b3c4d"
    }
}
}
```

示例 4. 覆盖请求的现货价格

通过为单个启动说明指定现货价格的功能，您可对出价过程进行更多控制。以下示例使用三个启动说明中的两个启动说明单独使用的现货价格来覆盖请求的现货价格 (0.070)。请注意，请求的现货价格用于未单独指定现货价格的任何启动说明。竞价型队列使用价格最低的实例类型启动实例。

可用区域

```
{
    "SpotPrice": "1.68",
    "TargetCapacity": 30,
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "SpotPrice": "0.04"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "SpotPrice": "0.06"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

子网

```
{
    "SpotPrice": "1.68",
    "TargetCapacity": 30,
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.04"
        }
    ]
}
```

```
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.06"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

示例 5：使用多样化分配策略启动竞价型队列

以下示例使用 `diversified` 分配策略。启动说明具有不同的实例类型，但具有相同的 AMI 和可用区或子网。竞价型队列在 3 个启动说明间分配 30 个实例，每种类型 10 个实例。有关更多信息，请参阅 [竞价型队列分配策略 \(p. 165\)](#)。

可用区域

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

子网

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

示例 6：使用实例权重启动竞价型队列

以下示例使用实例权重，这意味着出价是每单位小时出价而不是每实例小时出价。每个启动配置列出不同的实例类型和不同的权重。竞价型队列选择每单位小时价格最低的实例类型。竞价型队列通过将目标容量除以实例权重来计算要启动的竞价型实例数。如果结果不是整数，则竞价型队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。

如果 r3.2xlarge 出价成功，竞价将预置 4 个这类实例。（将 20 除以 6 可得到总共 3.33 个实例，然后向上舍入为 4 个实例。）

如果 c3.xlarge 出价成功，竞价将预置 7 个这类实例。（将 20 除以 3 可得到总共 6.66 个实例，然后向上舍入为 7 个实例。）

有关更多信息，请参阅 [竞价型队列实例权重 \(p. 166\)](#)。

可用区域

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "WeightedCapacity": 6  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2a"  
            },  
            "WeightedCapacity": 14  
        }  
    ]  
}
```

```
        "Placement": {
            "AvailabilityZone": "us-west-2b"
        },
        "WeightedCapacity": 3
    }
}
```

子网

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 20,
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 6
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 3
        }
    ]
}
```

优先级

您也可以使用实例权重为可用区或子网指定优先级。例如，以下启动说明几乎完全相同，只是指定了不同的子网和权重。竞价型队列会查找具有最高 WeightedCapacity 值的说明，并尝试在相应子网中价格最低的竞价型实例池中为请求预置资源。（请注意，第二个启动说明不包含权重，因此其默认为 1。）

```
{
    "SpotPrice": "0.42",
    "TargetCapacity": 40,
    "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.2xlarge",
            "SubnetId": "subnet-482e4972",
            "WeightedCapacity": 2
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.2xlarge",
            "SubnetId": "subnet-bb3337d"
        }
    ]
}
```

竞价型队列的 CloudWatch 指标

Abstract

了解 Amazon EC2 为竞价型队列提供的 CloudWatch 指标。

Amazon EC2 提供了可用来监控竞价型队列的 Amazon CloudWatch 指标。



Important

为确保准确性，我们建议您在使用这些指标时启用详细监控。有关更多信息，请参阅[对您的实例启用或禁用详细监控 \(p. 452\)](#)。

有关 Amazon EC2 提供的 CloudWatch 指标的详细信息，请参阅[使用 CloudWatch 监控您的实例 \(p. 452\)](#)。

竞价型队列指标

AWS/EC2Spot 命名空间包含以下指标以及针对队列中的竞价型实例的 CloudWatch 指标。有关更多信息，请参阅[实例指标 \(p. 454\)](#)。

指标	说明
AvailableInstance-PoolsCount	竞价型队列请求中指定的竞价型实例池。 单位：计数
BidsSubmittedForCapacity	Amazon EC2 已提交竞价的容量。 单位：计数
EligibleInstancePoolCount	在 Amazon EC2 可以完成出价的竞价型队列请求中指定的竞价型实例池。在您的出价低于现货价格或者现货价格高于按需实例价格的池中，Amazon EC2 不会完成出价。 单位：计数
FulfilledCapacity	Amazon EC2 已执行的容量。 单位：计数
MaxPercentCapacityAllocation	在竞价型队列请求中指定的所有竞价实例池中的 PercentCapacityAllocation 最大值。 单位：百分比
PendingCapacity	TargetCapacity 与 FulfilledCapacity 之间的区别。 单位：计数
PercentCapacityAllocation	针对所指定维度的竞价型实例池分配的容量。要获取所有竞价型实例池中记录的最大值，请使用 MaxPercentCapacityAllocation。 单位：百分比
TargetCapacity	竞价型队列请求的目标容量。 单位：计数

指标	说明
TerminatingCapacity	由于竞价型实例中断而正终止使用的容量。
	单位：计数

如果指标的度量单位是 Count，则最有用的统计信息是 Average。

竞价型队列维度

要筛选竞价型队列的数据，可使用以下维度。

维度	描述
AvailabilityZone	按照可用区筛选数据。
FleetRequestId	按照竞价型队列请求筛选数据。
InstanceType	按实例类型筛选数据。

查看竞价型队列的 CloudWatch 指标

可使用 Amazon CloudWatch 控制台查看竞价型队列的 CloudWatch 指标。这些指标显示为监控图表。如果竞价型队列处于活动状态，这些图表会显示数据点。

指标首先按命名空间进行分组，然后按各命名空间内的各种维度组合进行分组。例如，您可以按竞价型队列请求 ID、实例类型或可用区来查看所有竞价型队列指标或竞价型队列指标组。

查看竞价型队列指标

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 在导航窗格中，在 Metrics 下，选择 EC2 Spot 命名空间。
3. (可选) 要按维度筛选指标，请选择下列选项之一：
 - Fleet Request Metrics - 按竞价型队列请求分组
 - By Availability Zone - 按竞价型队列请求和可用区分组
 - By Instance Type - 按竞价型队列请求和实例类型分组
 - By Availability Zone/Instance Type - 按竞价型队列请求、可用区和实例类型分组
4. 要查看指标的数据，请选中指标旁边的复选框。

The screenshot shows the AWS CloudWatch Metrics search interface. At the top, there's a search bar with 'Search Metrics' and a dropdown set to 'EC2 Spot'. Below the search bar, there 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 says '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 message: 'Select All' and 'Clear'. Below this, there's a table header 'EC2 Spot > Fleet Request Metrics' with columns 'Metric Name' and 'FleetRequestId'. The table lists 18 metrics, each with a checkbox next to it. One metric, 'CPUUtilization', has its checkbox checked. Other metrics listed include 'AvailableInstancePoolsCount', 'BidsSubmittedForCapacity', and 'DiskReadBytes'. The metrics are listed in descending order of creation date.

竞价出价状态

Abstract

使用出价状态来跟踪您的竞价型实例请求。

为帮助您跟踪竞价型实例请求、计划对竞价型实例的使用，以及有策略地进行出价，Amazon EC2 提供了出价状态。例如，出价状态会帮助您了解竞价请求尚未完成的原因或列出会阻碍竞价请求完成的限制。

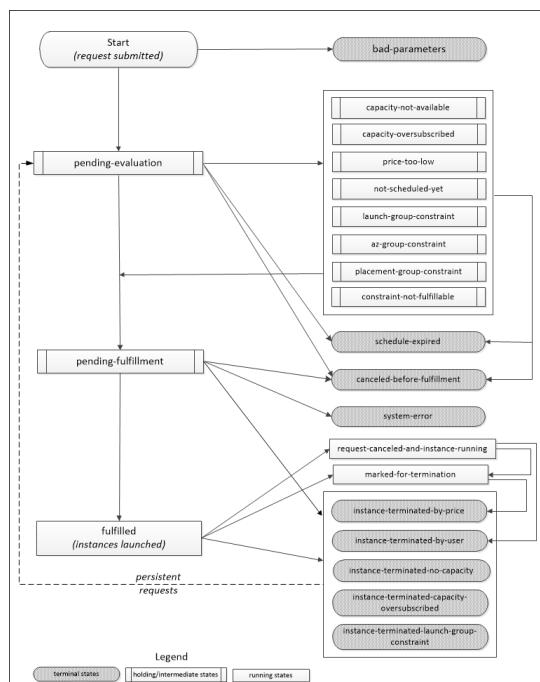
在此过程（也称为竞价请求生命周期）中的每一步，都有特定的事件确定连续的请求状态。

内容

- 竞价请求的生命周期 (p. 193)
- 获取出价状态信息 (p. 195)
- 竞价出价状态代码 (p. 196)

竞价请求的生命周期

以下图表显示您的竞价请求在其整个生命周期中从提交到终止所遵循的路径。每个步骤用节点表示，每个节点状态代码描述您的竞价请求和竞价型实例的状态。



待评估

当您提交竞价型实例请求之后，除非一个或多个请求参数无效 (bad-parameters)，否则就会进入 pending-evaluation 状态。

状态代码	请求状态	实例状态
pending-evaluation	open	无
bad-parameters	closed	无

备用

如果一个或多个请求约束有效但目前无法满足，或者如果没有足够的容量，那么请求将进入备用状态，等待满足约束。请求选项影响请求完成的可能性。例如，如果您指定的出价低于当前现货价格，您的请求将保持为备用状态，直至现货价格低于您的出价。如果您指定了可用区组，则该请求将保持为备用状态，直至满足可用区的约束。

状态代码	请求状态	实例状态
capacity-not-available	open	无
capacity-oversubscribed	open	无
price-too-low	open	无
not-scheduled-yet	open	无
launch-group-constraint	open	无
az-group-constraint	open	无
placement-group-constraint	open	无
constraint-not-fulfillable	open	无

等待评估/最终执行

您的竞价型实例在以下几种情况下可能进入 terminal 状态：您创建的请求仅在特定时段内有效，但该时段在您的请求到达等待执行阶段之前过期；您取消了请求；或者，出现系统错误。

状态代码	请求状态	实例状态
schedule-expired	closed	无
canceled-before-fulfillment*	cancelled	无
bad-parameters	failed	无
system-error	closed	无

* 如果您取消请求。

等待履行

当您指定的约束（如果有）得到满足且您的出价等于或高于当前现货价格时，您的竞价请求会进入 pending-fulfillment 状态。

此时，Amazon EC2 已经准备好为您预置您请求的实例。如果此进程在此时停止，则可能是因为用户在竞价型实例启动之前取消了请求，或者是因为出现了意外的系统错误。

状态代码	请求状态	实例状态
pending-fulfillment	open	无

已完成

当您的竞价型实例的所有规格都得到满足时，您的竞价请求将会执行。Amazon EC2 会启动竞价型实例，这可能需要几分钟时间。

状态代码	请求状态	实例状态
fulfilled	active	pending → running

执行的最终

只要您的出价等于或高于现货价格，您的实例类型拥有备用竞价容量，且您没有终止您的竞价型实例，实例就会继续运行。如果现货价格或可用容量的变化要求 Amazon EC2 终止您的竞价型实例，竞价请求将转入最终状态。例如，如果您的出价等于现货价格，但是在该价格对竞价型实例的订阅过多，那么状态代码为 `instance-terminated-capacity-oversubscribed`。如果您取消竞价请求或终止竞价型实例，请求也将进入最终状态。

状态代码	请求状态	实例状态
<code>request-canceled-and-instance-running</code>	<code>cancelled</code>	<code>running</code>
<code>marked-for-termination</code>	<code>closed</code>	<code>running</code>
<code>instance-terminated-by-price</code>	<code>closed</code> (一次性), <code>open</code> (持久性)	<code>terminated</code>
<code>instance-terminated-by-user</code>	<code>closed</code> 或者 <code>cancelled</code> *	<code>terminated</code>
<code>instance-terminated-no-capacity</code>	<code>closed</code> (一次性), <code>open</code> (持久性)	<code>terminated</code>
<code>instance-terminated-capacity-oversubscribed</code>	<code>closed</code> (一次性), <code>open</code> (持久性)	<code>terminated</code>
<code>instance-terminated-launch-group-constraint</code>	<code>closed</code> (一次性), <code>open</code> (持久性)	<code>terminated</code>

* 如果您终止实例但未取消出价，则请求状态为 `closed`。如果您终止实例并取消出价，则请求状态为 `cancelled`。请注意，即使您在取消实例请求之前终止了竞价型实例，在 Amazon EC2 检测到您的竞价型实例已终止之前仍可能存在延迟。在这种情况下，请求状态可能是 `closed` 或 `cancelled`。

持久性请求：

当您的竞价型实例终止时（由您或由 Amazon EC2），如果竞价请求为持久性请求，则该请求返回 `pending-evaluation` 状态，并且在满足约束时，Amazon EC2 可以启动新的竞价型实例。

获取出价状态信息

您可以使用 AWS 管理控制台或命令行工具获取出价状态信息。

使用控制台获取出价状态信息

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，请选择 Spot Requests，然后选择竞价请求。
3. 在 Description (描述) 选项卡中检查 Status (状态) 的值。

使用命令行获取出价状态信息

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

- [describe-spot-instance-requests](#) (AWS CLI)
- [Get-EC2SpotInstanceRequest](#) (适用于 Windows PowerShell 的 AWS 工具)

竞价出价状态代码

竞价出价状态信息包括出价状态代码、更新时间和状态消息。同时，它们还帮助您决定竞价请求的处置。

以下列表描述了竞价出价状态代码：

- az-group-constraint**
Amazon EC2 无法在同一可用区中启动您请求的所有实例。
- bad-parameters**
您的竞价请求的一个或多个参数无效（例如，您指定的 AMI 不存在）。出价状态消息指示哪个参数无效。
- cancelled-before-fulfillment**
用户在请求执行前取消了竞价请求。
- capacity-not-available**
您请求的实例没有足够的容量可用。
- capacity-oversubscribed**
现货价格等于或高于您出价的竞价请求数量超过了此竞价型实例池的可用容量。
- constraint-not-fulfillable**
由于一个或多个约束无效（例如，可用区不存在），竞价请求无法完成。出价状态消息指示哪个约束无效。
- fulfilled**
竞价请求处于 `active` 状态，Amazon EC2 正在启动您的竞价型实例。
- instance-terminated-by-price**
现货价格超过您的出价。如果请求是一个持久性出价，过程会重新启动，因此，您的出价等待评估。
- instance-terminated-by-user 或者 spot-instance-terminated-by-user**
您终止了已完成的竞价型实例，因此出价状态会变成 `closed`（持久性出价除外），实例状态为 `terminated`。
- instance-terminated-capacity-oversubscribed**
因为现货价格等于或高于您的出价的竞价请求数量已超出此竞价型实例池的可用容量，您的实例已被终止。（请注意，现货价格可能未更改。）竞价服务随机选择要终止的实例。
- instance-terminated-launch-group-constraint**
您的启动组中的一个或多个实例已终止，因此不再满足启动组的约束。
- instance-terminated-no-capacity**
此实例不再有足够的竞价容量可用。
- launch-group-constraint**
Amazon EC2 无法同时启动您请求的所有实例。启动组内的所有实例都一起启动和终止。
- marked-for-termination**
您的竞价型实例被标记为终止。
- not-scheduled-yet**
您的竞价请求在指定日期之前不会被评估。
- pending-evaluation**
当您提交竞价型实例请求之后，该请求会进入 `pending-evaluation` 状态，同时系统会评估您的请求中的参数。
- pending-fulfillment**
Amazon EC2 尝试预置您的竞价型实例。

placement-group-constraint

因为竞价型实例目前不能添加到置放群组中，因此尚无法完成竞价请求。

price-too-low

由于出价低于现货价格，尚无法执行出价请求。在这种情况下，没有实例启动且您的出价保持 open。

request-cancelled-and-instance-running

在竞价型实例仍在运行时，您取消了竞价请求。请求为 cancelled，但是，实例保持为 running。

schedule-expired

由于没有在指定日期前完成，竞价请求已过期。

system-error

出现意外系统错误。如果这是反复出现的问题，请联系客户支持获得帮助。

竞价型实例中断

Abstract

了解如何准备您的应用程序来处理 Amazon EC2 终止您的竞价型实例的情况。

对竞价型实例的需求在不同时间可能有显著的差异，竞价型实例的可用性也会因为未使用 EC2 实例的数量而差别巨大。此外，不论您的出价有多高，您的竞价型实例仍有可能会中断。因此，必须确保应用程序针对竞价型实例中断做好准备。我们强烈建议您不要为不能中断的应用程序使用竞价型实例。

下面列出了 Amazon EC2 终止您的竞价型实例的可能原因：

- 价格 – 现货价格高于您的出价。
- 容量 – 如果没有足够的未用 EC2 实例来满足对竞价型实例的需求，Amazon EC2 将从出价最低的实例开始终止竞价型实例。如果多个竞价型实例的出价相同，则随机确定实例的终止顺序。
- 约束 - 如果您的请求包含约束，例如启动组或可用区组，那么，当不再满足约束条件时，这些竞价型实例将成组终止。

准备中断

下面提供了在您使用竞价型实例时可以遵循的最佳实践：

- 选择一个合理的出价。您的出价应该足够高，这样您的请求才有机会完成，但又不能高于您愿意支付的价格。这非常重要，因为在长时间供应不足的情况下，现货价格可能会在这段时间内居高不下，因为此时价格依据的是最高出价。我们强烈建议您的出价高于按需实例的价格。
- 使用包含所需软件配置的 Amazon 系统映像 (AMI)，确保您的实例在请求完成时随时可以启动。您还可以使用用户数据在启动时运行命令。
- 在不会受竞价型实例终止影响的位置例行存储重要数据。例如，您可以使用 Amazon S3、Amazon EBS 或 DynamoDB。
- 将工作拆分为小的任务（使用网格、Hadoop 或基于队列的架构）或者使用检查点，以便您经常保存工作。
- 使用竞价型实例终止通知监控您的竞价型实例的状态。
- 测试您的应用程序，确保它很好地处理了意外终止的实例。您可以使用按需实例来运行应用程序，然后自行终止该按需实例，以便确认这一点。

竞价型实例终止通知

防范竞价型实例中断的最佳方法是为应用程序设计容错能力。此外，您还可以利用竞价型实例终止通知，该通知可在 Amazon EC2 必须终止您的竞价型实例时，提前两分钟发出警告。

此警告使用实例元数据中的项目，提供给在您的竞价型实例上运行的应用程序。例如，您可以使用以下查询定期检查实例元数据中的此警告（建议每 5 秒检查一次）：

```
C:\> invoke-restmethod -uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

有关检索实例元数据的其他方式的信息，请参阅 [检索实例元数据 \(p. 239\)](#)。

如果 Amazon EC2 将您的竞价型实例标记为终止，将存在 `termination-time` 项目，该项目以 UTC 时间指定实例将收到关闭信号的大致时间。例如：

```
2015-01-05T18:02:00Z
```

如果 Amazon EC2 未准备终止实例，或者，如果您自己终止了竞价型实例，则 `termination-time` 项目或者不存在（这样您会收到 HTTP 404 错误），或者包含并非时间值的值。

请注意，虽然我们会尽力在 Amazon EC2 将您的竞价型实例标记为终止时提供此警告，您的竞价型实例仍可能会在 Amazon EC2 提供此警告之前终止。因此，您必须确保应用程序已经准备好处理意外的竞价型实例中断，即使您在监视竞价型实例终止通知的情况下也应如此。

如果 Amazon EC2 未能终止实例，则竞价出价状态将设置为 `fulfilled`。请注意，`termination-time` 会将实例元数据保持原始大致时间（现已成为过去时间）。

竞价型实例数据源

Abstract

订阅数据源以记录您的竞价型实例使用情况。

为了帮助您了解您的竞价型实例费用情况，Amazon EC2 通过提供的数据元说明您的竞价型实例的使用情况和定价。此数据源会发送到您在订阅数据源时指定的 Amazon S3 存储桶。

数据源文件一般一小时到达您的存储桶一次，且每小时使用量一般都包含在单个数据文件中。这些文件在传送到您的存储桶前要进行压缩 (gzip)。当文件很大时（例如，当一小时的文件内容在压缩前超过 50 MB 时），Amazon EC2 可以将给定小时的使用情况写入多个文件。



Note

如果在特定小时中没有竞价型实例运行，则您不会收到该小时的数据源文件。

内容

- [数据源文件名和格式 \(p. 198\)](#)
- [Amazon S3 存储桶要求 \(p. 199\)](#)
- [订阅您的竞价型实例数据源 \(p. 199\)](#)
- [删除您的竞价型实例数据源 \(p. 200\)](#)

数据源文件名和格式

竞价型实例数据源的文件名采用以下格式（用 UTC 日期和时间）：

```
bucket-name.s3.amazonaws.com/{optional prefix}/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

例如，如果您的存储桶名称为 `myawsbucket` 并且前缀为 `myprefix`，则您的文件名类似如下：

`myawsbucket.s3.amazonaws.com/myprefix/111122223333.2014-03-17-20.001.pwBdGTJG.gz`

竞价型实例数据源文件采用制表符分隔格式。数据文件的每一行都对应一小时实例使用时间，并且包含在下表中列出的字段。

字段	说明
Timestamp	使用时间戳来确定针对此一小时实例使用时间收取的费用。
UsageType	指示使用类型和被收取费用的实例类型。对于 m1.small 竞价型实例，此字段设置为 SpotUsage。对于所有其他实例类型，此字段设置为 SpotUsage:{instance-type}。例如：SpotUsage:c1.medium。
Operation	指示被收取费用的产品。对于 Linux 竞价型实例，此字段设置为 RunInstances。对于 Microsoft Windows 竞价型实例，此字段设置为 RunInstances:0002。竞价使用情况按照可用区分组。
InstanceID	生成此一小时实例使用时间的竞价型实例的 ID。
MyBidID	生成此一小时实例使用时间的竞价型实例请求的 ID。
MyMaxPrice	为此竞价型实例请求指定的最高价。
MarketPrice	在 Timestamp 字段中指定的时刻的现货价格。
Charge	此一小时实例使用时间的价格。
Version	此记录的数据源文件名中包含的版本。

Amazon S3 存储桶要求

在您订阅数据源时，必须指定 Amazon S3 存储桶来存储数据源文件。在为数据源选择 Amazon S3 存储桶之前，请考虑以下内容：

- 您必须使用来自 美国东部（弗吉尼亚北部）(us-east-1) 区域的存储桶。
- 您必须拥有存储桶的 FULL_CONTROL 权限。

如果您是存储桶所有者，根据默认情况，您有此权限。或者，存储桶拥有者必须授予您的 AWS 账户此权限。

- 当您创建您的数据源订阅时，Amazon S3 更新指定存储桶的 ACL，向 AWS 数据源账户提供读取和写入权限。
- 撤销数据源账户的权限不会禁用该数据源。如果您撤销这些权限但不禁用数据源，我们将在数据源账户下次需要写入存储桶时恢复这些权限。
- 每一个数据源文件都有其自己的 ACL（不同于存储桶的 ACL）。存储桶拥有者具有数据文件的 FULL_CONTROL 权限。数据源账户具有读取和写入权限。
- 如果您删除您的数据源订阅，Amazon EC2 不会撤销数据源账户在存储桶或数据文件上的读取和写入权限。您必须自行撤销这些权限。

订阅您的竞价型实例数据源

要订阅您的数据源，请使用以下 `create-spot-datafeed-subscription` 命令：

```
C:\> aws ec2 create-spot-datafeed-subscription --bucket myawsbucket [--prefix myprefix]
```

下面是示例输出：

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "111122223333",  
        "Prefix": "myprefix",  
        "Bucket": "myawsbucket",  
        "State": "Active"  
    }  
}
```

删除您的竞价型实例数据源

要删除数据源，请使用以下 [delete-spot-datafeed-subscription](#) 命令：

```
C:\> aws ec2 delete-spot-datafeed-subscription
```

竞价型实例限量

Abstract

了解竞价型实例的限制。

竞价型实例请求受以下限制的约束：

限制

- [不支持的实例类型 \(p. 200\)](#)
- [竞价请求限制 \(p. 200\)](#)
- [竞价出价限制 \(p. 201\)](#)
- [竞价型队列限制 \(p. 201\)](#)
- [不支持的 Amazon EBS 加密 \(p. 201\)](#)

不支持的实例类型

竞价不支持以下实例类型：

- T2
- HS1

一些竞价型实例类型并非在所有区域均可用。要查看某个区域支持的实例类型，请转至[竞价型实例定价](#)并选择区域。

竞价请求限制

默认情况下，每个区域的账户限制为 20 个竞价型实例。如果您终止了竞价型实例，但没有取消请求，那么您请求的次数会算在此限制内，直到 Amazon EC2 检测到终止情况并关闭您的请求为止。

竞价型实例限制是动态的。如果您的账户是新账户，那么您的限制在开始时可能会低于 20，不过随着时间的推移会逐渐增加。此外，您的账户对特定竞价型实例类型可能存在一些限制。如果您提交竞价型实例请求，并且收到错误 `Max spot instance count exceeded`，您可以转到[AWS 支持中心](#)并提交限额提升申请表。对于 Use Case Description，请指出您需要提升您的竞价型实例请求限制。

竞价出价限制

竞价型实例的出价限制为按需价格的十倍。此限制旨在保护您免于产生额外费用。

竞价型队列限制

通用 Amazon EC2 限制（例如，竞价出价限制、实例限制和卷限制）适用于竞价型队列所启动的实例。此外，以下限制将适用：

- 每个区域的活动竞价型队列数：1000
- 每个队列的启动说明数：50
- 启动说明中的用户数据大小：16 KB
- 每个竞价型队列的目标容量：3000
- 跨区域中所有竞价型队列的目标容量：5000
- 竞价型队列请求不能跨区域。
- 竞价型队列请求不能跨同一可用区内的不同子网。

不支持的 Amazon EBS 加密

您可以在竞价型实例的启动说明中指定加密的 EBS 卷，但这些卷未加密。

专用主机

Abstract

专用主机是被物理隔离的 Amazon EC2 服务器，支持自带许可和合规性使用案例。

Amazon EC2 专用主机是指 EC2 实例容量完全供您专用的物理服务器。专用主机允许您使用现有的按套接字、按内核或按 VM 软件授权的许可证，包括 Microsoft Windows Server、Microsoft SQL Server、SUSE、Linux Enterprise Server 等。

内容

- [专用主机与专用实例之间的区别 \(p. 201\)](#)
- [定价和记账 \(p. 202\)](#)
- [专用主机的限制 \(p. 203\)](#)
- [专用主机配置 \(p. 204\)](#)
- [支持的实例类型 \(p. 204\)](#)
- [使用专用主机 \(p. 205\)](#)
- [监控专用主机 \(p. 213\)](#)

专用主机与专用实例之间的区别

Abstract

比较专用主机与专用实例。

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、安全性或物理方面没有区别。但是，专用主机可让您更清楚地了解和更有力地控制在物理服务器上放置实例的方式。

使用专用主机时，您可以使用“主机关联”和“实例自动放置”设置控制实例在主机上的放置。使用专用实例时，您无法控制实例在哪个主机上启动和运行。如果您的组织希望使用 AWS，但现有软件许可证具有硬件合规性要求，则可以了解主机硬件以满足要求。

有关专用主机与专用实例之间的区别的更多信息，请参阅 [Amazon EC2 专用主机](#)。

有关使用专用主机和专用实例的更多信息，请参阅[修改实例租赁 \(p. 210\)](#)。

定价和记账

Abstract

专用主机的付款选项；按需和预留。

按需专用主机

按需计费在您将专用主机分配到您的账户时自动激活。

系统将以按需费率每小时对您计费一次。费率因专用主机支持的实例类型和运行专用主机的区域而异。实例类型大小或在专用主机上运行的实例的数量不会影响该主机的费用。

要终止按需计费，您必须先停止在专用主机上运行的实例，然后将其释放。有关更多信息，请参阅[管理和释放专用主机 \(p. 210\)](#)。

专用预留主机

对比运行按需专用主机，专用预留主机提供账单折扣。预留有三种付款方式。

- 无费用预付 - 无费用预付预留为某个期限内的专用主机使用提供折扣，并且不需要预付款。仅提供一年期限。
- 预付部分费用 - 必须支付一部分预留费用，期限内的剩余时间享受折扣。可以选择一年或三年期限。
- 预付全费 - 提供最低的有效价格。提供一年和三年期限，覆盖整个前期费用，无需额外付费。

您的账户中必须有活动的专用主机才能购买预留。在您的账户中，每个预留包含一个特定的专用主机。预留的实例系列和区域必须与您希望包括的专用主机匹配。



Note

当专用主机包括在预留中后，其将无法释放，直到期限结束。但是，您可将预留重新分配到您账户中的其他专用主机，只要区域和实例系列与预留匹配即可。有关信息，请联系支持人员或者您的客户经理。

购买专用预留主机

您可以通过向您的客户经理发送电子邮件或记录支持请求来购买预留。在两个实例中，您都需要提供包含以下信息的 CSV 或 XLS 文件：

- 账户 ID - 该账户的 ID。
- 主机 ID - 预留包括的专用主机。您可以在 AWS 管理控制台中获取主机 ID，或使用 [DescribeHosts API](#) 操作获取。
- 区域 - 专用主机运行的区域。
- 实例类型 - 专用主机的实例类型。
- 期限 - 一年或三年。（无费用预付专用主机预留只提供一年期限。）
- 付款选项 - 预留付款选项（无费用预付、预付部分费用或预付全费）。

下表为请求格式的示例。

账户 ID	主机 ID	区域	实例类型	术语	付款选项
12345768	h-068984f7c97	us-east-1	C4	3 岁	预付全费

使用支持控制台购买预留

1. [打开支持服务单。](#)
2. 选择账户和账单支持，输入以下值：
 - 服务 - 账单
 - 类别 - 其他账单问题
 - 主题 - 专用主机预留购买
3. 提供上表中所列的信息。
4. 选择 Submit。

当您的订单处理完毕时，支持人员或您的客户经理将会联系您。降低的小时费率最多需要 24 小时显示在 AWS 管理控制台中的 Billing & Cost Management 页。

有关其他专用主机预留支持要求，请联系支持人员或您的客户经理。

有关更多信息，请参阅[专用主机定价](#)。

专用主机的限制

Abstract

专用主机的限制

在分配专用主机之前，请注意以下限制。

- 由 AWS 提供的或者在 AWS Marketplace 中提供的非 BYOL RHEL、SUSE Linux 或 Windows AMI 均无法用于专用主机。
- 可为每个区域的每个实例系列分配最多两个按需专用主机。可以请求提高限制：[请求提高 Amazon EC2 专用主机上的分配限制](#)。
- 在专用主机上运行的实例只能在 VPC 中启动。
- 主机限制独立于实例限制。正在专用主机上运行的实例不会计入您的实例限制。
- 不支持 Auto Scaling 组。
- 不支持 Amazon RDS 实例。
- AWS 免费使用套餐不适用于专用主机。
- 实例放置控制是指管理专用主机中的实例启动。专用主机不支持置放群组。

专用主机配置

Abstract

专用主机支持单个实例类型容量。

专用主机配置为支持单个实例类型和大小容量。您可在专用主机上启动的实例的数量取决于专用主机配置所支持的实例类型。例如，如果您分配了一个 c3.xlarge 专用主机，则您有权在该专用主机上启动多达 8 个 c3.xlarge 实例。要确定您可在特定专用主机上运行的实例类型大小的数量，请参阅[支持的实例类型 \(p. 204\)](#)。

支持的实例类型

Abstract

可以在专用主机上启动的实例类型。

每个专用主机支持一个实例大小和类型（例如，c3.xlarge）。可将正在运行的实例的租赁修改为 host，但它必须是支持的实例类型。

主机类型	套接字	物理内核	实例容量
c3.large	2	20	16
c3.xlarge	2	20	8
c3.2xlarge	2	20	4
c3.4xlarge	2	20	2
c3.8xlarge	2	20	1
c4.large	2	20	16
c4.xlarge	2	20	8
c4.2xlarge	2	20	4
c4.4xlarge	2	20	2
c4.8xlarge	2	20	1
g2.2xlarge	2	20	4
g2.8xlarge	2	20	1
m3.medium	2	20	32
m3.large	2	20	16
m3.xlarge	2	20	8
m3.2xlarge	2	20	4
d2.xlarge	2	24	8

主机类型	套接字	物理内核	实例容量
d2.2xlarge	2	24	4
d2.4xlarge	2	24	2
d2.8xlarge	2	24	1
r3.large	2	20	16
r3.xlarge	2	20	8
r3.2xlarge	2	20	4
r3.4xlarge	2	20	2
r3.8xlarge	2	20	1
m4.large	2	24	22
m4.xlarge	2	24	11
m4.2xlarge	2	24	5
m4.4xlarge	2	24	2
m4.10xlarge	2	24	1
i2.xlarge	2	20	8
i2.2xlarge	2	20	4
i2.4xlarge	2	20	2
i2.8xlarge	2	20	1

使用专用主机

Abstract

在您的账户中分配、启动、使用和释放专用主机。

要使用专用主机，首先在您的账户中分配要使用的主机。然后通过为实例指定一个 host 租赁在主机上启动实例。实例自动放置设置可让您控制某个实例是否可在特定主机上启动。当某个实例停止并重新启动时，主机关联设置将确定该实例是在同一主机上还是在另一个主机上重新启动。如果您不再需要某个按需主机，则可以停止在该主机上运行的实例，指示它们在另一个主机上启动，然后释放该专用主机。

内容

- [自带许可 \(p. 206\)](#)
- [分配专用主机 \(p. 206\)](#)
- [在专用主机上启动实例 \(p. 207\)](#)
- [了解实例放置与主机关联 \(p. 208\)](#)
- [修改实例租赁 \(p. 210\)](#)

- [管理和释放专用主机 \(p. 210\)](#)
- [API 和 CLI 命令概览 \(p. 211\)](#)
- [使用 AWS Config 跟踪配置更改 \(p. 212\)](#)

自带许可

Abstract

在专用主机上导入和使用您自己的软件许可证。

您可以在专用主机上使用您自己的软件许可证。为了将您自己的卷许可的虚拟机镜像引入 Amazon EC2，您需要遵循以下常规步骤。

1. 验证控制您的虚拟机镜像 (AMI) 使用的许可证条款是否允许在虚拟化的云环境中使用虚拟机镜像。有关 Microsoft 许可的更多信息，请参阅 [Amazon Web Services 和 Microsoft 许可](#)。
2. 在确认您的虚拟机镜像可在 Amazon EC2 内使用后，使用由 VM Import/Export 工具实现的 ImportImage API 操作导入您的虚拟机镜像。有关限制的更多信息，请参阅 [VM Import/Export 的先决条件](#)。有关如何使用 ImportImage 导入 VM 的信息，请参阅 [使用 ImportImage 将 VM 导入 Amazon EC2](#)。
3. 如果您需要用于跟踪您的镜像在 AWS 中使用的方式的机制，请在 AWS Config 服务中启用主机记录。您可以使用 AWS Config 来记录专用主机的配置更改并将输出用作许可证报告的数据源。有关更多信息，请参阅 [使用 AWS Config 跟踪配置更改 \(p. 212\)](#)。
4. 在导入虚拟机映像后，您可以在您的账户中在活动专用主机上从此映像启动实例。
5. 在运行这些实例时，根据操作系统，您可能需要针对自己的 KMS 服务器（例如，Windows Server 或 Windows SQL Server）激活这些实例。您无法针对 Amazon Windows KMS 服务器激活已导入的 Windows AMI。

分配专用主机

Abstract

将专用主机分配到您的账户。

要开始使用专用主机，则需要将它们分配到您的账户。您可以使用 AWS 管理控制台、直接与 API 进行交互或使用命令行界面来执行这些任务。每次分配专用主机时可遵循这些步骤。

将专用主机分配到您的账户

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在专用主机页面上，选择 分配专用主机。
3. 使用提供的选项配置主机：
 - a. 实例类型 - 可在专用主机使用的实例类型。
 - b. 可用区 - 专用主机的可用区。
 - c. Allow instance auto-placement - 默认设置为 Off。专用主机只接受 host 租赁实例启动（假设容量可用）。当实例自动设置为 On 时，租赁为 host 并且与专用主机的配置匹配的任何实例都可以启动到该主机。
 - d. Quantity - 使用这些设置分配的主机的数量。
4. 选择 Allocate host。

专用主机容量可立即在您的账户中使用。

如果您启动了带有租赁 host 的实例，但您的账户中没有任何活动的专用主机，您将收到一个错误，并且实例启动失败。

在专用主机上启动实例

Abstract

启动在专用主机上使用的实例。

在分配一个专用主机后，您可以在该主机上启动实例。带有租赁 host 的实例可在特定专用主机上启动，或者可让 Amazon EC2 为您选择合适的专用主机（自动放置）。如果您的账户中的活动专用主机没有与要启动的实例的实例类型配置相符的可用容量，则您无法启动带有租赁 host 的实例。



Note

在专用主机上启动的实例只能在 VPC 中启动。有关更多信息，请参阅 [VPC 简介](#)。

在启动实例之前，请注意限制。有关更多信息，请参阅 [专用主机的限制 \(p. 203\)](#)。

从“Dedicated Hosts”页面将实例启动到专用主机

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Dedicated Hosts 页面上，选择一个主机，选择 Actions，然后选择 Launch Instance(s) onto Host。
3. 选择要使用的 AMI。如果您导入了自己的 AMI，请选择左侧边栏上的 My AMIs，然后选择相关的 AMI。
4. 为专用主机选择实例类型；这是您可在该主机上启动的唯一实例类型。
5. 在 Configure Instance Details 页面上，系统预先选择了 Tenancy 和 Host 选项。您可以将 Affinity 设置切换到 On 或 Off。
 - On - 如果停止，实例将始终在该特定主机上重新启动。
 - Off - 实例启动到指定的专用主机上，但不保证停止后仍在其上重新启动。
6. 完成剩余步骤并选择 Launch Instances。

实例会自动启动到您指定的专用主机上。要在专用主机上查看实例，请转至 Dedicated Hosts 页面，然后选择您在启动该实例时指定的专用主机。

从“Instances”页面将实例启动到特定专用主机

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Instances 页面上，选择 Launch Instance。
3. 从列表中选择一个 AMI。如果您已导入自己的 AMI，则选择 My AMIs，然后选择导入的镜像。并非所有 AMI 均可用于专用主机。
4. 选择要启动的实例的类型。
5. 在 Configure Instance Details 页面上，专用主机设置为：
 - Tenancy - Dedicated host - 在专用主机上启动此实例。如果无法选择此选项，请检查您是否选择了不兼容的 AMI 或实例类型。
 - Host - 选择主机。如果无法选择专用主机，请检查：
 - 所选子网是否与主机在不同可用区中。
 - 所选实例类型是否与专用主机支持的实例类型匹配。如果没有匹配的正在运行的主机，则唯一可用选项是 Use auto-placement，但除非您账户中有可用的匹配专用主机容量，否则实例将失败。
 - 关联 - 默认设置是 Off。实例启动到指定的专用主机上，但不保证停止后仍在其上重新启动。



Note

如果您无法看到这些设置，请检查是否在 Network 菜单中选择了一个 VPC。

6. 完成剩余的配置步骤。选择 Review and Launch。
7. 选择 Launch 以启动您的实例。
8. 选择现有密钥对或创建新密钥对。选择 Launch Instances。

从“Instances”页面将实例启动到任意专用主机

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Instances 页面上，选择 Launch Instance。
3. 从列表中选择一个 AMI。如果您已导入自己的 AMI，则选择 My AMIs，然后选择导入的镜像。并非所有 AMI 均可用于专用主机。
4. 选择要启动的实例的类型。
5. 在 Configure Instance Details 页面上，专用主机设置为：
 - Tenancy - Dedicated host - Launch this instance on a Dedicated host 如果无法选择此选项，请检查是否选择了不兼容的 AMI 或实例类型。
 - Host - 对于此类启动，请将设置保留为 Use auto-placement。
 - 关联 - 默认设置是 Off。实例启动到您账户中的任意可用专用主机，但不保证停止后仍在其上重新启动。

如果您无法看到这些设置，请检查是否在 Network 菜单中选择了一个 VPC。

6. 完成剩余的配置步骤。选择 Review and Launch。
7. 选择 Launch 以启动您的实例。
8. 选择现有密钥对或创建新密钥对。选择 Launch Instances。

了解实例放置与主机关联

Abstract

控制实例的启动位置以及是在相同还是不同专用主机上重新启动。

放置控制发生在实例级别和主机级别。

内容

- [实例自动放置 \(p. 208\)](#)
- [主机关联 \(p. 209\)](#)
- [修改实例自动放置和主机关联 \(p. 209\)](#)
- [修改实例主机关联 \(p. 209\)](#)

实例自动放置

自动放置允许您管理所启动的实例是启动到特定主机还是启动到有匹配配置的任意主机。默认设置为 Off。这意味着您所分配的专用主机只接受指定唯一主机 ID 的 host 租赁实例启动。未指定主机 ID 启动的实例不能启动到实例自动放置设置为 Off 的主机。

主机关联

主机关联在实例和专用主机之间建立启动关系。当关联设置为 `host` 时，启动到特定主机的实例在停止时始终在同一主机上重新启动。这适用于定向启动和非定向启动。

如果将关联设置为 `default`，并且您停止并重新启动了实例，则该实例可在任意可用主机上重新启动，但它将尝试回到其上次运行的专用主机上启动（尽力）。

您可以通过将关联从 `host` 更改为 `default`（或相反）来修改实例与专用主机之间的关系。有关更多信息，请参阅 [修改实例租赁 \(p. 210\)](#)。

修改实例自动放置和主机关联

您可以使用 Amazon EC2 控制台、API 或 CLI 管理实例放置控制。

要修改您的实例的实例放置设置，请先停止实例，然后编辑实例放置设置。



Note

如果实例停止并重新启动，无法保证它在同一专用主机上重新启动。

编辑实例的放置设置（任何可用主机）

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Instances 页面上，选择要编辑的实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 将实例租赁更改为 Launch this instance on a Dedicated host。
6. 选择 This instance can run on any one of my Hosts。实例会启动到任何启用了自动放置的专用主机上。
7. 选择 Save 以继续。
8. 打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Start。

编辑实例的放置设置（特定专用主机）

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Instances 页面上，选择要编辑的实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 依次选择 Actions、Instance Settings 和 Modify Instance Placement。
5. 将实例租赁更改为 Launch this instance on a Dedicated host。
6. 选择 This instance can only run on the selected Host。然后为 Target Host 选择一个值，选择是要将实例放置在任意主机上还是特定主机上。
7. 选择 Save 以继续。
8. 打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Start。

修改实例主机关联

如果您不再希望实例与主机之间存在关联，您可停止实例，并将其关联更改为 `default`。这会消除实例与主机之间的关联性。但当您重新启动实例时，它可能会回到同一专用主机上启动（具体取决于您的账户中的专用主机可用性，尽力）。但如果实例再次被停止，它将不会在同一主机上重新启动。

修改实例租赁

Abstract

将专用实例修改到专用主机上。

如果某个专用实例的租赁未使用由 Amazon EC2 提供的 Windows、SUSE 或 RHEL AMI，您可以将该租赁从 `dedicated` 更改为 `host`。要执行此操作，您需要停止您的专用实例。带有 `shared` 租赁的实例无法修改为 `host` 租赁。

将实例租赁从 `dedicated` 更改为 `host`

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择 Instances，然后选择要修改的专用实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 打开实例的上下文（右键单击）菜单，选择 Instance Settings，然后选择 Modify Instance Placement。
5. 在 Modify Instance Placement 页面上，执行以下操作：
 - Tenancy - 选择 Launch this instance on a Dedicated host。
 - Affinity - 选择 This instance can run on any one of my Hosts 或 This instance can only run on the selected Host。

如果选择 This instance can run on any one of my Hosts，实例会启动到您账户中的任意可用兼容专用主机。

如果选择 This instance can only run on the selected Host，请为 Target Host 选择一个值。如果未列出目标主机，则您账户中可能没有可用的兼容专用主机。

6. 选择 Save。
7. 当您重启实例时，Amazon EC2 会将实例放在您账户中的可用专用主机上，如果它支持您所启动的实例类型。

管理和释放专用主机

Abstract

查看有关您的专用主机和实例的详细信息。释放按需专用主机。

您可以使用控制台，与 API 直接交互，或使用命令行界面来查看主机上单个实例的详细信息并释放按需专用主机。

查看专用主机上实例的详细信息

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Dedicated Hosts 页面上，选择要查看更多详细信息的主机。
3. 选择 Description 选项卡以获取有关该主机的信息。选择 Instances 选项卡以获取有关您的主机上运行的实例的信息。

释放专用主机

需要先停止在专用主机上运行的任何实例，然后才能释放主机。这些实例可以迁移至您账户的其他专用主机，这样您就可以继续使用它们。有关更多信息，请参阅 [修改实例自动放置和主机关联 \(p. 209\)](#)。这些步骤只适用于按需专用主机。

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在专用主机页面上，选择要释放的专用主机。
3. 选择 Actions、Release Hosts。
4. 通过选择 Release 确认您的选择。

在释放某个专用主机后，您无法再次重用同一主机或主机 ID。

在释放专用主机后，将不再向您收取它产生的按需费用。专用主机状态将更改为 `released`，您无法在该主机上启动任何实例。

如果您最近释放了专用主机，则它们可能要过一段时间才会停止计入您的限制。在此期间，如果尝试分配新的专用主机，可能会遇到 `LimitExceeded` 错误。如果出现这种情况，请在几分钟后再次尝试分配新的主机。

已停止的实例仍可以使用和列在 Instances 页面上。这些实例将保留其 host 租赁设置。

API 和 CLI 命令概览

Abstract

使用 API 和 CLI 执行任务。

您可以使用 API 或命令行执行本节中所述的任务。

将专用主机分配到您的账户

- [allocate-hosts](#) (AWS CLI)
- [AllocateHosts](#) (Amazon EC2 查询 API)
- [New-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

描述您的专用主机

- [describe-hosts](#) (AWS CLI)
- [DescribeHosts](#) (Amazon EC2 查询 API)
- [Get-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

修改您的专用主机

- [modify-hosts](#) (AWS CLI)
- [ModifyHosts](#) (Amazon EC2 查询 API)
- [Edit-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

修改实例自动放置

- [modify-instance-placement](#) (AWS CLI)
- [ModifyInstancePlacement](#) (Amazon EC2 查询 API)
- [Edit-EC2InstancePlacement](#) (适用于 Windows PowerShell 的 AWS 工具)

释放您的专用主机

- [release-hosts](#) (AWS CLI)
- [ReleaseHosts](#) (Amazon EC2 查询 API)
- [Remove-EC2Hosts](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 AWS Config 跟踪配置更改

Abstract

使用 AWS Config 跟踪实例和专用主机配置更改。

您可以使用 AWS Config 记录专用主机的配置更改以及在这些主机上启动、停止或终止的实例的配置更改。然后，您可以将由 AWS Config 捕获的信息用作许可证报告的数据源。

AWS Config 分别记录专用主机和实例的配置信息并通过关系将这类信息配对。存在三种报告条件。

- AWS Config 记录状态 - 当其状态为 On 时，AWS Config 将记录一个或多个 AWS 资源类型，其中可包含专用主机和专用实例。要捕获许可证报告所需的信息，请使用以下字段验证是否记录了主机和实例。
- 主机记录状态 - 当其状态为 Enabled 时，将记录专用主机的配置信息。
- 实例记录状态 - 当其状态为 Enabled 时，将记录专用实例的配置信息。

如果禁用了这三个条件中的任一个，则 Edit Config Recording 按钮中的图标为红色。要发挥此工具的所有优点，请确保这三种记录方法都已启用。当这三种方法全部启用时，图标为绿色。要编辑设置，请选择 Edit Config Recording。您将被定向到 AWS Config 控制台中的 Set up AWS Config 页面，在该页面中，您可以设置 AWS Config 并启动对您的主机、实例和其他支持的资源类型的记录。有关更多信息，请参阅 [AWS Config 开发人员指南 中的使用控制台设置 AWS Config](#)。



Note

AWS Config 将在发现您的资源后记录它们，此过程可能需要几分钟。

在 AWS Config 开始记录对您的主机和实例的配置更改后，您可以获取已分配或已释放的任何主机以及已启动、已停止或已终止的任何实例的配置历史记录。例如，在专用主机的配置历史记录中的任何时间点上，您均可以查看在该主机上启动的实例的数量以及该主机上的套接字和内核的数量。对于任何这些实例，您还可以查看其 Amazon 系统映像 (AMI) 的 ID。您可以使用此信息来报告您拥有的服务器端绑定软件（按套接字或按内核授予许可）的许可。

您可以采用以下任一方法查看配置历史记录。

- 通过使用 AWS Config 控制台。对于每个已记录的资源，您可以查看一个时间线页面，该页面提供了配置详细信息的历史记录。要查看此页面，请选择 Dedicated Hosts 页面的 Config Timeline 列中的灰色图标。有关更多信息，请参阅 [AWS Config 开发人员指南 中的在 AWS Config 控制台中查看配置详细信息](#)。
- 通过运行 AWS CLI 命令。首先，您可以使用 `list-discovered-resources` 命令获取一个包含所有主机和实例的列表。然后，您可以使用 `get-resource-config-history` 命令获取特定时间间隔内某个主机或实例的配置详细信息。有关更多信息，请参阅 [AWS Config 开发人员指南 中的使用 CLI 查看配置详细信息](#)。
- 通过在您的应用程序中使用 AWS Config API。首先，您可以使用 `ListDiscoveredResources` 操作获取一个包含所有主机和实例的列表。然后，您可以使用 `GetResourceConfigHistory` 操作获取特定时间间隔内某个主机或实例的配置详细信息。

例如，要从 AWS Config 中获取包含您的所有专用主机的列表，请运行 CLI 命令，例如下面的命令：

```
aws configservice list-discovered-resources --resource-type
    AWS::EC2::Host
```

要从 AWS Config 中获取某个专用主机的配置历史记录，请运行 CLI 命令，例如下面的命令：

```
aws configservice get-resource-config-history --resource-type
    AWS::EC2::Instance --resource-id i-36a47fdf
```

使用 AWS 管理控制台管理 AWS Config 设置

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Dedicated Hosts 页面上，选择 Edit Config Recording。
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[在 AWS Config 控制台中查看配置详细信息](#)。
- 要使用 Amazon EC2 API，请参阅 [GetResourceConfigHistory](#)。

监控专用主机

Abstract

监控专用主机的状态。

Amazon EC2 持续监控您的专用主机的状态；更新内容将在 Amazon EC2 控制台上发送。您还可以使用 API 或 CLI 来获取有关您的专用主机的信息。

下表说明了控制台中可能的 State 值。

州	说明
available	AWS 未在专用主机上检测到问题；没有制定维护或修复计划。实例可在此专用主机上启动。
released	已释放专用主机。主机 ID 不再使用。无法重新使用已释放的主机。
under-assessment	AWS 正在寻找专用主机可能存在的问题。如果需要采取措施，系统将通过 AWS 管理控制台或电子邮件通知您。实例无法在处于此状态的专用主机上启动。
permanent-failure	检测到了一个不可恢复的故障。您将通过您的实例或通过电子邮件接收到一个移出通知。您的实例可能会继续运行。如果在处于此状态的专用主机上停止或终止所有实例，AWS 将重试该主机。实例无法在处于此状态的专用主机上启动。
released-permanent-failure	AWS 一直释放已发生故障的专用主机并且不再在这些主机上运行实例。专用主机 ID 不再可供使用。

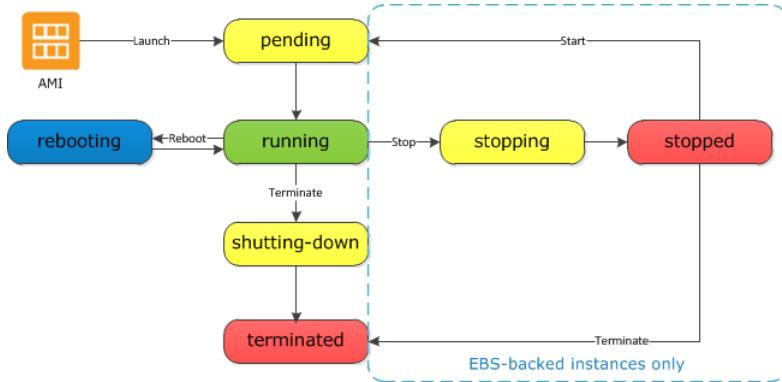
实例生命周期

Abstract

描述 Amazon EC2 实例从启动到终止的生命周期。

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 \(p. 63\)](#)。



实例启动

当您启动实例时，实例进入 `pending` 状态。启动时指定的实例类型将决定您实例的主机硬件。我们使用您在启动时指定的Amazon 系统映像 (AMI) 来启动实例。当实例准备就绪后，其进入 `running` 状态。您可以连接到正在运行的实例，然后像使用您面前的计算机一样来使用它。

只要您的实例转换为 `running` 状态，实例保持运行的每个小时或不足一小时都会计费；即使实例处于闲置状态并且您并未连接到该实例。

有关更多信息，请参阅[启动实例 \(p. 216\)](#)和[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。

停止和启动实例（仅限 Amazon EBS 支持的实例）

如果您的实例未能通过状态检查或未按预期运行应用程序，并且实例的根卷为 Amazon EBS 卷，则您可以先停止该实例再启动，以尝试解决该问题。

当您停止实例时，它会进入 `stopping` 状态，然后进入 `stopped` 状态。我们不对已停止的示例收取小时使用费或数据传输费，但会对所有 Amazon EBS 卷的存储收费。当实例处于 `stopped` 状态时，您可以修改实例的某些属性，包括实例类型。

当您启动实例时，它会进入 `pending` 状态，在大多数情况下，我们会将该实例移至新主机。（您的实例可能驻留在同一主机上，前提是此主机正常。）当您停止实例再启动时，将丢失先前主机的实例存储卷上的所有数据。

如果您的实例在 EC2-Classic 中运行，它会收到一个新的私有 IP 地址，这意味着与私有 IP 地址关联的弹性 IP 地址 (EIP) 不再与您的实例关联。如果您的实例在 EC2-VPC 中运行，它会保留其私有 IP 地址，这意味着与该私有 IP 地址或网络接口关联的 EIP 仍与您的实例关联。

您每次将实例从 `stopped` 状态转换到 `running` 状态时，我们都按一个完整实例小时收费，即使这些转换在一小时内发生多次也一样。

有关更多信息，请参阅[停止和启动您的实例 \(p. 227\)](#)。

实例重启

您可以使用 Amazon EC2 控制台、命令行工具和 Amazon EC2 API 来重新启动实例。我们建议您使用 Amazon EC2 来重启实例，而非在实例中运行操作系统重启命令。

重启实例等同于重启操作系统；实例位于同一主机上并保留其公有 DNS 名称、私有 IP 地址以及其实例存储卷上的所有数据。完成重启通常需要花费几分钟的时间，该时间具体取决于实例配置。

重启实例不会启动新的实例计费小时。

有关更多信息，请参阅 [重启您的实例 \(p. 230\)](#)。

实例停用

实例计划在 AWS 检测到托管实例的底层硬件发生无法弥补的故障时停用。当实例到达其计划的停用日期时，AWS 会将其停止或终止。如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

有关更多信息，请参阅 [实例停用 \(p. 231\)](#)。

实例终止

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，就不再产生与该实例相关的费用。

请注意，如果您启用终止保护，则无法使用控制台、CLI 或 API 来终止实例。

在您终止实例之后，短时间内仍可在控制台中看见该实例，然后该条目将被删除。您还可以使用 CLI 和 API 来描述已终止的实例。您无法连接至或恢复已终止的实例。

每个由 Amazon EBS 支持的实例都支持 `InstanceInitiatedShutdownBehavior` 属性，该属性决定当从实例内部启动关闭命令时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 \(p. 232\)](#)。

重启、停止与终止之间的区别

下表总结重启、停止与终止实例之间的主要区别。

性能	重启	停止/启动（仅限 Amazon EBS 支持的实例）	终止
主机	实例保持在同一主机上运行	实例在新主机上运行	无
私有和公有 IP 地址	这些地址保持不变	EC2-Classic：实例获得新的私有和公有 IP 地址 EC2-VPC：实例保留其私有 IP 地址。实例获取新的公有 IP 地址，除非它具有弹性 IP 地址 (EIP)（该地址在停止/启动过程中不更改）。	无
弹性 IP 地址 (EIP)	EIP 保持与实例关联	EC2-Classic：EIP 不再与实例关联 EC2-VPC：EIP 保持与实例关联	EIP 不再与实例关联
实例存储卷	数据保留	数据将擦除	数据将擦除
根设备卷	卷将保留	卷将保留	默认情况下将删除卷

性能	重启	停止/启动 (仅限 Amazon EBS 支持的实例)	终止
记账功能	实例计费小时不更改。	实例的状态一旦变为 <code>stopping</code> ，就不再产生与该实例相关的费用。每次实例从 <code>stopped</code> 转换为 <code>running</code> 时，我们都会启动新的实例计费小时。	实例的状态一旦变为 <code>shutting-down</code> ，就不再产生与该实例相关的费用。

请注意，操作系统的 shutdown 命令始终会终止实例存储支持实例。您可以控制操作系统 shutdown 命令是停止还是终止 Amazon EBS 支持的实例。有关更多信息，请参阅[更改实例的启动关闭操作 \(p. 234\)](#)。

启动实例

Abstract

启动一个作为 AWS 云中虚拟服务器的实例。

实例是 AWS 云中的虚拟服务器。您可以从 Amazon 系统映像 (AMI) 中启动实例。AMI 为实例提供操作系统、应用程序服务器和应用程序。

注册 AWS 后，您可以通过[AWS 免费套餐](#)开始免费使用 Amazon EC2。您可以利用免费套餐来免费启动和使用微型实例，免费时间为 12 个月。如果您启动不在免费套餐范围内的实例，则需要为该实例支付标准 Amazon EC2 使用费。有关更多信息，请参阅[Amazon EC2 定价](#)。

您可以使用以下方法启动实例。

方法	文档
将 Amazon EC2 控制台与您选择的 AMI 一起使用	启动实例 (p. 216)
使用 Amazon EC2 控制台，通过将现有实例用作模板来启动实例	使用现有实例作为模板来启动实例 (p. 222)
将 Amazon EC2 控制台与您从 AWS Marketplace 购买的 AMI 一起使用	启动 AWS Marketplace 实例 (p. 223)
将 AWS CLI 与您选择的 AMI 一起使用	通过 AWS CLI 使用 Amazon EC2
将适用于 Windows PowerShell 的 AWS 工具与所选的 AMI 结合使用	适用于 Windows PowerShell 的 AWS 工具中的 Amazon EC2

启动实例之后，您可以连接并使用该实例。开始时，实例的状态为 `pending`。当实例状态为 `running` 时，实例已经开始启动。可能要过一小段时间才能连接到实例。实例会获得一个公有 DNS 名称，可用于从 Internet 与该实例通信。实例还会获得一个私有 DNS 名称，相同 Amazon EC2 网络 (EC2-Classic 或 EC2-VPC) 内的其他实例可以用其与该实例通信。有关连接到实例的更多信息，请参阅[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。

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 \(p. 232\)](#)。

启动实例

Abstract

使用 Amazon EC2 控制台从 AMI 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 \(p. 13\)](#)。

根据您创建账户的时间以及您使用的区域，您的 AWS 账户可能同时支持 EC2-Classic 和 EC2-VPC 平台。要查明您的账户支持的平台，请参阅 [支持的平台 \(p. 577\)](#)。如果您的账户支持 EC2-Classic，则可以在任一平台中启动实例。如果您的账户仅支持 EC2-VPC，则只能在 VPC 中启动实例。



Important

当您启动不在 [AWS 免费套餐](#)范围内的实例时，即使该实例处于闲置状态，您也需为该实例运行的时间付费。

从 AMI 启动实例

启动实例时，您必须选择配置（称为 Amazon 系统映像 (AMI)）。AMI 包含创建新实例所需的信息。例如，AMI 可能包含用作 Web 服务器所需的软件：例如 Windows、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.amazonaws.cn/ec2/>。
2. 在屏幕顶部的导航栏中，会显示当前区域。选择实例的区域。该选择很重要，这是因为有些 Amazon EC2 资源可以在区域间共享，另一些却不能。请选择能满足您的需求的区域。有关更多信息，请参阅 [资源位置 \(p. 729\)](#)。



3. 从 Amazon EC2 控制台控制面板中，选择 Launch Instance。

4. 在 Choose an Amazon Machine Image (AMI) (选择 Amazon 系统映像 (AMI)) 页上，选择某个 AMI，如下所示：

- a. 在左侧窗格中选择要使用的 AMI 类型：

快速启动

一组精选的常用 AMI 可帮助您快速开始。要确保选择符合免费套餐条件的 AMI，请在左侧窗格中选择 Free tier only。（请注意，这些 AMI 标记为 Free tier eligible (符合条件的免费套餐)。）

我的 AMI

您拥有的私有 AMI，或与您共享的私有 AMI。

AWS Marketplace

一个在线商店，您可以从中购买在 AWS 上运行的软件（包括 AMI）。有关从 AWS Marketplace 启动实例的更多信息，请参阅[启动 AWS Marketplace 实例 \(p. 223\)](#)。

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 \(p. 63\)](#)。
- 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。
- 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 \(p. 110\)](#)。

要保持符合免费套餐条件，请选择 t2.micro 实例类型。有关更多信息，请参阅[T2 实例 \(p. 113\)](#)。

默认情况下，向导显示当前一代实例类型，并根据您选择的 AMI 选择第一可用实例类型。要查看上一代实例类型，请从筛选列表中选择 All generations。



Note

如果您刚刚接触 AWS 并希望快速设置实例以进行测试，那么目前可以选择 Review and Launch 以接受默认配置设置，然后启动您的实例。否则，若要进一步配置实例，请选择 Next: Configure Instance Details。

6. 在 Configure Instance Details 页面上，根据需要更改以下设置（展开 Advanced Details 查看所有设置），然后选择 Next: Add Storage：

- Number of instances (实例的数量)：输入要启动的实例的数量。



Note

为帮助确保保持正确数量的实例来处理应用程序，您可选择 Launch into Auto Scaling Group 以创建启动配置和 Auto Scaling 组。Auto Scaling 将根据您的规格来扩展组中的实例数。有关更多信息，请参阅[Auto Scaling 用户指南](#)。

- Purchasing option：选择 Request Spot Instances 可启动竞价型实例。有关更多信息，请参阅[竞价型实例 \(p. 160\)](#)。

- 您的账户可能支持 EC2-Classic 和 EC2-VPC 平台，或者仅支持 EC2-VPC。要查明您的账户支持的平台，请参阅 [支持的平台 \(p. 577\)](#)。如果您的账户仅支持 EC2-VPC，则可以在默认 VPC 或非默认 VPC 中启动实例。否则，您可以在 EC2-Classic 或非默认 VPC 中启动实例。



Note

必须在 VPC 中启动 T2 实例。如果您没有 VPC，可以让向导为您创建一个。

在 EC2-Classic 中启动：

- Network (网络)：选择 Launch into EC2-Classic (在 EC2-Classic 中启动)。
- Availability Zone (可用区)：选择您想使用的可用区。要使 AWS 为您选择可用区，请选择 No preference (无首选项)。

在 VPC 中启动：

- Network：选择 VPC，若要创建新 VPC，请选择 Create new VPC 转到 Amazon VPC 控制台。完成后，返回到向导并选择 Refresh 按钮，以便将您的 VPC 加载到列表中。
- Subnet (子网)：选择您要将实例启动到其中的子网。如果您的账户仅为 EC2-VPC，请选择 No preference (无首选项) 让 AWS 在任何可用区中选择默认子网。要创建新子网，请选择 Create new subnet 转到 Amazon VPC 控制台。完成此操作后，返回到向导并选择 Refresh 按钮，以便将您的子网加载到列表中。
- Auto-assign Public IP (自动分配公有 IP)：指定您的实例是否接收公有 IP 地址。默认情况下，默认子网中的实例接收公有 IP 地址，非默认子网中的实例则不接收。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 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。
- Domain join directory：选择您的 Windows 实例所加入到的 AWS Directory Service 目录 (域)。目录必须位于您为该实例选择的同一 VPC 中。如果您选择域，则必须选择 IAM 角色。有关更多信息，请参阅 [将 Windows 实例加入 AWS Directory Service 域 \(p. 299\)](#)。
- IAM role (IAM 角色)：如果适用，请选择 AWS Identity and Access Management (IAM) 角色以便与实例关联。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
- 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 \(p. 234\)](#)。
- Enable termination protection (启用终止保护)：选中此复选框可防止意外终止。有关更多信息，请参阅 [为实例启用终止保护 \(p. 234\)](#)。
- 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 \(p. 452\)](#)。
- EBS-Optimized instance (EBS 优化实例)：Amazon EBS 优化实例使用优化的配置堆栈，为 Amazon EBS I/O 提供附加专用容量。如果实例类型支持此功能，请选中此复选框将其启用。将收取额外费用。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。
- Tenancy：如果您要将实例启动到 VPC，则可选择在独立的专用硬件 (Dedicated) 或专用主机 (Dedicated host) 上运行实例。可能收取额外费用。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [专用实例](#) 以及 [专用主机 \(p. 201\)](#)。
- Network interfaces (网络接口)：如果要在 VPC 中启动实例，并且没有为子网选择 No Preference (无首选项)，则可以在向导中指定最多两个网络接口。选择 Add IP 以向所选接口分配多个 IP 地址。有关网络接口的更多信息，请参阅 [弹性网络接口 \(ENI\) \(p. 612\)](#)。如果指定不止一个网络接口，您的实例将无法获得公有 IP 地址。此外，对于非默认子网，如果您为 eth0 指定了一个现有的网络接口，您的实例将无法获得公有 IP 地址。有关更多信息，请参阅 [分配公有 IP 地址 \(p. 601\)](#)。
- Kernel ID (内核 ID)：(仅对半虚拟化 (PV) AMI 有效) 除非您想使用某个特定内核，否则选择 Use default (使用默认值)。
- RAM disk ID (RAM 磁盘 ID)：(仅对半虚拟化 (PV) AMI 有效) 除非您想使用某个特定 RAM 磁盘，否则选择 Use default (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。

- Placement group (置放群组)：置放群组是对您的集群实例加以组织的逻辑分组。选择现有置放群组或创建新群组。仅当您选择了支持置放群组的实例类型时，此选项才可用。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。
- User data：您可以指定用户数据在启动时配置实例或运行配置脚本。要附加文件，请选择 As file (以文件形式) 选项并浏览到要附加的文件。

7. 在 Add Storage (添加存储) 页面上，除 AMI 指定的卷之外（例如根设备卷），您还可以指定要附加到实例的卷。您可以更改以下选项，然后在完成时选择 Next: Tag Instance：

- 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 \(p. 701\)](#) 和 [Amazon EBS 卷 \(p. 640\)](#)。
- Device (设备)：从卷的可用设备名称列表中进行选择。
- Snapshot (快照)：输入要从其中还原卷的快照的名称或 ID。您还可以通过在 Snapshot (快照) 字段中键入文本来搜索公有快照。快照描述区分大小写。
- Size (大小)：对于 Amazon EBS 支持的卷，您可以指定存储大小。请注意，即使您选择了有资格享用免费套餐的 AMI 和实例，仍需保持总存储大小低于 30 GiB，以便保持在免费套餐限制之内。



Note

下面的 Amazon EBS 卷注意事项适用于 Windows 引导卷：

- 如果引导卷大小为 2 TiB (2048 GiB) 或更大，则 Windows 2003 实例不会启动。
- Windows 启动卷必须使用 MBR 分区表，无论卷大小如何，它都将可用空间限制为 2 TiB。
- 已转换为使用动态 MBR 分区表的 2 TiB (2048 GiB) 的 Windows 引导卷在用 Disk Manager 检查时会显示错误。

下面的 Amazon EBS 卷注意事项适用于 Windows 数据（非引导）卷：

- 2 TiB (2048 GiB) 或更大的 Windows 卷必须使用 GPT 分区表才能访问整个卷。
- 将自动使用 GPT 分区表对启动时附加到 Windows 实例的 2048 GiB 以上的 Amazon EBS 卷进行格式设置。
- 必须使用 GPT 分区表手动对启动后附加到 Windows 实例的 Amazon EBS 卷进行初始化。有关更多信息，请参阅 [使 Amazon EBS 卷可用](#)。



Note

如果此时增加根卷（或从快照创建的任何其他卷）的大小，则需要扩展该卷上的文件系统以使用额外空间。有关在实例启动之后扩展文件系统的更多信息，请参阅 [在 Windows 上扩展 EBS 卷的存储空间 \(p. 671\)](#)。

- Volume Type (卷类型)：对于 Amazon EBS 卷，请选择 通用型 SSD、Provisioned IOPS 或磁介质卷。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。



Note

如果选择 磁介质 启动卷，则在您完成向导时，系统会提示您将 通用型 SSD 卷设为此实例和将来的控制台启动的默认启动卷。（此首选项保留在浏览器会话中，不会影响具有 Provisioned IOPS 启动卷的 AMI。）我们建议您将 通用型 SSD 卷设为默认卷，因为它们可提供更快的体验，是大多数工作负载的最佳卷类型。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。



Note

2012 年之前创建的某些 AWS 账户可能能够访问 us-east-1、us-west-1 或 ap-northeast-1 中的可用区，这些可用区不支持 provisioned IOPS (io1) 卷。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。

- IOPS：如果选择了 Provisioned IOPS 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 \(p. 235\)](#)。
 - Encrypted (加密)：选中此复选框可加密新的 Amazon EBS 卷。从加密快照还原的 Amazon EBS 卷会自动加密。加密卷只能连接到[支持的实例类型 \(p. 687\)](#)。
8. 在 Tag Instance (标签实例) 页面上，通过提供密钥和值组合为实例指定[标签 \(p. 737\)](#)。选择 Create Tag 以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 [Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。）按如下所示选择或创建安全组，然后选择 Review and Launch。

选择现有安全组：

1. 选择 Select an existing security group。会显示您的安全组。（如果您要在 EC2-Classic 中启动，则这些是用于 EC2-Classic 的安全组。如果您要在某个 VPC 中启动，则这些是用于该 VPC 的安全组。）
2. 从列表中选择安全组。
3. （可选）您无法编辑现有安全组的规则，但是可以通过单击 Copy to new (复制到新项目) 将它们复制到新组。随后您可以按下一过程所述添加规则。

创建新安全组：

1. 选择 Create a new security group。向导会自动定义 launch-wizard-x 安全组。
2. （可选）您可以编辑安全组的名称和描述。
3. 向导会自动定义入站规则以允许您通过适用于 Linux 的 SSH (端口 22) 或适用于 Windows 的 RDP (端口 3389) 连接到实例。



Caution

此规则使所有 IP 地址 (0.0.0.0/0) 都可以通过指定端口访问您的实例。您可以在本次简短练习中使用此方法，但是在生产环境中使用时，其安全性有所欠缺。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

4. 您可以根据需要添加规则。例如，如果您的实例是 Web 服务器，则打开端口 80 (HTTP) 和 443 (HTTPS) 以允许 Internet 流量。

要添加规则，请选择 Add Rule，选择用于打开网络流量的协议，然后指定源。从 Source (源) 列表中选择 My IP (我的 IP)，让向导添加您计算机的公有 IP 地址。但是，如果您在没有静态 IP 地址的情况下通过 ISP 或从防火墙后面进行连接，则您需要了解客户端计算机使用的 IP 地址范围。

10. 在 Review Instance Launch (查看实例启动) 页面上，检查您的实例的详细信息，然后单击相应的 Edit (编辑) 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 (选择现有密钥对) , 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 \(p. 446\)](#)。
13. 如果实例状态立即变为 terminated , 而不是 running , 您可以获取有关实例无法启动的相关原因的信息。有关更多信息 , 请参阅 [实例立即终止 \(p. 823\)](#)。

使用现有实例作为模板来启动实例

Abstract

使用 Amazon EC2 控制台中的“Launch More Like This (启动更多类似项)”功能可基于现有实例启动实例。

Amazon EC2 控制台提供启动更多类似项向导选项 , 通过该选项可以将当前实例用作启动其他实例的模板。此选项自动使用所选实例中的特定配置详细信息来填充 Amazon EC2 启动向导。



Note

启动更多类似项向导选项不克隆所选实例 ; 仅复制某些配置详细信息。要创建实例的副本 , 请先从它创建 AMI , 然后从 AMI 启动更多实例。

以下配置详细信息会从所选实例复制到启动向导中 :

- AMI ID
- 实例类型
- 可用区 , 或所选实例所在的 VPC 和子网
- 公有 IP 地址。如果所选实例当前具有公有 IP 地址 , 则无论所选实例的默认公有 IP 地址设置如何 , 新实例都会接收公有 IP 地址。有关公有 IP 地址的更多信息 , 请参阅 [公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。
- 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

- **关联信息。**如果所选实例已与某个配置文件关联，那么该文件会自动与新实例关联。如果该配置文件包含域加入配置，那么新实例将加入到同一个域中。有关加入域的更多信息，请参阅[将 Windows 实例加入 AWS Directory Service 域 \(p. 299\)](#)。

以下配置详细信息不会从所选实例进行复制；而是由向导应用默认设置或行为：

- (仅限 VPC) 网络接口数量：默认为一个网络接口，即主网络接口 (eth0)。
- Storage (存储)：默认存储配置由 AMI 和实例类型确定。

将当前实例用作模板

1. 在“实例”页面上，选择要使用的实例。
2. 选择 Actions，然后选择 Launch More Like This。
3. 启动向导会在 Review Instance Launch (查看实例启动) 页面上打开。您可以查看实例的详细信息，然后通过单击相应的 Edit (编辑) 链接进行任何所需更改。

准备就绪时，请选择 Launch 以选择密钥对并启动实例。

启动 AWS Marketplace 实例

Abstract

订阅 AWS Marketplace 产品，并使用 Amazon EC2 启动向导从 AMI 启动实例。

您可以订阅 AWS Marketplace 产品，可以使用 Amazon EC2 启动向导从产品的 AMI 启动实例。有关付费 AMI 的更多信息，请参阅[付费 AMI \(p. 72\)](#)。要在启动之后取消订阅，必须先停止从订阅运行的所有实例。有关更多信息，请参阅[管理 AWS Marketplace 订阅 \(p. 75\)](#)。

使用启动向导从 AWS Marketplace 启动实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Amazon EC2 控制面板中，单击 Launch Instance (启动实例)。
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。单击 Select (选择) 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。准备就绪时，单击 Continue (继续)。



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。

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。完成时请单击 Next: Configure Instance Details (下一步：配置实例详细信息)。
6. 在向导的后续页面上，可以配置实例、添加存储和添加标签。有关可以配置的不同选项的更多信息，请参阅[启动实例 \(p. 216\)](#)。单击 Next (下一步)，直至到达 Configure Security Group (配置安全组) 页面。

向导会根据产品的供应商规格来创建新的安全组。安全组可能包括允许通过 Linux 上的 SSH (端口 22) 或 Windows 上的 RDP (端口 3389) 进行所有 IP 地址 (0.0.0.0/0) 访问的规则。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。

准备就绪时，单击 Review and Launch (查看和启动)。

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。准备就绪时，单击 Launch (启动) 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，单击 View Instances (查看实例) 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单击 Connect (连接)。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[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。



Important

仔细查看供应商的使用说明，因为您可能需要使用特定用户名登录实例。有关访问订阅详细信息的更多信息，请参阅[管理 AWS Marketplace 订阅 \(p. 75\)](#)。

使用 API 和 CLI 启动 AWS Marketplace AMI 实例

要使用 API 或命令行工具从 AWS Marketplace 产品启动实例，请首先确保订阅了产品。然后您可使用以下方法通过该产品的 AMI ID 启动一个实例：

方法	文档
AWS CLI	使用 run-instances 命令或参阅以下主题以了解更多信息： 启动实例 。
适用于 Windows PowerShell 的 AWS 工具	使用 New-EC2Instance 命令，或参阅以下主题了解更多信息： 使用 Windows PowerShell 启动 Amazon EC2 实例
查询 API	使用 RunInstances 请求。

使用 RDP 连接到 Windows 实例

Abstract

使用 RDP 客户端连接到 Windows 实例。

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

如果您在尝试连接到实例时收到错误，请参阅 [对 Windows 实例进行故障排除 \(p. 813\)](#)。

如需连接到 Linux 实例，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [连接到您的 Linux 实例](#)。

先决条件

- 安装 RDP 客户端

默认情况下，Windows 计算机包含有 RDP 客户端。您可以通过在命令提示符窗口中键入 mstsc 来检查 RDP 客户端。如果您的计算机不能识别此命令，请访问 [Microsoft Windows 主页](#) 并搜索远程桌面连接的下载。对于 Mac OS X，您可以使用 Apple 应用商店中的 Microsoft 远程桌面应用程序，或者访问 Microsoft 网站上的 [Microsoft 远程桌面连接客户端](#)。对于 Linux，您可以使用 [rdesktop](#)。



Important

Mac OS X 用户：如果您连接的是 Windows 2012 R2 实例，Microsoft 网站上的远程桌面连接客户端可能并不适用。请改用 Apple 应用商店中的 Microsoft 远程桌面应用程序。

- 获得实例的 ID

您可以通过使用 Amazon EC2 控制台（位于 Instance ID (实例 ID) 列中）获得您的实例的 ID。如果您愿意，您可以使用 [describe-instances](#) (AWS CLI) 或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令。

- 获得实例的公有 DNS 名称

您可以使用 Amazon EC2 控制台获取实例的公有 DNS（勾选 Public DNS (公有 DNS) 列；如果此列处于隐藏状态，请单击 Show/Hide (显示/隐藏) 图标并选择 Public DNS (公有 DNS)）。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。

- 查找私有密钥

您需要使用您在启动实例时指定的密钥对的 .pem 文件的完全限定路径。

- 允许从您的 IP 地址到您的实例的入站 RDP 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 RDP 流量。有关更多信息，请参阅 [为您的 Windows 实例授权入站流量 \(p. 570\)](#)。



Important

默认情况下，您的默认安全组不允许传入 RDP 流量。

- 要获得 Internet Explorer 的最佳使用体验，请运行最新版本。

连接到您的 Windows 实例

要连接到 Windows 实例，必须获取初始管理员密码，然后在使用远程桌面连接到实例时指定该密码。



Note

如果您已将实例加入域，则可以使用您在 AWS Directory Service 中定义的域证书连接实例。有关连接域中实例的更多信息，请参阅[使用域证书连接到实例 \(p. 305\)](#)。

管理员账户的名称取决于操作系统语言。例如，在英语中是 Administrator，在法语中是 Administrateur，在葡萄牙语中是 Administrador。有关更多信息，请参阅 Microsoft TechNet Wiki 中的 [Localized Names for Administrator Account in Windows](#)。

借助适用于 Windows Server 操作系统 (OS) 的许可证，可以同时进行两个远程连接以进行管理。适用于 Windows Server 的许可证包含在您的 EC2 实例的价格中。如果您需要同时进行两个以上的远程连接，则必须购买远程桌面服务 (RDS) 许可证。如果尝试第三个连接，将产生错误。有关更多信息，请参阅[Configure the Number of Simultaneous Remote Connections Allowed for a Connection](#)。

使用 RDP 客户端连接到 Windows 实例

1. 在 Amazon EC2 控制台中，选择实例，然后选择 Connect。
2. 在 Connect To Your Instance 对话框中，选择 Get Password (密码在实例启动几分钟之后才可用)。
3. 选择 Browse 并导航至您启动实例时所创建的私有密钥文件。选择该文件并选择 Open，将文件的全部内容复制到内容框中。
4. 选择 Decrypt Password。控制台将在 Connect To Your Instance (连接到您的实例) 对话框中显示实例的默认管理员密码，会将先前显示的 Get Password (获取密码) 链接替换为实际密码。
5. 记录下默认管理员密码，或将其复制到剪贴板。需要使用此密码连接实例。
6. 选择 Download Remote Desktop File。您的浏览器会提示您打开或保存 .rdp 文件。两种选择都可以。完成后，可选择 Close 以关闭 Connect To Your Instance 对话框。
 - 如果已打开 .rdp 文件，您将看到 Remote Desktop Connection (远程桌面连接) 对话框。
 - 如果已保存 .rdp 文件，请导航至下载目录，然后打开 .rdp 文件以显示该对话框。
7. 您可能看到一条警告，指出远程连接发布者未知。如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 Connect 以连接到您的实例。如果您正在 Mac 上使用 Microsoft Remote Desktop (Microsoft 远程桌面)，请跳过下一步。
8. 当收到系统提示时，使用操作系统的管理员账户和您在之前记录或复制的密码登录该实例。如果您的 Remote Desktop Connection 已设置了管理员账户，您可能需要选择 Use another account 选项并手动输入用户名和密码。



Note

有时复制和粘贴内容可能会损坏数据。如果您在登录时遇到“Password Failed (密码失败)”错误，请尝试手动键入密码。

9. 由于自签名证书的固有特性，您可能会看到一条警告，指出无法验证该安全证书。请使用以下步骤验证远程计算机的标识；或者，如果您信任该证书，则直接选择 Yes 或 Continue 以继续操作。
 - a. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 View certificate。如果您正在 Mac 上使用 Microsoft Remote Desktop，请选择 Show Certificate。
 - b. 选择 Details 选项卡，并向下滚动到 Thumbprint 条目（在 Windows PC 上）或 SHA1 Fingerprints 条目（在 Mac 上）。这是远程计算机的安全证书的唯一标识符。
 - c. 在 Amazon EC2 控制台中，选择该实例，选择 Actions，然后选择 Get System Log。
 - d. 在系统日志输出中，查找标记为 RDPCERTIFICATE-THUMBPRINT 的条目。如果此值与证书指纹匹配，则表示您已验证了远程计算机的标识。

- e. 如果您正在从 Windows PC 使用 Remote Desktop Connection , 请返回到 Certificate 对话框并选择 OK。如果您正在 Mac 上使用 Microsoft Remote Desktop , 请返回到 Verify Certificate 并选择 Continue。
- f. 如果您正在从 Windows PC 使用 Remote Desktop Connection , 请选择 Remote Desktop Connection 窗口中的 Yes 以连接到您的实例。如果您正在 Mac 上使用 Microsoft Remote Desktop (Microsoft 远程桌面) , 请使用默认 Administrator 账户和您先前记录或复制的默认管理员密码按提示登录实例。



Note

在 Mac 上 , 您可能需要切换空间才能看到 Microsoft Remote Desktop (Microsoft 远程桌面) 登录屏幕。有关空间的更多信息 , 请参阅 <http://support.apple.com/kb/PH14155>。

连接之后 , 建议执行以下操作 :

- 更改默认的管理员密码。在登录实例本身后更改密码 , 其做法与任何其他 Windows Server 上的做法类似。
- 在实例上创建另一个具有管理员权限的用户账户。作为一种预防措施 , 您可以另外创建一个具有管理员权限的账户 , 以防忘记管理员密码或管理员账户出现问题。

将文件传输到 Windows Server 实例

您可以像操作任何 Windows 服务器那样操作您的 Windows 实例。例如 , 您可以使用 Microsoft 远程桌面软件的本地文件共享功能 , 在 Windows 实例与您的本地计算机之间传输文件。如果您启用此选项 , 那么您可以从 Windows 实例访问您的本地文件。您可以访问硬盘驱动器、DVD 驱动器、便携式媒体驱动器和映射网络驱动器上的本地文件。有关此功能的更多信息 , 请访问以下文章 :

- 如何访问基于 Windows XP 或基于 Windows Server 2003 的主机计算机的远程桌面会话中的本地文件
- 使本地设备和资源可用于远程会话
- Mac 上的远程桌面客户端入门

停止和启动您的实例

Abstract

停止和启动将 Amazon EBS 卷作为根设备的任何实例。

您可以停止和重启将 Amazon EBS 卷作为其根设备的实例。实例会保留其实例 ID , 但是可以按照“概述”部分所述的方式进行修改。

当您终止一个实例时 , 我们会将其关闭。我们不对已停止的示例收取小时使用费或数据传输费 , 但我们会对所有 Amazon EBS 卷的存储收费。您每次启动一个已停止的实例 , 我们都会计为一个实例小时 , 即使这些转换在一小时内发生多次也是如此。

当实例停止时 , 您可以像对待所有其他卷一样修改根卷 (例如 , 修复文件系统问题或更新软件) 。您只需从停止的实例断开卷 , 将其连接到运行中的实例并进行修改 , 然后将其断开 , 再次连接到该已停止实例即可。请确保您已使用设备名称被指定为实例块储存设备映射中的根设备对其进行重新连接。

当您决定不再需要实例时 , 可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated` , 我们就会停止收取与该实例相关的费用。有关更多信息 , 请参阅 [终止您的实例 \(p. 232\)](#)。

内容

- [概述 \(p. 228\)](#)
- [停止和启动您的实例 \(p. 229\)](#)
- [修改已停止的实例 \(p. 229\)](#)
- [故障排除 \(p. 230\)](#)

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 \(p. 63\)](#)。

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。
- 实例会在启动时迁移到新的底层主机。
- EC2-Classic：当您停止实例时，我们会释放该实例的公有和私有 IP 地址，并在重启实例时为其分配新的 IP 地址。

EC2-VPC：实例在停止和重启时会保留其私有 IP 地址。我们会在您重启它时释放公有 IP 地址并分配新地址。

- EC2-Classic：对于与该实例关联的所有弹性 IP 地址，我们会取消其关联。您需要对未与该实例关联的弹性 IP 地址支付费用。当您重启实例时，必须将弹性 IP 地址与该实例关联；我们不自动执行此操作。

EC2-VPC：实例会保留其关联的弹性 IP 地址。您需要对所有与已停止实例关联的弹性 IP 地址付费。

- 当您停止和启动 Windows 实例时，EC2Config 服务会对该实例执行任务，例如，更改所有附加的 Amazon EBS 卷的驱动器号。有关这些默认值以及如何更改它们的更多信息，请参阅 [Amazon EC2 用户指南（适用于 Microsoft Windows 实例）](#) 中的 [使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)。
- 如果您在负载均衡器上注册该实例，那么当您停止并重启该实例后，负载均衡器很可能不能向您的实例传输数据流量。停止实例后，您必须从该负载均衡器取消注册，然后在启动后重新注册。有关更多信息，请参阅 [Elastic Load Balancing 用户指南](#) 中的 [利用负载均衡器注销和注册 EC2 实例](#)。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。有关更多信息，请参阅 [Auto Scaling 用户指南](#) 中的 [Auto Scaling 实例的健康检查](#)。
- 当您停止 ClassicLink 实例时，它会从链接的 VPC 取消链接。您必须在重新启动之后将实例再次链接到 VPC。有关 ClassicLink 的更多信息，请参阅 [ClassicLink \(p. 578\)](#)。

有关更多信息，请参阅 [重启、停止与终止之间的区别 \(p. 215\)](#)。

只有在实例停止时，您才能修改以下实例属性：

- 实例类型
- 用户数据
- 内核
- RAM 磁盘

如果您在实例运行时尝试修改这些属性，Amazon EC2 会返回 `IncorrectInstanceState` 错误。

停止和启动您的实例

您可以使用控制台或命令行启动和停止由 Amazon EBS 支持的实例。

在默认情况下，当您通过由 Amazon EBS 支持的实例启动关闭（使用 shutdown、halt 或 poweroff 命令）时，该实例会停止。您可以更改此行为，以便使其终止。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 234\)](#)。

使用控制台停止和启动由 Amazon EBS 支持的实例

1. 在导航窗格中，选择 Instances，然后选择实例。
2. [EC2-Classic] 如果实例具有关联的弹性 IP 地址，则写下详细信息窗格中显示的弹性 IP 地址和实例 ID。
3. 依次选择 Actions、Instance State 和 Stop。如果 Stop (停止) 处于禁用状态，则表示要么实例已停止，要么其根设备是一个实例存储卷。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，选择 Yes, Stop。停止实例可能需要几分钟时间。

[EC2-Classic] 当实例状态变为 stopped 时，详细信息窗格中的 Elastic IP (弹性 IP)、Public DNS (公有 DNS)、Private DNS (私有 DNS) 和 Private IPs (私有 IP) 字段为空，表明旧值不再与实例关联。

5. 当实例停止时，您可以修改特定的实例属性。有关更多信息，请参阅 [修改已停止的实例 \(p. 229\)](#)。
6. 要重启已停止的实例，请选择该实例，然后依次选择 Actions、Instance State 和 Start。
7. 在确认对话框中，选择 Yes, Start。实例进入 running 状态可能需要几分钟时间。

[EC2-Classic] 当实例状态为 running 时，详细信息窗格中的 Public DNS (公有 DNS)、Private DNS (私有 DNS) 和 Private IPs (私有 IP) 字段包含我们指定给实例的新值。

8. [EC2-Classic] 如果您的实例具有关联的弹性 IP 地址，则您必须按以下方式对其进行重新关联：
 - a. 在导航窗格中，选择 Elastic IPs。
 - b. 选择您在停止实例前所记下的弹性 IP 地址。
 - c. 选择 Actions，然后选择 Associate Address。
 - d. 选择您在停止实例前所记下的实例 ID，然后选择 Associate。

使用命令行停止和启动由 Amazon EBS 支持的实例

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

- stop-instances 和 start-instances (AWS CLI)
- Stop-EC2Instance 和 Start-EC2Instance (适用于 Windows PowerShell 的 AWS 工具)

修改已停止的实例

您可以使用 AWS 管理控制台或命令行界面来更改已停止实例的实例类型、用户数据或 EBS 优化属性。您无法使用 AWS 管理控制台修改 DeleteOnTermination、内核或 RAM 磁盘属性。

修改实例属性

- 要更改实例类型，请参阅[调整您的实例大小 \(p. 133\)](#)。
- 要更改您的实例的用户数据，请参阅[使用用户数据配置实例 \(p. 241\)](#)。
- 要为您的实例启用或禁用 EBS 优化，请参阅[修改 EBS 优化 \(p. 685\)](#)。
- 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 \(p. 718\)](#)。

使用命令行修改实例属性

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

- [modify-instance-attribute \(AWS CLI\)](#)
- [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

故障排除

如果停止了 Amazon EBS 支持的实例，该实例“卡在”了 stopping 状态，则可以强制停止它。有关更多信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的[排查实例的停止问题](#)。

重启您的实例

Abstract

使用 Amazon EC2 重启实例以便进行所需维护。

实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。重启实例时，其仍驻留在相同的物理主机上，因此您的实例将保留其公有 DNS 名称、私有 IP 地址及其实例存储卷上的任何数据。

重启实例不会启动新的实例计费时间，这与停止并重新启动您的实例不同。

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 \(p. 448\)](#)。

我们建议您使用 Amazon EC2 来重启实例，而非在实例中运行操作系统重启命令。如果您使用 Amazon EC2 重启实例，而实例在 4 分钟内未完全关闭，我们会执行硬重启。如果您使用 AWS CloudTrail，则使用 Amazon EC2 重启实例还会创建一条关于实例重启时间的 API 记录。

使用控制台重启实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances。
3. 选择相应实例，选择 Actions，然后依次选择 Instance State 和 Reboot。
4. 当系统提示您确认时，选择 Yes, Reboot。

使用命令行重启实例

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

- [reboot-instances \(AWS CLI\)](#)
- [Restart-EC2Instance \(适用于 Windows PowerShell 的 AWS 工具\)](#)

实例停用

Abstract

确定计划停用的实例，以及要用于管理停用的操作。

实例计划在 AWS 检测到托管实例的底层硬件发生无法弥补的故障时停用。当实例到达其计划的停用日期时，AWS 会将其停止或终止。如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。启动停止的实例会将其迁移到新的硬件。如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

主题

- [确认计划停用的实例 \(p. 231\)](#)
- [使用计划停用的实例 \(p. 231\)](#)

有关实例事件类型的更多信息，请参阅[实例的计划事件 \(p. 448\)](#)。

确认计划停用的实例

如果实例已计划停用，您将在事件发生之前收到包含实例 ID 和停用日期的电子邮件。该电子邮件将发送至与您账户关联的地址，也就是您用于登录 AWS 管理控制台的电子邮件地址。如果您使用的是并不定期检查的电子邮件账户，则可以使用 Amazon EC2 控制台或命令行确定是否有计划停用的实例。要更新您的账户的联系人信息，请转到[Account Settings \(账户设置\) 页面](#)。

使用控制台确认计划停用的实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 EC2 Dashboard。在 Scheduled Events (计划的事件) 下方，您可以看到与您的 Amazon EC2 实例和卷相关的事件，这些事件按区域划分。

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实例资源，然后从第二个筛选列表中选择实例停用。
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 \(p. 231\)](#)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 (根设备类型) 字段。如果值为 ebs，则说明您的实例是由 EBS 提供支持。如果值为 instance-store，则说明您的实例是由实例存储提供支持。

使用命令行确定您的实例根设备的类型

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

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

管理计划停用的实例

您可以执行下列操作中的一种，以保存将要停用的实例上的数据。务必要在实例停止日期前采取此操作，以防止意外的停机和数据丢失。



Warning

如果超过停用日期，由实例存储提供支持的实例就会停止，且无法恢复实例或存储在该实例上的任何数据。无论您的实例根设备是哪种类型，存储在实例存储卷上的数据都会在停用实例后丢失，即使它们附加到由 EBS 提供支持的实例也是如此。

实例根设备类型	操作
EBS	等到计划的停用日期（实例停止的日期），或在停用日期之前自行停止实例。您可随时重新启动实例。有关停止和启动实例以及停止实例后的预期情况（例如对与实例关联的公有、私有和弹性 IP 地址的影响）的更多信息，请参阅 停止和启动您的实例 (p. 227) 。
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 Windows AMI (p. 76) 。
实例存储	捆绑您的实例，然后从捆绑过程中生成的清单创建由实例存储提供支持的 AMI。您可以从新 AMI 启动替换实例。有关更多信息，请参阅 创建实例存储支持的 Windows AMI (p. 78) 。

终止您的实例

Abstract

终止不再需要的实例并停止该实例产生的费用。

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，就不再产生与该实例相关的费用。

在您终止之后，您将无法连接至或重新启动实例。但是您可以使用同一 AMI 启动其他实例。如果您宁愿停止并重启您的实例，请参阅[停止和启动您的实例 \(p. 227\)](#)。有关更多信息，请参阅[重启、停止与终止之间的区别 \(p. 215\)](#)。

主题

- [实例终止 \(p. 233\)](#)
- [终止实例 \(p. 233\)](#)
- [为实例启用终止保护 \(p. 234\)](#)
- [更改实例的启动关闭操作 \(p. 234\)](#)
- [在实例终止时保留 Amazon EBS 卷 \(p. 235\)](#)

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。您无法自行删除已终止的实例条目。

当实例终止时，与该实例关联的所有实例存储卷上的数据都会被删除。

默认情况下，当实例终止时，Amazon EBS 根设备卷将自动删除。但是，在默认情况下，即使在实例终止后，您在启动时挂载的所有额外 EBS 卷或您挂载到现有实例的所有 EBS 卷也会保留。这一操作是由卷的 `DeleteOnTermination` 属性控制的，您可以对其进行修改。有关更多信息，请参阅[在实例终止时保留 Amazon EBS 卷 \(p. 235\)](#)。

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 \(p. 234\)](#)。

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 \(p. 234\)](#)。

如果您在实例终止时运行脚本，您的实例可能会出现异常终止的情况，因为我们无法确保关闭脚本运行。Amazon EC2 会尝试彻底关闭实例，并运行任一系统关闭脚本；但某些事件（如硬件故障）可能会妨碍这些系统关闭脚本的运行。

终止实例

您可以使用 AWS 管理控制台或命令行终止实例。

使用控制台终止实例

1. 在终止实例前，请验证您不会丢失任何数据，方法是确认您的 Amazon EBS 卷不会在终止时被删除，并且您已将所需数据从实例存储卷复制到 Amazon EBS 或 Amazon S3。
2. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
3. 在导航窗格中，选择 Instances。
4. 选择相应实例，选择 Actions，然后依次选择 Instance State 和 Terminate。
5. 当系统提示您确认时，请选择 Yes, Terminate。

使用命令行终止实例

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

- `terminate-instances` (AWS CLI)
- `Stop-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

为实例启用终止保护

默认情况下，您可以使用 Amazon EC2 控制台、命令行界面或 API 终止您的实例。如果您希望使用 Amazon EC2 防止实例意外终止，可以启用实例终止保护。`DisableApiTermination` 属性可控制是否可以使用控制台、CLI 或 API 终止实例。在默认情况下，终止保护处于禁用状态。您可以在实例启动、运行或已停止时设置该属性值（针对由 Amazon EBS 支持的实例）。

当设置 `InstanceInitiatedShutdownBehavior` 属性时，`DisableApiTermination` 属性不会阻止您通过从实例启动关闭来终止实例（使用操作系统的系统关闭命令）。有关更多信息，请参阅 [更改实例的启动关闭操作 \(p. 234\)](#)。

您无法使用终止保护来阻止属于 Auto Scaling 组一部分的实例终止。不过，您可以指定首先应终止哪些实例。有关更多信息，请参阅 [Auto Scaling 用户指南](#) 中的 [选择终止策略](#)。

您不能为竞价型实例启用终止保护 – 当现货价格超过您的出价时，竞价型实例将终止。不过，您可以准备应用程序来处理竞价型实例中断。有关更多信息，请参阅 [竞价型实例中断 \(p. 197\)](#)。

您可以使用 AWS 管理控制台或命令行启用或禁用终止保护。

要在实例启动时启用终止保护

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在控制面板中，选择 Launch Instance 并按照向导中的说明操作。
3. 在 Configure Instance Details (配置实例详细信息) 页面上，选中 Enable termination protection (启用终止保护) 复选框。

启用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Termination Protection。
2. 选择 Yes, Enable。

禁用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Termination Protection。
2. 选择 Yes, Disable。

使用命令行启用或禁用终止保护

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

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (适用于 Windows PowerShell 的 AWS 工具)

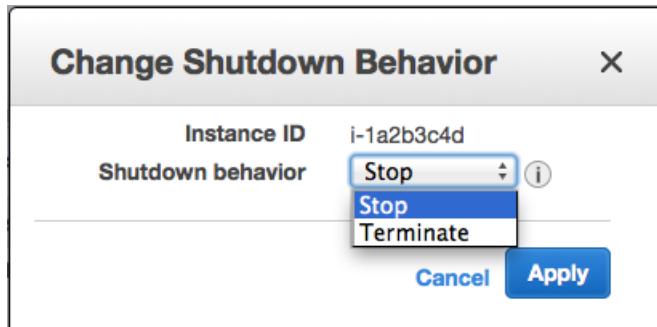
更改实例的启动关闭操作

在默认情况下，当通过由 Amazon EBS 支持实例使用关闭命令启动关闭（使用 `shutdown`、`halt` 或 `poweroff` 等命令）时，该实例会停止。您可以使用实例的 `InstanceInitiatedShutdownBehavior` 属性更改此操作，以便终止实例。您可以在实例运行或停止时更新此属性。

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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择相应实例，然后依次选择 Actions、Instance Settings、Change Shutdown Behavior。已选定当前操作。
4. 要更改该操作，请从 Shutdown behavior 列表中选择一个选项，然后选择 Apply。



使用命令行更改实例的关闭行为

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

- [modify-instance-attribute \(AWS CLI\)](#)
- [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在实例终止时保留 Amazon EBS 卷

当实例终止时，Amazon EC2 会使用每个挂载的 Amazon EBS 卷的 DeleteOnTermination 属性的值来确定是保留还是删除该卷。

默认情况下，实例的根卷的 DeletionOnTermination 属性将设置为 true。因此，当某个实例终止时，默认为删除该实例的根卷。

默认情况下，当您将 EBS 卷挂载到某个实例时，其 DeleteOnTermination 属性将设置为 false。因此，默认为保留这些卷。在该实例终止后，您可以为保留的卷拍摄快照，或将其挂载到另一个实例。

要验证使用中的 EBS 卷的 DeleteOnTermination 属性的值，请查看该实例的块储存设备映射。有关更多信息，请参阅 [查看实例块储存设备映射中的 EBS 卷 \(p. 718\)](#)。

在启动该实例或在该实例正在运行时，您可以更改卷的 DeleteOnTermination 属性的值。

示例

- [使用控制台将根卷更改为在启动时持久保留 \(p. 235\)](#)
- [使用命令行将根卷更改为在启动时持久保留 \(p. 236\)](#)
- [使用命令行更改要持久保留正在运行的实例的根卷 \(p. 236\)](#)

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.amazonaws.cn/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，单击根设备卷的条目。默认情况下，Delete on termination (终止时删除) 为 True。如果您更改默认行为，Delete on termination (终止时删除) 将为 False。

使用命令行将根卷更改为在启动时持久保留

当您启动实例时，您可以使用下列命令之一将根设备卷更改为持久保留。根设备通常是 /dev/sda1。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

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

例如，将以下选项添加到 run-instances 命令：

```
--block-device-mappings file://mapping.json
```

在 mapping.json 中指定以下内容：

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false,  
      "SnapshotId": "snap-1234567890abcdef0",  
      "VolumeType": "gp2"  
    }  
  }  
]
```

使用命令行更改要持久保留正在运行的实例的根卷

您可以使用下列命令之一将正在运行的实例的根设备卷更改为持久保留。根设备通常是 /dev/sda1。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：

```
C:\> 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  
    }  
  }  
]
```

恢复您的实例

Abstract

如果您的 Amazon EC2 实例因底层硬件故障而受损，您可以通过创建可恢复实例的 Amazon CloudWatch 警报来恢复该实例。

您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。有关使用 Amazon CloudWatch 警报恢复实例的更多信息，请参阅[创建停止、终止、重启或恢复实例的警报 \(p. 483\)](#)。要对实例恢复故障进行故障排除，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的[排除实例恢复故障](#)。

当 StatusCheckFailed_System 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您会注意到，实例在已恢复的实例上重启。

导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题



Important

恢复操作仅受到以下项支持：

- C3、C4、M3、M4、R3、T2 和 X1 实例类型。
- VPC 中的实例



Note

如果您的实例有公有 IP 地址，它会在恢复后保留相同的公有 IP 地址。

- 使用共享租赁的实例（实例的租赁属性设置为 default）
- 完全使用 Amazon EBS 存储的实例

目前，以下实例不支持恢复操作：

- EC2-Classic 实例

- 专用租赁实例
- 运行在专用主机上的实例
- 使用加密 EBS 卷的实例
- 使用任何实例存储卷的实例，包括使用实例存储卷的块储存设备映射启动的实例



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- `ec2:DescribeInstanceStatus` 和 `ec2:DescribeInstances`，针对有关 Amazon EC2 实例状态指标的所有警报。
- `ec2:StopInstances`，针对包含停止操作的警报。
- `ec2:TerminateInstances`，针对包含终止操作的警报。
- `ec2:DescribeInstanceRecoveryAttribute` 和 `ec2:RecoverInstances`，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 *IAM 用户指南* 中的 [权限与策略](#)。

如果您正在使用 IAM 角色（例如 Amazon EC2 实例配置文件），则无法使用警报操作来停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您正在使用 AWS Security Token Service (AWS STS) 授予的临时安全凭证，则无法使用警报操作来停止、终止或重启 Amazon EC2 实例。

配置您的 Windows 实例

Abstract

自定义您的 Windows 实例。

Windows 实例在云中运行 Microsoft Windows Server 的虚拟服务器。

在成功启动和登录您的实例之后，您可以对其进行更改，以便配置满足特定应用程序的需要。下面是一些可帮助您入门的常见任务。

内容

- [实例元数据和用户数据 \(p. 239\)](#)
- [使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)
- [半虚拟化驱动程序 \(p. 272\)](#)
- [设置 Windows 实例的密码 \(p. 288\)](#)
- [为 Windows 实例设置时间 \(p. 292\)](#)
- [管理 Windows 实例配置 \(p. 294\)](#)
- [将 Windows 实例加入 AWS Directory Service 域 \(p. 299\)](#)
- [使用 Amazon EC2 Simple Systems Manager 将性能计数器发送到 CloudWatch，将日志发送到 CloudWatch Logs \(p. 308\)](#)

- 为 VPC 中的 Windows 实例配置辅助私有 IP 地址 (p. 319)
- 将 Windows Server EC2 实例升级到新版本 Windows Server (p. 324)

实例元数据和用户数据

Abstract

访问实例元数据、动态数据和用户数据，以配置和管理正在运行的实例。

实例元数据 是有关您的实例的数据，可以用来配置或管理正在运行的实例。实例元数据可划分成不同类别。有关更多信息，请参阅 [实例元数据类别 \(p. 245\)](#)。

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 \(p. 248\)](#)。

您也可以访问在启动您的实例时所提供的用户数据。例如，您可指定参数以便配置实例，也可连接简单的脚本。您也可以使用这些数据来构建更多可通过启动时提供的配置文件来修改的通用 AMI。例如，如果您为各种小型企业运行 Web 服务器，则这些企业都可以使用相同的 AMI，并在启动时从您在用户数据中指定的 Amazon S3 存储桶中检索其各自的内容。要随时添加一个新客户，您只需为该客户创建一个存储桶，将客户的内容添加进去，然后启动您的 AMI 即可。如果您同时启动多个实例，则用户数据可供该预留中的所有实例使用。



Important

虽然您只能从实例自身内部访问实例元数据和用户数据，但数据并未进行加密保护。可访问实例的人员均可查看其元数据。因此，您应当采取适当的预防措施来保护敏感数据（例如永久加密密钥）。不应将敏感数据（例如密码）存储为用户数据。

内容

- [检索实例元数据 \(p. 239\)](#)
- [使用用户数据配置实例 \(p. 241\)](#)
- [检索用户数据 \(p. 244\)](#)
- [检索动态数据 \(p. 244\)](#)
- [实例元数据类别 \(p. 245\)](#)
- [实例标识文档 \(p. 248\)](#)

检索实例元数据

由于您的正在运行的实例存在实例元数据，因此您无需使用 Amazon EC2 控制台或 AWS CLI。这在您编写脚本以实现从实例运行时非常有用。例如，您可从实例元数据访问您的实例的本地 IP 地址来以管理与外部应用程序的连接。

要从运行实例内部查看所有类别的实例元数据，请使用以下 URI：

```
http://169.254.169.254/latest/meta-data/
```

请注意，您无需为用于检索实例元数据和用户数据的 HTTP 请求付费。

您可以安装一种诸如 GNU Wget 或 cURL 的工具以在命令行中检索实例元数据，或者您可以将 URI 复制并粘贴到浏览器中。如果您不想安装任何第三方工具，则可以使用 PowerShell cmdlet 检索 URI。例如，如果您在运行 3.0 版本或更高版本的 PowerShell，请使用以下 cmdlet：

```
PS C:\> invoke-restmethod -uri http://169.254.169.254/latest/meta-data/
```



Important

如果您在 Windows 实例上安装第三方工具，请确保您仔细阅读随附的文档，因为调用 HTTP 的方法以及输出格式可能与此处记录的内容不同。

所有元数据以文本形式返回（内容类型 `text/plain`）。对特定元数据资源的请求会返回一个相应的值，如果该资源不可用，则会返回 HTTP 错误代码 `404 - Not Found`。

对通用元数据资源的请求（以 / 结尾的 URI）会返回一个可用资源列表，如果此类资源不存在，则会返回 HTTP 错误代码 `404 - Not Found`。列表中的各个项目位于被换行符 (ASCII 10) 终止的不同的行上。

检索实例元数据的示例

此示例可以获取实例元数据的可用版本。这些版本不一定与 Amazon EC2 API 版本相关联。如果您有依赖于以前版本中所存在的结构和信息的脚本，则您可使用早期版本。

```
C:\> curl http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
latest
```

此示例获得顶级元数据项目。一些项目只可用于 VPC 中的实例。有关这些项目中每一项的更多信息，请参阅 [实例元数据类别 \(p. 245\)](#)。

```
C:\> curl http://169.254.169.254/latest/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
instance-action  
instance-id  
instance-type  
kernel-id  
local-hostname  
local-ipv4  
mac  
network/  
placement/  
public-hostname  
public-ipv4  
public-keys/
```

```
reservation-id  
security-groups  
services/
```

这些示例获得前面示例中的一些元数据项目的值。

```
C:\> curl http://169.254.169.254/latest/meta-data/ami-id  
ami-2bb65342
```

```
C:\> curl http://169.254.169.254/latest/meta-data/reservation-id  
r-fca54097
```

```
C:\> curl http://169.254.169.254/latest/meta-data/hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

此示例显示可用于 EC2-Classic 平台中 NAT 实例上特定网络接口（由 MAC 地址表示）的信息。

```
C:\> curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/  
device-number  
local-hostname  
local-ipv4s  
mac  
owner-id  
public-hostname  
public-ipv4s
```

此示例获得启动至 VPC 的实例的子网 ID。

```
C:\> curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id  
subnet-be9b61d7
```

使用用户数据配置实例

指定用户数据时，请注意以下几点：

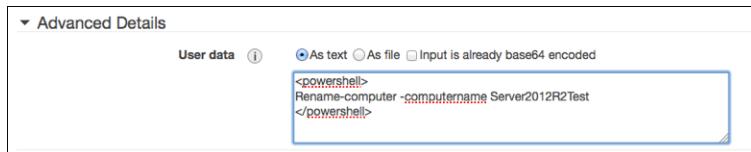
- 用户数据会被视为非透明数据；您提供什么数据您就会得到什么数据。由实例对其进行解释。
- 用户数据被限制在 16 KB 以内。这种限制适用于原始形式的数据，而不是 Base64 编码形式的数据。
- 用户数据必须在提交给 API 前先进行 Base64 编码。EC2 命令行工具为您执行 base64 编码。在提交给实例之前，数据会被解码。有关 base64 编码的更多信息，请参阅 <http://tools.ietf.org/html/rfc4648>。
- 用户数据仅在启动时执行。如果停止实例，修改用户数据，然后启动实例，则新的用户数据不会自动执行。

主题

- [使用用户数据执行脚本 \(p. 242\)](#)
- [使用用户数据覆盖初始化驱动器设置 \(p. 243\)](#)
- [为正在运行的实例修改用户数据 \(p. 244\)](#)

使用用户数据执行脚本

您可指定脚本在实例启动时执行。在实例配置向导的 User data 部分中输入脚本。User data 选项位于 Step 3: Configure Instance Details 页面上的 Advanced Details 部分中。下图中的示例将在实例启动时将实例名称更改为 *Server2012R2Test*。



为了 EC2Config 能执行用户数据脚本，您必须将指定脚本的各行包含在以下某个特殊标签内：

<script></script>
运行您可以在命令提示符窗口运行的任何命令。

示例：
<script>dir > c:\test.log</script>
<powershell></powershell>
运行您可以通过 Windows PowerShell 命令提示符运行的任何命令。

如果您使用的 AMI 包含适用于 Windows PowerShell 的 AWS 工具，您还可以使用以上 cmdlet。如果您在启动自己的实例时指定了一个 IAM 角色，那么您不必为 cmdlet 指定凭证，因为实例上运行的应用程序可以使用该角色的凭证访问 AWS 资源，例如 Amazon S3 存储桶。

示例：
<powershell>Read-S3Object -BucketName myS3Bucket -Key myFolder/myFile.zip
-File c:\destinationFile.zip</powershell>

您可以在脚本中使用换行符分隔命令。

如果 EC2Config 发现 script 或 powershell 标记，它会将脚本保存到其 /Scripts 文件夹中的批处理文件或 PowerShell 文件中。并在实例启动时运行这些文件。如果 script 和 powershell 标签同时存在，则无论它们以什么顺序显示，都会先运行批处理脚本，然后再运行 PowerShell 脚本。

/Logs 文件夹中包含源自标准输出和标准错误流的输出。

EC2Config 预计用户数据会以 base64 编码的形式显示。如果用户数据不是以 base64 编码的形式显示，EC2Config 会记录有关无法找到要执行的 script 或 powershell 标签的错误。如果您的编码不正确，以下示例指明了如何使用 PowerShell 设置编码。

```
$UserData = [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Initial Boot (初始启动)

默认情况下，所有 Amazon AMI 均已为初始启动启用用户数据执行。如果您在 EC2Config 中单击 Shutdown with Sysprep，无论 User Data 复选框的设置如何，系统都会启用用户数据脚本执行。

仅当随机密码生成之后，本地管理员用户才可执行用户数据脚本。这是因为 EC2Config 会生成密码，并且暂时获知凭证（在发送到控制台之前）。EC2Config 不会存储或跟踪密码更改，因此如果您没有生成随机密码，则 EC2Config 服务账户会执行用户数据。

Subsequent Boots (后续启动)

因为初次启动后 Amazon AMI 会自动禁用用户数据脚本执行，所以必须执行以下操作之一，才能在重新启动后保留用户数据：

- 您可以借助 `schtasks.exe /Create` 以编程的方式创建系统启动时要运行的计划任务，然后将计划任务指向 `C:\Program Files\Amazon\Ec2ConfigService\Scripts\UserScript.ps1` 处的用户数据脚本（或其他脚本）。
- 使用类似于以下内容的脚本在 `Config.xml` 中以编程方式启用用户数据插件：

```
<powershell>
$EC2SettingsFile="C:\Program Files\Amazon\Ec2ConfigService\Settings\Config.xml"
$xml = [xml](get-content $EC2SettingsFile)
$xmlElement = $xml.get_DocumentElement()
$xmlElementToModify = $xmlElement.Plugins

foreach ($element in $xmlElementToModify.Plugin)
{
    if ($element.name -eq "Ec2SetPassword")
    {
        $element.State="Enabled"
    }
    elseif ($element.name -eq "Ec2HandleUserData")
    {
        $element.State="Enabled"
    }
}
$xml.Save($EC2SettingsFile)
</powershell>
```

- 从 EC2Config 版本 2.1.10 开始，您可以在执行用户数据后使用 `<persist>true</persist>` 来重新启用该插件。

```
<powershell>
    insert script here
</powershell>
<persist>true</persist>
```

使用用户数据覆盖初始化驱动器设置

使用以下设置用用户数据覆盖初始化驱动器设置。每次重新启动实例时都会使用这些设置。

```
<InitializeDrivesSettings>
    <SettingsGroup>FormatWithoutTRIM</SettingsGroup>
</InitializeDrivesSettings>
```



Note

使用设置组指定要如何初始化驱动器。

- `FormatWithoutTRIM`：在格式化驱动器时，此设置禁用 TRIM 命令并在 Windows 中改进格式化时间。在驱动器格式化和初始化后，系统还原 TRIM 配置。
- `DisableInitializeDrives`：此设置禁止格式化新驱动器。使用此设置可手动初始化驱动器。

为正在运行的实例修改用户数据

您可以为之前已分配有用户数据且当前正在运行的实例修改用户数据。在重启您的实例之后，新用户数据在实例上可用。

修改 Amazon EBS 支持的实例的用户数据

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 单击 Actions，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，单击 Yes, Stop。停止实例可能需要几分钟时间。
5. 在实例仍处于选中状态的情况下，选择 Actions，选择 Instance Settings，然后选择 View/Change User Data。请注意，如果实例正在运行，您不能更改用户数据，但是可以查看。
6. 在 View/Change User Data 对话框中，更新用户数据，然后选择 Save。

检索用户数据

要检索用户数据，请使用以下 URI：

```
http://169.254.169.254/latest/user-data
```

请求用户数据时，所返回的是未经任何更改的原样数据（内容类型 application/x-octetstream）。

此处显示的是返回逗号分隔用户数据的示例。

```
C:\> curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

此处显示的是返回行分隔的用户数据的示例。

```
C:\> curl http://169.254.169.254/latest/user-data
[general]
instances: 4

[instance-0]
s3-bucket: <user_name>

[instance-1]
reboot-on-error: yes
```

检索动态数据

要在运行实例内部检索动态数据，请使用以下 URI：

```
http://169.254.169.254/latest/dynamic/
```

此示例介绍如何检索高级实例标识类别：

```
C:\> curl http://169.254.169.254/latest/dynamic/instance-identity/  
pkcs7  
signature  
document
```

有关动态数据的详细信息和如何对其进行检索的示例，请参阅 [实例标识文档 \(p. 248\)](#)。

实例元数据类别

下表列举了实例元数据的类别。

Data	说明	引入的版本
ami-id	用于启动实例的 AMI ID。	1.0
ami-launch-index	如果您同时启动了多个实例，此值表示实例启动的顺序。第一个启动的实例的值是 0。	1.0
ami-manifest-path	指向 Amazon S3 中的 AMI 清单文件的路径。如果您使用 Amazon EBS 支持的 AMI 来启动实例，则返回的结果为 unknown。	1.0
ancestor-ami-ids	为创建此 AMI 而重新绑定的任何实例的 AMI ID。仅当 AMI 清单文件包含一个 ancestor-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 Amazon EBS 卷相关联的虚拟设备（如果存在）。如果 Amazon EBS 卷在启动时存在或者在上一次启动该实例时存在，那么这些卷仅在元数据中可用。N 表示 Amazon EBS 卷的索引（例如 ebs1 或 ebs2）。	2007-12-15
block-device-mapping/ephemeral 否	与短暂设备相关联的虚拟设备，如果存在的话。N 表示临时卷的索引。	2007-12-15
block-device-mapping/root	与根设备相关联的虚拟设备或分区，或虚拟设备上的分区（在根（/ 或 C:）文件系统与给定实例相关联的情况下）。	2007-12-15
block-device-mapping/swap	与 swap 相关联的虚拟设备。并不总是存在。	2007-12-15
hostname	实例的私有主机名。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

Data	说明	引入的版本
iam/info	如果启动时存在与实例关联的 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/ <i>role-name</i>	如果启动时存在与实例关联的 IAM 角色，则 <i>role-name</i> 为角色的名称，并且 <i>role-name</i> 包含与角色关联的临时安全凭证（有关更多信息，请参阅 通过实例元数据检索安全证书 (p. 566) ）。如果没有，则不显示。	2012-01-12
instance-action	通知实例在准备打包时重新启动。有效值：none shutdown bundle-pending。	2008-09-01
instance-id	此实例的 ID。	1.0
instance-type	实例的类型。有关更多信息，请参阅 实例类型 (p. 110) 。	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 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	该实例的私有 IP 地址。在存在多个网络接口的情况下，其指的是 eth0 设备（设备号为 0 的设备）。	1.0
mac	实例的媒体访问控制 (MAC) 地址。在存在多个网络接口的情况下，其指的是 eth0 设备（设备号为 0 的设备）。	2011 年 1 月 1 日
network/interfaces/macs/mac/device-number	与该接口相关联的唯一设备号。设备号与设备名称对应；例如，device-number 为 2 对应于 eth2 设备。此类别对应的是 Amazon EC2 API 和 AWS CLI 的 EC2 命令使用的 DeviceIndex 和 device-index 字段。	2011 年 1 月 1 日
network/interfaces/macs/mac/ipv4-associations/public-ip	与每个 public-ip 地址相关联并被分配给该接口的私有 IPv4 地址。	2011 年 1 月 1 日
network/interfaces/macs/mac/local-hostname	实例的本地主机名称。	2011 年 1 月 1 日
network/interfaces/macs/mac/local-ipv4s	与接口相关联的私有 IP 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

Data	说明	引入的版本
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	实例的公有 DNS。如果实例在 VPC 中，则仅当 enableDnsHostnames 属性设置为 true 时返回此类别。有关更多信息，请参阅 在您的 VPC 中使用 DNS 。	2011 年 1 月 1 日
network/interfaces/macs/mac/public-ipv4s	与接口相关联的弹性 IP 地址。一个实例上可能有多个 IP 地址。	2011 年 1 月 1 日
network/interfaces/macs/mac/security-groups	网络接口所属的安全组。仅对启动至 VPC 的实例返回。	2011 年 1 月 1 日
network/interfaces/macs/mac/security-group-ids	网络接口所属的安全组的 ID。仅对启动至 VPC 的实例返回。有关 EC2-VPC 平台上安全组的更多信息，请参阅 您的 VPC 的安全组 。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-id	接口所驻留的子网的 ID。仅对启动至 VPC 的实例返回。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-ipv4-cidr-block	接口所驻留的子网的 CIDR 块。仅对启动至 VPC 的实例返回。	2011 年 1 月 1 日
network/interfaces/macs/mac/vpc-id	接口所驻留的 VPC 的 ID。仅对启动至 VPC 的实例返回。	2011 年 1 月 1 日
network/interfaces/macs/mac/vpc-ipv4-cidr-block	接口所驻留的 VPC 的 CIDR 块。仅对启动至 VPC 的实例返回。	2011 年 1 月 1 日
placement/availability-zone	实例启动的可用区域。	2008-02-01
product-codes	与实例相关联的产品代码，如果有的话。	2007-03-01
public-hostname	实例的公有 DNS。如果实例在 VPC 中，则仅当 enableDnsHostnames 属性设置为 true 时返回此类别。有关更多信息，请参阅 在您的 VPC 中使用 DNS 。	2007-01-19
public-ipv4	公用 IP 地址。如果弹性 IP 地址与实例相关联，返回的值是弹性 IP 地址。	2007-01-19
public-keys/0/openssh-key	公用密钥。仅在实例启动时提供了公用密钥的情况下可用。	1.0
ramdisk-id	启动时指定的 RAM 磁盘的 ID，如果适用的话。	2007-10-10
reservation-id	预留的 ID。	1.0

Data	说明	引入的版本
security-groups	应用到实例的安全组的名称。启动之后，您只能更改正在 VPC 中运行的实例的安全组。这些更改将体现在此处和 network/interfaces/macs/ <i>mac</i> /security-groups 中。	1.0
services/domain	用于区域的 AWS 资源的域；例如用于 us-east-1 的 amazonaws.com。	2014-02-25
services/partition	资源所处的分区。对于标准 AWS 区域，分区是 aws。如果资源位于其他分区，则分区是 aws- <i>partition-name</i> 。例如，位于中国（北京）区域的资源的分区为 aws-cn。	2015-10-20
spot/termination-time	竞价型实例操作系统将收到关闭信号的大致时间 (UTC)。仅当竞价型实例已由 Amazon EC2 标记为终止时，此项目才会出现并包含时间值（例如，2015-01-05T18:02:00Z）。如果您自己终止了竞价型实例，那么终止时间项目不会设置时间。	2014-11-05

动态数据类别

下表列举了动态数据的类别。

Data	说明	引入的版本
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 实例标识文档 (p. 248) 。	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 实例标识文档 (p. 248) 。	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 实例标识文档 (p. 248) 。	2009-04-04

实例标识文档

Abstract

使用实例标识文档验证实例的属性。

实例标识文档是描述实例的 JSON 文件。实例标识文档带有一个签名和一个 PKCS7 签名，这些签名可用于验证文档中提供的信息的准确性、来源和真实性。例如，您可能下载了包含付费更新的免费软件。

实例标识文档在实例启动时生成，并通过[实例元数据 \(p. 239\)](#)向实例公开。它会验证实例的属性，如订阅的软件、实例大小、实例类型、操作系统和 AMI。



Important

由于实例标识文档和签名的动态性质，我们建议定期检索一次实例标识文档和签名。

获取实例标识文档和签名

若要取回实例身分文件，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/document

{
    "devpayProductCodes" : null,
    "availabilityZone" : "us-east-1d",
    "privateIp" : "10.158.112.84",
    "version" : "2010-08-31",
    "region" : "us-east-1",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t1.micro",
    "accountId" : "123456789012",
    "pendingTime" : "2015-11-19T16:32:11Z",
    "imageId" : "ami-5fb8c835",
    "kernelId" : "aki-919dcraf8",
    "ramdiskId" : null,
    "architecture" : "x86_64"
}
```

若要取回实例身分签名，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/signature

dExamplesjNQhhJan7pORLpLSr7lJEF4V2DhKGlyoYVB0UWrY9nJyBCmhEayaGrhtS/AWY+LPx
1VSQURF5n0gwPNCuO6ICT0fNrm5IH7w9ydyalexamplejJw8XvWPxbuRkcN0TAA1p4RtCAqm4ms
x2oALjWSCBExample=
```

若要取回 PKCS7 签名，请对正在运行的实例使用以下 URL：

```
http://169.254.169.254/latest/dynamic/instance-identity/pkcs7

MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTA1dBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgnVBAsTC01BTsBDb25zb2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEg5vb251QGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxJCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTA1dBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgnVBAsTC01BTsBDb25z
b2x1MRIwEAYDVQQDEwlUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEg5vb251QGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAaRHd1QWIMm2nrAgMBAAwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYS5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE
```

使用 EC2Config 服务配置 Windows 实例

Abstract

使用 EC2Config 服务配置 Windows 实例以访问高级功能。

AWS Windows AMI 包含 Amazon Web Services 安装的一项附加服务：EC2Config 服务。尽管此服务是可选的，但可让您访问否则无法访问的高级功能。此服务会在 LocalSystem 账户中运行并执行实例上的相关任务。例如，它可以将 Windows 事件日志和 IIS 请求日志发送至 Amazon CloudWatch Logs。有关如何配置 EC2Config 以用于 CloudWatch Logs 的更多信息，请参阅[使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。 \(p. 260\)](#)。服务二进制文件和其他文件位于 %ProgramFiles%\Amazon\EC2ConfigService 目录中。

实例启动时 EC2Config 服务也会启动。初始实例启动期间以及您每次停止和启动实例时，该服务会执行相关任务。它还可按需执行任务。部分任务可自动启用，而其他任务必须手动启用。EC2Config 会使用设置文件来控制它的操作。您可以通过图形工具或直接编辑 XML 文件来更新这些设置文件。

EC2Config 服务会运行 Sysprep，借助该 Microsoft 工具您可以创建可重复使用的自定义 Windows AMI。有关更多信息，请参阅[使用 Sysprep 创建标准 Amazon 系统映像 \(AMI\) \(p. 105\)](#)。

EC2Config 调用 Sysprep 时，会使用 EC2ConfigService\Settings 中的设置文件来确定要执行的操作。您可以使用 Ec2 Service Properties 对话框间接编辑这些文件，也可以使用 XML 编辑器或文本编辑器直接进行编辑。然而，有些高级设置并未包含在 Ec2 Service Properties (Ec2 服务属性) 对话框中，因此您必须直接编辑这些条目。

如果您在更新某实例的设置之后从中创建了一个 AMI，则新设置会应用到所有从新 AMI 启动的实例。有关创建 AMI 的信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

内容

- [EC2Config 任务概述 \(p. 250\)](#)
- [Ec2 服务属性 \(p. 251\)](#)
- [EC2Config 设置文件 \(p. 253\)](#)
- [配置 EC2Config 服务的代理设置 \(p. 257\)](#)
- [管理 EC2Config 服务 \(p. 258\)](#)
- [使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。 \(p. 260\)](#)
- [排查 EC2Config 服务的问题 \(p. 271\)](#)

EC2Config 任务概述

当系统首次启动实例后又将其禁用时，EC2Config 会运行初始启动任务。要再次运行这些任务，您必须在关闭实例之前明确启用它们，或者手动运行 Sysprep。这些任务如下所示：

- 设置管理员账户的随机加密密码。
- 生成和安装远程桌面连接使用的主机证书。
- 请动态扩展操作系统分区，以包含所有未分区的空间。
- 执行指定的用户数据（和 Cloud-Init，如果已安装）。

每次实例启动时，EC2Config 会执行以下任务：

- 更改主机名称以与十六进制表示法的私有 IP 地址匹配（此任务在默认情况下处于禁用状态，必须启用才能在实例启动时运行）。
- 配置密钥管理服务器 (KMS)，检查 Windows 激活状态并根据需要激活 Windows。
- 格式化并挂载所有 Amazon EBS 卷和实例存储卷，并且将卷名称映射到驱动器盘符。

- 将事件日志条目写入控制台以帮助排查问题（此任务在默认情况下处于禁用状态，必须进行启用才能在实例启动时运行）。
- 将 Windows 已准备就绪写入控制台。
- 已连接多个 NIC 时，向主网适配器添加自定义路由，以启用以下 IP 地址：169.254.169.250、169.254.169.251 和 169.254.169.254。当您访问实例元数据时，Windows 激活会使用这些地址。

每次用户登录时，EC2Config 都会执行以下任务：

- 在桌面背景中显示墙纸信息。

实例运行时，您可以请求 EC2Config 按需执行以下任务：

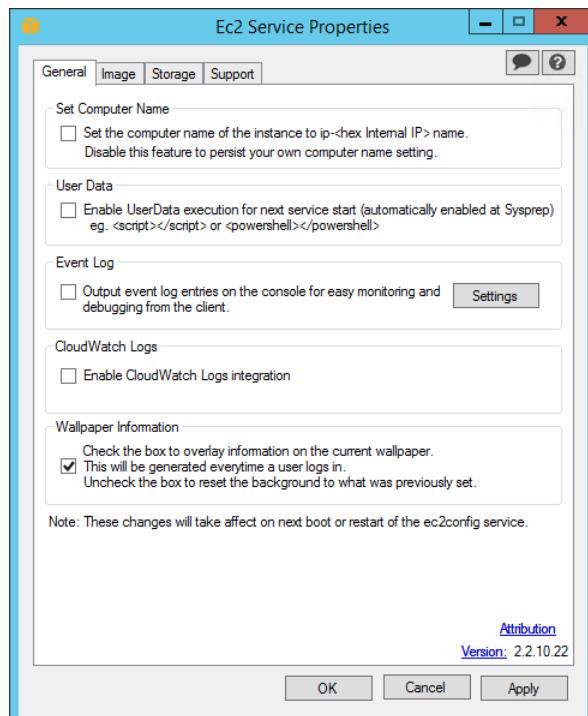
- 运行 Sysprep 并关闭实例，以便您可以从实例中创建一个 AMI。有关更多信息，请参阅 [使用 Sysprep 创建标准 Amazon 系统映像 \(AMI\) \(p. 105\)](#)。

Ec2 服务属性

以下过程介绍如何使用 Ec2 Service Properties 对话框来启用或禁用设置。

使用 Ec2 Service Properties 对话框更改设置

1. 启动并连接到您的 Windows 实例。
2. 在 Start (开始) 菜单中，单击 All Programs (所有程序)，然后单击 EC2ConfigService Settings (EC2ConfigService 设置)。



3. 在 Ec2 Service Properties 对话框的 General 标签上，您可以启用或禁用以下设置。

Set Computer Name

如果此设置已启用（默认情况下已启用），则会在每次启动时将主机名与当前内部 IP 地址进行比较；如果主机名和内部 IP 地址不匹配，则重置主机名以包含内部 IP 地址，随后系统重启以接受新主机名。若要设置您自己的主机名或防止修改现有主机名，请不要启用该设置。

User Data

执行用户数据让您可以在首次启动期间将脚本插入实例元数据。在实例中，您可以通过 <http://169.254.169.254/latest/user-data/> 读取用户数据。实例存在期间此类信息保持不变，而且在实例停止和启动时会持久保留直到实例终止。

如果您使用的是大型脚本，我们建议您使用用户数据来下载该脚本，然后再执行它。

有关更多信息，请参阅 [使用用户数据执行脚本 \(p. 242\)](#)。

Event Log (事件日志)

使用此设置可在启动期间在控制台上显示事件日志条目，以便轻松监控和调试。

单击 Settings (设置)，为发送到控制台的日志条目指定筛选条件。默认筛选条件会将来自系统事件日志的最近三个错误条目发送到控制台。

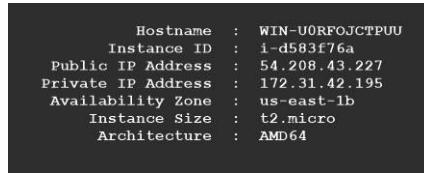
CloudWatch Logs (CloudWatch 日志)

从 EC2Config 版本 2.2.5 开始（建议使用版本 2.2.6 或更高版本），可以将系统日志、安全日志、应用程序日志和 IIS 日志中的所有 Windows Server 消息导出到 CloudWatch Logs，并使用 CloudWatch 指标对它们进行监控。EC2Config 版本 2.2.10 或更高版本添加了将任何事件日志数据、事件跟踪 (Windows) 数据或基于文本的日志文件导出到 CloudWatch Logs 的功能。此外，您还可以将性能计数器数据导出到 CloudWatch。有关更多信息，请参阅 Amazon CloudWatch 开发者指南中的 [监控系统、应用程序和自定义日志文件](#)。

1. 选择 Enable CloudWatch integration (启用 CloudWatch 集成)，然后单击 OK (确定)。
2. 编辑 `\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` 文件并配置要发送到 CloudWatch Logs 的日志的类型。有关更多信息，请参阅 [使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。 \(p. 260\)](#)。

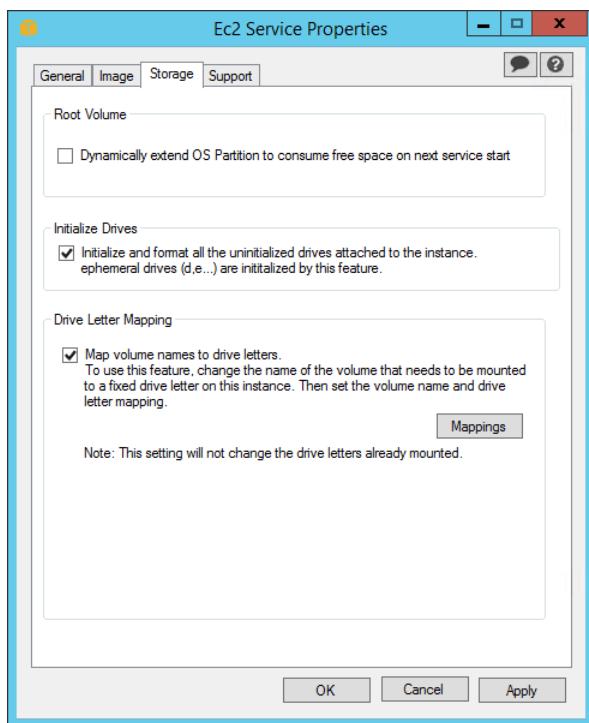
Wallpaper Information (壁纸信息)

使用此设置可在桌面背景中显示系统信息。以下是桌面背景上所显示信息的示例。



桌面背景上显示的信息受设置文件 `EC2ConfigService\Settings\WallpaperSettings.xml` 控制。

4. 单击 Storage 标签。您可以启用或禁用以下设置。



Root Volume

此设置可将磁盘 0/卷 0 动态扩展以包含所有未分区的空间。从具有自定义大小的根设备卷启动实例时，此设置非常有用。

Initialize Drives

此设置可格式化并挂载在启动期间附加到实例的所有卷。

Drive Letter Mapping (驱动器号映射)

系统会将附加到实例的卷映射到驱动器号。对于 Amazon EBS 卷，默认以从 D: 到 Z: 的顺序分配驱动器盘符。对于实例存储卷，默认设置则取决于驱动器。Citrix 半虚拟化驱动程序以从 Z: 到 A: 的顺序分配实例存储卷驱动器盘符。Red Hat 驱动程序按 D: 到 Z: 的顺序分配实例存储卷驱动器号。

要为您的卷选择驱动器号，请单击 **Mappings** (映射)。在 **DriveLetterSetting** (驱动器盘符设置) 对话框中，为每个卷指定 **Volume Name** (卷名称) 和 **Drive Letter** (驱动器盘符) 值，然后单击 **OK** (确定)。我们建议您选择诸如字母表中间的字母作为驱动器号，以避免与可能在使用的驱动器号发生冲突。

在指定驱动器号映射并连接与您指定的某个卷名称具有相同标签的卷之后，EC2Config 会自动为该卷分配您指定的驱动器号。然而，如果驱动器号已在使用，则驱动器号映射会失败。请注意，在您指定驱动器号映射之后，EC2Config 不会更改已装载卷的驱动器号。

5. 要保存您的设置并在稍后继续对其进行处理，请单击 **OK** (确定) 以关闭 **Ec2 Service Properties** (**Ec2 服务属性**) 对话框。如果您已完成实例自定义并要从该实例创建 AMI，请参阅 [使用 Sysprep 创建标准 Amazon 系统映像 \(AMI\) \(p. 105\)](#)。

EC2Config 设置文件

设置文件会控制 EC2Config 服务的操作。这些文件位于 C:\Program Files\Amazon\Ec2ConfigService\Settings 目录中：

- ActivationSettings.xml – 使用密钥管理服务器 (KMS) 控制产品激活。

- AWS.EC2.Windows.CloudWatch.json – 控制要发送到 CloudWatch 的性能计数器以及要发送到 CloudWatch Logs 的日志。有关如何更改此文件中的设置的更多信息，请参阅[使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。\(p. 260\)](#)。
- BundleConfig.xml - 控制 EC2Config 为 AMI 创建准备实例存储支持的实例的方式。请注意，只有 Windows Server 2003 实例才是可以由实例存储支持的 Windows 实例。
- Config.xml : 控制基本设置。
- DriveLetterConfig.xml : 控制驱动器号映射。
- EventLogConfig.xml : 控制实例启动时控制台上显示的事件日志信息。
- WallpaperSettings.xml : 控制桌面背景上显示的信息。

ActivationSettings.xml

此文件包含用于控制产品激活的设置。当 Windows 启动时，EC2Config 服务会检查是否已激活 Windows。如果尚未激活 Windows，它会通过搜索指定的 KMS 服务器激活 Windows。

- SetAutodiscover – 指示是否自动检测 KMS。
- TargetKMSServer – 存储 KMS 的私有 IP 地址。KMS 必须与您的实例位于相同地区。
- DiscoverFromZone : 发现指定 DNS 区域中的 KMS 服务器。
- ReadFromUserData : 发现 UserData 中的 KMS 服务器。
- LegacySearchZones : 发现指定 DNS 区域中的 KMS 服务器。
- DoActivate – 尝试使用本部分中的指定设置进行激活。该值可以是 true 或 false。
- LogResultToConsole : 在控制台中显示结果。

BundleConfig.xml

此文件包含用于控制 EC2Config 为 AMI 创建过程准备实例的方式的设置。

- AutoSysprep – 指明是否自动使用 Sysprep。将值更改为 Yes 可使用 Sysprep。
- SetRDPCertificate : 为 Windows 2003 实例上运行的远程桌面服务器设置自签名证书。这样一来，您可以将 RDP 安全应用到实例中。如果新实例应该具有该证书，请将该值改为 Yes。

该设置不适用于 Windows Server 2008 或 Windows Server 2012 实例，因为它们会生成自己的证书。

- SetPasswordAfterSysprep : 在新启动的实例上设置随机密码，使用用户启动密钥对其进行加密并且将该加密密码输出到控制台中。如果新实例不应设置为随机加密密码，请将该设置的值改为 No。

Config.xml

插件

- Ec2SetPassword : 在您每次启动实例时生成随机加密密码。默认情况下，首次启动之后该功能会被禁用，因此重新启动该实例并不会更改用户设置的密码。每次您启动实例时，请将该设置改为 Enabled，以继续生成密码。

如果您计划从自己的实例创建一个 AMI，则该设置非常重要。

- Ec2SetComputerName – 根据实例的 IP 地址将实例的主机名设置为唯一名称，并且重新启动实例。若要设置您自己的主机名或防止修改您的现有主机名，必须禁用此设置。
- Ec2InitializeDrives - 在启动期间初始化和格式化所有卷。该功能已默认启用。
- Ec2EventLog : 在控制台中显示事件日志条目。默认情况下，会显示来自系统事件日志的最近三个错误条目。要指定将显示的事件日志条目，请编辑 EC2ConfigService\Settings 目录中的 EventLogConfig.xml 文件。有关该文件中设置的信息，请参阅 MSDN 库中的 [Eventlog Key](#)。
- Ec2ConfigureRDP : 在实例上设置自签名证书，以便用户可以使用远程桌面安全访问实例。Windows Server 2008 和 Windows Server 2012 实例上已禁用该功能，因为它们可以生成自己的证书。

- Ec2OutputRDPCert：在控制台中显示远程桌面证书信息，以便用户可以根据指纹对其进行验证。
- Ec2SetDriveLetter：根据用户定义的设置，设置已装载卷的驱动器号。默认情况下，Amazon EBS 卷挂载到实例之后，系统会根据实例上的驱动器号进行装载。要指定您的驱动器号映射，请编辑 EC2ConfigService\Settings 目录中的 DriveLetterConfig.xml 文件。
- Ec2WindowsActivate - 该插件处理 Windows 激活。它检查 Windows 是否已激活。如果未激活，则它会更新 KMS 客户端设置，然后激活 Windows。

要修改 KMS 设置，请编辑 EC2ConfigService\Settings 目录中的 ActivationSettings.xml 文件。

- Ec2DynamicBootVolumeSize：将磁盘 0/卷 0 扩展到包含所有未分区的空间。
- Ec2HandleUserData：创建脚本并在运行 Sysprep 后首次启用实例时执行用户创建的脚本。脚本标签包含的命令会保存到批处理文件中，而 PowerShell 标签包含的命令会保存到 .ps1 文件中。

全局设置

- ManageShutdown – 确保从实例存储支持的 AMI 启动的实例不会在运行 Sysprep 时终止。
- SetDnsSuffixList – 为 Amazon EC2 设置网络适配器的 DNS 后缀。这允许 Amazon EC2 中运行的服务器的 DNS 解析，无需提供完全限定域名。
- WaitForMetaDataAvailable – 确保 EC2Config 服务会在继续启动之前等待元数据处于可访问状态并且网络可用。此检查确保了 EC2Config 可以从激活和其他插件的元数据获取信息。
- ShouldAddRoutes – 已连接多个 NIC 时，向主网适配器添加自定义路由，以启用以下 IP 地址：169.254.169.250、169.254.169.251 和 169.254.169.254。当您访问实例元数据时，Windows Activation 会使用这些地址。
- RemoveCredentialsfromSysprepOnStartup – 在下一次启动服务时从 Sysprep.xml 中删除管理员密码。要确保该密码持久保留，请编辑该设置。

DriveLetterConfig.xml

此文件包含用于控制驱动器号映射的设置。默认情况下，一个卷可映射到任何可用的驱动器号。您可按以下方式将卷装载为特定的驱动器号。

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- VolumeName：卷标签。例如：*My Volume*。要为实例存储卷指定映射，请使用标签 Temporary Storage x，其中 x 为 0 到 25 之间的数字。
- DriveLetter：驱动器号。例如：*M:*。如果驱动器号已在使用，则映射会失败。

EventLogConfig.xml

此文件包含用于控制实例启动时显示在控制台上的事件日志信息的设置。默认情况下，我们会显示来自系统事件日志的最近三个错误条目。

- Category : 监视器的事件日志密钥。
- ErrorType – 事件类型（例如 Error、Warning、Information。）
- NumEntries : 此类别中所存储事件的数目。
- LastMessageTime : 为防止重复推送相同的消息，服务会在每次推送消息时更新此值。
- AppName : 事件源或记录事件的应用程序。

WallpaperSettings.xml

此文件包含用于控制在桌面背景上显示的信息的设置。默认情况下显示以下信息。

- Hostname – 显示计算机名称。
- Instance ID : 显示实例的 ID。
- Public IP Address : 显示实例的公有 IP 地址。
- Private IP Address : 显示实例的私有 IP 地址。
- Availability Zone : 显示实例在其中运行的可用区域。
- Instance Size : 显示实例的类型。
- Architecture : 显示 PROCESSOR_ARCHITECTURE 环境变量的设置。

您可以通过删除条目删除默认显示的任何信息。您可以按如下所示添加其他要显示的实例元数据。

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

您可以按如下所示添加其他要显示的系统环境变量。

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

此文件包含控制 EC2Config 如何初始化驱动器的设置。默认情况下，EC2Config 用操作系统初始化未联机的驱动器。您可以使用以下设置自定义插件。

```
<InitializeDrivesSettings>
  <SettingsGroup>FormatWithoutTRIM</SettingsGroup>
</InitializeDrivesSettings>
```



Note

使用设置组指定要如何初始化驱动器。

- FormatWithoutTRIM : 在格式化驱动器时，此设置禁用 TRIM 命令并在 Windows 中改进格式化时间。在驱动器格式化和初始化后，系统还原 TRIM 配置。
- DisableInitializeDrives : 此设置禁止格式化新驱动器。使用此设置可手动初始化驱动器。

配置 EC2Config 服务的代理设置

您可以将 EC2Config 服务配置为通过代理通信。本部分介绍了三种方法：使用适用于 .NET 的 AWS 开发工具包、使用 .Net 系统元素和使用 Microsoft 组策略及 Internet Explorer。使用适用于 .NET 的 AWS 开发工具包时可以指定用户名和密码，因此，请优先使用此方法。

使用适用于 .NET 的 AWS 开发工具包配置代理设置（首选方法）

您可以通过在 Ec2Config.exe.config 文件中指定 proxy 元素来配置 EC2Config 服务的代理设置。有关 proxy 元素的更多信息，请参阅[适用于 .NET 的 AWS 开发工具包配置文件参考](#)。

在 Ec2Config.exe.config 文件中指定 proxy 元素

1. 在需要 EC2Config 服务通过代理进行通信的实例上编辑 Ec2Config.exe.config 文件。默认情况下，此文件位于下面的目录中：%ProgramFiles%\Amazon\Ec2ConfigService。
2. 在 <configSections> 中添加下面的 aws 元素。不要在任何现有 <sectionGroups> 中添加此内容。

```
<configSections>
  <section name="aws" type="Amazon.AWSSection, AWSSDK" />
</configSections>
```

3. 在 Ec2Config.exe.config 文件中添加下面的 <aws> 元素。

```
<aws>
  <proxy
    host="string value"
    port="string value"
    username="string value"
    password="string value" />
</aws>
```

4. 保存您的更改。

使用 .Net 系统元素配置代理设置

您可以在 Ec2Config.exe.config 文件的 <system.net> 元素中指定代理设置。有关 <system.net> 元素的更多信息，请参阅 MSDN 上的[<defaultProxy> 元素（网络设置）](#)。

在 Ec2Config.exe.config 文件中指定 <system.net> 元素

1. 在需要 EC2Config 服务通过代理进行通信的实例上编辑 Ec2Config.exe.config 文件。默认情况下，此文件位于下面的目录中：%ProgramFiles%\Amazon\Ec2ConfigService。
2. 在 Ec2Config.exe.config 文件中添加下面的 <system.net> 元素。

```
<configuration>
  <system.net>
    <defaultProxy
      enabled="true|false"
      useDefaultCredentials="true|false"
      <bypasslist> ... </bypasslist>
      <proxy> ... </proxy>
      <module> ... </module>
    />
```

3. 保存您的更改。

使用 Microsoft 组策略及 Microsoft Internet Explorer 配置代理设置

EC2Config 服务以本地系统用户账户运行。更改实例上的组策略设置后，您可以在 Internet Explorer 中为此账户指定实例级代理设置。

使用组策略及 Internet Explorer 配置代理设置

1. 在需要 EC2Config 服务通过代理进行通信的实例上，以管理员身份打开命令提示符，键入 gpedit.msc，然后按 Enter。
2. 在本地组策略编辑器中，依次选择本地计算机策略下的计算机配置、管理模板、Windows 组件、Internet Explorer。
3. 在右侧窗格中，选择按计算机进行代理服务器设置(不是按用户)，然后选择编辑策略设置。
4. 选择启用，然后选择应用。
5. 打开 Internet Explorer，然后选择工具按钮。
6. 选择 Internet 选项，然后选择连接选项卡。
7. 选择局域网设置。
8. 在代理服务器下，选择为 LAN 使用代理服务器选项。
9. 指定地址和端口信息，然后选择确定。

管理 EC2Config 服务

本节包含可帮助您管理 EC2Config 服务的信息。

内容

- [安装最新版的 EC2Config \(p. 258\)](#)
- [停止、重新启动、删除或卸载 EC2Config \(p. 259\)](#)
- [订阅 EC2Config 服务通知 \(p. 260\)](#)

安装最新版的 EC2Config

默认情况下，EC2Config 服务包含在每个 AWS Windows AMI 中。我们发布更新版本时，会将所有 AWS Windows AMI 中的版本更新为最新版本。不过，您需要将自己的 Windows AMI 和实例更新为最新版本。

要找到 EC2Config 更新通知，请转到 [订阅 EC2Config 服务通知 \(p. 260\)](#)。有关每个版本中所进行更改的更多信息，请参阅下载页面上的“What's New”部分。

验证 Windows AMI 随附的 EC2Config 版本

1. 从 AMI 启动实例并连接到该实例。
2. 在控制面板中，选择 Programs and Features (程序和功能)。
3. 在已安装程序的列表中查找 Ec2ConfigService。其版本号会显示在 Version (版本) 列中。

在实例上安装最新版本的 EC2Config

您可使用 EC2 Run Command 远程安装 EC2Config 服务的最新版本。有关更多信息，请参阅 [使用 Amazon EC2 Run Command 更新 EC2Config 服务 \(p. 363\)](#)。或者，也可以使用以下过程手动安装最新版本。

1. (可选) 如果您更改了任何设置，请记录下这些更改，因为您需要在安装最新版 EC2Config 之后将它们还原。
2. 转到 [Amazon Windows EC2Config 服务](#)。

3. 单击 Download (下载)。
4. 下载文件并进行解压。
5. 运行 EC2Install.exe。有关选项的完整列表，请使用 /? 选项运行 EC2Install。请注意以下几点：
 - 默认情况下，安装程序会在安装期间用默认设置文件替换您的设置文件，并在安装完成时重启 EC2Config 服务。要保持您在步骤 1 中保存的自定义设置，请利用 /norestart 选项运行 EC2Install，还原您的设置，然后手动重启 EC2Config 服务。
 - 默认情况下，安装程序会显示提示。要运行该命令而不显示提示，请使用 /quiet 选项。

停止、重新启动、删除或卸载 EC2Config

您可以像对其他任何服务那样管理 EC2Config 服务。

要将更新的设置应用到您的实例，可以停止并重新启动服务。如果您要手动安装 EC2Config，则必须首先停止该服务。

停止 EC2Config 服务

1. 启动并连接到您的 Windows 实例。
2. 在开始菜单上，指向管理工具，然后单击服务。
3. 在服务列表中，右键单击 EC2Config 并选择停止。

重新启动 EC2Config 服务

1. 启动并连接到您的 Windows 实例。
2. 在开始菜单上，指向管理工具，然后单击服务。
3. 在服务列表中，右键单击 EC2Config 并选择 Restart。

如果您不需要更新配置设置、想要创建自己的 AMI 或是使用 Amazon EC2 Simple Systems Manager (SSM)，则可以删除并卸载该服务。删除服务会删除它的注册表子项。卸载服务会删除与此服务相关的文件、注册表子项和所有快捷方式。

删除 EC2Config 服务

1. 启动命令提示符窗口。
2. 运行以下命令：

```
C:\> sc delete ec2config
```

卸载 EC2Config

1. 启动并连接到您的 Windows 实例。
2. 在开始菜单上，单击控制面板。
3. 双击程序和功能。
4. 在程序列表上，选择 EC2ConfigService 并单击卸载。

订阅 EC2Config 服务通知

Amazon SNS 可在 EC2Config 服务的新版本发布时向您发送通知。使用以下过程订阅这些通知。

订阅 EC2Config 通知

1. 打开 Amazon SNS 控制台。
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）。您必须选择此区域，因为您订阅的 SNS 通知是在此区域中创建的。
3. 在导航窗格中，单击 Subscriptions。
4. 单击 Create Subscription (创建订阅)。
5. 在 Create Subscription (创建事件订阅) 对话框中，请执行以下操作：
 - a. 在 TopicARN 中，输入以下 Amazon 资源名称 (ARN)：
`arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config`
 - b. 在 Protocol 中，选择 Email。
 - c. 在 Endpoint 中，输入用于接收通知的电子邮件地址。
 - d. 单击 Subscribe (订阅)。
6. 您将收到一封包含主题行 EC2Config Interest 的确认电子邮件。打开电子邮件，然后单击 Confirm subscription 以完成订阅。

当 EC2 Config 服务的新版本发布时，我们会向订户发送通知。如果您不希望再收到这些通知，请通过以下步骤取消订阅。

从 EC2Config 通知中取消订阅

1. 打开 Amazon SNS 控制台。
2. 在导航窗格中，单击 Subscriptions。
3. 选择订阅内容，然后单击 Delete Subscriptions。当系统提示您进行确认时，单击 Yes, Delete。

使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。

从 EC2Config 版本 2.2.5 开始（建议使用版本 2.2.6 或更高版本），可以将系统日志、安全日志、应用程序日志和 IIS 日志中的所有 Windows Server 消息导出到 CloudWatch Logs，并使用 CloudWatch 指标对它们进行监控。EC2Config 版本 2.2.10 或更高版本添加了将任何事件日志数据、事件跟踪（Windows）或基于文本的日志文件导出到 CloudWatch Logs 的功能。此外，您还可以将性能计数器数据导出到 CloudWatch。要管理多个实例的性能计数器和日志，可以使用 Amazon EC2 Simple Systems Manager (SSM)。有关更多信息，请参阅 [使用 Amazon EC2 Simple Systems Manager 将性能计数器发送到 CloudWatch，将日志发送到 CloudWatch Logs \(p. 308\)](#)。



Note

您的 Amazon EC2 实例必须有出站 Internet 访问权限才能将日志数据发送到 Amazon CloudWatch Logs。有关如何配置 Internet 访问权限的更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [Internet 网关](#)。

要设置 EC2Config 以将数据发送到 CloudWatch Logs，请完成以下步骤：

主题

- 步骤 1：配置 IAM 权限 (p. 261)
- 步骤 2：启用 CloudWatch Logs 集成 (p. 261)
- 步骤 3：为 CloudWatch 和 CloudWatch Logs 配置证书 (p. 263)
- 步骤 4：配置发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志 (p. 264)
- 步骤 5：配置流程控制 (p. 270)
- 步骤 6：重新启动 EC2Config (p. 270)
- 在 EC2Config 中对 CloudWatch Logs 进行故障排除 (p. 270)

步骤 1：配置 IAM 权限

您可以在启用某个 Amazon EC2 实例时在附加到该实例的实例配置文件中使用以下 IAM 权限。EC2Config 在将 CloudWatch 指标或日志上传到 CloudWatch Logs 时使用该实例配置文件。有关实例配置文件的更多信息，请参阅 [IAM 用户指南中的实例配置文件](#)。有关使用 IAM 角色启动实例的更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。



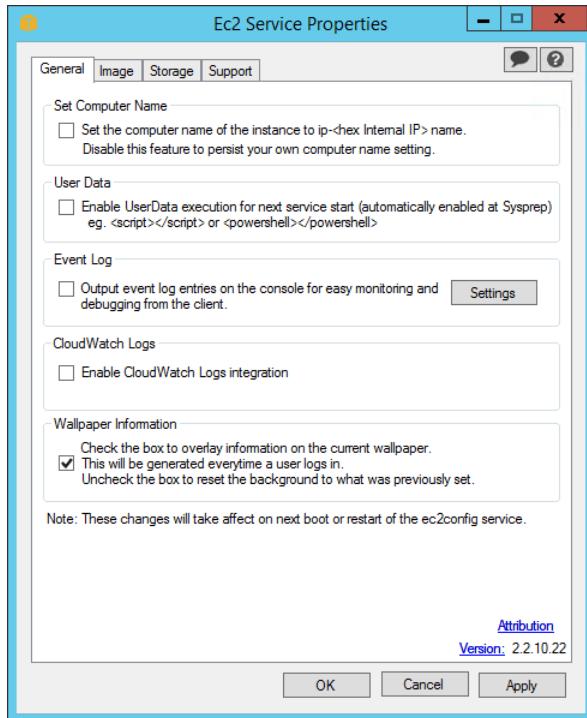
Note

这些 IAM 权限仅适用于本地 JSON 配置文件。如果您要通过 Amazon EC2 Simple Systems Manager (SSM) 上传日志，请参阅 [使用 Amazon EC2 Simple Systems Manager 将性能计数器发送到 CloudWatch，将日志发送到 CloudWatch Logs \(p. 308\)](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAccessToSSM",  
            "Effect": "Allow",  
            "Action": [  
                "cloudwatch:PutMetricData",  
                "logs>CreateLogGroup",  
                "logs>CreateLogStream",  
                "logs>DescribeLogGroups",  
                "logs>DescribeLogStreams",  
                "logs>PutLogEvents"  
            ],  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

步骤 2：启用 CloudWatch Logs 集成

1. 启动并连接到您的 Windows 实例。
2. 在 Start (开始) 菜单中，单击 All Programs (所有程序)，然后单击 EC2ConfigService Settings (EC2ConfigService 设置)。



3. 在 Ec2 Service Properties (Ec2 服务属性) 对话框的 General (常规) 选项卡的 CloudWatch Logs (CloudWatch 日志) 下，选择 Enable CloudWatch Logs integration (启用 CloudWatch 日志集成)，然后单击 OK (确定)。
4. 创建一个名为 AWS.EC2.Windows.CloudWatch.json 的配置文件。

要下载文件的示例，请参阅 [AWS.EC2.Windows.CloudWatch.json](#)。



Note

您还可以通过在启动实例时将以下脚本添加到用户数据字段来启用 CloudWatch Logs。EC2Config 会在实例每次重新启动时运行此脚本，以确保启用 CloudWatch Logs 集成。要仅在实例首次启动时运行此脚本，请从脚本中删除 <persist>true</persist>。

```
<powershell>
$EC2SettingsFile="C:\Program Files\Amazon\Ec2ConfigService\Settings\Config.xml"
$xml = [xml](get-content $EC2SettingsFile)
$xmlElement = $xml.get_DocumentElement()
$xmlElementToModify = $xmlElement.Plugins

foreach ($element in $xmlElementToModify.Plugin)
{
    if ($element.name -eq "AWS.EC2.Windows.CloudWatch.Plugin")
    {
        $element.State="Enabled"
    }
}
$xml.Save($EC2SettingsFile)
</powershell>
<persist>true</persist>
```

步骤 3：为 CloudWatch 和 CloudWatch Logs 配置证书

为 CloudWatch 设置证书、区域和指标命名空间

JSON 文件的此部分定义组成数据发送目标的证书、区域和指标命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatch2”、“CloudWatch3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。



Note

如果您使用 EC2Config 并且计划将性能计数器发送到 CloudWatch，则只需设置 CloudWatch 证书。如果您使用 Amazon EC2 Simple Systems Manager，则您的证书是在您启动 Amazon EC2 实例时使用的 IAM 角色中配置的。

1. 在 JSON 文件中，找到 CloudWatch 部分。

```
{  
    "Id": "CloudWatch",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputCom  
ponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "AccessKey": "",  
        "SecretKey": "",  
        "Region": "us-west-1",  
        "NameSpace": "Windows/Default"  
    }  
},
```

2. 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
3. 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
4. 在 Region 参数中，输入希望将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。虽然可以将性能计数器发送到与日志数据发送目标不同的区域，但是我们建议您将此参数设置为运行实例的区域。
5. 在 NameSpace 参数中，输入要用于在 CloudWatch 中写入性能计数器数据的指标命名空间。

为 CloudWatch Logs 设置证书、区域、日志组和日志流

JSON 文件的此部分定义组成数据发送目标的证书、区域、日志组名称和日志流命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatchLogs2”、“CloudWatchLogs3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。

1. 在 JSON 文件中，找到 CloudWatchLogs 部分。

```
{  
    "Id": "CloudWatchLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Win  
dows.CloudWatch",  
    "Parameters": {  
        "AccessKey": "",  
        "SecretKey": "",  
        "Region": "us-east-1",  
    }  
},
```

```
        "LogGroup": "Default-Log-Group",
        "LogStream": "{instance_id}"
    },
},
```

2. 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
3. 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
4. 在 Region 参数中，输入希望 EC2Config 将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。
5. 在 LogGroup 参数中，输入日志组的名称。这是在 CloudWatch 控制台 Log Groups (日志组) 屏幕上显示的名称。
6. 在 LogStream 参数中，输入目标日志流。如果使用 {instance_id} 默认设置，则 EC2Config 将该实例的实例 ID 用作日志流名称。

如果输入不存在的日志流名称，则 CloudWatch Logs 会自动创建该名称。您可以使用文字字符串或预定义的变量 ({instance_id}、{hostname}、{ip_address})，或所有这三个变量的组合来定义日志流名称。

此参数中指定的日志流名称会显示在 CloudWatch 控制台中的 Log Groups (日志组) > Streams for <*YourLogStream*> (<YourLogStream> 的流) 屏幕上。

步骤 4：配置发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志

配置发送到 CloudWatch 的性能计数器

可以选择性能监视器中提供的任何性能计数器。您可以选择不同类别作为指标上传到 CloudWatch，如 .NET CLR 数据、ASP.NET 应用程序、HTTP 服务、内存或进程和处理器。

对于要上传到 CloudWatch 的每个性能计数器，复制 PerformanceCounter 部分，更改 Id 参数使其唯一（例如“PerformanceCounter2”），然后根据需要更新其他参数。

1. 在 JSON 文件中，找到 PerformanceCounter 部分。

```
{
    "Id": "PerformanceCounter",
    "FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "CategoryName": "Memory",
        "CounterName": "Available MBytes",
        "InstanceName": "",
        "MetricName": "AvailableMemory",
        "Unit": "Megabytes",
        "DimensionName": "",
        "DimensionValue": ""
    }
},
```

2. 在 CategoryName 参数中，输入性能计数器类别。
 - a. 要查找可用类别和计数器，请打开性能监视器。
 - b. 单击 Monitoring Tools (监控工具)，然后单击 Performance Monitor (性能监视器)。

c. 在结果窗格中，单击绿色 + (加号) 按钮。

类别和计数器会在 Add Counters (添加计数器) 对话框中列出。

3. 在 CounterName 参数中，输入性能计数器的名称。
4. 在 InstanceName 参数中，从性能监视器的 Add Counters 对话框中输入值，可以是下列值之一：
 - 空白，如果所选对象没有实例。
 - 所选对象的单个实例。
 - _Total，将使用所有实例的汇总。



Note

请勿使用星号 (*) 标识所有实例，因为每个性能计数器组件仅支持一个指标。

5. 在 MetricName 参数中，输入希望性能数据所属的 CloudWatch 指标。
6. 在 Unit 参数中，为指标输入合适的度量单位：
秒 | 微秒 | 毫秒 | 字节 | 千字节 | 兆字节 | 千兆字节 | 太兆字节 | 位 | 千位 | 千兆位 | 太兆位 | 百分比 | 计数 | 字节/秒 | 千字节/秒 | 兆字节/秒 | 千兆字节/秒 | 太兆字节/秒 | 位/秒 | 千位/秒 | 千兆位/秒 | 太兆位/秒 | 计数/秒 | 无。
7. (可选) 您可以在 DimensionName 和 DimensionValue 参数中输入维度名称和值以便为指标指定维度。这些参数在列出指标时提供另一个视图。您还可以对多个指标使用同一个维度，以便可以查看属于特定维度的所有指标。

将 Windows 应用程序事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 ApplicationEventLog 部分。

```
{  
    "Id": "ApplicationEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Application",  
        "Levels": "1"  
    }  
},
```

2. 在 Levels 参数中，输入以下值之一：

1 – 仅上传错误消息。

2 – 仅上传警告消息。

4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将安全日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 SecurityEventLog 部分。

```
{  
    "Id": "SecurityEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Security",  
        "Levels": "7"  
    }  
},
```

2. 在 Levels 参数中，输入 7，以便上传所有消息。

将系统事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 SystemEventLog 部分。

```
{  
    "Id": "SystemEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "System",  
        "Levels": "7"  
    }  
},
```

2. 在 Levels 参数中，输入以下值之一：

- 1 – 仅上传错误消息。
- 2 – 仅上传警告消息。
- 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将其他类型的事件日志数据发送到 CloudWatch Logs

除了应用程序、系统和安全日志之外，您还可以上传其他类型的事件类型。

1. 在 JSON 文件中，添加新部分。

```
{  
    "Id": "",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "",  
        "Levels": "7"  
    }  
},
```

2. 在 Id 参数中，为要上传的日志输入名称（例如 WindowsBackup）。

3. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器的导航窗格中，单击 Applications and Services Logs (应用程序和服务日志)。
 - b. 在日志列表中，右键单击要上传的日志（例如“Microsoft>Windows>Backup (备份)>Operational (运行)”），然后单击 Create Custom View (创建自定义视图)。
 - c. 在 Create Custom View (创建自定义视图) 对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-Backup）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。
4. 在 Levels 参数中，输入以下值之一：
 - 1 – 仅上传错误消息。
 - 2 – 仅上传警告消息。
 - 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将事件跟踪 (Windows) 数据发送到 CloudWatch Logs

ETW (Windows 事件跟踪) 提供了高效且详细的日志记录机制，供应用程序写入日志。每个 ETW 都由可以启动和停止日志记录会话的会话管理器控制。每个会话都具有一个提供者以及一个或多个使用者。

1. 在 JSON 文件中，找到 ETW 部分。

```
{  
    "Id": "ETW",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Microsoft-Windows-WinINet/Analytic",  
        "Levels": "7"  
    }  
},
```

2. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器中的 View (视图) 菜单上，单击 Show Analytic and Debug Logs (显示分析和调试日志)。
 - b. 在导航窗格中，单击 Applications and Services Logs (应用程序和服务日志)。
 - c. 在 ETW 日志的列表中，右键单击要上传的日志，然后单击 Enable Log (启用日志)。
 - d. 再次右键单击该日志，然后单击 Create Custom View (创建自定义视图)。
 - e. 在 Create Custom View (创建自定义视图) 对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-WinINet/Analytic）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。
3. 在 Levels 参数中，输入以下值之一：
 - 1 – 仅上传错误消息。
 - 2 – 仅上传警告消息。

4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将自定义日志（任何基于文本的日志文件）发送到 CloudWatch Logs

- 在 JSON 文件中，找到 CustomLogs 部分。

```
{  
    "Id": "CustomLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\\\CustomLogs\\\\",  
        "TimestampFormat": "MM/dd/yyyy HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "Local",  
        "LineCount": "5"  
    }  
},
```

- 在 LogDirectoryPath 参数中，输入日志在实例上的存储路径。
- 在 TimestampFormat 参数中，输入要使用的时间戳格式。有关支持的值的列表，请参阅 MSDN 上的[自定义日期和时间格式字符串](#)主题。



Important

源日志文件必须在每个日志行开头具有时间戳，且时间戳后必须有一个空格。

- 在 Encoding 参数中，输入要使用的文件编码（例如 UTF-8）。有关支持的值的列表，请参阅 MSDN 上的[Encoding](#) 类主题。



Note

使用编码名称（而不是显示名称）作为此参数的值。

- （可选）在 Filter 参数中，输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表，请参阅 MSDN 上的[FileSystemWatcherFilter 属性](#)主题。
- （可选）在 CultureName 参数中，输入在其中记录时间戳的区域设置。如果 CultureName 为空，则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表，请参阅 MSDN 上的[区域语言支持 \(NLS\) API 参考](#)主题。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

- （可选）在 TimeZoneKind 参数中，输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息，则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息，则忽略此参数。

8. (可选) 在 LineCount 参数中，在标头中输入行数以识别日志文件。例如，IIS 日志文件拥有几乎相同的标头。您可以输入 5，系统会读取日志文件标头的前三行以进行识别。在 IIS 日志文件中，第三行为日期和时间戳，但无法始终保证时间戳在日志文件之间是不同的。为此，建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

将 IIS 日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 IISLog 部分。

```
{  
    "Id": "IISLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\W3SVC1",  
        "TimestampFormat": "yyyy-MM-dd HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "UTC",  
        "LineCount": "5"  
    }  
},
```

2. 在 LogDirectoryPath 参数中，输入为单个站点存储 IIS 日志的文件夹（例如 C:\\inetpub\\logs\\LogFiles\\W3SVC_n）。



Note

仅支持 W3C 日志格式。不支持 IIS、NCSA 和自定义格式。

3. 在 TimestampFormat 参数中，输入要使用的时间戳格式。有关支持的值的列表，请参阅 MSDN 上的[自定义日期和时间格式字符串](#)主题。
4. 在 Encoding 参数中，输入要使用的文件编码（例如 UTF-8）。有关支持的值的列表，请参阅 MSDN 上的[Encoding](#) 类主题。



Note

使用编码名称（而不是显示名称）作为此参数的值。

5. (可选) 在 Filter 参数中，输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表，请参阅 MSDN 上的[FileSystemWatcherFilter 属性](#)主题。
6. (可选) 在 CultureName 参数中，输入在其中记录时间戳的区域设置。如果 CultureName 为空，则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表，请参阅 MSDN 上的[区域语言支持 \(NLS\) API 参考](#)主题。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

7. (可选) 在 TimeZoneKind 参数中，输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息，则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息，则忽略此参数。

8. (可选) 在 LineCount 参数中 , 在标头中输入行数以识别日志文件。例如 , IIS 日志文件拥有几乎相同的标头。您可以输入 5 , 系统会读取日志文件标头的前五行以进行识别。在 IIS 日志文件中 , 第三行为日期和时间戳 , 但无法始终保证时间戳在日志文件之间是不同的。为此 , 建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

步骤 5 : 配置流程控制

要将性能计数器数据发送到 CloudWatch 或将日志数据发送到 CloudWatch Logs , 每种数据类型都必须在 Flows 部分中列出对应目标。例如 , 要将在 JSON 文件的 "Id": "PerformanceCounter" 部分中定义的性能计数器发送到在 JSON 文件的 "Id": "CloudWatch" 部分定义的 CloudWatch 目标 , 应在 Flows 部分输入 "PerformanceCounter,CloudWatch" 。同样 , 要将自定义日志、ETW 日志和系统日志发送到 CloudWatch Logs , 会输入 "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs" 。此外 , 还可以将相同性能计数器或日志文件发送到多个目标。例如 , 要将应用程序日志发送到在 JSON 文件的 "Id": "CloudWatchLogs" 部分定义的两个不同目标 , 应在 Flows 部分输入 "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)" 。

1. 在 JSON 文件中 , 找到 Flows 部分。

```
"Flows" : {  
    "Flows" : [  
        "PerformanceCounter,CloudWatch",  
        "(PerformanceCounter,PerformanceCounter2), CloudWatch2",  
        "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs",  
        "CustomLogs, CloudWatchLogs2",  
        "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"  
    ]  
}
```

2. 在 Flows 参数中 , 输入要上传的每种数据类型 (例如 ApplicationEventLog) 以及要将它发送到的目标 (例如 CloudWatchLogs) 。

步骤 6 : 重新启动 EC2Config

更新完 C:\Program Files\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json 文件后 , 您应该重新启动 EC2Config 。有关更多信息 , 请参阅 [停止、重新启动、删除或卸载 EC2Config \(p. 259\)](#) 。

在 EC2Config 中对 CloudWatch Logs 进行故障排除

如果遇到与上传性能计数器或日志有关的问题 , 首先应检查 C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt 文件。下面列出了一些最常遇到的问题。

我在 CloudWatch 控制台中看不到日志。

请验证您使用的是 EC2Config 版本 2.2.6 或更高版本。如果您仍使用 EC2Config 版本 2.2.5 , 请通过以下步骤解决该问题 :

1. 在 Microsoft 管理控制台 (MMC) 的“Services (服务)”管理单元中 , 重新启动 EC2Config 服务。要打开 Services (服务) 管理单元 , 请单击 Start (开始) 菜单 , 然后在 Run (运行) 框中键入 services.msc 。
2. 登录 AWS 管理控制台 并通过以下网址打开 CloudWatch 控制台 <https://console.amazonaws.cn/cloudwatch/> 。
3. 在导航栏中 , 选择适当的区域。
4. 在导航窗格中 , 单击 Logs (日志) 。
5. 在内容窗格中的 Expire Events After (事件过期时间) 列中 , 单击刚创建的日志组的保留设置。

- 在 Edit Retention (编辑保留期) 对话框中的 New Retention (新保留期) 列表中，选择 10 years (3653 days) (10 年(3653 天))，然后单击 OK (确定)。



Note

也可以使用以下 Windows PowerShell 命令设置日志保留期（以天为单位）：

```
Write-CWLRetentionPolicy -LogGroupName Default-Log-Group -RetentionInDays 3653
```

在我单击 OK (确定) 后重新打开 EC2Config 时，Enable CloudWatch Logs integration (启用 CloudWatch 日志集成) 复选框未保持选中状态。

如果执行了从 EC2Config 的早期版本到版本 2.2.5 的升级，则可能会出现该问题。要解决该问题，请安装版本 2.2.6 或更高版本。

我看到像 *Log events cannot be more than 2 hours in the future* (日志事件在将来不能超过 2 小时) 或 *InvalidOperationException* 这样的错误。

如果您使用的是 EC2Config 版本 2.2.5，并且实例的时区位于 UTC-12:00 和 UTC-02:00 之间，则可能發生这种错误。要解决这一问题，请安装 EC2Config 版本 2.2.6 或更高版本。

我在 CloudWatch 控制台中看不到 SQL Server 日志，并且在 Ec2ConfigLog.txt 中看到此错误 [Error] *Exception occurred: Index and length must refer to a location within the string. Parameter name: length.* 要解决这一问题，请安装 EC2Config 版本 2.2.11 或更高版本。

我运行十个或更少的工作流程，EC2Config 占用了超过 500 MB 的内存。

要解决这一问题，请安装版本 2.3.313 或更高版本。

只上传了前一个或两个 IIS 日志，其他 IIS 日志都没有上传。

更新 C:\Program Files\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json 文件的 IISlog 部分，并将 LineCount 参数设置为 3，这样系统会读取日志文件标头的前三行以进行识别。在 IIS 日志文件中，第三行是日期和时间戳，各日志文件的日期和时间戳互不相同。

排查 EC2Config 服务的问题

本节包含可帮助您排查 EC2Config 服务问题的信息。

更新无法访问的实例上的 EC2Config

通过执行以下过程，使用远程桌面更新无法访问的 Windows Server 实例上的 EC2Config 服务。

更新您无法连接到的 Amazon EBS 支持的 Windows 实例上的 EC2Config

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 在导航窗格中，选择 Instances。
- 找到受影响的实例。打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

- 选择 Launch Instance 并在与受影响实例相同的可用区中创建临时 t2.micro 实例。使用 Windows Server 2003 Amazon 系统映像 (AMI)。如果您使用 Windows Server 的更高版本，则在还原原始实

例的根卷时将无法启动该实例。要查找适用于 Windows Server 2003 的 AMI，请搜索名为 Windows_Server-2003-R2_SP2 的公用 Windows AMI。



Important

如果您未在与受影响实例相同的可用区中创建该实例，则无法将受影响的实例的根卷挂载到新实例。

5. 在 EC2 控制台中，选择 Volumes。
6. 找到受影响的实例的根卷。分离该卷并将其挂载到早先创建的临时实例。使用默认设备名称 (xvdf) 挂载该卷。
7. 使用远程桌面连接临时实例，然后通过磁盘管理实用工具使该卷可供使用。
8. 从 Amazon Windows EC2Config 服务下载最新的 EC2Config。将文件从 .zip 文件提取到所连接的驱动器上的 Temp 目录。
9. 在临时实例上，打开“运行”对话框，键入 regedit，然后按 Enter。
10. 选择 HKEY_LOCAL_MACHINE。从 File 菜单中，选择 Load Hive。选择驱动器，然后导航到并打开以下文件：Windows\System32\config\SOFTWARE。当系统提示时，请指定密钥名称。
11. 选择刚加载的键并导航至 Microsoft\Windows\CurrentVersion。选择 RunOnce 密钥。如果此密钥不存在，则从上下文（右键单击）菜单中选择 CurrentVersion，然后选择 New 和 Key。为密钥 RunOnce 命名。
12. 从上下文（右键单击）菜单中，依次选择 RunOnce 密钥、New 和 String Value。输入 Ec2Install 作为名称并输入 C:\Temp\Ec2Install.exe /quiet 作为数据。
13. 选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 密钥。从上下文（右键单击）菜单中选择 New，然后选择 String Value。输入 AutoAdminLogon 作为名称并输入 1 作为值数据。
14. 选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon>密钥。从上下文（右键单击）菜单中选择 New，然后选择 String Value。输入 DefaultUserName 作为名称并输入 Administrator 作为值数据。
15. 选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 密钥。从上下文（右键单击）菜单中选择 New，然后选择 String Value。输入 DefaultPassword 作为名称并在值数据中输入密码。
16. 在注册表编辑器导航窗格中，选择您在首次打开注册表编辑器时创建的临时项。
17. 从文件菜单中，选择卸载配置单元。
18. 在磁盘管理实用工具中，选择您之前挂载的驱动器，打开上下文（右键单击）菜单，然后选择脱机。
19. 在 Amazon EC 控制台中，将受影响的实例从临时实例分离，然后将其重新挂载到您的具有设备名称 /dev/sda1 的 2 实例。您必须指定此设备名称才能将卷指派为根卷。
20. 启动实例。
21. 在实例启动后，检查系统日志并确认看到消息 Windows is ready to use。
22. 打开注册表编辑器并选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon。删除您之前创建的字符串值密钥：AutoAdminLogon、DefaultUserName 和 DefaultPassword。
23. 删除或停止您在本过程中创建的临时实例。

半虚拟化驱动程序

Abstract

描述 Amazon EC2 使用的半虚拟化 (PV) 驱动程序，包括如何升级驱动程序和对其进行故障排除。

Amazon Windows AMI 包含一系列驱动程序，以允许访问 Xen 虚拟化硬件。Amazon EC2 会使用这些驱动程序将实例存储和 Amazon EBS 卷映射到其设备。下表显示了不同驱动程序之间的主要区别。

	RedHat 半虚拟化驱动程序	Citrix 半虚拟化驱动程序	AWS 半虚拟化驱动程序
实例类型	并非对所有实例类型都支持。如果您指定了不受支持的实例类型，实例将受损。	对于所有实例类型都支持。	对于所有实例类型都支持。
已连接的卷	支持最多 16 个连接卷。	支持超过 16 个连接卷。	支持超过 16 个连接卷。
网络	此驱动程序在高负载下（例如，快速 FTP 文件传输）重置网络连接时存在已知问题。		若采用兼容的实例类型，此驱动程序会在网络适配器上自动配置超大框架。当实例位于 置放群组 (p. 624) 中时，这可以在置放群组中的实例间提供更好的网络性能。

内容

- [AWS 半虚拟化驱动程序 \(p. 273\)](#)
- [Citrix 半虚拟化驱动程序 \(p. 274\)](#)
- [RedHat 半虚拟化驱动程序 \(p. 274\)](#)

取决于 Windows 版本的驱动程序

下面的列表显示了应在 AWS 中每个版本的 Windows Server 上运行的 PV 驱动程序。

- Windows Server 2003 和 2003 R2，Citrix PV 5.9
- Windows Server 2008，Citrix 半虚拟化驱动程序 5.9
- Windows Server 2008 R2，AWS PV
- Windows Server 2012 和 2012 R2，AWS PV

AWS 半虚拟化驱动程序

AWS 半虚拟化驱动程序存储在 %ProgramFiles%\Amazon\Xentools 目录中。此目录还包含公有符号和一个命令行工具 xenstore_client.exe，使用该工具可以访问 XenStore 中的条目。例如，以下 PowerShell 命令从虚拟机监控程序返回当前时间：

```
[DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl AWSXenStoreBase).XenTime).ToString("hh:mm:ss")  
11:17:00
```

AWS 半虚拟化驱动程序在 Windows 注册表中列于 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 之下。这些驱动程序组件如下所示：XENBUS、xeniface、xennet、xenvbd 和 xenvif。

AWS 半虚拟化驱动程序还有一个名为 LiteAgent 的驱动程序组件，它以 Windows 服务的形式运行。它会处理相关任务，例如通过 API 进行的关闭和重启事件。您可以通过从命令行运行 Services.msc 来访问和管理服务。

AWS 半虚拟化驱动程序版本历史记录

您可以在 [Amazon EC2 Windows 驱动程序](#) 页面上查看有关不同的驱动程序版本和对最新驱动程序进行的更改的详细信息。

Citrix 半虚拟化驱动程序

Citrix 半虚拟化驱动程序存储在 %ProgramFiles%\Citrix\XenTools (32 位实例) 或 %ProgramFiles(x86)%\Citrix\XenTools (64 位实例) 目录中。

Citrix 半虚拟化驱动程序组件列出在 Windows 注册表的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services 下。这些驱动程序组件如下：xenevtchn、xeniface、xennet、Xennet6、xensvc、xenvbd 和 xenvif。

Citrix 还有一个名为 XenGuestAgent 的驱动程序组件，它以 Windows 服务的形式运行。它会处理相关任务，例如启动时的时间同步（仅限 Windows Server 2003）以及通过 API 进行的关闭和重启事件。您可以通过从命令行运行 Services.msc 来访问和管理服务。

如果您在执行某些工作负载时遇到联网错误，可能需要禁用 Citrix PV 驱动程序的 TCP 卸载功能。有关更多信息，请参阅 [TCP 卸载 \(p. 285\)](#)。

RedHat 半虚拟化驱动程序

支持对旧实例使用 RedHat 驱动程序，但不建议对具有 12GB 以上的 RAM 的较新的实例使用该驱动程序，因为存在驱动程序限制。运行 RedHat 驱动程序并具有 12GB 以上的 RAM 的实例可能无法启动并变得无法访问。我们建议将 RedHat 驱动程序升级为 Citrix 半虚拟化或 AWS 半虚拟化驱动程序。

RedHat 驱动程序的源文件在 %ProgramFiles%\RedHat (32 位实例) 或 %ProgramFiles(x86)%\RedHat (64 位实例) 目录中。这两种驱动程序分别为 RedHat 半虚拟化网络驱动程序 rhelnet 和 RedHat SCSI 微端口驱动程序 rhelscsi。

订阅 Amazon EC2 Windows 驱动程序通知

Amazon SNS 可在 EC2 Windows 驱动程序的新版本发布时向您发送通知。使用以下过程订阅这些通知。

订阅 EC2 通知

1. 打开 Amazon SNS 控制台。
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）。您必须选择此区域，因为您订阅的 SNS 通知是从此区域中创建的。
3. 在导航窗格中，单击 Subscriptions。
4. 单击 Create Subscription (创建订阅)。
5. 在 Create Subscription (创建事件订阅) 对话框中，请执行以下操作：
 - a. 在 TopicARN 中，输入以下 Amazon 资源名称 (ARN)：
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. 在 Protocol 中，选择 Email。
 - c. 在 Endpoint 中，输入用于接收通知的电子邮件地址。
 - d. 单击 Subscribe (订阅)。

6. 您将收到一封包含主题行 EC2 Window 的确认电子邮件。打开电子邮件，然后单击 Confirm subscription 以完成订阅。

每当发布新的 EC2 Windows 驱动程序时，我们都会向订户发送通知。如果您不希望再收到这些通知，请通过以下步骤取消订阅。

从 Amazon EC2 Windows 驱动程序通知中取消订阅

1. 打开 Amazon SNS 控制台。
2. 在导航窗格中，单击 Subscriptions。
3. 选择订阅内容，然后单击 Delete Subscriptions。当系统提示您进行确认时，单击 Yes, Delete。

相关主题

升级：有关升级半虚拟化驱动程序的更多信息，请参阅在 Windows AMI 上升级半虚拟化驱动程序 (p. 275)。

故障排除：有关对 EC2 驱动程序进行故障排除的信息，请参阅对半虚拟化驱动程序进行故障排除 (p. 281)。有关对 EC2 Windows 实例进行故障排除的信息，请参阅对 Windows 实例进行故障排除 (p. 813)。

在 Windows AMI 上升级半虚拟化驱动程序

Abstract

在您的 Windows AMI 上升级半虚拟化驱动程序以允许访问 Xen 虚拟化硬件。

要确认您的 Windows 实例所使用的驱动程序，请在控制面板中打开 Network Connections (网络连接)，查看 Local Area Connection (本地连接)。验证驱动程序是否是以下一种：

- AWS PV Network Device
- Citrix PV Ethernet Adapter
- RedHat PV NIC Driver

或者，您可检查 pnputil -e 命令的输出。

内容

- 升级 Windows Server 2008 R2、2012 和 2012 R2 实例 (AWS PV 驱动程序升级) (p. 275)
- 升级 Windows Server 2008 和 2008 R2 实例 (Redhat 到 Citrix 半虚拟化升级) (p. 277)
- 升级 Windows Server 2003 实例 (Redhat 到 Citrix 半虚拟化驱动程序) (p. 279)
- 升级 Citrix Xen 来宾代理服务 (p. 281)

升级 Windows Server 2008 R2、2012 和 2012 R2 实例 (AWS PV 驱动程序升级)

使用以下过程在 Windows Server 2012 R2、Windows Server 2012 或 Windows Server 2008 R2 上对 AWS PV 驱动程序执行就地升级，或从 Citrix PV 驱动程序升级到 AWS PV 驱动程序。此升级不适用于 RedHat 驱动程序或 Windows Server 的其他版本。



Important

如果您的实例是域控制器，请参阅[升级作为域控制器的实例 \(AWS PV 驱动程序升级 \) \(p. 276\)](#)。与非域控制器实例相比，域控制器的升级过程需要额外的步骤。

升级 AWS PV 驱动程序

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择需要驱动程序升级的实例，打开上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在实例停止后创建备份。打开实例的上下文（右键单击）菜单，选择 Image，然后选择 Create Image。
5. 从实例的上下文（右键单击）菜单中选择 Instance State，然后选择 Start。
6. 使用远程桌面连接到实例并进行实例升级准备。建议您在执行此升级前使所有非系统磁盘脱机。请注意，如果您要对 AWS 半虚拟化驱动程序执行就地升级，则不需要此步骤。我们还建议在 Services 控制台中将不必要的服务设置为 Manual 启动。
7. 将最新[驱动程序包](#)下载到实例。
8. 提取文件夹的内容，然后运行 AWSPVDriverSetup.msi。

在运行 MSI 后，实例将自动重启，然后升级驱动程序。实例将有长达 15 分钟的时间不可用。在升级完成并且实例在 Amazon EC2 控制台中通过了两项健康检查后，请使用远程桌面连接到实例并验证新驱动程序是否已安装。在设备管理器中的存储控制器下，找到 AWS PV 存储主适配器。确认驱动程序版本与 [Amazon EC2 Windows 驱动程序](#)页上列出的最新版本相同。



Note

如果您之前使用适用于 Citrix 半虚拟化驱动程序的 Netsh 禁用了 [TCP 卸载 \(p. 285\)](#)，建议您升级到 AWS 半虚拟化驱动程序后重新启用此功能。Citrix 驱动程序的 TCP 卸载问题在 AWS 半虚拟化驱动程序中不会出现。因此，通过使用 AWS 半虚拟化驱动程序，TCP 卸载可提供更高的性能。

升级作为域控制器的实例（AWS PV 驱动程序升级）

使用以下过程在域控制器上对 AWS 半虚拟化驱动程序执行就地升级，或从 Citrix 半虚拟化驱动程序升级到 AWS 半虚拟化驱动程序。

升级域控制器

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择需要驱动程序升级的实例，打开上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在实例停止后创建备份。打开实例的上下文（右键单击）菜单，选择 Image，然后选择 Create Image。
5. 从实例的上下文（右键单击）菜单中选择 Instance State，然后选择 Start。
6. 运行以下命令。此命令将在系统重启之后将 Windows 配置为启动到 DSRM 模式：

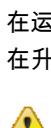
```
bcdedit /set {default} safeboot dsrepair
```



Warning

运行此命令后，请勿手动重启系统。系统将无法访问，因为 Citrix 半虚拟化驱动程序不支持 DSRM。

7. 打开注册表编辑器并创建以下项：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup。
8. 从上下文（右键单击）菜单中，选择 New，然后选择 String Value。指定名称为 `DisableDCCheck`，值为 `true`。
9. 将最新驱动程序包[下载](#)到实例。
10. 提取文件夹的内容，然后运行 `AWSPVDriverSetup.msi`。



Important

您必须通过按以下格式指定用户名来连接到实例：`hostname\administrator`。例如，`Win2k12TestBox\administrator`。

12. 从命令提示符，运行以下命令以删除 DSRM 启动配置：

```
bcdedit /deletevalue safeboot
```

13. 要完成升级过程，请验证是否安装了新驱动程序。在设备管理器中的存储控制器下，找到 AWS PV 存储主适配器。确认驱动程序版本与 [Amazon EC2 Windows 驱动程序](#)页上列出的最新版本相同。



Note

如果您之前使用适用于 Citrix 半虚拟化驱动程序的 Netsh 禁用了 [TCP 卸载 \(p. 285\)](#)，建议您升级到 AWS 半虚拟化驱动程序后重新启用此功能。Citrix 驱动程序的 TCP 卸载问题在 AWS 半虚拟化驱动程序中不会出现。因此，通过使用 AWS 半虚拟化驱动程序，TCP 卸载可提供更高的性能。

升级 Windows Server 2008 和 2008 R2 实例 (Redhat 到 Citrix 半虚拟化升级)

开始将 RedHat 驱动程序升级为 Citrix 半虚拟化驱动程序之前，请务必执行以下操作：

- 转到 [Amazon Windows EC2Config 服务](#)，安装最新版本的 EC2Config。有关 EC2Config 服务的更多信息，请参阅[使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)。
- 验证您是否安装了 Windows PowerShell 2.0。要验证已安装的版本，请在 PowerShell 窗口中运行以下命令：

```
PS C:> $PSVersionTable.PSVersion
```

如果需要安装版本 2.0，请参阅 Microsoft Support 网站上的 [Windows Management Framework \(Windows PowerShell 2.0, WinRM 2.0, and BITS 4.0\)](#)。

- 备份实例上的重要信息或者从实例创建一个 AMI。有关创建 AMI 的更多信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。如果您要创建 AMI，请务必执行以下操作：
 - 写下您的密码。
 - 请勿手动运行 Sysprep 工具或使用 EC2Config 服务。

- 将您的以太网适配器设置为使用 DHCP 自动获取 IP 地址。有关更多信息，请参阅 Microsoft TechNet 库中的[配置 TCP/IP 设置](#)。

升级 Redhat 驱动程序

- 连接到您的实例并以本地管理员身份登录。有关连接到实例的更多信息，请参阅[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
- 在您的实例中，转到 [Amazon EC2 Windows Paravirtual Driver Upgrade Script](#)，下载 Citrix 半虚拟化升级包。
- 将升级包的内容解压到您所选的位置。
- 双击 Upgrade.bat 文件。如果您收到安全警告，请单击 Run。
- 在 Upgrade Drivers 对话框中，查看此信息并单击 Yes (如果您已开始升级)。
- 在 Red Hat Paravirtualized Xen Drivers for Windows uninstaller 对话框中，单击 Yes 以删除 RedHat 软件。您的实例会重新启动。



Note

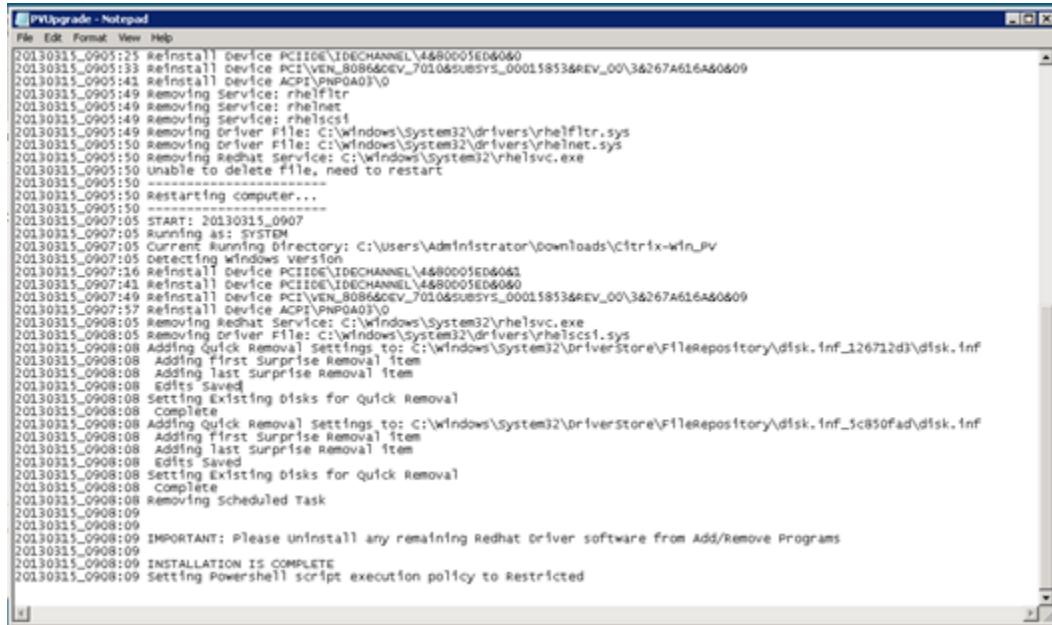
如果您没有看到卸载程序对话框，请单击 Windows 任务栏中的 Red Hat Paravirtualize...。



- 检查实例是否已重新启动并且可以使用。
 - 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
 - 在 Instances 页面上，右键单击您的实例并选择 Get System Log (获取系统日志)。
 - 升级操作应该已重新启动服务器 3 到 4 次。您可以在日志文件中看到此信息 (依据 Windows is Ready to use 的显示次数)。

```
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF064F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>L79ThJPF8LyIL38I2htOFBrjet3vnT2csTiU/XGVMRC7kQtBnznAnXrKdlsirXlx19BwVMs9b38jFJqv01IUpgNNJRZoCdc7IbUw</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception: 
at Ec2Config.Service.On()
at Ec2Config.Service.On()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF064F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF064F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use
```

- 连接到您的实例并以本地管理员身份登录。
- 关闭 Red Hat Paravirtualized Xen Drivers for Windows uninstaller 对话框。
- 确认安装已完成。导航至您之前解压的 Citrix-WIN_PV 文件夹，打开 PVUpgrade.log 文件，然后检查是否有文本 INSTALLATION IS COMPLETE。



```
PVUpgrade - Notepad
File Edit Format View Help
20130315_0905:25 Reinstall Device PCIIDE\JDECHANNEL\4&80005ED040
20130315_0905:33 Reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0&0
20130315_0905:41 Reinstall Device ACPI\PNP0403\0
20130315_0905:49 Removing Service: rhelfltr
20130315_0905:49 Removing Service: rhelnet
20130315_0905:49 Removing Service: rhelscsf
20130315_0905:49 Removing Driver File: C:\Windows\System32\drivers\rhelfltr.sys
20130315_0905:50 Removing Driver File: C:\Windows\System32\drivers\rhelnet.sys
20130315_0905:50 Removing Redhat Service: C:\Windows\System32\rhelsvc.exe
20130315_0905:50 Unable to delete file, need to restart
20130315_0905:50
20130315_0905:50 Restarting computer...
20130315_0905:50
20130315_0907:00 START: 20130315_0907
20130315_0907:00 Running as: SYSTEM
20130315_0907:00 Current Running Directory: C:\users\Administrator\downloads\Citrix-Win_PV
20130315_0907:00 Detecting Windows Version
20130315_0907:16 Reinstall Device PCIIDE\JDECHANNEL\4&80005ED040
20130315_0907:16 Reinstall Device PCIIDE\JDECHANNEL\4&80005ED040
20130315_0907:16 Reinstall Device PCIIDE\JDECHANNEL\4&80005ED040
20130315_0907:19 Reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0&0
20130315_0907:37 Reinstall Device ACPI\PNP0403\0
20130315_0908:05 Removing Redhat Service: C:\Windows\System32\rhelsvc.exe
20130315_0908:05 Removing Driver File: C:\Windows\System32\drivers\rhelscs1.sys
20130315_0908:08 Adding Quick Removal Settings to: C:\Windows\DriverStore\FilterRepository\disk.inf_126712d3\disk.inf
20130315_0908:08 Adding First Surprise Removal Item
20130315_0908:08 Adding Last Surprise Removal Item
20130315_0908:08 Edits Saved
20130315_0908:08 Setting Existing Disks for Quick Removal
20130315_0908:08 Complete
20130315_0908:08 Adding Quick Removal Settings to: C:\Windows\System32\DriverStore\FilterRepository\disk.inf_5c850fad\disk.inf
20130315_0908:08 Adding First Surprise Removal Item
20130315_0908:08 Adding Last Surprise Removal Item
20130315_0908:08 Edits Saved
20130315_0908:08 Setting Existing Disks for Quick Removal
20130315_0908:08 Complete
20130315_0908:08 Removing Scheduled Task
20130315_0908:09
20130315_0908:09 IMPORTANT: Please Uninstall any remaining Redhat Driver software from Add/Remove Programs
20130315_0908:09
20130315_0908:09 INSTALLATION IS COMPLETE
20130315_0908:09 Setting PowerShell script execution policy to Restricted
```

升级 Windows Server 2003 实例 (Redhat 到 Citrix 半虚拟化驱动程序)

开始将 RedHat 驱动程序升级为 Citrix 半虚拟化驱动程序之前，请务必执行以下操作：

- 验证您的 Windows Server 2003 实例上是否安装了 Windows PowerShell 2.0。升级过程需要 PowerShell 2.0。有关如何安装 PowerShell 2.0 的信息，请参阅 [Windows Management Framework Core 程序包 \(Windows PowerShell 2.0 和 WinRM 2.0 \)](#)。
- 备份实例上的重要信息或者从实例创建一个 AMI。有关创建 AMI 的更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76 \)](#)。如果您要创建 AMI，请务必执行以下操作：
 - 不在 EC2Config 服务中启用 Sysprep 工具。
 - 写下您的密码。
 - 将您的以太网适配器设为 DHCP。
- 转到 [Amazon Windows EC2Config 服务](#)，安装最新版本的 EC2Config。有关 EC2Config 服务的更多信息，请参阅 [使用 EC2Config 服务配置 Windows 实例 \(p. 250 \)](#)。

升级 Redhat 驱动程序

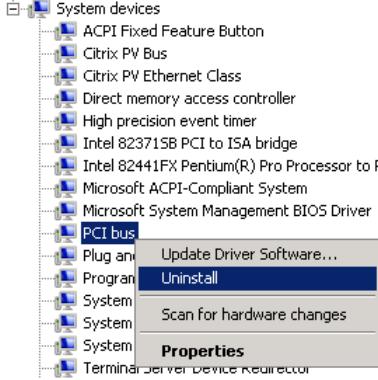
- 连接到您的实例并以本地管理员身份登录。有关连接到实例的更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225 \)](#)。
- 在您的实例中，转到 [Amazon EC2 Windows Paravirtual Driver Upgrade Script](#)，下载 Citrix 半虚拟化升级包。
- 将升级包的内容解压到您所选的位置。
- 双击 Upgrade.bat 文件。如果您收到安全警告，请单击 Run。
- 在 Upgrade Drivers 对话框中，查看此信息并单击 Yes (如果您已开始升级)。
- 在 Red Hat Paravirtualized Xen Drivers for Windows uninstaller 对话框中，单击 Yes 以删除 RedHat 软件。您的实例会重新启动。

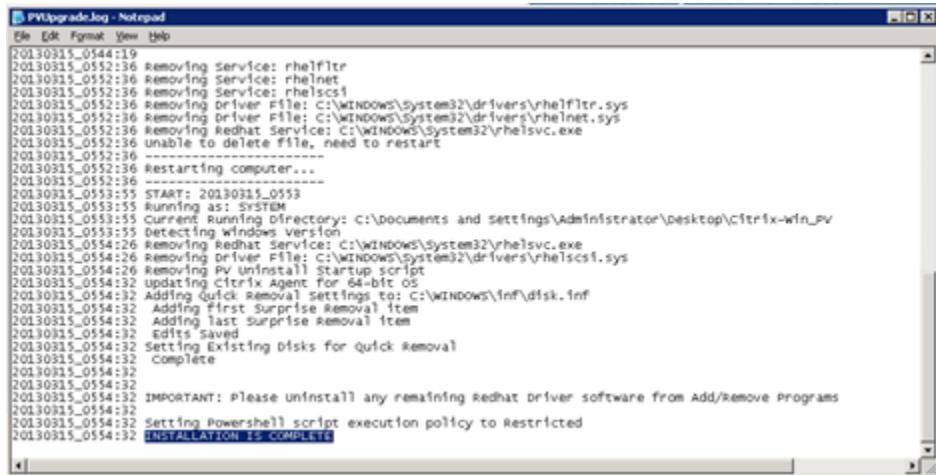


Note

如果您没有看到卸载程序对话框，请单击 Windows 任务栏中的 Red Hat Paravirtualize...。



7. 检查实例是否已重新启动并且可以使用。
 - a. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
 - b. 在 Instances 页面上，右键单击您的实例并选择 Get System Log (获取系统日志)。
 - c. 检查该日志消息的末尾。它应该为 Windows is Ready to use。
8. 连接到您的实例并以本地管理员身份登录。升级会打开以下四个应用程序并继续：PowerShell、RedHat 卸载程序、PVUpgrade.log 和 Windows 设备管理器。
9. 卸载 PCI BUS。
 - a. 在 Device Manager (设备管理器) 窗口中，展开 System devices (系统设备)，右键单击 PCI bus (PCI 总线) 并单击 Uninstall (卸载)。
 - b. 在系统提示时，单击 OK (确定)。
 - c. 在系统设置改变对话框中，单击否 (如果您不想立即重新启动自己的实例)。
 - d. 关闭设备管理器。升级脚本会重新启动您的实例。
10. 重复第 7 步中的流程，看看实例是否已准备就绪。确认实例已准备就绪之后，请以管理员的身份进行登录。
11. 确认安装已完成。导航至您之前解压的 Citrix-WIN_PV 文件夹，打开 PVUpgrade.log 文件，然后检查是否有文本 INSTALLATION IS COMPLETE。



```
PVUpgradeLog - Notepad
File Edit Format View Help
20130315_0544:19
20130315_0552:36 Removing Service: rhelflitr
20130315_0552:36 Removing Service: rhelnet
20130315_0552:36 Removing Service: rhelscs1
20130315_0552:36 Removing driver File: C:\WINDOWS\System32\drivers\rhelflitr.sys
20130315_0552:36 Removing Driver File: C:\WINDOWS\System32\drivers\rhelnet.sys
20130315_0552:36 Removing Redhat Service: C:\WINDOWS\System32\rhelsvc.exe
20130315_0552:36 Unable to delete file, need to restart
20130315_0552:36
20130315_0552:36 Restarting computer...
20130315_0552:36
20130315_0553:55 START: 20130315_0553
20130315_0553:55 Running as: SYSTEM
20130315_0553:55 Current Running Directory: C:\documents and settings\Administrator\desktop\citrix-win_pv
20130315_0553:55 Detecting Windows Version
20130315_0554:20 Removing Redhat Service: C:\WINDOWS\System32\rhelsvc.exe
20130315_0554:20 Removing Driver File: C:\WINDOWS\System32\drivers\rhelscs1.sys
20130315_0554:20 Removing Pv Uninstall Agent 64-bit
20130315_0554:20 Updating Pv Uninstall Agent for 64-bit OS
20130315_0554:32 Adding Quick Removal settings to: C:\WINDOWS\inf\dfsk.inf
20130315_0554:32 Adding First Surprise Removal Item
20130315_0554:32 Adding last Surprise Removal Item
20130315_0554:32 Edits saved
20130315_0554:32 Setting Existing Disks for quick Removal
20130315_0554:32 complete
20130315_0554:32
20130315_0554:32 IMPORTANT: Please uninstall any remaining Redhat driver software from Add/Remove Programs
20130315_0554:32 Setting Powershell script execution policy to Restricted
20130315_0554:32 INSTALLATION IS COMPLETE
```

升级 Citrix Xen 来宾代理服务

如果您要在 Windows Server 上使用 Citrix 半虚拟化驱动程序，则可以升级 Citrix Xen 来宾代理服务。这一 Windows 服务处理相关任务，例如启动时的时间同步，以及通过 API 进行的关闭和重新启动事件。您可以在任意版本的 Windows Server（包括 Windows Server 2012）上运行此升级包，前提是 Windows Server 2012 实例正在运行 Citrix 半虚拟化驱动程序。



Important

请勿在运行 AWS 半虚拟化驱动程序的 Windows Server 2012 或 2012 R2 实例上执行这些步骤。

升级您的驱动程序之前，请确保您已经备份实例上的重要信息，或者从实例创建了一个 AMI。有关创建 AMI 的更多信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。如果您要创建 AMI，请务必执行以下操作：

- 不在 EC2Config 服务中启用 Sysprep 工具。
- 写下您的密码。
- 将您的以太网适配器设为 DHCP。

升级 Citrix Xen 代理客户服务

1. 连接到您的实例并以本地管理员身份登录。有关连接到实例的更多信息，请参阅[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
2. 在您的实例中，转到[Amazon EC2 Windows Paravirtual Driver Upgrade Script](#)，下载 Citrix 升级包。
3. 将升级包的内容解压到您所选的位置。
4. 双击 Upgrade.bat 文件。如果您收到安全警告，请单击 Run。
5. 在 Upgrade Drivers 对话框中，查看此信息并单击 Yes（如果您已开始升级）。
6. 升级完成后，PVupgrade.log 文件会打开并包含文本 UPGRADE IS COMPLETE。
7. 重新启动您的实例。

对半虚拟化驱动程序进行故障排除

本主题介绍了您在 Amazon EC2 半虚拟化驱动程序方面可能遇到的常见问题的解决方案。

内容

- [Windows Server 2012 R2 在实例重启后丢失网络和存储连接 \(p. 282\)](#)
- [TCP 卸载 \(p. 285\)](#)
- [时间同步 \(p. 287\)](#)

Windows Server 2012 R2 在实例重启后丢失网络和存储连接

在 2014 年 9 月 10 日之前提供的 Windows Server 2012 R2 Amazon 系统映像 (AMI) 可能在实例重启后丢失网络和存储连接。AWS 管理控制台系统日志中的错误指明：“Difficulty detecting PV driver details for Console Output”。连接丢失由 Windows Server 2012 R2 即插即用清理功能导致。此功能每 30 天扫描一次不活动的系统设备并禁用它们。此功能错误地将 EC2 网络设备识别为不活动状态并将其从系统中删除。出现这种情况时，实例在重启后会丢失网络连接。

对于您怀疑可能受此问题影响的系统，您可以下载并运行就地驱动程序升级。如果您无法执行就地驱动程序升级，则可以运行帮助程序脚本。该脚本将确定您的实例是否受影响。如果实例受影响，并且 Amazon EC2 网络设备尚未移除，该脚本将禁用即插即用清理扫描。如果 Amazon EC2 网络设备已移除，该脚本将修复设备，禁用即插即用清理扫描，并允许您的实例重新启动并启用网络连接。

本节内容

- [选择您想要的修复此问题的方式 \(p. 282\)](#)
- [方法 1 - 增强联网 \(p. 282\)](#)
- [方法 2 - 注册表配置 \(p. 283\)](#)
- [运行修正脚本 \(p. 284\)](#)

选择您想要的修复此问题的方式

有两种方法可以恢复与受此问题影响的实例的网络和存储连接。选择以下方法之一：

方法	先决条件	过程概述
方法 1 - 增强联网	增强联网仅在需要 C3 实例类型的 Virtual Private Cloud (VPC) 中可用。如果服务器当前不使用 C3 实例类型，则必须临时更改它。增强联网不可用于 ec2-classic。	您应将服务器实例类型更改为 C3 实例。增强联网随后可让您连接到受影响的实例并修复问题。修复问题后，您将实例更改回原始的实例类型。此方法通常比方法 2 更快，导致用户错误的可能性也小。只要 C3 实例运行，您就会产生额外费用。
方法 2 - 注册表配置	能够创建或访问辅助服务器。能够更改注册表设置。	您将根卷从受影响的实例分离，将其挂载到其他实例，连接该实例，然后在注册表中进行更改。只要额外的服务器运行，您就会产生额外费用。此方法比方法 1 慢一些，但此方法在方法 1 无法解决问题的情况下有效。

方法 1 - 增强联网

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 找到受影响的实例。打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在实例停止后创建备份。打开实例的上下文（右键单击）菜单，选择 Image，然后选择 Create Image。
 5. 将实例类型更改为任何 C3 实例类型。
 6. 启动实例。
 7. 使用远程桌面连接到实例，然后将 <https://s3.amazonaws.com/ec2-downloads-windows/Drivers/AWS PV Driver Setup.zip> 下载到实例。
 8. 提取文件夹的内容，然后运行 AWS PV Driver Setup.msi。
- 在运行 MSI 后，实例将自动重启，然后升级驱动程序。实例将有长达 15 分钟的时间不可用。
9. 在升级已完成并且实例在 Amazon EC2 控制台中通过了两项健康检查后，请使用远程桌面连接到实例并验证新驱动程序是否已安装。在设备管理器中的存储控制器下，找到 AWS PV 存储主适配器。确认驱动程序版本与 [Amazon EC2 Windows 驱动程序](#) 页上列出的最新版本相同。
 10. 停止实例并将实例更改回原始的实例类型。
 11. 启动实例并恢复正常使用。

方法 2 - 注册表配置

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 找到受影响的实例。打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 选择 Launch Instance 并在与受影响实例相同的可用区中创建临时的 Windows Server 2008 或 Windows Server 2012 实例。不要创建 Windows Server 2012 R2 实例。



Important

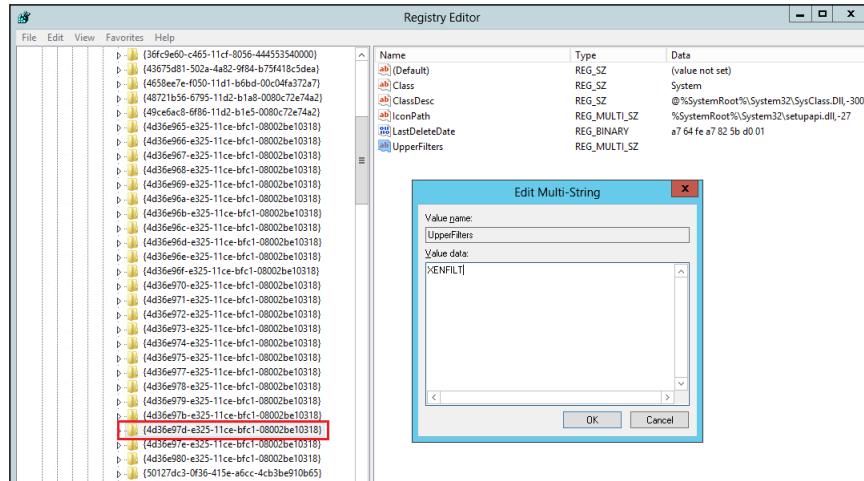
如果您未在与受影响实例相同的可用区中创建该实例，则无法将受影响的实例的根卷挂载到新实例。

5. 在导航窗格中，选择 Volumes。
6. 找到受影响的实例的根卷。分离该卷并将其挂载到早先创建的临时实例。使用默认设备名称 (xvdf) 挂载该卷。
7. 使用远程桌面连接临时实例，然后通过磁盘管理实用工具使该卷可供使用。
8. 在临时实例上，打开“运行”对话框，键入 regedit，然后按 Enter。
9. 在注册表编辑器导航窗格中，选择 HKEY_Local_Machine，然后从文件菜单中选择加载配置单元。
10. 在加载配置单元对话框中，导航到受影响的卷\Windows\System32\config\System 并在项名称对话框中键入临时名称。例如，输入 OldSys。
11. 在注册表编辑器的导航窗格中，找到以下项：

HKEY_LOCAL_MACHINE
\ControlSet001\Control\Class\4d36e97d-e325-11ce-bfc1-08002be10318

HKEY_LOCAL_MACHINE\
\ControlSet001\Control\Class\4d36e96a-e325-11ce-bfc1-08002be10318

12. 对于每个项，双击 UpperFilters，输入值 XENFILT，然后单击确定。



13. 找到以下项：

HKEY_LOCAL_MACHINE\ \ControlSet001\Services\XENBUS\Parameters

14. 使用名称 ActiveDevice 和以下值创建新字符串 (REG_SZ)：

PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. 找到以下项：

HKEY_LOCAL_MACHINE\ \ControlSet001\Services\XENBUS

16. 将 Count 从 0 更改为 1。

17. 找到并删除以下项：

HKEY_LOCAL_MACHINE\ \ControlSet001\Services\xenvbd\StartOverride

HKEY_LOCAL_MACHINE\ \ControlSet001\Services\xenfilt\StartOverride

18. 在注册表编辑器导航窗格中，选择您在首次打开注册表编辑器时创建的临时项。

19. 从文件菜单中，选择卸载配置单元。

20. 在磁盘管理实用工具中，选择您之前挂载的驱动器，打开上下文（右键单击）菜单，然后选择脱机。

21. 在 Amazon EC2 控制台中，将受影响的实例从临时实例分离，然后将其重新挂载到您的具有设备名称 /dev/sda1 的 Windows Server 2012 R2 实例。您必须指定此设备名称才能将卷指派为根卷。

22. 启动实例。

23. 使用远程桌面连接到实例，然后将 <https://s3.amazonaws.com/ec2-downloads-windows/Drivers/AWSPVDriverSetup.zip> 下载到实例。

24. 提取文件夹的内容，然后运行 AWS PV Driver Setup.msi。

在运行 MSI 后，实例将自动重启，然后升级驱动程序。实例将有长达 15 分钟的时间不可用。

25. 在升级已完成并且实例在 Amazon EC2 控制台中通过了两项健康检查后，请使用远程桌面连接到实例并验证新驱动程序是否已安装。在设备管理器中的存储控制器下，找到 AWS PV 存储主适配器。确认驱动程序版本与 [Amazon EC2 Windows 驱动程序](#) 页上列出的最新版本相同。

26. 删除或停止您在本过程中创建的临时实例。

运行修正脚本

如果您无法执行就地驱动程序升级或无法迁移到较新的实例，则可以运行修正脚本来修复即插即用清理任务导致的问题。

运行修正脚本

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择要为其运行修正脚本的实例。打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。



Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在实例停止后创建备份。打开实例的上下文（右键单击）菜单，选择 Image，然后选择 Create Image。
5. 打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Start。
6. 使用远程桌面连接到实例，然后将 RemediateDriverIssue.zip 文件夹 [下载](#) 到实例。
7. 提取文件夹的内容。
8. 根据 Readme.txt 文件中的指示运行修正脚本。该文件位于您提取 RemediateDriverIssue.zip 的文件夹中。

TCP 卸载

默认情况下，会为 Windows AMI 中的 Citrix 半虚拟化驱动程序启用 TCP 卸载。如果您遇到传输级错误或数据包传输错误（在 Windows 性能监视器上可见，例如在运行特定 SQL 工作负载时），可能需要禁用此功能。



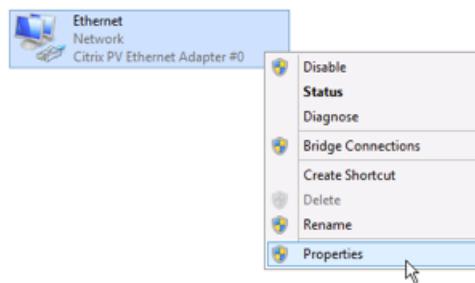
Important

禁用 TCP 卸载可能会降低实例的网络性能。

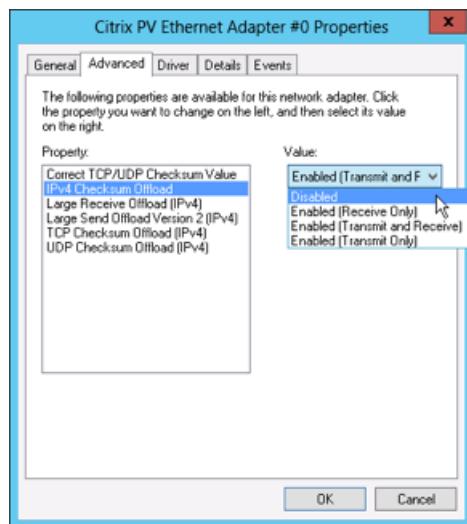
您不需要在运行 Windows Server 2012 R2 的实例上执行此过程。Windows Server 2012 R2 实例使用了 AWS 半虚拟化驱动程序和 Intel 驱动程序。

为 Windows Server 2012 和 2008 禁用 TCP 卸载

1. 连接到您的实例并以本地管理员身份登录。
2. 如果您使用 Windows Server 2012，请按 Ctrl+Esc 访问 Start (开始) 屏幕，然后单击 Control Panel (控制面板)。如果您使用 Windows Server 2008，请单击 Start (开始) 并选择 Control Panel (控制面板)。
3. 单击 Network and Internet (网络和 Internet)，然后单击 Network and Sharing Center (网络和共享中心)。
4. 单击 Change adapter settings (更改适配器设置)。
5. 右键单击 Citrix PV Ethernet Adapter #0 (Citrix 半虚拟化以太网适配器 #0)，然后选择 Properties (属性)。



6. 在 Local Area Connection Properties (本地连接属性)对话框中，单击 Configure (配置) 打开 Citrix PV Ethernet Adapter #0 Properties (Citrix 半虚拟化以太网适配器 #0 属性) 对话框。
7. 在 Advanced (高级) 选项卡上，通过在 Property (属性) 列表中选择属性并从 Value (值) 列表中选择 Disabled (禁用)，来禁用以下每个属性：
 - IPv4 Checksum Offload (IPv4 校验和卸载)
 - Large Receive Offload (IPv4) (大量接收卸载(IPv4))
 - Large Send Offload Version 2 (IPv4) (大量发送卸载版本 2 (IPv4))
 - TCP Checksum Offload (IPv4) (TCP 校验和卸载(IPv4))
 - UDP Checksum Offload (IPv4) (UDP 校验和卸载(IPv4))



8. 单击 OK (确定)。
9. 从命令提示符窗口运行以下命令。

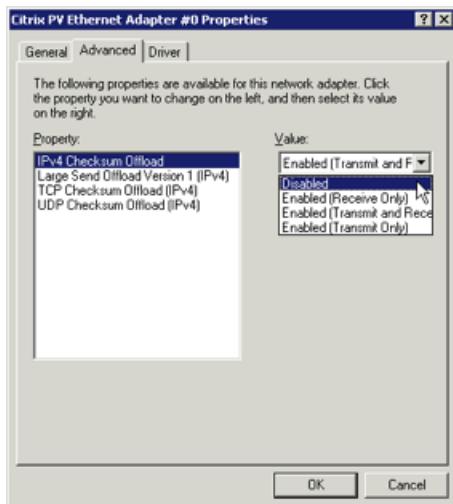
```
C:\> netsh int ip set global taskoffload=disabled
C:\> netsh int tcp set global chimney=disabled
C:\> netsh int tcp set global rss=disabled
C:\> netsh int tcp set global netdma=disabled
```

10. 重启实例。

为 Windows Server 2003 禁用 TCP 卸载

1. 连接到您的实例并以本地管理员身份登录。
2. 单击 Start (开始)，依次选择 Control Panel (控制面板)、Network Connections (网络连接) 和 Local Area Connection 3 (本地连接 3)。
3. 单击 Properties (属性)。
4. 在 Local Area Connection 3 (本地连接 3) 对话框中，单击 Configure... (配置...) 以打开 Citrix PV Ethernet Adapter #0 Properties (Citrix 半虚拟化以太网适配器 #0 属性) 对话框。
5. 在 Advanced (高级) 选项卡上，通过在 Property (属性) 列表中选择属性并从 Value (值) 列表中选择 Disabled (禁用)，来禁用以下每个属性：
 - IPv4 Checksum Offload (IPv4 校验和卸载)
 - Large Send Offload Version 1 (IPv4) (大量发送卸载版本 1 (IPv4))

- TCP Checksum Offload (IPv4) (TCP 校验和卸载(IPv4))
- UDP Checksum Offload (IPv4) (UDP 校验和卸载(IPv4))



6. 单击 OK (确定)。
7. 运行以下 PowerShell 脚本。

```
$n = Get-ItemProperty "HKLM:\SYSTEM\Select" | Select -expand Current

$root = "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00$n\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}"
$item = Get-ChildItem -Path Registry::$Root -Name

Foreach ($item in $items) {
    if ($item -ne "Properties") {
        $path = $root + "\\" + $item
        $DriverDesc = Get-ItemProperty -Path Registry::$path | Select-Object
        -expandproperty DriverDesc
        if ($DriverDesc -eq "Citrix PV Ethernet Adapter") {
            Set-ItemProperty -path Registry::$path -Name *IPChecksumOffloadIPv4
            -Value 0
            Set-ItemProperty -path Registry::$path -Name *TCPChecksumOffloadIPv4
            -Value 0
            Set-ItemProperty -path Registry::$path -Name *UDPChecksumOffloadIPv4
            -Value 0
            Set-ItemProperty -path Registry::$path -Name *LSOv1IPv4 -Value 0
        }
    }
}
```

8. 重启实例。

时间同步

在 2013.02.13 Windows AMI 版本前，Citrix Xen 代理客户无法正确设置系统时间。这可能导致您的 DHCP 租约过期。如果您在连接到您的实例时遇到问题，可能需要更新代理。

要确定您是否有更新的 Citrix Xen 客户代理，请检查 C:\Program Files\Citrix\XenGuestAgent.exe 文件时间是否为 2013 年 3 月。如果此文件的日期早于这个时间，则请更新 Citrix Xen 代理客户服务。有关更多信息，请参阅 [升级 Citrix Xen 来宾代理服务 \(p. 281\)](#)。

相关主题

有关对 EC2 Windows 实例进行故障排除的信息，请参阅 [对 Windows 实例进行故障排除 \(p. 813\)](#)。

设置 Windows 实例的密码

Abstract

了解如何管理您的 Windows 实例的密码。

在连接到 Windows 实例时，必须指定拥有该实例访问权限的用户账户以及账户密码。首次连接到实例时，请指定管理员账户和默认密码。默认密码是由 EC2Config 服务自动生成的。

在您连接到实例后，建议更改管理员密码的默认值。如果丢失了密码或密码过期，您可以手动配置 EC2Config 以生成新密码。

内容

- [连接后更改管理员密码 \(p. 288\)](#)
- [重置丢失或过期的管理员密码 \(p. 288\)](#)

连接后更改管理员密码

执行以下步骤可更改实例的管理员账户密码。



Important

将新密码存储在安全位置，因为您无法使用 Amazon EC2 控制台获取该密码；控制台始终获取默认密码。如果您尝试在更改密码后使用默认密码连接到实例，则会收到错误“Your credentials did not work (您的证书不起作用)”。

更改本地管理员密码

1. 连接到您的实例。
2. 从实例打开命令提示符窗口。
3. 从命令提示符窗口运行以下命令：

```
C:\> net user Administrator new_password
```

重置丢失或过期的管理员密码

如果您丢失了 Windows 实例的本地管理员账户密码，或者该密码过期，可以使用 EC2Config 服务重置密码。请注意，如果已禁用本地管理员账户，则无法重置密码。

通过修改需重置密码的实例的根卷上的一个配置文件，可以使用 EC2Config 服务重置管理员密码。但是，除非该卷当前不是根卷，否则无法修改该文件。因此，必须将根卷与实例分离，将该卷作为辅助卷连接到其他实例，更改配置设置，然后将该卷重新连接为根卷。



Important

按下面过程所述停止和启动实例后，实例获取新的公有 IP 地址。重置密码后，请务必使用实例的当前公有 DNS 名称连接到实例。如果实例位于 EC2-Classic 中，则所有弹性 IP 地址都与实例解除关联，因此必须重新关联。有关更多信息，请参阅 [实例生命周期 \(p. 213\)](#)。

重置管理员密码

1. 验证需重置密码的实例上是否安装了 EC2Config 服务。（在此过程中，该实例称为原始实例。）默认情况下，所有 Amazon Windows AMI 上均提供了 EC2Config，您也可以下载该服务。有关更多信息，请参阅 [安装最新版的 EC2Config \(p. 258\)](#)。
2. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
3. 通过以下操作停止原始实例：
 - a. 在导航窗格中，选择 Instances。
 - b. 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。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

- c. 在 Stop Instances 对话框中，选择 Yes, Stop。停止实例之后，继续下一步操作。
4. 在原始实例所在的可用区中启动 Windows 实例。（在此过程中，该实例称为临时实例。）



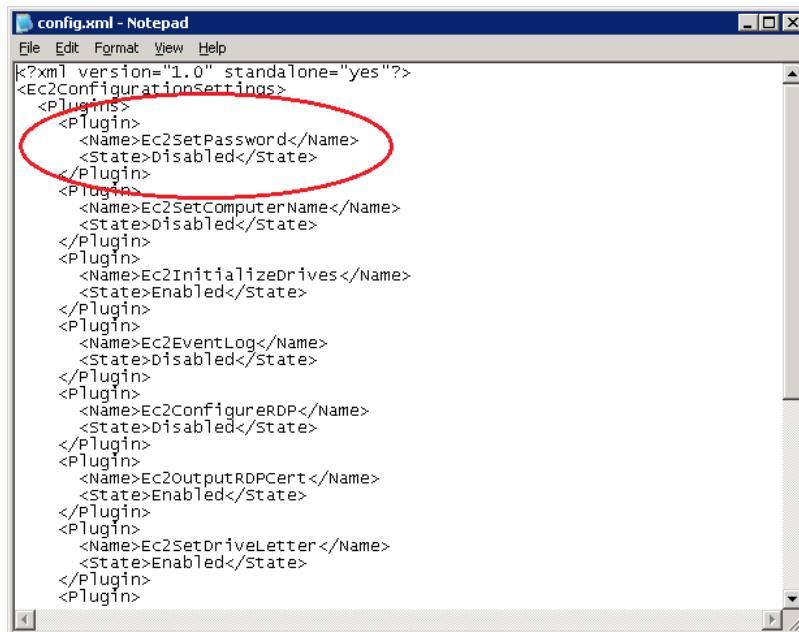
Warning

（可选）如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成额外的步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。或者，可以为临时实例选择不同的 AMI。例如，如果原始实例使用 Windows Server 2008 R2 的 AWS Windows AMI，则使用 Windows Server 2012 或 Windows Server 2003 的 AWS Windows AMI 来启动临时实例。（要查找适用于 Windows Server 2003 的 AMI，请使用名称 Windows_Server-2003-R2_SP2 来搜索 AMI。）

5. 通过以下操作将根卷与原始实例分离：
 - a. 在原始实例的 Description 窗格上，记下作为 Root device 列出的卷的 EBS ID。
 - b. 在导航窗格中，选择 Volumes。
 - c. 在卷列表中，选择该卷，然后选择 Actions、Detach Volume。当卷的状态变为 available (可用) 之后，继续下一步操作。
6. 通过以下操作，将卷作为辅助卷连接到临时实例：
 - a. 选择 Actions、Attach Volume。
 - b. 在 Attach Volume (连接卷) 对话框中，在 Instances 字段中键入临时实例的名称或 ID，然后从建议选项的列表中选择该实例。
 - c. 在 Device 框中，键入 `xvdf`（如果此处没有），然后选择 Attach。
 - d. 连接到临时实例，打开磁盘管理实用工具，使用以下说明使驱动器联机：[使卷可在 Windows 上使用 \(p. 658\)](#)。

7. 在辅助卷上，按照以下说明修改配置文件：

- a. 从临时实例导航到辅助卷，使用文本编辑器（如“记事本”）打开 \Program Files\Amazon\Ec2ConfigService\Settings\config.xml。
- b. 在文件顶部，查找名为 Ec2SetPassword 的插件，如图所示。将状态从 Disabled 更改为 Enabled，然后保存文件。



8. (可选) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成以下步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。



Warning

以下过程介绍了如何使用注册表编辑器编辑 Windows 注册表。如果您不熟悉注册表或不知道如何使用注册编辑器安全地做出更改，请阅读 [Microsoft TechNet](#) 上的注册表。

- a. 打开命令提示，键入 regedit.exe，并按“Enter”键。
- b. 在注册表编辑器中，从上下文菜单中选择 HKEY_LOCAL_MACHINE（右击），然后选择“查找”。
- c. 键入 Windows Boot Manager，然后选择“查找下一个”。
- d. 选择名为 11000001 的密钥。此密钥与您在之前步骤中找到的密钥处于同一层级。
- e. 在右侧窗格中，选择“ ”，然后从上下文菜单中选择“修改”（右击）。
- f. 在数据中的偏移 0x38 处查找四字节磁盘签名。颠倒这些字节以创建磁盘签名并将其记下。例如，由以下数据表示的磁盘签名为 E9EB3AA5：

```
...
0030 00 00 00 00 01 00 00 00
0038 A5 3A EB E9 00 00 00 00
0040 00 00 00 00 00 00 00 00
...
```

- g. 在命令提示符窗口中，运行以下命令以启动 Microsoft DiskPart。

```
C:\> diskpart
```

- h. 运行以下 DiskPart 命令以选择卷。（您可以使用 Disk Management（磁盘管理）实用工具来验证磁盘编号为 1。）

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

- i. 运行以下 DiskPart 命令以获取磁盘签名。

```
DISKPART> uniqueid disk

Disk ID: 0C764FA8
```

- j. 如果上一步骤中显示的磁盘签名与前面记下的 BCD 中的磁盘签名不匹配，请使用以下 DiskPart 命令更改磁盘签名以使其匹配：

```
DISKPART> uniqueid disk id=E9EB3AA5
```

9. 通过以下操作从临时实例分离辅助卷：

- a. 使用 Disk Management（磁盘管理）实用工具，将该卷脱机。



Note

如果临时实例运行的操作系统与受影响实例相同，则驱动器将自动脱机，因此您无需手动使其脱机。

- b. 在 Amazon EC2 控制台的导航窗格中，选择 Volumes。

- c. 选择卷，然后选择 Actions、Detach Volume。当卷的状态变为 available（可用）之后，继续下一步操作。

10. 通过以下操作，将卷作为根卷连接到原始实例：

- a. 选择卷，然后选择 Actions、Attach Volume。

- b. 在 Attach Volume（连接卷）对话框中，在 Instances 列表中键入原始实例的名称或 ID，然后选择该实例。

- c. 在 Device（设备）框中，输入 /dev/sda1。

- d. 选择 Yes, Attach。

11. 通过以下步骤重新启动原始实例：

- a. 在导航窗格中，选择 Instances。

- b. 选择原始实例，然后依次选择 Actions、Instance State、Start。

- c. 在 Start Instances 对话框中，选择 Yes, Start。

12. 通过以下步骤检索新的默认密码：
 - a. 在导航窗格中，选择 Instances。
 - b. 选择原始实例，然后选择 Actions、Get Windows Password。
 - c. 在 Retrieve Default Windows Administrator Password 对话框中，选择 Browse，然后选择对应于启动实例时指定的密钥对的 .pem 文件。
 - d. 选择 Decrypt Password。您将使用解密的密码以及本地管理员账户连接到原始实例。

为 Windows 实例设置时间

Abstract

为 Windows 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。建议对 Windows 实例使用协调世界时 (UTC)。不过，如果需要，可以使用其他时区。

内容

- [更改时区 \(p. 292\)](#)
- [配置网络时间协议 \(NTP\) \(p. 293\)](#)
- [配置 Windows Server 2008 及更高版本的时间设置 \(p. 293\)](#)
- [配置 Windows Server 2003 的时间设置 \(p. 294\)](#)
- [相关主题 \(p. 294\)](#)

更改时区

默认情况下，Windows 实例设置为 UTC 时区。您可以更改时间以符合本地时区或您的网络中其他部分的时区。

更改实例上的时区

1. 从实例打开命令提示符窗口。
2. 确定将在实例上使用的时区。要获取时区的列表，请使用以下命令：tzutil /l。此命令用以下格式返回所有可用时区的列表：

```
display name
time zone ID
```

3. 查找要分配给该实例的时区 ID。
4. 使用以下命令将时区分配给实例：

```
C:\> tzutil /s "Pacific Standard Time"
```

新时区应立即生效。

配置网络时间协议 (NTP)

Windows 实例使用 time.windows.com NTP 服务器来配置系统时间；不过，您可以更改该实例以根据需要使用另外一组 NTP 服务器。例如，如果您的 Windows 实例不能接入 Internet，则可以将它们配置为使用位于您的私有网络内的 NTP 服务器。您的实例的安全组必须允许端口 123 (NTP) 上的出站 UDP 流量。本节中的步骤说明如何验证和更改实例的 NTP 配置。

验证 NTP 配置

1. 从实例打开命令提示符窗口。
2. 通过键入以下命令获取当前 NTP 配置：

```
C:\> w32tm /query /configuration
```

此命令返回 Windows 实例的当前配置设置。

3. (可选) 通过键入以下命令获取当前配置的状态：

```
C:\> w32tm /query /status
```

此命令返回实例与 NTP 服务器同步的最后时间和轮询间隔等信息。

更改 NTP 配置

1. 从命令提示符窗口运行以下命令：

```
C:\> w32tm /config /manualpeerlist:comma-delimited list of NTP servers /syncfromflags:manual /update
```

其中，*comma-delimited list of NTP servers* 是所使用的实例的 NTP 服务器列表。

2. 使用以下命令验证新设置：

```
C:\> w32tm /query /configuration
```

配置 Windows Server 2008 及更高版本的时间设置

在更改 Windows 实例上的时间时，必须确保该时间在系统重新启动后仍然保留。否则，当实例重新启动时，它会恢复使用 UTC 时间。对于 Windows Server 2008 及更高版本，可通过添加 RealTimeIsUniversal 注册表项来保留时间设置。

设置 RealTimeIsUniversal 注册表项

1. 从实例打开命令提示符窗口。
2. 使用以下命令添加注册表项：

```
C:\> reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. 如果您使用的是在 2013 年 2 月 22 日之前创建的 Windows Server 2008 AMI（不是 Windows Server 2008 R2），则应验证是否安装了 Microsoft 修补程序 [KB2800213](#)。如果未安装该修补程序，请将其

安装。该修补程序解决了一个已知问题，即 RealTimelsUniversal 项会造成 Windows CPU 在夏令时期间以及在每个日历年开始时（1月1日）在100% 负荷下运行。

如果使用的是运行 Windows Server 2008 R2（不是 Windows Server 2008）的 AMI，则必须验证是否安装了 Microsoft 修补程序 [KB2922223](#)。如果未安装该修补程序，请将其安装。该修补程序解决了一个已知问题，即 RealTimelsUniversal 项阻止系统更新 CMOS 时钟。

4. （可选）验证该实例是否使用以下命令成功保存了该注册表项：

```
C:\> reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /s
```

此命令返回 TimeZoneInformation 注册表项的子项。列表底部应具有 RealTimelsUniversal 项，与下面类似：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
  Bias                               REG_DWORD      0x1e0
  DaylightBias                      REG_DWORD      0xfffffff4
  DaylightName                      REG_SZ        @tzres.dll,-211
  DaylightStart                     REG_BINARY
  00000300020002000000000000000000
    StandardBias                    REG_DWORD      0x0
    StandardName                   REG_SZ        @tzres.dll,-212
    StandardStart                  REG_BINARY
  00000B00010002000000000000000000
    TimeZoneKeyName                REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled   REG_DWORD      0x0
    ActiveTimeBias                 REG_DWORD      0x1a4
    RealTimeIsUniversal            REG_DWORD      0x1
```

配置 Windows Server 2003 的时间设置

在更改运行 Windows Server 2003 的实例上的时区时，必须确保该时间在系统重新启动后仍然保留。否则，如果重新启动该实例，它会对您所在的时区恢复使用 UTC 时钟，导致与时间偏移相关的时间差。您可通过更新 Citrix 半虚拟化驱动程序来保留时间设置。有关更多信息，请参阅 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。

在更新 Citrix 半虚拟化驱动程序后，用于虚拟机服务的 Citrix 工具会在服务启动时设置实例上的时间。

相关主题

有关 Windows 操作系统如何协调和管理时间（包括闰秒的添加）的更多信息，请参阅以下主题：

- [Windows 时间服务的工作方式 \(TechNet\)](#)
- [W32tm \(TechNet\)](#)
- [Windows 时间服务如何处理闰秒 \(TechNet\)](#)
- [有关闰秒和 Windows 的案例：可能不是 Y2K \(博客\)](#)

管理 Windows 实例配置

Abstract

在 EC2 实例运行时管理其配置。

利用 Amazon EC2 Simple Systems Manager (SSM) Config 功能，您可以管理运行中的 Windows 实例的配置。您可以创建描述配置任务（例如，安装软件）的 SSM 文档，然后将该 SSM 文档与一个或多个运行中的 Windows 实例关联。实例上的配置代理负责处理 SSM 文档并按指定方式配置实例。

从实例解除 SSM 文档的关联不会更改实例的配置。要在解除 SSM 文档的关联后更改实例的配置，您必须创建描述配置任务（例如，卸载软件）的新 SSM 文档，然后将该文档与实例关联。

若要仅在实例启动时运行脚本，请考虑改用用户数据执行。有关更多信息，请参阅 [使用用户数据执行脚本 \(p. 242\)](#)。

有关更复杂的自动方案，请考虑改用 AWS CloudFormation 或 AWS OpsWorks。有关更多信息，请参阅 [AWS CloudFormation 用户指南](#) 或 [AWS OpsWorks 用户指南](#)。

先决条件

EC2Config 服务可处理 SSM 文档并按照指定配置该实例。将最新版本的 [Amazon Windows EC2Config 服务](#) 下载到要使用 SSM Config 配置的每个服务器。

限制

- 仅 Windows 实例支持 SSM Config。
- 在以下[区域](#)提供 SSM Config。

要使用 SSM Config 管理您的 Windows 实例的配置，请完成以下任务。

向 IAM 用户授予对 SSM Config 的访问权限

由于 EC2Config 服务在本地系统账户中运行，因此 SSM 文档通过 Windows 实例上的管理权限运行。如果用户有权执行任何预定义的 SSM 文档，则该用户也具有实例的管理员访问权。合理地委派对 SSM Config 和 EC2 Run Command 的访问权限。如果您创建自己的 SSM 文档，这一点会变得非常重要。Amazon Web Services 不提供有关如何创建安全 SSM 文档的指导。您自行承担创建 SSM 文档和委派对 Run Command 操作的访问权限的风险。作为最佳安全做法，建议您为安全性较低的任务创建低级别 SSM 文档，并向非管理员委派访问权限。

准备实例

SSM Config 和 Run Command 具有相同的限制、先决条件和 IAM 权限要求。准备您的环境，如 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#) 中所述。

创建 JSON 文件

打开文本编辑器，添加 JSON 以描述配置，然后以 .json 为文件扩展名保存该文件。

有关 SSM 文档的 JSON 结构的更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 中的 [SSM 文档](#)。

示例：安装应用程序

以下 JSON 描述了要安装在实例上的应用程序。对于每个应用程序，source 是其 .msi 文件的 URL。

```
{  
  "schemaVersion": "1.0",  
  "description": "Example instance configuration tasks",  
  "runtimeConfig": {  
    "aws:applications": {  
      "properties": [  
        {  
          "name": "My Application",  
          "source": "http://example.com/app.msi"  
        }  
      ]  
    }  
  }  
}
```

```
        "action": "Install",
        "source": "http://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-
installer-community-5.6.22.0.msi"
    },
    {
        "action": "Install",
        "source": "https://www.python.org/ftp/python/2.7.9/python-2.7.9.msi"

    },
    {
        "action": "Install",
        "source": "http://download.winzip.com/winzip190-64.msi",
        "parameters": "INSTALLDIR=\"C:\\Program Files\\WinZipXX\""
    }
]
}
}
```

示例：安装 PowerShell 模块并运行命令

以下 JSON 描述了要安装在您的实例上的 PowerShell 模块。对于每个模块，`source` 是该模块的 URL，且 `runCommand` 指定要运行的 PowerShell 命令。

```
{
    "schemaVersion": "1.0",
    "description": "Example instance configuration tasks",
    "runtimeConfig": {
        "aws:psModule": {
            "properties": [
                {
                    "description": "Example to install windows update PS module and install
all .NET 4 updates.",
                    "source": "https://gallery.technet.microsoft.com/scriptcenter/2d191bcd-
3308-4edd-9de2-88dff796b0bc/file/41459/43/PSWindowsUpdate.zip",
                    "runCommand": "Get-WUInstall -ServiceID 9482f4b4-e343-43b6-b170-
9a65bc822c77 -Title \".NET Framework 4\" -AcceptAll"
                },
                {
                    "description": "Example to install chocolatey package provider and
use it to install 7zip and GoogleChrome.",
                    "runCommand": [
                        "$url = 'https://chocolatey.org/install.ps1'",
                        "iex ((new-object net.webclient).DownloadString($url))",
                        "choco install -y 7zip",
                        "choco install -y GoogleChrome"
                    ]
                }
            ]
        }
    }
}
```

示例：加入 AWS 域

有关使用 SSM Config 将 Windows 实例加入目录的信息，请参阅[将 Windows 实例加入 AWS Directory Service 域 \(p. 299\)](#)。

示例：将数据发送到 Amazon CloudWatch

有关使用 SSM Config 将数据发送到 Amazon CloudWatch 的信息，请参阅 [使用 Amazon EC2 Simple Systems Manager 将性能计数器发送到 CloudWatch，将日志发送到 CloudWatch Logs \(p. 308\)](#)。

创建 SSM 文档

使用 AWS CLI 或 Windows PowerShell 工具 创建配置文档，同时指定您在上一任务中创建的 JSON 文件。

AWS CLI

使用下面的 [create-document](#) 命令可为此配置命名并使其可用。

```
aws ssm create-document --content file://my-config.json --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [New-SSMDocument](#) 命令可为此配置命名并使其可用。

```
$doc = Get-Content my-config.json | Out-String  
New-SSMDocument -Content $doc -Name "my-custom-config"
```

将 SSM 文档与实例关联

使用 AWS CLI 或 Windows PowerShell 工具可将配置文档与实例关联。您需要指定在上一任务中创建的配置文档的名称。一个实例一次只能与一个配置文档关联。如果将一个配置文档与一个已有关联配置文档的实例关联，新配置文档会替换现有配置文档。

AWS CLI

使用下面的 [create-association](#) 命令可将您的配置文档与 Windows 实例关联。

```
aws ssm create-association --instance-id i-1a2b3c4d --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [New-SSMAssociation](#) 命令可将您的配置文档与 Windows 实例关联。

```
New-SSMAssociation -InstanceId i-1a2b3c4d -Name "my-custom-config"
```

手动应用配置

如果需要确保实例按其当前 SSM 文档中的指定内容进行配置，可在实例上运行 `ec2config-cli` 工具，如下所示：

```
ec2config-cli --apply-configuration
```

或者，您可以使用 Windows 任务计划程序定期运行 `ec2config-cli`，以确保实例保持该配置。

通过在 `C:\Program Files\Amazon\Ec2ConfigService` 目录中查找 `ec2config-cli`，可以确认是否已安装该工具。如果没有 `ec2config-cli`，通过安装最新版本的 EC2Config 服务，您就可以获得它。有关更多信息，请参阅 [安装最新版的 EC2Config \(p. 258\)](#)。

解除 SSM 文档与实例的关联

配置文档在创建后不能更新。要将不同配置文档与您的实例关联，可以删除现有关联，然后将新配置文档与实例关联。请注意，终止实例不会自动解除关联配置文档的关联。

AWS CLI

使用下面的 [delete-association](#) 命令可解除配置文档与 Windows 实例的关联。

```
aws ssm delete-association --instance-id i-1a2b3c4d --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [Remove-SSMAssociation](#) 命令可解除配置文档与 Windows 实例的关联。

```
Remove-SSMAssociation -InstanceId i-1a2b3c4d -Name "my-custom-config"
```

删除 SSM 文档

用完配置文档后可以将其删除。要删除配置文档，必须先解除配置文档与所关联的任意实例的关联。

AWS CLI

使用下面的 [delete-document](#) 命令可删除您的配置文档。

```
aws ssm delete-document --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [Remove-SSMDocument](#) 命令可删除您的配置文档。

```
Remove-SSMDocument -Name "my-custom-config"
```

故障排除

本节包括可帮助您排查 SSM Config 问题的信息。

Log4net 日志记录

EC2Config 服务使用 Apache log4net 将信息记录在以下文件中。这些文件中的信息可帮助您排查问题。

- C:\Windows\System32\winevt\Logs\EC2ConfigService.evtx
- C:\Program Files\Amazon\Ec2ConfigService\Logs
- LocalSystem %LOCALAPPDATA%
- Windows Server 2008 或更高版本

C:\Windows\System32\config\systemprofile\AppData\Local\Amazon\Ec2Config\Logs\Ec2ConfigPluginFramework.txt
• Windows Server 2003

C:\Documents and Settings\Default User\Local
Settings\Amazon\Ec2Config\InstanceData\Logs\Ec2ConfigPluginFramework.txt

您可通过更新 log4net.config 文件来启用延长日志记录。默认情况下，配置文件位于以下位置：

C:\Program Files\Amazon\Ec2ConfigService\log4net.config

有关 log4net 配置的更多信息，请参阅 [Apache log4net 手册 - 配置](#)。有关 log4net 配置的示例，请参阅 [Apache log4net 配置示例](#)。

Windows 事件日志

EC2Config 服务还会在名为 *Ec2ConfigService* 的 Windows 事件日志中记录信息。

您可通过从提升的 PowerShell 提示符下执行以下命令来将此事件日志中的信息提取到日志文件：

```
Get-EventLog Ec2ConfigService | Sort-Object Index | Format-Table Message  
-AutoSize -Wrap | Out-File -Width 240 "C:\Program  
Files\Amazon\Ec2ConfigService\Logs\PluginFramework.txt"
```

如果要在启用调试的情况下将 Windows 事件记录到日志文件，您必须更新 log4net.config 文件根元素，如下所示：`<root> <level value="DEBUG"/> <appender-ref ref="RollingFileAppender"/>
<appender-ref ref="EventLogAppender"/> </root>`

EC2 控制台系统日志

EC2 控制台系统日志中的以下输出表示 EC2Config 服务无法连接到 SSM Config 终端节点。这些问题指明了与授权和 IAM 角色权限相关的问题，如以下输出消息中所指出：

```
Info: EC2Config configuration status:3;region:us-east-1;iam:0;authz:0 The  
output can  
    help you troubleshoot the cause of the failure: configuration status:3: The  
    calls to (SSM)  
        failed. Ensure that you have granted the required IAM permissions to IAM  
    users. (SSM) also  
        requires an Internet connection from your instance.
```

```
iam:0: The instance was not launched with an IAM role. You cannot download  
documents  
    if there is no IAM role/credentials associated with the instance.
```

```
authz:0: The instance is not authorized to access SSM. This happens if you  
launched  
    the instance without an IAM role, or if the role associated with your instance  
does not  
    have the necessary permissions to access the service.
```

您可以通过使用 [describe-association](#) (AWS CLI) 命令或 [Get-SSMAssociation](#) (适用于 Windows PowerShell 的工具) 命令检查关联的状态，从而找到 SSM 文档执行失败的具体原因。

将 Windows 实例加入 AWS Directory Service 域

Abstract

将您的实例加入 AWS Directory Service 目录。

您可以使用 Amazon EC2 Simple Systems Manager (SSM) Config 将 Amazon EC2 Windows 实例加入活动的 AWS Directory Service 目录或 AD Connector 目录。要使用 SSM Config 执行此任务，可使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具创建一个指定域加入详细信息的 SSM 文档，然后将该 SSM 文档与正在运行的实例关联。

或者，可以使用 Amazon EC2 控制台中的启动实例向导来启动实例并指定要加入的域。该向导会在您的账户中搜索域的任何现有 SSM 文档以便与实例关联；如果找不到这样一个文档，则它会为您创建一个 SSM 文档，然后立即将它与正在运行的实例关联。

将 SSM 文档与实例关联之后，可以使用在 AWS Directory Service 目录中定义的域凭证连接到实例。

对于使用 SSM Config 或将实例加入域，没有额外费用。对于实例和 AWS Directory Service 的使用，适用标准费率。

有关 SSM Config 的更多信息，请参阅[管理 Windows 实例配置 \(p. 294\)](#)。

内容

- [限制 \(p. 300\)](#)
- [先决条件 \(p. 300\)](#)
- [使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具 加入域 \(p. 301\)](#)
- [使用 Amazon EC2 启动向导加入域 \(p. 304\)](#)
- [获取域加入状态 \(p. 304\)](#)
- [使用域证书连接到实例 \(p. 305\)](#)
- [故障排除 \(p. 306\)](#)
- [查看有关您的关联的信息 \(p. 307\)](#)
- [更改关联 \(p. 307\)](#)
- [删除 SSM 文档 \(p. 307\)](#)

限制

- 仅 Windows 实例支持 SSM Config。
- 在以下[区域](#)提供 SSM Config。

在其他区域，您可以手动将实例连接到域。有关更多信息，请参阅 *AWS Directory Service Administration Guide* 中的[将实例连接到 AWS Directory Service 目录](#)。

先决条件

- 要加入域，请确保您在 AWS 账户中提供或配置了以下资源：
 - 活动 AWS Directory Service 目录。有关创建目录的更多信息，请参阅 *AWS Directory Service Administration Guide* 中的[AWS Directory Service 入门](#)。
 - 要创建目录，您必须有一个包含两个子网的 VPC。有关创建 VPC 的更多信息，请参阅 [Amazon VPC 是什么？\(Amazon VPC 用户指南中\)](#)。您加入到域的实例必须在域所处的同一 VPC 中启动。
 - 符合[准备实例 \(p. 295\)](#)所述要求的 Windows 实例。
 - 供实例与 SSM Config 通信所用的 Internet 连接。请确保您有在其中启动实例的公有子网，并确保您的实例具有公有 IP 地址。此外，您还可以在私有子网中启动实例而不向它分配公有 IP 地址，并使用公有子网中的 NAT 实例发起到 Internet 的流量。有关 NAT 的更多信息，请参阅 [Amazon VPC 用户指南](#) 中的[NAT 实例](#)。
- 如果使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具 创建配置文档，则需要以下信息：
 - 要加入的目录的名称和 ID。
 - AWS Directory Service 目录中的 DNS 服务器的 IP 地址。有关更多信息，请参阅 *AWS Directory Service Administration Guide* 中的[获取 DNS 服务器地址](#)。

使用 SSM 托管策略

SSM 的 IAM 托管策略可帮助您为用户和实例快速配置访问权限和其他权限。可通过搜索 SSM 在 IAM 控制台中查找这些策略，如以下屏幕截图所示。



托管策略执行以下功能：

- **AmazonEC2RoleForSSM**（实例信任策略）：此策略使实例能够与 SSM Config API 进行通信。
- **AmazonSSMFulAccess**（用户信任策略）：此策略向用户授予对 SSM Config API 和 SSM 文档的访问权限。将此策略分配给管理员和可信高级用户。
- **AmazonSSMReadOnlyAccess**（用户信任策略）：此策略向用户授予对只读 API 操作（例如 Get 和 List）的访问权限。



Note

在您创建实例时，您必须在启动向导中分配实例角色。在您创建实例后则不能分配角色。向现有实例分配角色：

1. 从现有实例创建 AMI。
2. 从该 AMI 启动新实例。
3. 在创建新实例时，请在启动向导中分配实例角色。

有关如何配置这些策略的信息，请参阅[托管策略和内联策略](#)。

使用 AWS CLI 或 适用于 Windows PowerShell 的 AWS 工具 加入域

要使用 AWS CLI 或 适用于 Windows PowerShell 的 AWS 工具 加入域，您必须创建配置文档，然后将该 SSM 文档与已在运行的实例关联。

要构建 SSM 文档，请使用您选择的文本编辑器，然后使用 *.json 扩展名保存文件。有关 SSM 文档的结构的更多信息，请参阅 *Amazon EC2 Simple Systems Manager API Reference* 中的 [SSM 文档](#)。

由于 EC2Config 服务在本地系统账户中运行，因此 SSM 文档通过 Windows 实例上的管理权限运行。如果用户有权执行任何预定义的 SSM 文档，则该用户也具有实例的管理员访问权。合理地委派对 SSM Config 和 Run Command 的访问权限。如果您创建自己的 SSM 文档，这一点会变得非常重要。Amazon Web Services 不提供有关如何创建安全 SSM 文档的指导。您自行承担创建 SSM 文档和委派对 Run Command 操作的访问权限的风险。作为最佳安全做法，建议您为安全性较低的任务创建低级别 SSM 文档，并向非管理员委派访问权限。

使用以下 AWS CLI 或 适用于 Windows PowerShell 的 AWS 工具 命令创建 SSM 文档，启动实例，然后将该文件与实例关联。

操作	AWS CLI	适用于 Windows PowerShell 的 AWS 工具
在账户中创建 SSM 文档。	<code>create-document</code>	<code>New-SSMDocument</code>

操作	AWS CLI	适用于 Windows PowerShell 的 AWS 工具
启动实例。您也可以将现有实例加入域，前提是它满足先决条件。有关更多信息，请参阅 先决条件 (p. 300) 。	run-instances	New-EC2Instance
将 SSM 文档与实例关联。	create-association	New-SSMAssociation

使用 AWS CLI 或 适用于 Windows PowerShell 的 AWS 工具 加入域

- 在计算机上打开一个文本编辑器，然后编写 SSM 文档。完成后，使用 .json 扩展名保存文件。下面是允许实例加入域 d-1234567890 的 SSM 文档示例：

```
{  
    "schemaVersion": "1.0",  
    "description": "Sample configuration to join an instance to a domain",  
    "runtimeConfig": {  
        "aws:domainJoin": {  
            "properties": {  
                "directoryId": "d-1234567890",  
                "directoryName": "test.example.com",  
                "dnsIpAddresses": [  
                    "198.51.100.1",  
                    "198.51.100.2"  
                ]  
            }  
        }  
    }  
}
```



Note

如果有效的组织部门 (OU) 存在，您也可以指定以下内容：

```
{  
    "schemaVersion": "1.0",  
    "description": "Sample configuration to join an instance to a do  
main",  
    "runtimeConfig": {  
        "aws:domainJoin": {  
            "properties": {  
                "directoryId": "d-1234567890",  
                "directoryName": "test.example.com",  
                "directoryOU": "OU=Computers,OU=example,DC=test,DC=ex  
ample,DC=com",  
                "dnsIpAddresses": [  
                    "198.51.100.1",  
                    "198.51.100.2"  
                ]  
            }  
        }  
    }  
}
```

}

- 在账户中创建 SSM 文档，然后为其指定名称。文件名长度必须在 1 到 64 个字符之间。

AWS CLI

```
aws ssm create-document --content file://path/to/myconfigfile.json --name "My_Custom_Config_File"
```

Windows PowerShell 工具

首先创建一个包含文件内容的变量，然后创建文档。

```
$doc = Get-Content C:\temp\myconfigfile.json | Out-String  
New-SSMDocument -Content $doc -Name "My_Custom_Config_File"
```

- 在域 (d-1234567890) 所处的同一 VPC 中启动一个 EC2 实例。必须向该实例分配 IAM 角色。还必须确保该实例具有公有 IP 地址，除非使用 NAT 实例进行 Internet 通信。记下输出中的实例 ID。

AWS CLI

```
aws ec2 run-instances --image-id ami-1a2b3c4d --subnet-id subnet-33cc44dd  
--key-name my-key-pair --instance-type m1.large --iam-profile MyInstanceProfile  
--associate-public-ip-address  
  
{  
    "OwnerId": "123456789101",  
    "ReservationId": "r-bbaall22",  
    "Groups": [  
        {  
            "GroupName": "default",  
            "GroupId": "sg-5c5c5c5c"  
        }  
    ],  
    "Instances": [  
        ...  
        {"InstanceId": "i-1234567890abcdef0"},  
        ...  
    ]  
}
```

Windows PowerShell 工具

```
New-EC2Instance -ImageId ami-1a2b3c4d -SubnetId subnet-33cc44dd -KeyName  
my-key-pair -InstanceType m1.large -InstanceProfile_Id MyInstanceProfile  
-associatePublicIp $true
```

- 将 SSM 文档与正在运行的实例关联。

AWS CLI

```
aws ssm create-association --instance-id i-1234567890abcdef0 --name  
"My_Custom_Config_File"
```

Windows PowerShell 工具

```
New-SSMAssociation -InstanceId i-1234567890abcdef0 -Name "My_Custom_Con  
fig_File"
```

5. 检查域加入的状态。有关更多信息，请参阅 [获取域加入状态 \(p. 304\)](#)。

使用 Amazon EC2 启动向导加入域

可以使用 Amazon EC2 控制台中的启动实例向导将新实例加入指定的域。如果您还没有配置文档，该向导会为您创建 SSM 文档，然后将它与新实例关联。



Note

您不能使用 Amazon EC2 控制台将 SSM 文档与现有实例关联。

使用启动向导加入域

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在 Amazon EC2 控制台中，单击 Launch Instance。
3. 在向导的第一页，选择一个 Windows AMI。在下一页上，选择实例类型，然后单击 Next: Configure Instance Details。
4. 在 Step 3: Configure Instance Details 页上，从 Network 列表中选择一个 VPC，然后从 Subnet 列表中选择一个子网。应确保选择 AWS Directory Service 域所处的 VPC。
5. 在 Auto-assign Public IP 列表中，选择 Enable（如果子网设置未默认设置为启用）。



Note

如果您在私有子网中启动实例并使用公有子网中的 NAT 实例进行 Internet 通信，则不必向实例分配公有 IP 地址。

6. 从 Domain join directory 列表中选择域，然后从 IAM role 列表中选择要与实例关联的 IAM 角色。
7. 根据需要完成其余配置步骤，然后单击 Next，直到到达 Step 6: Configure Security Group 页。确保选择或创建的安全组包含一个规则，该规则允许从您的 IP 地址或从网络中某个 IP 地址范围进行 RDP 访问。有关安全组规则的更多信息，请参阅 [为您的 Windows 实例授权入站流量 \(p. 570\)](#)。
8. 单击 Review and Launch 以启动实例。
9. 检查域加入的状态。有关更多信息，请参阅 [获取域加入状态 \(p. 304\)](#)。

获取域加入状态

您可以通过查看实例的系统日志，或者通过检查关联的状态来检查域加入的状态。



Note

将配置文件与实例关联之后，可能需要几分钟使实例加入域。

可以使用 Amazon EC2 控制台、AWS CLI 或 Windows PowerShell 工具 检查实例的系统日志。

使用控制台获取系统日志

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 Instances。
3. 选择实例，右键单击，选择 Instance Settings，然后单击 Get System Log。

使用命令行工具获取系统日志

- 使用 [get-console-output](#) (AWS CLI) 命令；例如：

```
aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

- 使用 [Get-EC2ConsoleOutput](#) (适用于 Windows PowerShell 的 AWS 工具) 命令；例如：

```
Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0
```

在系统日志中，以下输出指示域加入已成功：

```
2015/02/02 10:59:36Z: Info: EC2Config configuration status:2;region:us-east-1;iam:1;authz:1
2015/02/02 10:59:42Z: Info: EC2Config: Downloading config awsconfig_Domain_d-1234567890_corp.example.com
2015/02/02 10:59:45Z: Info: EC2Config: The instance is joining domain with id:d-1234567890, name:corp.example.com ...
2015/02/02 10:59:48Z: Info: EC2Config: The instance successfully joined the domain.
2015/02/02 10:59:48Z: Info: EC2Config: The instance will reboot shortly for domain join to take effect.
```

或者，也可以使用 AWS CLI 或 Windows PowerShell 工具 检查配置文档与实例之间的关联状态。

检查关联的状态

- 使用 [describe-association](#) (AWS CLI) 命令；例如：

```
aws ssm describe-association --name "My_Custom_Config_File" --instance-id i-1234567890abcdef0
```

- 使用 [Get-SSMAssociation](#) (Windows PowerShell 工具) 命令；例如：

```
Get-SSMAssociation -Name "My_Custom_Config_File" -InstanceId i-1234567890abcdef0
```

使用域证书连接到实例

将实例加入域之后，可以使用您在 AWS Directory Service 中定义的域证书连接到实例。

使用目录证书以管理员身份连接到实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 Instances，选择您的实例，然后单击 Connect。
3. 在对话框中，单击 Download Remote Desktop File，然后使用 RDP 客户端打开文件。
4. 在登录屏幕上，按如下所示输入详细信息（而不是使用从密钥对文件生成的本地计算机名称和密码）：
 - User name：输入完全限定的域名，后跟反斜杠，然后是用户名（在此例中为 Admin）；例如：corp.example.com\Admin。
 - Password：输入在创建域时指定的密码。

有关连接到实例的更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。

确认您可以作为管理员连接到实例之后，您域中的用户可以使用相同过程连接到实例（将 Admin 证书替换为他们自己的用户名和密码）。

故障排除

如果您在将实例加入域时遇到问题，或者，如果您在使用域证书连接到实例时遇到问题，请首先通过检查实例的系统日志，或者通过检查关联的状态来验证域加入的状态：[获取域加入状态 \(p. 304\)](#)。

无法连接到实例

如果域加入成功，但是您在登录实例时遇到问题，请尝试以下操作：

- 如果您可以连接到实例，但无法登录，请检查您使用的用户名和密码是否正确。用户名必须包含完全限定的域名（例如，corp.example.com），并且密码必须是域中配置的密码（而不是密钥对文件生成的密码）。
- 如果您无法连接到实例，请检查您的安全组设置。您必须具有允许从您的 IP 地址或网络进行 RDP 访问的规则。

域加入未成功

在系统日志中，以下输出指示 EC2Config 服务未能连接并下载关联 SSM 文档，因此域加入未成功：

```
Info: EC2Config configuration status:3;region:us-east-1;iam:0;authz:0
```

该输出可以帮助您排查失败的原因：

- configuration status:3：对 SSM Config 进行的调用失败。请确保您向 IAM 用户授予了所需的 IAM 权限。SSM Config 还需要从实例进行的 Internet 连接 - 实例必须具有公有 IP 地址，并且必须在公有子网中启动。有关公有子网的更多信息，请参阅 Amazon VPC 用户指南中的[带子网的 VPC](#)。
- iam:0：实例未使用 IAM 角色启动。如果没有与实例关联的 IAM 角色，则无法将实例加入域。
- authz:0：未授权实例访问 SSM Config。如果启动的实例没有 IAM 角色，或者，如果与实例关联的角色没有访问服务所需的权限，则会发生这种情况。

还可以使用 [describe-association \(AWS CLI\)](#) 命令或 [Get-SSMAssociation \(Windows PowerShell 工具\)](#) 命令检查关联的状态，从而排查域加入失败的特定原因。例如，以下输出指示与实例关联的 IAM 角色无权使用 ds>CreateComputer 操作：

```
Name : My_Config_Doc
InstanceId : i-1234567890abcdef0
Date : 2/10/2015 1:31:45 AM
Status.Name : Failed
Status.Date : 2/10/2015 1:38:38 AM
Status.Message : RunId=631148a7-894f-4684-8718-ee4cexample, status:Failed,
code:0,
message:RuntimeStatusCounts=[Failed=1],
RuntimeStatus=[aws:domainJoin={Failed,User:
arn:aws:sts::123456789101:assumed-role/NoDomainJoinPermission/i-1234567890abcdef0 is not authorized to
perform: ds>CreateComputer}]
Status.AdditionalInfo : {agent=EC2Config,ver=x.x.xx,osver=6.2.9200,os=Windows
Server 2012 Standard,lang=en-US}
```

查看有关您的关联的信息

您可以使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具 查看有关您的关联和 SSM 文档的信息。

操作	AWS CLI	适用于 Windows PowerShell 的 AWS 工具
查看有关特定实例和 SSM 文档的关联的信息。还可以使用此命令查看关联的状态。	describe-association	Get-SSMAssociation
查看有关指定 SSM 文档的信息。还可以使用此命令查看 SSM 文档的状态，例如 creating。	describe-document	Get-SSMDocumentDescription
查看指定 SSM 文档的内容。	get-document	Get-SSMDocument
查看指定 SSM 文档或指定实例的关联的列表。	list-associations	Get-SSMAssociationList
查看您的 SSM 文档的列表。	list-documents	Get-SSMDocumentList

更改关联

SSM 文档在创建后不能更新。如果要将实例加入新域，则必须先删除关联，然后使用新 SSM 文档创建新关联。配置更改可能最多需要 15 分钟才能生效。

有关删除关联的更多信息，请参阅[解除 SSM 文档与实例的关联 \(p. 298\)](#)。有关将新文档与实例关联的更多信息，请参阅[将 SSM 文档与实例关联 \(p. 297\)](#)。

删除关联不会更改实例上的配置。实例仍然会加入域，直到您通过修改实例的网络连接配置信息和系统属性手动从域中删除该实例。

删除 SSM 文档

如果您不再需要某一 SSM 文档，则可将其删除。必须先解除该文件与所关联的任意实例的关联，然后才能删除该文件。有关删除 SSM 文档的更多信息，请参阅[删除 SSM 文档 \(p. 298\)](#)。

使用 Amazon EC2 Simple Systems Manager 将性能计数器发送到 CloudWatch，将日志发送到 CloudWatch Logs

您可以使用 Amazon EC2 Simple Systems Manager (SSM) Config 配置与多个实例上的 Amazon CloudWatch 和 Amazon CloudWatch Logs 的集成以监控其日志文件。您可以将应用程序、系统、安全和事件跟踪 (Windows) 日志中的 Windows Server 消息发送到 Amazon CloudWatch Logs。在首次启用日志记录时，SSM Config 会发送从您开始上传该应用程序、系统、安全和 ETW 日志时起 1 分钟内生成的所有日志。其中不包括在此时间之前产生的日志。如果您禁用日志记录并在以后再次启用日志记录，那么 SSM Config 会从其上次停止时的位置继续发送日志。对于任何自定义日志文件和 Internet Information Services (IIS) 日志，SSM Config 会从头读取日志文件。此外，SSM Config 还可以将性能计数器数据发送到 CloudWatch。

利用 SSM Config，您可以管理运行中的 Windows 实例的配置。您可以创建描述配置任务（例如，将性能计数器发送到 CloudWatch 并将日志发送到 CloudWatch Logs）的配置文档，然后将该配置文档与一个或多个运行中的 Windows 实例关联。实例上的配置代理负责处理配置文档并按指定方式配置实例。



Important

由于 EC2Config 服务在本地系统账户中运行，因此 SSM 文档通过 Windows 实例上的管理权限运行。如果用户有权执行任何预定义的 SSM 文档，则该用户也具有实例的管理员访问权。合理地委派对 SSM Config 和 EC2 Run Command 的访问权限。如果您创建自己的 SSM 文档，这一点会变得非常重要。Amazon Web Services 不提供有关如何创建安全 SSM 文档的指导。您自行承担创建 SSM 文档和委派对 Run Command 操作的访问权限的风险。作为最佳安全做法，建议您为安全性较低的任务创建低级别 SSM 文档，并向非管理员委派访问权限。

如果您先前在 EC2Config 中启用了 CloudWatch 集成，则 SSM Config 设置会覆盖实例本地在 C:\Program Files\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json 文件中存储的任何设置。有关使用 EC2Config 管理单个实例上的性能计数器和日志的更多信息，请参阅[使用 EC2Config 将性能计数器发送至 CloudWatch，并将日志发送至 CloudWatch Logs。（p. 260）](#)。

要使用 SSM Config 管理您的 Windows 实例的配置，请完成以下任务。

任务

- [步骤 1：准备您的环境（p. 308）](#)
- [步骤 2：创建 JSON 文件（p. 308）](#)
- [步骤 3：配置 CloudWatch 和 CloudWatch Logs 的区域和命名空间（p. 311）](#)
- [步骤 4：配置发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志（p. 312）](#)
- [步骤 5：配置流程控制（p. 318）](#)
- [步骤 6：创建配置文档（p. 319）](#)
- [步骤 7：将配置文档与实例关联（p. 319）](#)

步骤 1：准备您的环境

SSM Config 和 Run Command 具有相同的限制、先决条件和 IAM 权限要求。准备您的环境，如[Amazon EC2 Run Command 先决条件（p. 333）](#)中所述。

步骤 2：创建 JSON 文件

如果您还没有 JSON 文件，则必须创建一个。打开文本编辑器，添加 JSON 以描述配置，然后以 .json 为文件扩展名保存该文件。

有关配置文档的 JSON 结构的更多信息，请参阅 *Amazon EC2 Simple Systems Manager API Reference* 中的[配置文档](#)。

在使用 SSM Config 时，只能为您的实例关联一个 JSON 文件。无论您是创建新的 JSON 文件还是已有一个与您的实例关联的 JSON 文件，都需要将以下部分添加到该文件。

```
{  
    "schemaVersion": "1.0",  
    "description": "Example CloudWatch Logs tasks",  
    "runtimeConfig": {  
        "aws:cloudWatch": {  
            "properties": {  
                "EngineConfiguration": {  
                    "PollInterval": "00:00:15",  
                    "Components": [  
                        {  
                            "Id": "ApplicationEventLog",  
                            "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogIn  
putComponent,AWS.EC2.Windows.CloudWatch",  
                            "Parameters": {  
                                "LogName": "Application",  
                                "Levels": "value"  
                            }  
                        },  
                        {  
                            "Id": "SystemEventLog",  
                            "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogIn  
putComponent,AWS.EC2.Windows.CloudWatch",  
                            "Parameters": {  
                                "LogName": "System",  
                                "Levels": "value"  
                            }  
                        },  
                        {  
                            "Id": "SecurityEventLog",  
                            "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogIn  
putComponent,AWS.EC2.Windows.CloudWatch",  
                            "Parameters": {  
                                "LogName": "Security",  
                                "Levels": "value"  
                            }  
                        },  
                        {  
                            "Id": "ETW",  
                            "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogIn  
putComponent,AWS.EC2.Windows.CloudWatch",  
                            "Parameters": {  
                                "LogName": "Microsoft-Windows-WinINet/Analytic",  
                                "Levels": "value"  
                            }  
                        },  
                        {  
                            "Id": "IISLogs",  
                            "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLo  
gInputComponent,AWS.EC2.Windows.CloudWatch",  
                            "Parameters": {  
                                "LogDirectoryPath": "path",  
                                "TimestampFormat": "value",  
                                "FileLogFormat": "text",  
                                "FileLogFormatVersion": "1",  
                                "FileLogFormatEncoding": "utf-8",  
                                "FileLogFormatSeparator": "\n",  
                                "FileLogFormatTimeFormat": "yyyy-MM-dd HH:mm:ss",  
                                "FileLogFormatTimeZone": "UTC",  
                                "FileLogFormatLogLevel": "Info",  
                                "FileLogFormatLogType": "All",  
                                "FileLogFormatLogCategory": "All",  
                                "FileLogFormatLogSource": "All",  
                                "FileLogFormatLogMessage": "All",  
                                "FileLogFormatLogFile": "All",  
                                "FileLogFormatLogFileCount": 1,  
                                "FileLogFormatLogFileSize": 10485760,  
                                "FileLogFormatLogFileRetention": 30,  
                                "FileLogFormatLogFileCompression": "None",  
                                "FileLogFormatLogFileCompressSize": 10485760,  
                                "FileLogFormatLogFileCompressTime": 86400,  
                                "FileLogFormatLogFileCompressType": "GZIP",  
                                "FileLogFormatLogFileCompressLevel": 9,  
                                "FileLogFormatLogFileCompressMethod": "Deflate",  
                                "FileLogFormatLogFileCompressType": "GZIP",  
                                "FileLogFormatLogFileCompressLevel": 9,}  
                            }  
                        }  
                    ]  
                }  
            }  
        }  
    }  
}
```

```
        "Encoding": "value",
        "Filter": "value",
        "CultureName": "locale",
        "TimeZoneKind": "value",
        "LineCount": "value"
    }
},
{
    "Id": "CustomLogs",
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLo
gInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogDirectoryPath": "path",
        "TimestampFormat": "value",
        "Encoding": "value",
        "Filter": "value",
        "CultureName": "locale",
        "TimeZoneKind": "value",
        "LineCount": "value"
    }
},
{
    "Id": "PerformanceCounter",
    "FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounter
Component.PerformanceCounterInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "CategoryName": "name",
        "CounterName": "name",
        "InstanceName": "name",
        "MetricName": "name",
        "Unit": "unit",
        "DimensionName": "name",
        "DimensionValue": "value"
    }
},
{
    "Id": "CloudWatchLogs",
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOut
put,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "access-key-id",
        "SecretKey": "secret-access-key",
        "Region": "region",
        "LogGroup": "group",
        "LogStream": "stream"
    }
},
{
    "Id": "CloudWatch",
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.Cloud
WatchOutputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "access-key-id",
        "SecretKey": "secret-access-key",
        "Region": "region",
        "NameSpace": "namespace"
    }
}
```

```
        ],
        "Flows": [
            "Flows": [
                "source,destination",
                "(source1, source2),destination",
                "source, (destination1,destination2)"
            ]
        }
    }
}
```

步骤 3：配置 CloudWatch 和 CloudWatch Logs 的区域和命名空间

下一步，您将定义构成数据发送目标的证书、区域和指标命名空间。

为 CloudWatch 设置证书、区域和指标命名空间

JSON 文件的此部分定义组成数据发送目标的证书、区域和指标命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatch2”、“CloudWatch3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。



Note

如果您使用 EC2Config 并且计划将性能计数器发送到 CloudWatch，则只需设置 CloudWatch 证书。如果您使用 Amazon EC2 Simple Systems Manager，则您的证书是在您启动 Amazon EC2 实例时使用的 IAM 角色中配置的。

1. 在 JSON 文件中，找到 CloudWatch 部分。

```
{
    "Id": "CloudWatch",
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputCom-
    ponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "",
        "SecretKey": "",
        "Region": "us-west-1",
        "NameSpace": "Windows/Default"
    }
},
```

2. 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
3. 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
4. 在 Region 参数中，输入希望将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。虽然可以将性能计数器发送到与日志数据发送目标不同的区域，但是我们建议您将此参数设置为运行实例的区域。
5. 在 NameSpace 参数中，输入要用于在 CloudWatch 中写入性能计数器数据的指标命名空间。

为 CloudWatch Logs 设置证书、区域、日志组和日志流

JSON 文件的此部分定义组成数据发送目标的证书、区域、日志组名称和日志流命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatchLogs2”、“CloudWatchLogs3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。

1. 在 JSON 文件中，找到 CloudWatchLogs 部分。

```
{  
    "Id": "CloudWatchLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "AccessKey": "",  
        "SecretKey": "",  
        "Region": "us-east-1",  
        "LogGroup": "Default-Log-Group",  
        "LogStream": "{instance_id}"  
    }  
},
```

2. 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
3. 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
4. 在 Region 参数中，输入希望 EC2Config 将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。
5. 在 LogGroup 参数中，输入日志组的名称。这是在 CloudWatch 控制台 Log Groups (日志组) 屏幕上显示的名称。
6. 在 LogStream 参数中，输入目标日志流。如果使用 {instance_id} 默认设置，则 EC2Config 将该实例的实例 ID 用作日志流名称。

如果输入不存在的日志流名称，则 CloudWatch Logs 会自动创建该名称。您可以使用文字字符串或预定义的变量（{instance_id}、{hostname}、{ip_address}），或所有这三个变量的组合来定义日志流名称。

此参数中指定的日志流名称会显示在 CloudWatch 控制台中的 Log Groups (日志组) > Streams for *<YourLogStream>* (<YourLogStream> 的流) 屏幕上。

步骤 4：配置发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志

下一步，您将配置要发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志。

配置发送到 CloudWatch 的性能计数器

可以选择性能监视器中提供的任何性能计数器。您可以选择不同类别作为指标上传到 CloudWatch，如 .NET CLR 数据、ASP.NET 应用程序、HTTP 服务、内存或进程和处理器。

对于要上传到 CloudWatch 的每个性能计数器，复制 PerformanceCounter 部分，更改 Id 参数使其唯一（例如“PerformanceCounter2”），然后根据需要更新其他参数。

1. 在 JSON 文件中，找到 PerformanceCounter 部分。

```
{  
    "Id": "PerformanceCounter",  
    "FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.Per  
formanceCounterInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "CategoryName": "Memory",  
        "CounterName": "Available MBytes",  
        "InstanceName": "",  
        "MetricName": "AvailableMemory",  
        "Unit": "Megabytes",  
        "DimensionName": "",  
        "DimensionValue": ""  
    }  
},
```

2. 在 CategoryName 参数中，输入性能计数器类别。
 - a. 要查找可用类别和计数器，请打开性能监视器。
 - b. 单击 Monitoring Tools (监控工具)，然后单击 Performance Monitor (性能监视器)。
 - c. 在结果窗格中，单击绿色 + (加号) 按钮。

类别和计数器会在 Add Counters (添加计数器) 对话框中列出。
3. 在 CounterName 参数中，输入性能计数器的名称。
4. 在 InstanceName 参数中，从性能监视器的 Add Counters 对话框中输入值，可以是下列值之一：
 - 空白，如果所选对象没有实例。
 - 所选对象的单个实例。
 - _Total，将使用所有实例的汇总。



Note

请勿使用星号 (*) 标识所有实例，因为每个性能计数器组件仅支持一个指标。

5. 在 MetricName 参数中，输入希望性能数据所属的 CloudWatch 指标。
6. 在 Unit 参数中，为指标输入合适的度量单位：
秒 | 微秒 | 毫秒 | 字节 | 千字节 | 兆字节 | 千兆字节 | 太兆字节 | 位 | 千位 | 兆位 | 千兆位 | 太兆位 | 百分比 | 计数 | 字节/秒 | 千字节/秒 | 兆字节/秒 | 千兆字节/秒 | 太兆字节/秒 | 位/秒 | 千位/秒 | 兆位/秒 | 千兆位/秒 | 太兆位/秒 | 计数/秒 | 无。
7. (可选) 您可以在 DimensionName 和 DimensionValue 参数中输入维度名称和值以便为指标指定维度。这些参数在列出指标时提供另一个视图。您还可以对多个指标使用同一个维度，以便可以查看属于特定维度的所有指标。

将 Windows 应用程序事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 ApplicationEventLog 部分。

```
{  
    "Id": "ApplicationEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",
```

```
"Parameters": {  
    "LogName": "Application",  
    "Levels": "1"  
}  
,
```

2. 在 **Levels** 参数中，输入以下值之一：

- 1 – 仅上传错误消息。
- 2 – 仅上传警告消息。
- 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将安全日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 **SecurityEventLog** 部分。

```
{  
    "Id": "SecurityEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Security",  
        "Levels": "7"  
    }  
,
```

2. 在 **Levels** 参数中，输入 7，以便上传所有消息。

将系统事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 **SystemEventLog** 部分。

```
{  
    "Id": "SystemEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "System",  
        "Levels": "7"  
    }  
,
```

2. 在 **Levels** 参数中，输入以下值之一：

- 1 – 仅上传错误消息。
- 2 – 仅上传警告消息。
- 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将其他类型的事件日志数据发送到 CloudWatch Logs

除了应用程序、系统和安全日志之外，您还可以上传其他类型的事件类型。

1. 在 JSON 文件中，添加新部分。

```
{  
    "Id": "",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "",  
        "Levels": "7"  
    }  
,
```

2. 在 Id 参数中，为要上传的日志输入名称（例如 WindowsBackup）。
3. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器的导航窗格中，单击 Applications and Services Logs（应用程序和服务日志）。
 - b. 在日志列表中，右键单击要上传的日志（例如“Microsoft>Windows>Backup (备份)>Operational (运行)”），然后单击 Create Custom View（创建自定义视图）。
 - c. 在 Create Custom View（创建自定义视图）对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-Backup）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。
4. 在 Levels 参数中，输入以下值之一：
 - 1 – 仅上传错误消息。
 - 2 – 仅上传警告消息。
 - 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将事件跟踪 (Windows) 数据发送到 CloudWatch Logs

ETW（Windows 事件跟踪）提供了高效且详细的日志记录机制，供应用程序写入日志。每个 ETW 都由可以启动和停止日志记录会话的会话管理器控制。每个会话都具有一个提供者以及一个或多个使用者。

1. 在 JSON 文件中，找到 ETW 部分。

```
{  
    "Id": "ETW",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Microsoft-Windows-WinINet/Analytic",  
    }  
,
```

```
        "Levels": "7"  
    },  
,
```

2. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器中的 View (视图) 菜单上，单击 Show Analytic and Debug Logs (显示分析和调试日志)。
 - b. 在导航窗格中，单击 Applications and Services Logs (应用程序和服务日志)。
 - c. 在 ETW 日志的列表中，右键单击要上传的日志，然后单击 Enable Log (启用日志)。
 - d. 再次右键单击该日志，然后单击 Create Custom View (创建自定义视图)。
 - e. 在 Create Custom View (创建自定义视图) 对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-WinINet/Analytic）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。
3. 在 Levels 参数中，输入以下值之一：
 - 1 – 仅上传错误消息。
 - 2 – 仅上传警告消息。
 - 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将自定义日志（任何基于文本的日志文件）发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 CustomLogs 部分。

```
{  
    "Id": "CustomLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\CustomLogs\\",  
        "TimestampFormat": "MM/dd/yyyy HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "Local",  
        "LineCount": "5"  
    },  
,
```

2. 在 LogDirectoryPath 参数中，输入日志在实例上的存储路径。
3. 在 TimestampFormat 参数中，输入要使用的时间戳格式。有关支持的值的列表，请参阅 MSDN 上的[自定义日期和时间格式字符串](#)主题。



Important

源日志文件必须在每个日志行开头具有时间戳，且时间戳后必须有一个空格。

- 在 Encoding 参数中，输入要使用的文件编码（例如 UTF-8）。有关支持的值的列表，请参阅 MSDN 上的 [Encoding 类主题](#)。



Note

使用编码名称（而不是显示名称）作为此参数的值。

- （可选）在 Filter 参数中，输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表，请参阅 MSDN 上的 [FileSystemWatcherFilter 属性主题](#)。
- （可选）在 CultureName 参数中，输入在其中记录时间戳的区域设置。如果 CultureName 为空，则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表，请参阅 MSDN 上的 [区域语言支持 \(NLS\) API 参考主题](#)。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

- （可选）在 TimeZoneKind 参数中，输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息，则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息，则忽略此参数。
- （可选）在 LineCount 参数中，在标头中输入行数以识别日志文件。例如，IIS 日志文件拥有几乎相同的标头。您可以输入 5，系统会读取日志文件标头的前三行以进行识别。在 IIS 日志文件中，第三行为日期和时间戳，但无法始终保证时间戳在日志文件之间是不同的。为此，建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

将 IIS 日志数据发送到 CloudWatch Logs

- 在 JSON 文件中，找到 IISLog 部分。

```
{  
    "Id": "IISLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\W3SVC1",  
        "TimestampFormat": "yyyy-MM-dd HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "UTC",  
        "LineCount": "5"  
    }  
},
```

- 在 LogDirectoryPath 参数中，输入为单个站点存储 IIS 日志的文件夹（例如 C:\\inetpub\\logs\\LogFiles\\W3SVC_n）。



Note

仅支持 W3C 日志格式。不支持 IIS、NCSA 和自定义格式。

- 在 TimestampFormat 参数中，输入要使用的时间戳格式。有关支持的值的列表，请参阅 MSDN 上的 [自定义日期和时间格式字符串主题](#)。

- 在 Encoding 参数中，输入要使用的文件编码（例如 UTF-8）。有关支持的值的列表，请参阅 MSDN 上的 [Encoding 类主题](#)。



Note

使用编码名称（而不是显示名称）作为此参数的值。

- （可选）在 Filter 参数中，输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表，请参阅 MSDN 上的 [FileSystemWatcherFilter 属性主题](#)。
- （可选）在 CultureName 参数中，输入在其中记录时间戳的区域设置。如果 CultureName 为空，则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表，请参阅 MSDN 上的 [区域语言支持 \(NLS\) API 参考主题](#)。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

- （可选）在 TimeZoneKind 参数中，输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息，则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息，则忽略此参数。
- （可选）在 LineCount 参数中，在标头中输入行数以识别日志文件。例如，IIS 日志文件拥有几乎相同的标头。您可以输入 5，系统会读取日志文件标头的前五行以进行识别。在 IIS 日志文件中，第三行为日期和时间戳，但无法始终保证时间戳在日志文件之间是不同的。为此，建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

步骤 5：配置流程控制

要将性能计数器数据发送到 CloudWatch 或将日志数据发送到 CloudWatch Logs，每种数据类型都必须在 Flows 部分中列出对应目标。例如，要将在 JSON 文件的 "Id": "PerformanceCounter" 部分中定义的性能计数器发送到在 JSON 文件的 "Id": "CloudWatch" 部分定义的 CloudWatch 目标，应在 Flows 部分输入 "PerformanceCounter,CloudWatch"。同样，要将自定义日志、ETW 日志和系统日志发送到 CloudWatch Logs，会输入 "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs"。此外，还可以将相同性能计数器或日志文件发送到多个目标。例如，要将应用程序日志发送到在 JSON 文件的 "Id": "CloudWatchLogs" 部分定义的两个不同目标，应在 Flows 部分输入 "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"。

- 在 JSON 文件中，找到 Flows 部分。

```
"Flows": {  
  "Flows": [  
    "PerformanceCounter,CloudWatch",  
    "(PerformanceCounter,PerformanceCounter2), CloudWatch2",  
    "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs",  
    "CustomLogs, CloudWatchLogs2",  
    "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"  
  ]  
}
```

- 在 Flows 参数中，输入要上传的每种数据类型（例如 ApplicationEventLog）以及要将它发送到的目标（例如 CloudWatchLogs）。

步骤 6：创建配置文档

使用 AWS CLI 或 Windows PowerShell 工具 创建配置文档，同时指定您在上一任务中创建的 JSON 文件。

AWS CLI

使用下面的 [create-document](#) 命令可为此配置命名并使其可用。

```
aws ssm create-document --content file://my-config.json --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [New-SSMDocument](#) 命令可为此配置命名并使其可用。

```
$doc = Get-Content my-config.json | Out-String  
New-SSMDocument -Content $doc -Name "my-custom-config"
```

步骤 7：将配置文档与实例关联

使用 AWS CLI 或 Windows PowerShell 工具可将配置文档与实例关联。您需要指定在上一任务中创建的配置文档的名称。一个实例一次只能与一个配置文档关联。如果将一个配置文档与一个已有关联配置文档的实例关联，新配置文档会替换现有配置文档。

AWS CLI

使用下面的 [create-association](#) 命令可将您的配置文档与 Windows 实例关联。

```
aws ssm create-association --instance-id i-1a2b3c4d --name "my-custom-config"
```

Windows PowerShell 工具

使用下面的 [New-SSMAssociation](#) 命令可将您的配置文档与 Windows 实例关联。

```
New-SSMAssociation -InstanceId i-1a2b3c4d -Name "my-custom-config"
```

要停止向 CloudWatch Logs 发送日志，您可以解除配置文档与实例的关联。有关更多信息，请参阅 [解除 SSM 文档与实例的关联 \(p. 298\)](#)。

在解除配置文档与实例的关联后，您可以将该文档删除。有关更多信息，请参阅 [删除 SSM 文档 \(p. 298\)](#)。

为 VPC 中的 Windows 实例配置辅助私有 IP 地址

Abstract

配置 Windows 实例以识别辅助私有 IP 地址。

在 EC2-VPC 平台上，您可以为实例指定多个私有 IP 地址。将辅助私有 IP 地址分配到 VPC 中的实例后，必须在实例上配置操作系统，以识别辅助私有 IP 地址。

要在 Windows 实例上配置操作系统来识别辅助私有 IP 地址，需要满足以下条件：

- 步骤 1：在您的 Windows 实例上配置静态 IP 寻址 (p. 320)
- 步骤 2：在您的 Windows 实例上配置辅助私有 IP 地址 (p. 321)

- 步骤 3：配置应用程序以使用辅助私有 IP 地址 (p. 322)



Note

以下说明是基于 Windows Server 2008 R2 的。这些步骤的具体实施会因 Windows 实例的操作系统不同而有所差异。

先决条件

在您开始之前，确保您满足以下要求：

- 最佳做法是，使用最新的 AMI 启动 Windows 实例。如果您使用的是较老的 Windows AMI，请确保它引用了 <http://support.microsoft.com/kb/2582281> 中的 Microsoft 快速修复补丁。
- 启动 VPC 中的实例后，请添加辅助私有 IP 地址。有关更多信息，请参阅 [分配辅助私有 IP 地址 \(p. 603\)](#)。
- 要在完成这些步骤中的任务之后允许指向您的网站的 Internet 请求，必须配置弹性 IP 地址并且将其与辅助私有 IP 地址相关联。有关更多信息，请参阅 [将弹性 IP 地址与辅助私有 IP 地址关联 \(p. 605\)](#)。

步骤 1：在您的 Windows 实例上配置静态 IP 寻址

要使 Windows 实例能够使用多个 IP 地址，必须配置实例，使其使用静态 IP 寻址，而不是 DHCP 服务器。



Important

当您在实例上配置静态 IP 寻址时，IP 地址必须与 控制台、CLI 或 API 中显示的地址精确匹配。如果您输入的 IP 地址不正确，实例可能会不可连接。

在 Windows 实例上配置静态 IP 寻址

1. 连接到您的实例。
2. 通过执行以下步骤，查找实例的 IP 地址、子网掩码和默认网关地址：
 - a. 选择 Start。在搜索中键入 cmd 打开命令提示窗口，然后按 Enter。
 - b. 在命令提示行，运行以下命令：ipconfig /all。查看输出中的以下部分，记下网络接口的 IPv4 Address (IPv4 地址)、Subnet Mask (子网掩码)、Default Gateway (默认网关) 和 DNS Servers (DNS 服务器) 值。

```
Ethernet adapter Local Area Connection:  
  
Connection-specific DNS Suffix . :  
Description . . . . . :  
Physical Address . . . . . :  
DHCP Enabled. . . . . :  
Autoconfiguration Enabled . . . . :  
IPv4 Address. . . . . : 10.0.0.131  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.0.1  
DNS Servers . . . . . : 10.1.1.10  
10.1.1.20
```

3. 从命令提示符运行以下命令，打开 Network and Sharing Center (网络和共享中心)：

```
C:\> %SystemRoot%\system32\control.exe ncpa.cpl
```

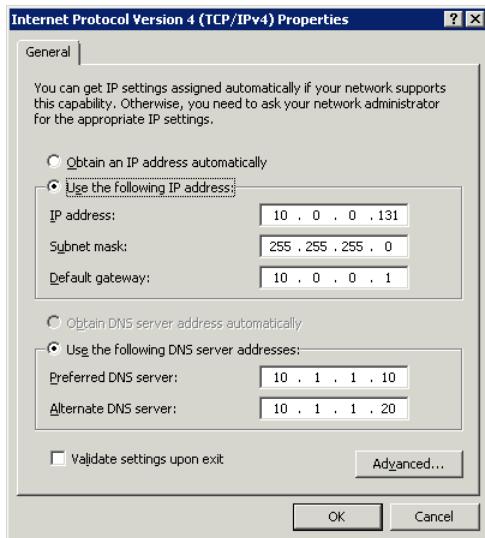
4. 打开网络接口（本地连接）的上下文（右键单击）菜单，选择属性。
5. 依次选择 Internet 协议版本 4 (TCP/IPv4)、属性。
6. 在 Internet 协议版本 4 (TCP/IPv4) 属性对话框中，选择使用下面的 IP 地址，输入以下值，然后选择确定。

字段	值
IP 地址	上面的步骤 2 中包含的 IPv4 地址。
子网掩码	上面的步骤 2 中包含的子网掩码。
默认网关	上面的步骤 2 中包含的默认网关地址。
首选 DNS 服务器	上面的步骤 2 中包含的 DNS 服务器。
备用 DNS 服务器	上面的步骤 2 中包含的备用 DNS 服务器。如果未列出备用 DNS 服务器，请将此字段留为空白。



Important

如果将 IP 地址设置为当前 IP 地址以外的任何值，则会丢失与实例的连接。



当实例从使用 DHCP 转为使用静态寻址时，会短时丢失与 Windows 实例的 RDP 连接。实例会像之前一样保留 IP 地址信息，但是现在，这些信息是静态的，且不受 DHCP 管理。

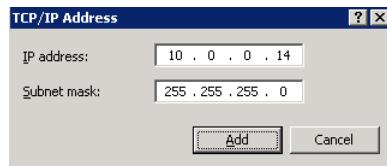
步骤 2：在您的 Windows 实例上配置辅助私有 IP 地址

在 Windows 实例上设置了静态 IP 寻址之后，您便可准备第二个私有 IP 地址。

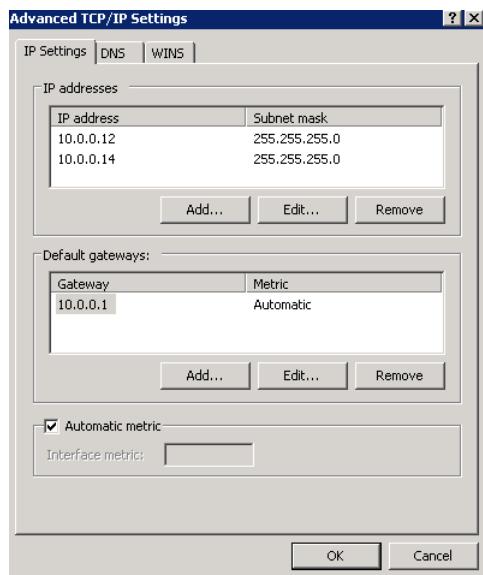
为 Windows 实例配置辅助私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 在 Description (描述) 选项卡上，记下辅助 IP 地址。
4. 连接到您的实例。
5. 在您的 Windows 实例上，选择开始、控制面板。
6. 选择网络和 Internet、网络和共享中心。
7. 选择网络接口 (本地连接)，然后选择属性。
8. 在本地连接属性页面上，选择 Internet 协议版本 4 (TCP/IPv4)、属性、高级。
9. 选择 Add。
10. 在 TCP/IP 地址对话框中，键入辅助私有 IP 地址作为 IP 地址。对于子网掩码，键入与 [步骤 1：在您的 Windows 实例上配置静态 IP 寻址 \(p. 320\)](#) 中为主私有 IP 地址输入的子网掩码，然后选择添加。



11. 验证 IP 地址设置，然后选择确定。



12. 选择确定、关闭。
13. 要确认辅助 IP 地址是否已添加到操作系统，可在命令提示符处运行命令 ipconfig /all。

步骤 3：配置应用程序以使用辅助私有 IP 地址

可配置任何应用程序来使用辅助私有 IP 地址。例如，如果您的实例在 IIS 上运行网站，则可以配置 IIS 使用辅助私有 IP 地址。

要配置 IIS 以使用辅助私有 IP 地址

1. 连接到您的实例。
2. 打开互联网信息服务 (IIS) 管理器。
3. 在“Connections”窗格，展开“Sites”。

4. 打开您网站的上下文（右键单击）菜单，选择编辑绑定。
5. 在网站绑定对话框中，对于类型，选择 http、编辑。
6. 在编辑网站绑定对话框中，对于 IP 地址，选择辅助私有 IP 地址。（在默认情况下，各网站均可接受来自所有 IP 地址的 HTTP 请求。）



7. 选择确定、关闭。

配置辅助弹性网络接口

您可以将另一个弹性网络接口连接到实例；但如果该弹性网络接口位于同一子网中，可能会遇到非对称路由。要解决此问题，您必须为网络接口配置静态路由，并将辅助网络接口的静态路由添加到您的 Windows 实例的本地路由表中。

配置另一个网络接口

1. 按照上面[步骤 1：在您的 Windows 实例上配置静态 IP 寻址 \(p. 320\)](#)中的过程为主弹性网络接口配置静态 IP 寻址。
2. 按照相同的过程为辅助弹性网络接口配置静态 IP 寻址；但在 Internet 协议版本 4 (TCP/IPv4) 属性对话框中不要为默认网关添加值（将此值留空）。
3. 在本地 IP 路由表中为辅助弹性网络接口添加静态路由：
 - a. 打开命令提示符。以管理员身份输入以下命令。在输出中，记下辅助弹性网络接口 ID。

```
netsh interface ipv4 show route
```
 - b. 向路由表添加静态路由。对于 metric 参数，确保值大于主网络接口。

```
route add -p <destination network> mask <subnet mask> gateway <default gateway of primary network interface> metric <metric value> if <interface>
```

4. 禁用主网络接口的源/目标检查。有关更多信息，请参阅[更改弹性网络接口的源/目标检查 \(p. 621\)](#)。



Note

或者，您也可以使用动态路由协议（如路由信息协议 (RIP) 版本 2）向路由表动态添加路由。

有关更多信息，请参阅以下 Microsoft 文章：

- [配置网络上的多个网关](#)

- [添加静态 IP 路由](#)

将 Windows Server EC2 实例升级到新版本 Windows Server

Abstract

将 Windows Server EC2 实例升级到新版本 Windows。

本主题介绍了两种将旧版本的 Windows Server EC2 实例升级到新版本的方法：就地升级和迁移（也称为“并行升级”）。传统上，Microsoft 会建议迁移到而不是升级到新版本的 Windows Server。虽然迁移所产生的升级错误或问题更少，但所需的时间可能多于就地升级所需的时间，因为需要预置新实例、规划和移植应用程序以及调整新实例上的配置设置。就地升级的速度更快，但软件不兼容可能会产生错误。



Note

本主题包含有关升级过程中的一个已知问题的信息，即安装程序会移除部分半虚拟化 (PV) 驱动程序，而这些驱动程序使用户能够使用远程桌面连接到实例。

内容

- [就地升级 \(p. 324\)](#)
- [迁移 \(p. 330\)](#)
- [排查升级问题 \(p. 331\)](#)

就地升级

在对 EC2 Windows Server 实例执行就地升级之前，您必须确定此实例正在运行的 PV 驱动程序。PV 驱动程序使您能够使用远程桌面访问实例。Windows Server 2012 RTM 和 R2 实例都使用 AWS PV 驱动程序。所有其他 Windows Server 实例使用 Citrix PV 驱动程序。有关更多信息，请参阅 [半虚拟化驱动程序 \(p. 272\)](#)。



Important

AWS 利用升级帮助程序服务（一种可帮助您执行涉及 Citrix PV 驱动程序的就地升级的 AWS 实用程序）提供对升级问题的支持。对于操作系统升级或迁移时发生的所有其他问题，我们建议您参阅本文档的准备工作部分中列出的 TechNet 文章。

本节包含以下信息：

- [在您开始之前 \(p. 324\)](#)
- [升级运行 AWS PV 驱动程序的实例 \(p. 325\)](#)
- [升级运行 Citrix PV 驱动程序的实例 \(p. 327\)](#)

在您开始之前

升级之前，请完成以下任务并注意以下重要详细信息。

- 阅读 Microsoft 文档了解更新要求、已知问题和限制。还应参阅有关升级的正式说明。
 - [Upgrading to Windows Server 2008](#)
 - [Upgrading to Windows Server 2008 R2](#)
 - [Upgrading to Windows Server 2012](#)

- [Upgrading to Windows Server 2012 R2](#)

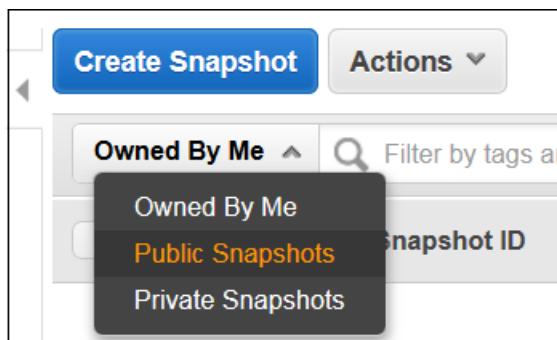
- 我们不建议对 T1 或 T2 实例类型执行系统升级。这些类型的实例可能没有足够的资源来管理升级过程。如果需要升级这些实例之一，则必须将实例大小调整至另一个实例类型，执行升级，再将大小调节回 T1 或 T2 实例类型。有关更多信息，请参阅 [调整您的实例大小 \(p. 133\)](#)。
- 出于备份或测试目的，创建计划升级的系统的 AMI。然后，您可以对副本执行升级以模拟测试环境。如果升级完成，就可以在停机时间很短的情况下将流量切换到此实例。如果升级失败，则可以转至备份。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。
- 确认 Windows 实例上的根卷有足够的可用磁盘空间。Windows 安装过程可能不会发出磁盘空间不足的警告。有关升级特定操作系统所需的磁盘空间的信息，请参阅 Microsoft 文档。如果卷没有足够空间，可将其扩展。有关更多信息，请参阅 [扩展 EBS 卷的存储空间 \(Windows\)](#)。
- 确定升级方法。您必须将操作系统升级到相同架构。例如，必须将 32 位系统升级到 32 位系统。Windows Server 2008 R2 及更高版本是纯粹的 64 位系统。
- 禁用反病毒和反间谍软件和防火墙。这些类型的软件可与升级程序发生冲突。在完成升级后，请重新启用反病毒和反间谍软件以及防火墙。
- 升级帮助程序服务仅支持运行 Citrix PV 驱动程序的实例。如果实例运行的是 Red Hat 驱动程序，则必须在升级前手动[升级](#)这些驱动程序。

升级运行 AWS PV 驱动程序的实例

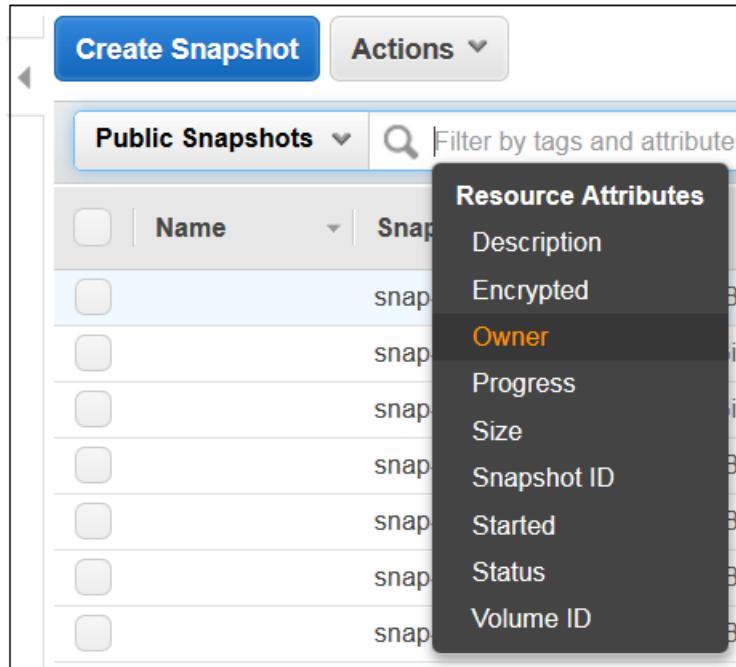
使用以下过程升级 EC2 Windows Server 2012 RTM 或 R2 实例。这些版本的 EC2 Windows 运行 AWS PV 驱动程序并且不需要您在就地升级期间运行 AWS 升级帮助程序服务。

升级运行 AWS PV 驱动程序的 EC2 Windows Server 实例

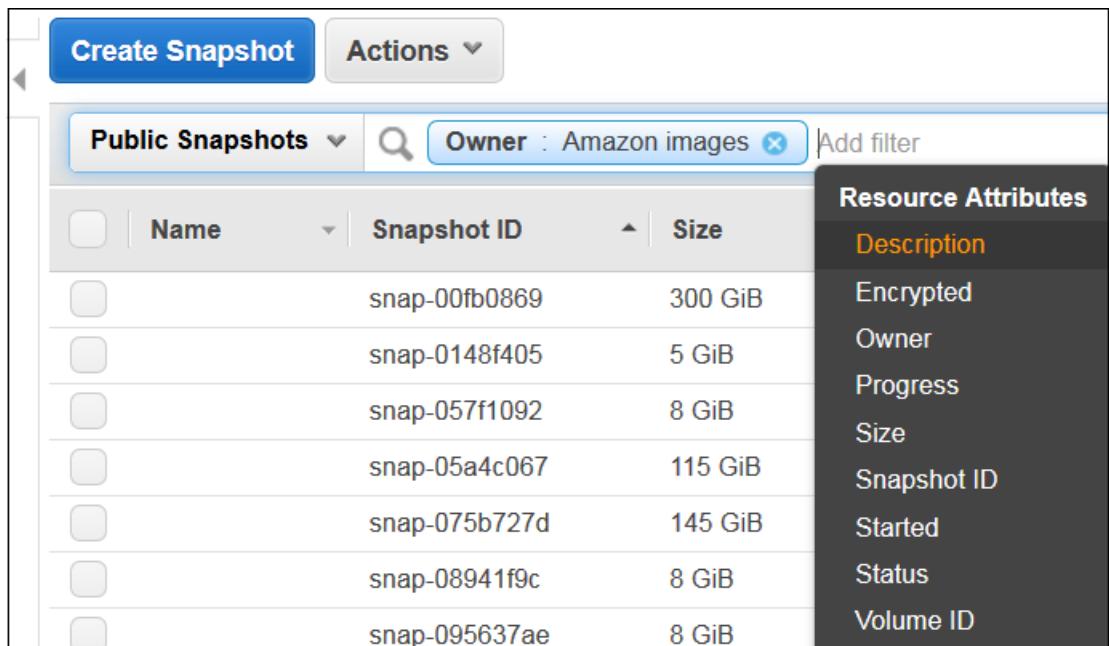
1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择实例，然后找出您想要升级的 Windows Server 的 EC2 实例。记录实例 ID 和可用区。在此过程稍后创建和连接 Windows 安装介质卷时，您要指定这些信息。
3. 从 Windows Server 安装介质快照创建新卷。
 - a. 在 EC2 控制台中，选择 Snapshots。
 - b. 选择 Owned by me，然后选择 Public Snapshots。



- c. 选择搜索 字段，然后从资源属性列表内选择所有者。



- d. 选择 Amazon 图像。
- e. 选择搜索 字段，然后从资源属性列表内选择描述。



- f. 键入 Windows 并按下输入键。
- g. 选择与您的系统架构匹配的快照。例如，如果您的实例当前运行 Windows Server 2012 RTM，则选择 Windows 2012 R2 Installation Media。
- h. 从上下文菜单（右键单击）中，选择创建容量 (Create Volume)。
- i. 在 Create Volume 对话框中，选择与您的 Windows 实例匹配的可用区，然后选择 Create。

4. 在 Volume Successfully Created 消息中，选择刚才创建的卷。
5. 在列表中选择容量，然后从上下文菜单（右键单击）中选择附加容量 (Attach Volume)。
6. 在 Attach Volume 对话框中，键入实例 ID，然后选择 Attach。
7. 通过 Windows 资源管理器打开在此过程前面已连接到实例的安装介质卷，开始升级。
8. 在 Sources 文件夹中，运行 Setup.exe。
9. 在 Select the operating system you want to install 页面上，选择与您的 Windows Server 实例匹配的完整安装 SKU，然后选择 Next。
10. 在 Which type of installation do you want? 页面上，选择 Upgrade。
11. 完成安装向导。

Windows Server 安装程序随后将复制并处理文件。几分钟后，远程桌面会话关闭。升级所用的时间取决于在 Windows Server 实例上运行的应用程序和服务器角色的数量。升级过程少则 40 分钟，多则数小时。在升级过程中，实例无法通过在 EC2 控制台中进行的两项状态检查之一。升级完成后，可以通过这两项状态检查。您可以检查系统日志中的控制台输出，或参阅磁盘和 CPU 活动的 Amazon CloudWatch 监控器以确定升级是否已停止。

如果在数小时后实例未通过两项状态检查，请参阅本主题中的 [排查升级问题](#)。

升级运行 Citrix PV 驱动程序的实例

本节介绍如何升级运行 Citrix PV 驱动程序的 EC2 Windows Server 实例。Windows Server 2003 和 2008 的所有版本中都使用 Citrix PV 驱动程序。升级过程中存在一个已知问题，即安装程序会移除部分 Citrix PV 驱动程序，而这些驱动程序使您能够使用远程桌面连接到实例。以下过程描述如何在就地升级过程中使用升级帮助程序服务来避免此问题。

关于升级帮助程序服务

开始升级之前，必须运行 UpgradeHelperService.exe。运行该实用工具后，它会创建一个在升级后的步骤中执行的 Windows 服务以纠正驱动程序状态。该可执行文件是用 C# 编写的，可在 .NET Framework 版本 2.0 至 4.0 上运行。

在升级之前 在系统上运行 UpgradeHelperService.exe 时，它执行以下任务：

- 创建名为 *UpgradeHelperService* 的新 Windows 服务。
- 验证是否已安装 Citrix PV 驱动程序。
- 检查是否有未签名的启动关键驱动程序，如果发现有，则显示警告。未签名的启动关键驱动程序如果与新的 Windows Server 版本不兼容，可能会在升级后造成系统失败。

在升级之后 在系统上运行 UpgradeHelperService.exe 时，它执行以下任务：

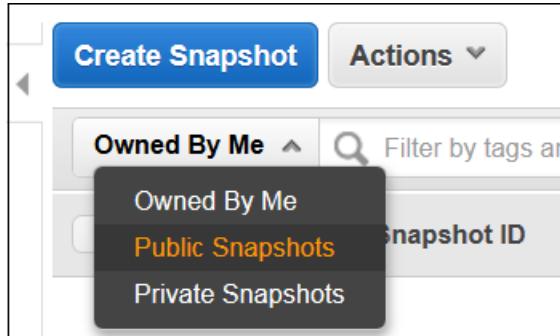
- 启用 RealTimeUniversal 注册表项以实现 Amazon Elastic Compute Cloud (Amazon EC2) 中的正确时间同步。
- 通过执行以下命令还原缺少的 PV 驱动程序：
`pnputil -i -a "C:\Program Files (x86)\Citrix\XenTools*.inf"`
- 通过执行以下命令安装缺少的设备：
`C:\Temp\EC2DriverUtils.exe install "C:\Program Files (x86)\Citrix\XenTools\xevtchn.inf"`
`ROOT\XENEVTCHN`
- 完成后，自动移除 *UpgradeHelperService* Windows 服务。

在运行 Citrix PV 驱动程序的实例上执行升级

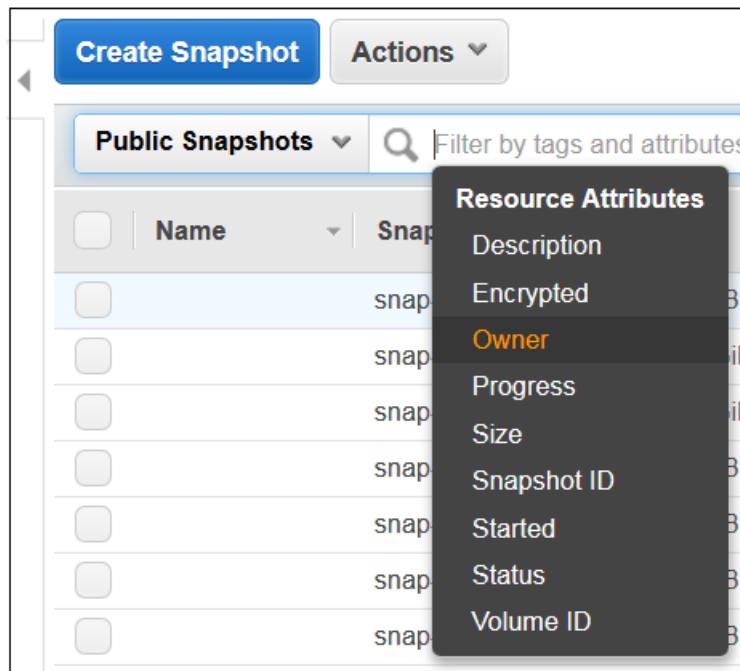
此过程介绍如何将安装介质卷连接到 EC2 实例，以及如何使用 UpgradeHelperService.exe 升级实例。

升级运行 Citrix PV 驱动程序的 EC2 Windows Server 实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择实例，然后找出您想要升级的 Windows Server 的 EC2 实例。记录实例 ID 和可用区。在此过程稍后创建和连接 Windows 安装介质卷时，您要指定这些信息。
3. 从 Windows Server 安装介质快照创建新卷。
 - a. 在 EC2 控制台中，选择 Snapshots。
 - b. 选择 Owned by me，然后选择 Public Snapshots。



- c. 选择搜索 字段，然后从资源属性列表内选择所有者。



- d. 选择Amazon 图像。
- e. 选择搜索 字段，然后从资源属性列表内选择描述。

The screenshot shows the AWS Management Console interface for creating snapshots. At the top, there is a blue button labeled "Create Snapshot". Below it, a search bar contains the text "Owner : Amazon images" and a "Public Snapshots" dropdown menu. To the right of the search bar is a "Actions" dropdown menu. A table lists several public snapshots, each with a checkbox, a name, a snapshot ID, and its size. To the right of the table is a "Resource Attributes" sidebar with a list of descriptions corresponding to the columns in the table.

	Name	Snapshot ID	Size	Resource Attributes
		snap-00fb0869	300 GiB	Description
		snap-0148f405	5 GiB	Encrypted
		snap-057f1092	8 GiB	Owner
		snap-05a4c067	115 GiB	Progress
		snap-075b727d	145 GiB	Size
		snap-08941f9c	8 GiB	Snapshot ID
		snap-095637ae	8 GiB	Started
				Status
				Volume ID

- f. 键入 Windows 并按下输入键。
- g. 选择与您的系统架构匹配的快照。例如，如果您的 Windows Server 2003 实例为 64 位，请选择 Windows 2008 64-bit Installation Media。
- h. 从上下文菜单（右键单击）中，选择创建容量 (Create Volume)。
- i. 在 Create Volume 对话框中，选择与您的 Windows 实例匹配的可用区，然后选择 Create。
4. 在 Volume Successfully Created 消息中，选择刚才创建的卷。
5. 在列表中选择容量，然后从上下文菜单（右键单击）中选择附加容量 (Attach Volume)。
6. 在 Attach Volume 对话框中，键入实例 ID，然后选择 Attach。
7. 在 C:\ 驱动器上的 Windows 实例上，创建名为 temp 的新文件夹。升级后，在这个同一位置必须提供此文件夹。在 Windows 系统文件夹或用户资料文件夹（例如桌面）中创建临时文件夹会造成更新失败。
8. 下载 OSUpgrade.zip 并将文件解压到 C:\temp 文件夹中。
9. 从 c:\temp 运行 UpgradeHelperService.exe，查看 c:\temp 中的 Log.txt 文件中是否有警告。
10. 使用 Microsoft 知识库文章 950376 从 Windows 2003 实例卸载 PowerShell，或执行以下不支持的步骤绕过 Windows Upgrade 检查：
 - a. 在 Windows Explorer 中，选择 WINDOWS，然后选择 System32。
 - b. 将 WindowsPowerShell 文件夹重命名为 old WindowsPowerShell。对于 64 位实例，必须还要重命名 WINDOWS > SysWow64 文件夹中的 WindowsPowerShell 文件夹。
11. 通过 Windows 资源管理器打开在此过程前面已连接到实例的安装介质卷，开始升级。
12. 在 Sources 文件夹中，运行 Setup.exe。
13. 在 Select the operating system you want to install 页面上，选择与您的 Windows Server 实例匹配的完整安装 SKU，然后选择 Next。
14. 在 Which type of installation do you want? 页面上，选择 Upgrade。
15. 完成安装向导。

Windows Server 安装程序随后将复制并处理文件。几分钟后，远程桌面会话关闭。升级所用的时间取决于在 Windows Server 实例上运行的应用程序和服务器角色的数量。升级过程少则 40 分钟，多则数小时。在升级过程中，实例无法通过在 EC2 控制台中进行的两项状态检查之一。升级完成后，可以通过这两项状态检查。您可以检查系统日志中的控制台输出，或参阅磁盘和 CPU 活动的 Amazon CloudWatch 监控器以确定升级是否已停止。

如果在数小时后实例未通过两项状态检查，请参阅本主题中的[排查升级问题](#)。

升级后的任务

1. 登录实例以启动 .NET Framework 的升级并在提示时重启系统。



Note

升级后，实例可能临时遇到高于平均 CPU 使用率的情况，而 .NET 运行时优化服务将优化 .NET 框架。这是预期行为。

2. 安装最新版本的 EC2Config 服务。有关更多信息，请参阅[安装最新版的 EC2Config \(p. 258\)](#)。
3. 安装 Microsoft 修补程序 [KB2800213](#)。
4. 安装 Microsoft 修补程序 [KB2922223](#)。
5. 如果您已升级到 Windows Server 2012 R2，我们建议您将半虚拟化驱动程序升级到 AWS 半虚拟化驱动程序（如果可用）。有关更多信息，请参阅[有关运行 Windows Server 2012 R2 的 Amazon EC2 实例的重要信息](#)。
6. 重新启用反病毒和反间谍软件以及防火墙。

迁移

迁移涉及捕获设置、配置和数据并将这些内容移植到单独硬件上的新版操作系统。经过验证之后，迁移的系统可提升到生产模式。您可以通过从新操作系统的 AMI 启动新实例来迁移 EC2 实例。您可以进一步简化该过程，方法是使用 [AWS CloudFormation](#) 和 [Amazon EC2 Simple Systems Manager](#) 并通过少量手动操作自动向新系统应用设置和配置。

迁移服务器

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 AMIs。
3. 选择 Owned by me，然后选择 Public images。
4. 在 Search 字段中，添加以下筛选条件，然后按 Enter。
 - a. Owner : Amazon images
 - b. AMI 名称 : Windows_Server-2008



Note

Search 字段区分大小写。

5. 从 AMI 启动新实例。
6. 登录新实例并安装全部更新。
7. 执行应用程序安装和配置更改。
8. 测试服务器。
9. 验证后，将服务器提升到生产模式。

排查升级问题

本节可帮助您查找和诊断错误或失败。

- 如果实例在数小时后未通过两项状态检查，请执行以下操作。
 - 如果已升级到 Windows Server 2008，但在数小时后两项状态检查均失败，则升级可能已失败，这时会显示 Click OK 提示以确认回滚。因为在这种状态下无法访问控制台，所以无法单击该按钮。要解决此问题，请通过 EC2 控制台或 API 执行重启。重启需要 10 分钟或更长时间才能开始。实例可能在 25 分钟后变为可用。
 - 从服务器移除应用程序或服务器角色，然后重试。
- 如果从服务器移除应用程序或服务器角色后实例未通过两项检查，请执行以下操作。
 - 停止实例，将根卷连接至其他实例。有关更多信息，请参阅[等待元数据服务](#)中有关如何停止根卷并将其实载到其他实例的描述。
 - 分析 Windows 安装程序日志文件和事件日志中有无失败。

远程管理您的实例

Abstract

使用 Amazon EC2 Run Command 远程管理您的 EC2 实例、本地服务器和虚拟机的配置或来自其他云提供商的虚拟机的配置。

可以使用 Amazon Elastic Compute Cloud (Amazon EC2) Run Command，通过脚本、命令或 Amazon EC2 控制台来远程管理本地环境中或由其他云提供商提供的环境中的 Amazon EC2 实例、虚拟机 (VM) 或服务器的配置。利用 Run Command，您可以跨队列执行常见管理任务和管理配置更改，而无需本地登录到每个实例、服务器或虚拟机。



Note

有关适用于 Linux 的 Run Command 的信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [Amazon EC2 Run Command](#)。

如何开始

下表包含可帮助您开始使用 Run Command 的信息。

主题	详细信息
教程：使用 Run Command 执行命令 (p. 40)	此教程介绍如何在适用于 Windows PowerShell 的 AWS 工具中使用 Run Command 快速发送命令。
Run Command 的组件和概念 (p. 332)	了解 Run Command 的功能和概念。
Run Command 先决条件 (p. 333)	验证您的实例是否满足 Run Command 的最低要求。
设置托管实例 (p. 335)	在本地服务器、虚拟机或由其他云提供商托管的服务器上注册到 AWS。一旦服务器或虚拟机完成注册，它将被称作托管实例。
Run Command 演练 (p. 379)	了解以下有关如何使用 Run Command 从 Amazon EC2 控制台或适用于 Windows 的 AWS 工具执行命令的详细演练。

相关内容

- [Amazon EC2 Simple Systems Manager API Reference](#)
- [适用于 Windows PowerShell 的 SSM AWS 工具参考](#)
- [SSM AWS CLI 参考](#)
- [AWS 软件开发工具包](#)

Amazon EC2 Run Command 的组件和概念

在您开始使用 Amazon EC2 Run Command 时，了解此功能的组件和概念会非常有用。

组件/概念	详细信息
Amazon EC2 Simple Systems Manager (SSM)	Run Command 是 SSM 的组件。Run Command 使用 SSM API。有关更多信息，请参阅 Amazon EC2 Simple Systems Manager API Reference 。
命令	可以通过从本地计算机发送命令，在本地环境中或从其他云提供商处配置 Amazon EC2 实例和虚拟机 (VM) 或服务器。无需本地登录即可配置计算机。可以使用 Amazon EC2 控制台 的 Command History 页、适用于 Windows PowerShell 的 AWS 工具、AWS Command Line Interface (AWS CLI)、SSM API 或 Amazon 开发工具包发送命令。有关更多信息，请参阅 适用于 Windows PowerShell 的 SSM AWS 工具参考 、 SSM AWS CLI 参考 和 AWS 开发工具包 。
SSM 文档	SSM 文档定义在计算机上执行命令时要运行的插件和要使用的参数。在执行命令时，您指定 Run Command 使用的 SSM 文档。Run Command 包含预定义的文档，可利用这些文档在计算机上快速执行常见任务。您还可以创建自己的 SSM 文档。首次从新的 SSM 文档执行命令时，系统将使用您的 AWS 账户存储此文档。有关更多信息，请参阅 创建 SSM 文档 (p. 368) 。
SSM 代理	SSM 代理是驻留在实例、服务器或虚拟机上的 AWS 软件。代理负责处理 Run Command 请求并按照请求中指定的方式配置计算机。有关更多信息，请参阅 安装 SSM 代理 (p. 337) 。
IAM 角色和策略	必须使用 AWS Identity and Access Management (IAM) 角色和信任策略来配置 AWS 用户账户和实例以便其能够与 SSM API 进行通信。有关更多信息，请参阅 委派对 Amazon EC2 Run Command 的访问权限 (p. 338) 。

有关 SSM 文档的更多信息

在配置 Run Command 先决条件后，您确定要对实例进行的配置更改类型以及哪个 SSM 文档使您能够进行此类更改。Run Command 包含预定义的 SSM 文档，这些文档使您能够快速对实例执行命令。对您可用的命令取决于管理员为您指定的权限。以 AWS-* 开头的任意命令均使用 AWS 提供的预定义 SSM 文档。开发人员或管理员可创建其他文档，并根据您的权限为您配置这些文档。有关更多信息，请参阅 [创建 SSM 文档 \(p. 368\)](#)。



Important

仅允许受信任的管理员使用 AWS 预配置文档。SSM 文档中指定的命令或脚本将通过管理特权在您的实例上运行，因为 EC2Config 服务在本地系统账户中运行。如果用户有权执行任何预定义的 SSM 文档（任何以 AWS-* 开头的文档），则该用户也具有实例的管理员访问权。对于所有其他用户，您应创建限制性文档并与特定用户共享这些文档。有关限制对 Run Command 的访问的更多信息，请参阅 [委派对 Amazon EC2 Run Command 的访问权限 \(p. 338\)](#)。

Run Command 包括下列预配置 SSM 文档。

适用于 Windows 的预配置 SSM 文档

名称	说明
AWS-JoinDirectoryServiceDomain	加入 AWS Directory
AWS-RunPowerShellScript	运行 PowerShell 命令或脚本
AWS-UpdateEC2Config	更新 EC2Config 服务
AWS-ConfigureWindowsUpdate	配置 Windows Update 设置
AWS-InstallApplication	使用 MSI 包安装、修复或卸载软件
AWS-InstallPowerShellModule	安装 PowerShell 模块
AWS-ConfigureCloudWatch	配置 Amazon CloudWatch 日志以监控应用程序和系统
AWS-ListWindowsInventory	收集有关在 Windows 中运行的 EC2 实例的信息。
AWS-FindWindowsUpdates	扫描实例并确定缺少的更新。
AWS-InstallMissingWindowsUpdates	在 EC2 实例上安装缺少的更新。
AWS-InstallSpecificWindowsUpdates	安装一个或多个特定更新。

您可在 [Amazon EC2 控制台](#) 的列表中选择文档，或使用 `list documents` 命令查看 AWS CLI 或 适用于 Windows PowerShell 的 AWS 工具 中的可用命令。

如何使用

当您发送指令时，请运行指令尝试执行一次此项指令。您可以同时发送多个命令。命令将异步执行。在实例上运行的 EC2Config 服务将处理命令，按指定方式配置实例并记录输出和结果。系统将管理每个命令的队列、执行、取消和报告。但是，不保证命令执行的顺序。默认情况下，Run Command 使用限制来确保每个实例每分钟发出的命令不超过 60 个。如果在您执行命令时实例未运行或没有响应，则系统会对命令进行排队并尝试在实例响应时运行命令。默认情况下，系统将对命令进行排队并且会在收到请求后尝试运行命令最多 31 天。有关指令状态的详细信息，请参阅 ([监控命令 \(p. 391\)](#))。

Run Command 报告每个实例、服务器或虚拟机的每条命令的状态和结果。Run Command 将存储 30 天的命令历史记录。信息还会存储在 AWS CloudTrail 中并一直保留，直到您删除这些数据。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 中的 [审核 API 调用](#)。

Amazon EC2 Run Command 先决条件

Amazon EC2 Run Command 具有下列限制和先决条件。有关 Linux 先决条件的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Amazon EC2 Run Command 先决条件](#)。

除非另有说明，否则以下限制和前提条件适用于 EC2 实例和托管实例（为 Run Command 配置的本地服务器和虚拟机）。有关托管实例的更多信息，请参阅[设置托管实例 \(p. 335\)](#)。

限制

Run Command [仅在以下区域提供](#)。



Note

对于托管实例，建议您选择离您的数据中心或计算环境最近的区域。

先决条件

要求	详细信息	了解更多信息
支持的操作系统	实例必须运行支持的 Windows Server 版本。支持的版本包含 Windows Server 2003 - 2012，包括所有 R2 版本。	查找 Windows AMI (p. 65)
代理	实例要求使用 SSM 代理处理命令。建议您下载并安装最新版本的 EC2Config 服务。EC2Config 服务是 Windows 实例上的 SSM 代理。 Important 由于已知问题，以下区域内的用户必须 下载 最新版本的 SSM 代理：亚太地区（首尔），ap-northeast-2 和中国（北京），cn-north-1。这是一次性安装。安装最新版本后，可以使用 Run Command 更新代理。	安装 SSM 代理 (p. 337)
对 Run Command 的访问权限	您必须先为将处理命令的实例配置 AWS Identity and Access Management (IAM) EC2 实例角色，然后才能使用 Run Command 执行命令。您还必须为执行命令的用户配置单独的 user 角色。两个角色都需要权限策略才能通过 SSM API 进行通信。 对于托管实例，还必须创建一个 IAM 服务角色，此角色使您的本地服务器或虚拟机能够与 SSM 服务进行通信。	委派对 Amazon EC2 Run Command 的访问权限 (p. 338)
Internet 访问	验证 EC2 实例是否具有出站 Internet 访问权。无需入站 Internet 访问权。	Internet 网关

要求	详细信息	了解更多信息
Amazon S3 存储桶 (可选)	您可以在 Amazon Simple Storage Service (S3) 存储桶中存储命令输出。Amazon EC2 控制台中的命令输出将在 2500 个字符后被截断。此外，您可能希望创建 Amazon S3 键前缀 (子文件夹) 来帮助您整理 Run Command 输出。	创建存储桶

在配置先决条件后，请参阅[使用 Amazon EC2 Run Command 执行命令 \(p. 345\)](#)以了解分步过程。要查看 Run Command 示例，请参阅[Amazon EC2 Run Command 演练 \(p. 379\)](#)。

相关主题

- [Amazon EC2 Simple Systems Manager API Reference](#)
- [AWS Command Line Interface Reference](#) 的 [Amazon EC2 Simple Systems Manager](#) 部分
- [适用于 Windows PowerShell 的 AWS 工具 Reference](#)

设置托管实例

您可以使用 Amazon EC2 Run Command 远程管理本地服务器和虚拟机 (VM) 以及来自其他云提供商的虚拟机。为 Run Command 配置的本地服务器或虚拟机称作**托管实例**。通过设置托管实例，您能够使用相同的工具或脚本，通过一致且安全的方法远程管理本地和云工作负载。



Note

有关设置适用于 Linux 的托管实例的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的[在托管实例上设置 Run Command \(本地服务器和虚拟机\)](#)。

开始在托管实例上使用 Run Command

1. 创建 IAM 服务和用户角色：利用 IAM 服务角色，您的本地服务器和虚拟机能够与 SSM 服务进行通信。IAM 用户角色使用户能够与 SSM API 进行通信，从 Amazon EC2 控制台中或直接调用 API 执行命令。有关更多信息，请参阅[委派对 Amazon EC2 Run Command 的访问权限 \(p. 338\)](#)。
2. 创建托管实例激活：本主题介绍如何创建托管实例激活。
3. 验证前提条件：验证您的本地服务器和虚拟机是否满足 Run Command 的最低要求。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
4. 部署 SSM 代理：在服务器/虚拟机上部署最新版本的 SSM 代理。有关更多信息，请参阅[安装 SSM 代理 \(p. 337\)](#)。

托管实例支持以下功能和服务。

- 使用[AWS CLI](#)、[适用于 Windows PowerShell 的 AWS 工具](#)、[Amazon EC2 控制台](#)中的 Commands 页或 AWS 开发工具包来发送命令。
- 使用公共 SSM 文档（不包括 AWS-JoinDirectoryServiceDomain 文档）或您创建的文档发送命令。
- 使用 AWS Identity and Access Management (IAM) 角色和策略控制用户可执行的 Run Command 操作。
- 使用 AWS CloudTrail 记录和审计用户执行的 Run Command 操作。
- 使用 Sysprep 将基础映像创建为用于启动新服务器的模板。
- 使用标准 Amazon Elastic Compute Cloud (EC2) 标记整理托管实例。

创建托管实例激活

要设置实例，您需要创建托管实例激活。完成激活后，您将收到一个激活代码和 ID。此代码/ID 组合具有 Amazon EC2 访问 ID 和私有密钥的功能，可提供从托管实例对 Run Command 访问的安全访问。



Important

在安全位置存储托管实例激活代码和 ID。在本地服务器或虚拟机上安装 SSM 代理时指定此代码和 ID。如果您丢失了此代码和 ID，则必须创建一个新激活。

此部分中的过程要求您指定 [SSM 适用于的区域](#)。建议您指定离您的数据中心或计算环境最近的区域。

使用控制台创建托管实例激活

1. 打开 [Amazon EC2 控制台](#)，在导航窗格中展开 Run Command，然后选择 Activations。
2. 选择 Create an Activation。
3. 填写表单，然后选择 Create Activation。

使用适用于 Windows PowerShell 的 AWS 工具 创建托管实例激活

1. 执行下面的命令。

```
New-SSMActivation -DefaultInstanceName name -IamRole IAM service role -RegistrationLimit number of managed instances -Region region
```

例如：

```
New-SSMActivation -DefaultInstanceName MyWebServers -IamRole RunCommandServiceRole -RegistrationLimit 10 -Region us-east-1
```

2. 按 Enter。如果激活成功，系统将返回一个激活代码和一个 ID。在安全位置存储激活代码和 ID。

使用 AWS CLI 创建托管实例激活

1. 在 CLI 中执行以下命令。

```
aws ssm create-activation --default-instance-name name --iam-role IAM service role --registration-limit number of managed instances --region region
```

例如：

```
aws ssm create-activation --default-instance-name MyWebServers --iam-role RunCommandServiceRole --registration-limit 10 --region us-east-1
```

2. 按 Enter。如果激活成功，系统将返回一个激活代码和一个 ID。在安全位置存储激活代码和 ID。

在收到激活代码和 ID 后，您必须完成以下步骤来为 Run Command 配置本地服务器和虚拟机：

- 验证您的本地服务器和虚拟机是否满足 Run Command 的最低要求。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
- 在服务器/虚拟机上部署 SSM 代理。有关更多信息，请参阅 [安装 SSM 代理 \(p. 337\)](#)。

完成这些步骤后，您的本地服务器和虚拟机将被视为托管实例，并且您可以使用 Run Command 对其进行配置。在控制台中，托管实例在列出时带有前缀“mi-”。您可以使用 List 命令查看所有实例。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#)。

安装 SSM 代理

Amazon EC2 Simple Systems Manager (SSM) 代理处理 Run Command 请求并配置该请求中指定的实例。使用以下过程可安装 SSM 代理。

此部分中的命令要求您将 *region* 替换为 [SSM 适用于的区域](#)。要避免下载产生跨区域数据传输费用，请指定您的 EC2 实例的区域。对于托管实例，不会产生跨区域数据传输费，但建议您指定离您的数据中心或计算环境最近的区域。

内容

- [在 EC2 实例上手动安装 SSM 代理 \(p. 337\)](#)
- [在托管实例上安装 SSM 代理 \(p. 337\)](#)

在 EC2 实例上手动安装 SSM 代理

EC2Config 服务是 Windows 实例上的 SSM 代理。默认情况下，EC2Config 服务将安装到所有 Windows Amazon 系统映像 (AMI) 上，不包括 Window Server 2016 的预发行版本。如果您需要升级到最新版本的 EC2Config 服务，则可从以下位置下载此最新版本：[Amazon Windows EC2Config 服务](#)。

有关将 EC2Config 服务配置为使用代理的信息，请参阅[配置 EC2Config 服务的代理设置 \(p. 257\)](#)。有关如何使用 Run Command 在托管实例上执行命令的信息，请参阅[使用 Amazon EC2 Run Command 执行命令 \(p. 345\)](#)。

在托管实例上安装 SSM 代理

在托管实例（要使用 Run Command 配置的本地服务器或虚拟机）上安装 SSM 代理之前，请确认您已完成托管实例激活过程并且已创建 IAM 角色服务。有关托管实例和激活过程的更多信息，请参阅[设置托管实例 \(p. 335\)](#)。有关托管实例的 IAM 服务角色的更多信息，请参阅[委派对 Amazon EC2 Run Command 的访问权限 \(p. 338\)](#)。

在托管实例上安装 SSM 代理

1. 登录到本地服务器或虚拟机。
2. 将以下命令块复制并粘贴到适用于 Windows PowerShell 的 AWS 工具。指定您的激活代码、ID 和要从中下载 SSM 代理的区域。

```
$dir = $env:TEMP + "\ssm"
New-Item -ItemType directory -Path $dir
cd $dir
(New-Object System.Net.WebClient).DownloadFile("https://amazon-ssm-$region.s3.amazonaws.com/latest/windows_amd64/AmazonSSMAgentSetup.exe", $dir + "\AmazonSSMAgentSetup.exe")
Start-Process .\AmazonSSMAgentSetup.exe -ArgumentList @("/q", "/log", "install.log", "CODE=$code", "ID=$id", "REGION=$region") -Wait
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```

3. 按 Enter。

此命令将下载 SSM 代理并将它安装到本地服务器或虚拟机上。此命令还将服务器或虚拟机注册到 SSM 服务。服务器或虚拟机现在为托管实例。

委派对 Amazon EC2 Run Command 的访问权限

Amazon EC2 Run Command 需要一个针对将处理命令的 EC2 实例的 IAM 角色和一个针对执行命令的用户的独立角色。两个角色都需要权限策略才能通过 [SSM API](#) 进行通信。您可以选择使用 SSM 托管策略或创建自己的角色并指定权限，如本节中所述。

如果您配置的是托管实例（要使用 Run Command 配置的本地服务器或虚拟机），则还必须配置 IAM 服务角色，如此部分中所述。有关托管实例的更多信息，请参阅[设置托管实例 \(p. 335\)](#)。

本节包含以下信息。

- [使用 SSM 托管策略 \(p. 338\)](#)
- [配置您自己的角色和策略 \(p. 338\)](#)
- [创建托管实例服务角色 \(p. 344\)](#)
- [创建使用 EC2 实例角色的 EC2 实例 \(p. 345\)](#)

在配置角色和策略后，建议您创建用于执行特定操作和为特定用户分配访问权限的命令来进一步委派访问权限。对于您的组中任何人都可执行的低级别操作，您可创建低级别命令并将这些命令公开。有关更多信息，请参阅[创建 SSM 文档 \(p. 368\)](#)。

使用 SSM 托管策略

SSM 的 IAM 托管策略可帮助您为 Run Command 用户和实例快速配置访问权限和其他权限。可通过搜索 SSM 在 IAM 控制台的 Policies 页面中查找这些策略，如以下屏幕截图所示。



托管策略执行以下功能：

- AmazonEC2RoleforSSM（实例信任策略）：使实例能够与 Run Command API 进行通信。
- AmazonSSMFullAccess（用户信任策略）：向用户授予对 Run Command API 和 SSM JSON 文档的访问权限。将此策略分配给管理员和可信高级用户。
- AmazonSSMReadOnlyAccess（用户信任策略）：向用户授予对只读 API 操作（例如 Get 和 List）的访问权限。

有关如何配置这些策略的信息，请参阅[托管策略和内联策略](#)。

配置您自己的角色和策略

如果您选择不使用 SSM 托管策略，则使用以下过程创建和配置一个 SSM EC2 实例角色和一个 SSM 用户账户。



Important

如果您要使用现有 EC2 实例角色和用户账户，则必须将此部分中显示的策略附加到该角色和该用户账户。还必须验证 EC2 实例角色的信任策略中是否列出了 ec2.amazonaws.com。有关更多信息，请参阅[验证信任策略 \(p. 343\)](#)。

主题

- 为 EC2 实例创建 IAM 策略 (p. 339)
- 创建 IAM 用户策略 (p. 340)
- 创建限制性的 IAM 用户策略 (p. 341)
- 创建 EC2 实例角色 (p. 343)
- 验证信任策略 (p. 343)
- 创建用户账户 (p. 344)

为 EC2 实例创建 IAM 策略

以下 IAM 策略使 EC2 实例能够与 Run Command API 进行通信。在本主题的后面部分，您将创建一个角色并将此策略附加到该角色。

为 EC2 实例创建 IAM 策略

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Policies。（如果这是您首次使用 IAM，请选择 Get Started，然后选择 Create Policy。）
3. 在 Create Your Own Policy 旁边，选择 Select。
4. 键入策略名称（例如，*RunCommandInstance*）和描述，然后将以下策略复制并粘贴到 Policy Document 字段中：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ssm:DescribeAssociation",  
                "ssm:GetDocument",  
                "ssm>ListAssociations",  
                "ssm:UpdateAssociationStatus",  
                "ssm:UpdateInstanceStateInformation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2messages:AcknowledgeMessage",  
                "ec2messages>DeleteMessage",  
                "ec2messages:FailMessage",  
                "ec2messages:GetEndpoint",  
                "ec2messages:GetMessages",  
                "ec2messages:SendReply"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "cloudwatch:PutMetricData"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
"Effect": "Allow",
"Action": [
    "ec2:DescribeInstanceStatus"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "ds>CreateComputer",
    "ds>DescribeDirectories"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "logs>CreateLogGroup",
    "logs>CreateLogStream",
    "logs>DescribeLogGroups",
    "logs>DescribeLogStreams",
    "logs>PutLogEvents"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:AbortMultipartUpload",
    "s3>ListMultipartUploadParts",
    "s3>ListBucketMultipartUploads"
],
"Resource": "*"
}
]
```



Important

在此 IAM 策略的最后一个部分，您可以通过指定 Amazon 资源名称 (ARN) 来限制对 Amazon S3 存储桶的访问。例如，您可以将最后一个 "Resource": "*" 项目更改为 "Resource": "arn:aws:s3:::*AnS3Bucket*/*"

- 选择 Validate Policy。验证策略是否有效。如果您收到错误，请验证您是否包含了左右大括号 {}。验证完策略后，请选择 Create Policy。

创建 IAM 用户策略

IAM 用户策略确定用户可在 Command document 列表中查看的 SSM 文档。用户可在 Amazon EC2 控制台中查看此列表，或者使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具调用 ListDocuments 来查看此列表。该策略还限制用户可对 SSM JSON 文档执行的操作。



Note

稍后，您将创建一个用户账户并将此策略附加到该账户。

以下步骤中的 IAM 策略允许用户对实例执行任何 SSM 操作。将此策略仅分配给受信任的管理员。对于所有其他用户，则创建一种限制性 IAM 策略，如本节中所述。

创建 IAM 用户策略

1. 重复上一过程以为用户创建策略。
 2. 将下面的策略复制并粘贴到 Policy Document 字段中并创建策略：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ssm:*",  
                "ec2:DescribeInstanceStatus"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

创建限制性的 IAM 用户策略

创建限制性 IAM 用户策略来进一步委派对 Run Command 的访问权限。以下示例 IAM 策略允许用户列出 SSM JSON 文档和查看有关这些文档的详细信息，使用 RestartService 文档发送命令，以及在发送命令后取消或查看有关命令的详细信息。用户有权对第二个“资源”部分中的“arn:aws:ec2:us-east-1:*:instance/i-xxxxxxxxxxxxxxx”项确定的三个实例执行 RestartService 文档。如果需要向用户授予对其当前可访问的任何实例（由 AWS 用户账户确定）运行命令的访问权，您可以在该“资源”部分中指定“arn:aws:ec2:us-east-1:*:instance/*”并删除其他实例资源。

请注意，“资源”部分包含一个 S3 ARN 条目：

`arn:aws:s3:::bucket_name`

您还可为此条目设置格式，如下所示：

```
arn:aws:s3:::bucket_name/*  
    arn:aws:s3:::bucket_name/key_prefix_name
```

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ssm>ListDocuments",  
                "ssm>DescribeDocument",  
                "ssm>GetDocument",  
                "ssm>PutDocument"  
            ]  
        }  
    ]  
}
```

```
        "ssm:DescribeInstanceInformation"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Action": "ssm:SendCommand",
    "Effect": "Allow",
    "Resource": [
        "arn:aws:ec2:us-east-1:*:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:*:instance/i-0598c7d356eba48d7",
        "arn:aws:ec2:us-east-1:*:instance/i-345678abcdef12345",
        "arn:aws:s3:::bucket_name",
        "arn:aws:ssm:us-east-1:*:document/RestartService"
    ]
},
{
    "Action": [
        "ssm:CancelCommand",
        "ssm>ListCommands",
        "ssm>ListCommandInvocations"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Action": "ec2:DescribeInstanceStatus",
    "Effect": "Allow",
    "Resource": "*"
}
]
```

以下 IAM 策略文档使用户能够使用 AWS-InstallApplication SSM 文档安装、卸载或修复应用程序。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm>ListDocuments",
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeInstanceInformation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ssm:SendCommand",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:us-east-1:*:document/AWS-InstallApplication",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        }
    ]
}
```

```
        },
        {
            "Action": [
                "ssm:CancelCommand",
                "ssm>ListCommands",
                "ssm>ListCommandInvocations"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ec2:DescribeInstanceStatus",
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

有关创建 IAM 用户策略的更多信息，请参阅[托管策略与内联策略](#)。

创建 EC2 实例角色

EC2 实例角色使实例能够与 Run Command API 进行通信。该角色使用您先前创建 EC2 实例策略。

创建 EC2 实例角色

1. 在 IAM 控制台的导航窗格中，选择 Roles，然后选择 Create New Role。
2. 在 Set Role Name 页面上，输入被指定为实例角色的角色的名称，例如 *RunCommandInstance*。选择 Next Step。
3. 在 Select Role Type 页面上，选择 Amazon EC2 旁的 Select。
4. 在 Attach Policy 页面上，选择您先前创建的 *RunCommandInstance* 策略。选择 Next Step。
5. 检查角色信息，然后选择 Create Role。

验证信任策略

如果您要使用现有的 EC2 实例角色，则必须验证该角色的信任策略中是否列出了 ec2.amazonaws.com。如果您创建了一个新的 EC2 实例角色，则必须添加 ec2.amazonaws.com 作为可信实体。

验证信任策略

1. 在 IAM 控制台的导航窗格中，选择 Roles，然后选择您刚刚创建的服务器角色。
2. 选择 Trust Relationships。
3. 在 Trusted Entities 下，验证是否列出了 ec2.amazonaws.com。如果未列出 ec2.amazonaws.com，请选择 Edit Trust Relationship。
4. 将下面的策略复制并粘贴到 Policy Document 字段中并创建策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
        }
    ]
}
```

```
        },
        "Action": "sts:AssumeRole"
    ]
}
```

创建用户账户

利用用户账户，用户可在实例上调用 Run Command API。此账户使用您先前创建的 IAM 用户策略。

创建用户账户

1. 从 [IAM 控制台](#) 上的 Users 页面中，选择 Create New Users。
2. 指定用户名（例如 *RunCommandUser*）并确认 Generate an access key for each user 选项已选定。
3. 选择 Create。
4. 选择 Download Credentials。默认情况下，系统将提示您将凭证另存为 .csv 文件。



Important

记下您下载的 .csv 文件中的 *RunCommandUser* 访问密钥和私有密钥。

5. 选择 Close。
6. 在 IAM Dashboard 中，选择 Users，然后找到您刚刚创建的用户。
7. 选择该用户名（不要选择名称旁边的选项），然后选择 Attach Policy。
8. 选择您先前创建的用户策略，然后选择 Attach Policy。

创建托管实例服务角色

托管实例（要使用 Run Command 配置的本地服务器或虚拟机）要求 IAM 角色与 SSM 服务进行通信。该角色向 AssumeRole 授予对 SSM 服务的信任。如果您此时未配置托管实例，则可以跳过此部分。

以下示例说明如何使用适用于 Windows PowerShell 的 AWS 工具为 SSM 创建 IAM 服务角色。有关如何使用 AWS 管理控制台或 AWS CLI 创建服务角色的示例，请参阅[创建向 AWS 服务委托权限的角色](#)



Note

您只需为每个 AWS 账户创建该服务角色一次。

为托管实例创建 IAM 服务角色

1. 使用以下信任策略创建文本文件（在此示例中，它名为 *SSMService-Trust.json*）。使用 .json 文件扩展名保存该文件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": ["Service": "ssm.amazonaws.com"],
            "Action": "sts:AssumeRole"
        }
    ]
}
```

```
}
```

2. 使用 [New-IAMRole](#) (如下所示) 创建服务角色。此示例创建一个名为 SSMServiceRole 的角色。

```
New-IAMRole -RoleName SSMServiceRole -AssumeRolePolicyDocument (Get-Content  
-raw SSMService-Trust.json)
```

3. 使用 [Register-IAMRolePolicy](#) (如下所示) 以允许 SSMServiceRole 创建会话令牌。此会话令牌向托管实例授予使用 Run Command 执行命令的权限。

```
Register-IAMRolePolicy -RoleName SSMServiceRole -PolicyArn  
arn:aws:iam::ssm:policy/role/AmazonEC2RoleforSSM
```

创建使用 EC2 实例角色的 EC2 实例

此过程介绍如何创建使用创建的角色的 EC2 实例。启动 EC2 实例时，必须为该实例分配角色。无法将角色分配给已在运行的实例。相反，您将创建实例的映像，然后从该映像启动实例与分配的角色。

创建使用 EC2 实例角色的实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择支持的**区域**。
3. 选择 Launch Instance，然后选择一个 Windows Server 实例。
4. 选择实例类型，然后选择 Next: Configure Instance Details。
5. 在 IAM role 下拉列表中，选择您先前创建的 EC2 实例角色。
6. 完成向导。

如果您创建要使用 Run Command 配置的其他实例，则必须为每个实例指定 EC2 实例角色。

使用 Amazon EC2 Run Command 执行命令

您可以使用 Amazon EC2 控制台中的 Commands 页面在 EC2 实例上运行命令。您也可以使用[适用于 Windows PowerShell 的 AWS 工具](#)执行命令、使用 [CLI](#) 执行命令或使用 SSM API 以编程方式执行命令。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#)。

主题

- [使用 Amazon EC2 Run Command 运行 PowerShell 命令或脚本 \(p. 346\)](#)
- [使用 Amazon EC2 Run Command 安装应用程序 \(p. 347\)](#)
- [使用 Amazon EC2 Run Command 安装 PowerShell 模块 \(p. 348\)](#)
- [使用 Amazon EC2 Run Command 将 EC2 实例加入域 \(p. 349\)](#)
- [使用 Amazon EC2 Run Command 将日志从 EC2 实例上传到 Amazon CloudWatch \(p. 350\)](#)
- [使用 Amazon EC2 Run Command 启用或禁用 Windows 更新 \(p. 361\)](#)
- [使用 Amazon EC2 Run Command 更新 EC2Config 服务 \(p. 363\)](#)
- [使用 Amazon EC2 Run Command 清查适用于 Windows 的 Amazon EC2 实例 \(p. 364\)](#)
- [使用 Amazon EC2 Run Command 管理 EC2 Windows 实例的更新 \(p. 365\)](#)

使用 Amazon EC2 Run Command 运行 PowerShell 命令或脚本

使用 AWS-RunPowerShellScript 文档将命令发送到 EC2 实例，或指定到要在实例上运行的脚本的路径。例如，您可以发送 dir c:\、ipconfig 或 net stop *service_name* 等命令。您也可以指定要运行的脚本的位置。例如，c:\script.ps1 或 *network_share*\script.ps1。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 运行 PowerShell 命令或脚本

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-RunPowerShellScript。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 在 Commands 字段中键入命令或到脚本的路径。
6. (可选) 在 Working Directory 字段中，键入要运行命令的 EC2 实例上的文件夹的路径。例如：C:\temp。
7. (可选) 在 Execution Timeout 字段中，键入 EC2Config 服务在超时前将尝试运行命令的秒数。
8. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在控制台的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

9. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
10. 在 Amazon S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

11. 在 S3 key prefix 中，键入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 安装应用程序

您可使用 AWS-InstallApplication 文档在 EC2 实例上安装、修复或卸载应用程序。您必须指定 URL 或 .msi 文件的路径。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 安装、修复或卸载应用程序

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-InstallApplication。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 在 Action 列表中，选择要执行的任务。
6. (可选) 在 Parameters 字段中，键入安装程序的参数。
7. 在 Source 字段中，键入 URL 或 .msi 文件的路径。例如：

URL : <http://sdk-for-net.amazonwebservices.com/latest/AWSToolsAndSDKForNet.msi>

文件 : file:///c:/temp/AWSToolsAndSDKForNet.msi

8. (可选) 在 Source Hash 字段中，键入安装程序的 SHA256 哈希。
9. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

10. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
11. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

12. 在 S3 key prefix 字段中，输入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 安装 PowerShell 模块

您可使用 AWS-InstallPowerShellModule 文档在 EC2 实例上安装 PowerShell 模块。您也可以指定在安装模块后运行的 PowerShell 命令。例如，您可以安装 EZOut 模块以实现灵活的 PowerShell 格式化，然后运行命令以安装 Windows 功能（如 XPS Viewer）来查看使用 EZOut 创建的文件。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 安装 PowerShell 模块

1. 打开[Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-InstallPowerShellModule。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
- 5.（可选）在 Working Directory 字段中，键入要运行命令的 EC2 实例上的文件夹的路径。例如：C:\temp。
6. 在 Source 字段中，键入 URL 或 .zip 文件的路径。例如：

URL : <http://www.microsoft.com/en-us/download/SomePSModule.msi>

文件 : file:///c:/temp/EZOut.zip

- 7.（可选）在 Source Hash 字段中，键入 .zip 文件的 SHA256 哈希。
- 8.（可选）在 Commands 字段中键入命令。选择加号添加其他命令。
- 9.（可选）在 Execution Timeout 字段中，键入 EC2Config 服务在超时前将尝试运行命令的秒数。
- 10.（可选）在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

11. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
12. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

13. 在 S3 key prefix 字段中，键入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 将 EC2 实例加入域

可使用 AWS-JoinDirectoryServiceDomain 命令将实例加入 AWS Directory Service 域。在执行此命令前，您必须[创建目录](#)。建议您了解有关 AWS Directory Service 的更多信息。有关更多信息，请参阅[什么是 AWS Directory Service ?](#)。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 将实例加入域

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-JoinDirectoryServiceDomain。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 在 Directory ID 字段中，键入 AWS 目录的 ID。例如：d-1234567890。
6. 在 Directory Name 字段中，键入目录名称。例如：example.com。
7. 在 Directory OU 字段中，键入目录的组织部门 (OU) 和目录组件 (DC)；例如，OU=Computers,OU=example,DC=test,DC=example,DC=com。
8. (可选) 在 DNS IP Addresses 字段中，键入 IP 地址。例如：198.51.100.1。选择加号添加更多 IP 地址。
9. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

10. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
11. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

12. 在 S3 key prefix 字段中，键入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 将日志从 EC2 实例上传到 Amazon CloudWatch

您可以使用 Run Command 配置与多个实例上的 Amazon CloudWatch 和 Amazon CloudWatch Logs 的集成以监控其日志文件。您可以将应用程序、系统、安全和事件跟踪(Windows) 日志中的 Windows Server 消息发送到 Amazon CloudWatch Logs。在首次启用日志记录时，Run Command 会发送从您开始上传应用程序、系统、安全的日志和 ETW 日志起 1 分钟内生成的所有日志。其中不包括在此时间之前产生的日志。如果您禁用日志记录，并在稍后重新启用日志记录，则 Run Command 会发送从禁用日志记录起生成的日志。对于任何自定义日志文件和 Internet Information Services (IIS) 日志，Run Command 会从头读取日志文件。此外，Run Command 还可以将性能计数器数据发送到 CloudWatch。

如果您先前在 EC2Config 中启用了 CloudWatch 集成，则 Run Command 设置会覆盖实例本地在 C:\Program Files\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json 文件中存储的任何设置。

在将日志上传到 CloudWatch 时，您可以选择在 JSON 代码示例中指定属性并将该示例粘贴到 Properties 字段中。如果您当前具有使用 Amazon Simple System Manager (SSM) 将日志上传到 CloudWatch 的 JSON 示例，则可在以下示例中指定属性并将其用于 Properties 字段。或者，您可以按照此部分所述来指定属性并复制/粘贴该属性。要了解有关可指定的属性和值的信息，请参阅 API 参考中的[aws:cloudWatch](#)。

创建 JSON 文件

如果您还没有 JSON 文件，则必须创建一个。将以下示例复制并粘贴到文本编辑器中，并使用 .json 文件扩展名保存文件。

有关 SSM 文档的 JSON 结构的更多信息，请参阅 *Amazon EC2 Simple Systems Manager API Reference* 中的 [SSM 文档](#)。

```
{  
    "EngineConfiguration": {
```

```
"PollInterval": "00:00:15",
"Components": [
    {
        "Id": "ApplicationEventLog",
        "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCom
ponent,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogName": "Application",
            "Levels": "value"
        }
    },
    {
        "Id": "SystemEventLog",
        "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCom
ponent,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogName": "System",
            "Levels": "value"
        }
    },
    {
        "Id": "SecurityEventLog",
        "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCom
ponent,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogName": "Security",
            "Levels": "value"
        }
    },
    {
        "Id": "ETW",
        "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCom
ponent,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogName": "Microsoft-Windows-WinINet/Analytic",
            "Levels": "value"
        }
    },
    {
        "Id": "IISLogs",
        "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInput
Component,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogDirectoryPath": "path",
            "TimestampFormat": "value",
            "Encoding": "value",
            "Filter": "value",
            "CultureName": "locale",
            "TimeZoneKind": "value",
            "LineCount": "value"
        }
    },
    {
        "Id": "CustomLogs",
        "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInput
Component,AWS.EC2.Windows.CloudWatch",
        "Parameters": {
            "LogDirectoryPath": "path",
```

```
        "TimestampFormat": "value",
        "Encoding": "value",
        "Filter": "value",
        "CultureName": "locale",
        "TimeZoneKind": "value",
        "LineCount": "value"
    }
},
{
    "Id": "PerformanceCounter",
    "FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "CategoryName": "name",
        "CounterName": "name",
        "InstanceName": "name",
        "MetricName": "name",
        "Unit": "unit",
        "DimensionName": "name",
        "DimensionValue": "value"
    }
},
{
    "Id": "CloudWatchLogs",
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "access-key-id",
        "SecretKey": "secret-access-key",
        "Region": "region",
        "LogGroup": "group",
        "LogStream": "stream"
    }
},
{
    "Id": "CloudWatch",
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "access-key-id",
        "SecretKey": "secret-access-key",
        "Region": "region",
        "NameSpace": "namespace"
    }
}
],
"Flows": {
    "Flows": [
        "source,destination",
        "(source1, source2),destination",
        "source, (destination1,destination2)"
    ]
}
}
```

配置 CloudWatch 和 CloudWatch Logs 的区域和命名空间

下一步，您将定义构成数据发送目标的证书、区域和指标命名空间。

为 CloudWatch 设置证书、区域和指标命名空间

JSON 文件的此部分定义组成数据发送目标的证书、区域和指标命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatch2”、“CloudWatch3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。



Note

如果您使用 EC2Config 并且计划将性能计数器发送到 CloudWatch，则只需设置 CloudWatch 证书。如果您使用 Amazon EC2 Simple Systems Manager，则您的证书是在您启动 Amazon EC2 实例时使用的 IAM 角色中配置的。

1. 在 JSON 文件中，找到 CloudWatch 部分。

```
{  
    "Id": "CloudWatch",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputCom  
ponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "AccessKey": "",  
        "SecretKey": "",  
        "Region": "us-west-1",  
        "NameSpace": "Windows/Default"  
    }  
},
```

- 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
 - 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
 - 在 Region 参数中，输入希望将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。虽然可以将性能计数器发送到与日志数据发送目标不同的区域，但是我们建议您将此参数设置为运行实例的区域。
 - 在 NameSpace 参数中，输入要用于在 CloudWatch 中写入性能计数器数据的指标命名空间。

为 CloudWatch Logs 设置证书、区域、日志组和日志流

JSON 文件的此部分定义组成数据发送目标的证书、区域、日志组名称和日志流命名空间。可以采用唯一 ID 添加其他部分（例如“CloudWatchLogs2”、“CloudWatchLogs3”等），并为每个新 ID 指定不同区域以将相同数据发送到不同位置。

1. 在 JSON 文件中，找到 CloudWatchLogs 部分。

```
"SecretKey": "",  
"Region": "us-east-1",  
"LogGroup": "Default-Log-Group",  
"LogStream": "{instance_id}"  
},  
,
```

2. 在 AccessKey 参数中，输入您的访问密钥 ID。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
3. 在 SecretKey 参数中，输入您的私有访问密钥。如果是使用 IAM 角色启动的实例，则不支持这样做。有关更多信息，请参阅 [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)。
4. 在 Region 参数中，输入希望 EC2Config 将日志数据发送到的区域。您可以指定 us-east-1、us-west-1、us-west-2、eu-west-1、eu-central-1、ap-southeast-1、ap-southeast-2 或 ap-northeast-1。
5. 在 LogGroup 参数中，输入日志组的名称。这是在 CloudWatch 控制台 Log Groups (日志组) 屏幕上显示的名称。
6. 在 LogStream 参数中，输入目标日志流。如果使用 {instance_id} 默认设置，则 EC2Config 将该实例的实例 ID 用作日志流名称。

如果输入不存在的日志流名称，则 CloudWatch Logs 会自动创建该名称。您可以使用文字字符串或预定义的变量 ({instance_id}、{hostname}、{ip_address})，或所有这三个变量的组合来定义日志流名称。

此参数中指定的日志流名称会显示在 CloudWatch 控制台中的 Log Groups (日志组) > Streams for *<YourLogStream>* (<YourLogStream> 的流) 屏幕上。

配置要发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志

下一步，您将配置要发送到 CloudWatch 和 CloudWatch Logs 的性能计数器和日志。

配置发送到 CloudWatch 的性能计数器

可以选择性能监视器中提供的任何性能计数器。您可以选择不同类别作为指标上传到 CloudWatch，如 .NET CLR 数据、ASP.NET 应用程序、HTTP 服务、内存或进程和处理器。

对于要上传到 CloudWatch 的每个性能计数器，复制 PerformanceCounter 部分，更改 Id 参数使其唯一（例如“PerformanceCounter2”），然后根据需要更新其他参数。

1. 在 JSON 文件中，找到 PerformanceCounter 部分。

```
{  
    "Id": "PerformanceCounter",  
    "FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "CategoryName": "Memory",  
        "CounterName": "Available MBytes",  
        "InstanceName": "",  
        "MetricName": "AvailableMemory",  
        "Unit": "Megabytes",  
        "DimensionName": "",  
        "DimensionValue": ""  
    },  
,
```

2. 在 CategoryName 参数中，输入性能计数器类别。

- a. 要查找可用类别和计数器，请打开性能监视器。
- b. 单击 Monitoring Tools (监控工具)，然后单击 Performance Monitor (性能监视器)。
- c. 在结果窗格中，单击绿色 + (加号) 按钮。

类别和计数器会在 Add Counters (添加计数器) 对话框中列出。

3. 在 CounterName 参数中，输入性能计数器的名称。
4. 在 InstanceName 参数中，从性能监视器的 Add Counters 对话框中输入值，可以是下列值之一：
 - 空白，如果所选对象没有实例。
 - 所选对象的单个实例。
 - _Total，将使用所有实例的汇总。



Note

请勿使用星号 (*) 标识所有实例，因为每个性能计数器组件仅支持一个指标。

5. 在 MetricName 参数中，输入希望性能数据所属的 CloudWatch 指标。
6. 在 Unit 参数中，为指标输入合适的度量单位：
秒 | 微秒 | 毫秒 | 字节 | 千字节 | 兆字节 | 千兆字节 | 太兆字节 | 位 | 千位 | 兆位 | 千兆位 | 太兆位 | 百分比 | 计数 | 字节/秒 | 千字节/秒 | 兆字节/秒 | 千兆字节/秒 | 太兆字节/秒 | 位/秒 | 千位/秒 | 兆位/秒 | 千兆位/秒 | 太兆位/秒 | 计数/秒 | 无.
7. (可选) 您可以在 DimensionName 和 DimensionValue 参数中输入维度名称和值以便为指标指定维度。这些参数在列出指标时提供另一个视图。您还可以对多个指标使用同一个维度，以便可以查看属于特定维度的所有指标。

将 Windows 应用程序事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 ApplicationEventLog 部分。

```
{  
    "Id": "ApplicationEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Application",  
        "Levels": "1"  
    }  
},
```

2. 在 Levels 参数中，输入以下值之一：

1 – 仅上传错误消息。

2 – 仅上传警告消息。

4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将安全日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 SecurityEventLog 部分。

```
{  
    "Id": "SecurityEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Security",  
        "Levels": "7"  
    }  
,
```

2. 在 Levels 参数中，输入 7，以便上传所有消息。

将系统事件日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 SystemEventLog 部分。

```
{  
    "Id": "SystemEventLog",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "System",  
        "Levels": "7"  
    }  
,
```

2. 在 Levels 参数中，输入以下值之一：

1 – 仅上传错误消息。

2 – 仅上传警告消息。

4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将其他类型的事件日志数据发送到 CloudWatch Logs

除了应用程序、系统和安全日志之外，您还可以上传其他类型的事件类型。

1. 在 JSON 文件中，添加新部分。

```
{  
    "Id": "",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputCompon  
ent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "",  
        "Levels": "7"
```

```
    },
```

2. 在 Id 参数中，为要上传的日志输入名称（例如 WindowsBackup）。
3. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器的导航窗格中，单击 Applications and Services Logs（应用程序和服务日志）。
 - b. 在日志列表中，右键单击要上传的日志（例如“Microsoft>Windows>Backup (备份)>Operational (运行)”），然后单击 Create Custom View（创建自定义视图）。
 - c. 在 Create Custom View（创建自定义视图）对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-Backup）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。
4. 在 Levels 参数中，输入以下值之一：
 - 1 – 仅上传错误消息。
 - 2 – 仅上传警告消息。
 - 4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将事件跟踪 (Windows) 数据发送到 CloudWatch Logs

ETW（Windows 事件跟踪）提供了高效且详细日志记录机制，供应用程序写入日志。每个 ETW 都由可以启动和停止日志记录会话的会话管理器控制。每个会话都具有一个提供者以及一个或多个使用者。

1. 在 JSON 文件中，找到 ETW 部分。

```
{  
    "Id": "ETW",  
    "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogName": "Microsoft-Windows-WinINet/Analytic",  
        "Levels": "7"  
    }  
},
```

2. 在 LogName 参数中，输入要上传的日志的名称。
 - a. 要查找日志的名称，请在事件查看器中的 View（视图）菜单上，单击 Show Analytic and Debug Logs（显示分析和调试日志）。
 - b. 在导航窗格中，单击 Applications and Services Logs（应用程序和服务日志）。
 - c. 在 ETW 日志的列表中，右键单击要上传的日志，然后单击 Enable Log（启用日志）。
 - d. 再次右键单击该日志，然后单击 Create Custom View（创建自定义视图）。
 - e. 在 Create Custom View（创建自定义视图）对话框中，单击 XML 选项卡。LogName 处于 <Select Path=> 标签中（例如 Microsoft-Windows-WinINet/Analytic）。将此文本复制到 AWS.EC2.Windows.CloudWatch.json 文件中的 LogName 参数中。

3. 在 Levels 参数中，输入以下值之一：

1 – 仅上传错误消息。

2 – 仅上传警告消息。

4 – 仅上传信息消息。

您可以将这些值加在一起添加以包含多种类型的消息。例如，输入 3 表示上传错误消息 (1) 和警告消息 (2)。输入 7 表示上传错误消息 (1)、警告消息 (2) 和信息消息 (4)。

将自定义日志（任何基于文本的日志文件）发送到 CloudWatch Logs

1. 在 JSON 文件中，找到 CustomLogs 部分。

```
{  
    "Id": "CustomLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\CustomLogs\\",  
        "TimestampFormat": "MM/dd/yyyy HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "Local",  
        "LineCount": "5"  
    }  
},
```

2. 在 LogDirectoryPath 参数中，输入日志在实例上的存储路径。
3. 在 TimestampFormat 参数中，输入要使用的时间戳格式。有关支持的值的列表，请参阅 MSDN 上的[自定义日期和时间格式字符串](#)主题。



Important

源日志文件必须在每个日志行开头具有时间戳，且时间戳后必须有一个空格。

4. 在 Encoding 参数中，输入要使用的文件编码（例如 UTF-8）。有关支持的值的列表，请参阅 MSDN 上的[Encoding](#)类主题。



Note

使用编码名称（而不是显示名称）作为此参数的值。

- 5.（可选）在 Filter 参数中，输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表，请参阅 MSDN 上的[FileSystemWatcherFilter 属性](#)主题。
- 6.（可选）在 CultureName 参数中，输入在其中记录时间戳的区域设置。如果 CultureName 为空，则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表，请参阅 MSDN 上的[区域语言支持 \(NLS\) API 参考](#)主题。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

7. (可选) 在 TimeZoneKind 参数中 , 输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息 , 则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息 , 则忽略此参数。
8. (可选) 在 LineCount 参数中 , 在标头中输入行数以识别日志文件。例如 , IIS 日志文件拥有几乎相同的标头。您可以输入 5 , 系统会读取日志文件标头的前三行以进行识别。在 IIS 日志文件中 , 第三行为日期和时间戳 , 但无法始终保证时间戳在日志文件之间是不同的。为此 , 建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

将 IIS 日志数据发送到 CloudWatch Logs

1. 在 JSON 文件中 , 找到 IISLog 部分。

```
{  
    "Id": "IISLogs",  
    "FullName": "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",  
    "Parameters": {  
        "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\W3SVC1",  
        "TimestampFormat": "yyyy-MM-dd HH:mm:ss",  
        "Encoding": "UTF-8",  
        "Filter": "",  
        "CultureName": "en-US",  
        "TimeZoneKind": "UTC",  
        "LineCount": "5"  
    }  
},
```

2. 在 LogDirectoryPath 参数中 , 输入为单个站点存储 IIS 日志的文件夹 (例如 C:\\inetpub\\logs\\LogFiles\\W3SVC1) 。



Note

仅支持 W3C 日志格式。不支持 IIS、NCSA 和自定义格式。

3. 在 TimestampFormat 参数中 , 输入要使用的时间戳格式。有关支持的值的列表 , 请参阅 MSDN 上的 [自定义日期和时间格式字符串](#) 主题。
4. 在 Encoding 参数中 , 输入要使用的文件编码 (例如 UTF-8) 。有关支持的值的列表 , 请参阅 MSDN 上的 [Encoding](#) 类主题。



Note

使用编码名称 (而不是显示名称) 作为此参数的值。

5. (可选) 在 Filter 参数中 , 输入日志名称的前缀。将此参数留空以监控所有文件。有关支持的值的列表 , 请参阅 MSDN 上的 [FileSystemWatcherFilter 属性](#) 主题。
6. (可选) 在 CultureName 参数中 , 输入在其中记录时间戳的区域设置。如果 CultureName 为空 , 则它默认为您 Windows 实例当前所使用的相同区域位置。有关支持的值的列表 , 请参阅 MSDN 上的 [区域语言支持 \(NLS\) API 参考](#) 主题。



Note

不支持 div、div-MV、hu 和 hu-HU 值。

7. (可选) 在 TimeZoneKind 参数中 , 输入 Local 或 UTC。可以设置此参数以在日志时间戳中不包含时区信息时提供时区信息。如果此参数留空且时间戳不包括时区信息 , 则 CloudWatch Logs 默认为本地时区。如果时间戳已包含时区信息 , 则忽略此参数。
8. (可选) 在 LineCount 参数中 , 在标头中输入行数以识别日志文件。例如 , IIS 日志文件拥有几乎相同的标头。您可以输入 5 , 系统会读取日志文件标头的前五行以进行识别。在 IIS 日志文件中 , 第三行为日期和时间戳 , 但无法始终保证时间戳在日志文件之间是不同的。为此 , 建议包含至少一行实际日志数据以便对日志文件进行唯一指纹识别。

配置流程控制

要将性能计数器数据发送到 CloudWatch 或将日志数据发送到 CloudWatch Logs , 每种数据类型都必须在 Flows 部分中列出对应目标。例如 , 要将在 JSON 文件的 "Id": "PerformanceCounter" 部分中定义的性能计数器发送到在 JSON 文件的 "Id": "CloudWatch" 部分定义的 CloudWatch 目标 , 应在 Flows 部分输入 "PerformanceCounter,CloudWatch"。同样 , 要将自定义日志、ETW 日志和系统日志发送到 CloudWatch Logs , 会输入 "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs"。此外 , 还可以将相同性能计数器或日志文件发送到多个目标。例如 , 要将应用程序日志发送到在 JSON 文件的 "Id": "CloudWatchLogs" 部分定义的两个不同目标 , 应在 Flows 部分输入 "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"。

1. 在 JSON 文件中 , 找到 Flows 部分。

```
"Flows": {  
    "Flows": [  
        "PerformanceCounter,CloudWatch",  
        "(PerformanceCounter,PerformanceCounter2), CloudWatch2",  
        "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs",  
        "CustomLogs, CloudWatchLogs2",  
        "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"  
    ]  
}
```

2. 在 Flows 参数中 , 输入要上传的每种数据类型 (例如 ApplicationEventLog) 以及要将它发送到的目标 (例如 CloudWatchLogs) 。

使用 Run Command 将日志上传到 Amazon CloudWatch



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令 , 请参阅 [在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 将日志上传到 Amazon CloudWatch

1. 打开 [Amazon EC2 控制台](#) , 并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中 , 选择 AWS-ConfigureCloudWatch。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表 , 则可能不会为 Run Command 正确配置缺少的实例。有关更多信息 , 请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. (可选) 在 Status 列表中 , 选择 Enable 将实例配置为将日志上传到 CloudWatch。选择 Disabled 将实例配置为停止向 CloudWatch 发送日志。
6. 将 JSON 示例复制并粘贴到 Properties 字段中。

7. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

8. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
9. 在 S3 bucket 字段中，键入要在其中存储命令输出的 AWS S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

10. 在 S3 key prefix 字段中，键入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

要了解有关 Amazon CloudWatch 的更多信息，请参阅[什么是 Amazon CloudWatch ?](#)

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 启用或禁用 Windows 更新

您可使用 AWS-ConfigureWindowsUpdate 文档对实例启用或禁用自动 Windows 更新。此命令将 Windows 更新代理配置为在您指定的日期和时间下载并安装 Windows 更新。如果更新需要重启，计算机将在安装更新 15 分钟后自动重启。利用此命令，您还可以将 Windows 更新配置为检查更新但不安装更新。AWS-ConfigureWindowsUpdate 文档可与 Windows Server 2008、2008 R2、2012 和 2012 R2 兼容。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Command 运行启用或禁用 Windows 更新

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-ConfigureWindowsUpdate。

4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 在 Update Level 列表中，选择 InstallUpdatesAutomatically 以使 Windows 自动下载和安装更新。如果更新需要重启，计算机将在安装更新 15 分钟后自动重启。或选择 NeverCheckForUpdates。如果选择此选项，Windows 绝不会检查或下载更新。



Important

如果选择 NeverCheckForUpdates，请注意，如果您不手动安装重要更新（例如，安全更新），则您的系统可能变得易受恶意攻击。

6. 在 Scheduled Install Day 字段中，选择您希望 Windows 在星期几下载和安装更新。这仅在选择 InstallUpdatesAutomatically 选项时适用。
7. 在 Scheduled Install Time 字段中，选择您希望 Windows 下载和安装更新的时间。这仅在选择 InstallUpdatesAutomatically 选项时适用。
- 8.（可选）在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

- 9.（可选）在 Execution Timeout 字段中，键入 EC2Config 服务在超时前将尝试运行命令的秒数。
- 10.（可选）在 Day 列表中，选择您希望系统在星期几下载和安装更新。
11. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
12. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅 [创建存储桶](#)。

13. 在 S3 key prefix 字段中，键入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅 [在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅 [使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#) 或 [适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅 [SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 更新 EC2Config 服务

您可使用 AWS-UpdateEC2Config 文档更新在实例上运行的 EC2Config 服务。您可以更新到最新版本或降级到较旧版本。在执行命令时，系统将从 AWS 下载并安装需要的版本，然后卸载运行命令前存在的版本。如果此过程中出现错误，系统将回滚到命令运行之前服务器上的版本，并且命令状态将显示命令失败。



Note

使用 Run Command 更新 EC2Config 服务仅在实例运行 EC2Config 服务版本 3.10.442 或更高版本时受支持。

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 更新 EC2Config 服务

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-UpdateEC2Config。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. (可选) 在 Version 字段中，输入要安装的 EC2Config 服务的特定版本。您可以安装服务的较旧版本。如果您不指定版本，服务将更新至最新版本。
6. (可选) 如果您要安装 EC2Config 服务的早期版本，可在 Allow downgrade 列表中，选择 True。如果您选择此选项，则必须指定早期版本号。如果您希望系统仅安装服务的最新版本，请选择 False。
7. (可选) 在 Comment 字段中，输入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

8. 在 Timeout (seconds) 字段中，输入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
9. 在 S3 bucket 字段中，输入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

10. 在 S3 key prefix 字段中，输入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 清查适用于 Windows 的 Amazon EC2 实例

您可使用 AWS-ListWindowsInventory 文档收集有关在 Windows 中运行的 Amazon EC2 实例的信息。该命令将返回以下信息：

- 操作系统版本、语言和详细信息
- 已安装的应用程序
- 已安装的系统更新



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 清查 EC2 实例

1. 打开[Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 AWS-ListWindowsInventory。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 选择要在命令中执行的列表选项。有关这些选项的详细信息，请查看工具提示帮助。
6. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

7. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
8. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

9. 在 S3 key prefix 字段中，输入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

使用 Amazon EC2 Run Command 管理 EC2 Windows 实例的更新

Run Command 包含三个文档，可帮助您管理 EC2 Windows 实例的更新。

AWS-FindWindowsUpdates

扫描实例并确定缺少的更新。

AWS-InstallMissingWindowsUpdates

在 EC2 实例上安装缺少的更新。

AWS-InstallSpecificWindowsUpdates

安装一个或多个特定更新。



Note

此过程不包括有关如何为 Amazon SNS 通知配置 Run Command 的信息。要了解有关 Command History 页面上的 Amazon SNS 通知字段的更多信息以及如何执行返回通知的命令，请参阅[在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)。

使用 Run Command 管理 EC2 实例的更新

1. 打开[Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择要使用的文档。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅[Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 选择要在命令中执行的更新和 KB 选项。有关这些选项的详细信息，请查看工具提示帮助。
6. (可选) 在 Comment 字段中，键入要提供的有关此命令的信息。注释存储在日志文件中，并显示在 Amazon EC2 控制台中的命令调用列表中。



Tip

建议您输入有关您运行的每个命令的特定注释。发送的命令的列表可能会快速增大，Comment 字段可帮助您识别要监视的命令。

7. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。最小值为 30 秒。最大值为 30 天。默认值为 10 分钟。
8. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。



Important

Amazon EC2 控制台中的 Run Command Output 页面将在 2500 个字符后截断输出。在使用 Run Command 执行命令之前，请配置 Amazon S3 存储桶。如果命令输出超过 2500 个字符，您可在 Amazon S3 存储桶中查看完整输出。有关更多信息，请参阅[创建存储桶](#)。

9. 在 S3 key prefix 字段中，输入 Amazon S3 存储桶中的子文件夹的名称。该子文件夹可帮助您组织 Run Command 输出。



Note

名为 AWS Command Line Interface command 的部分显示了根据您输入的参数生成的可用 CLI 脚本。

有关如何查看命令的结果的信息，请参阅[在 Amazon EC2 控制台中查看命令输出 \(p. 366\)](#)。

有关如何使用 Windows PowerShell 运行命令的信息，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 运行命令的信息，请参阅[SSM CLI 参考](#)。

在 Amazon EC2 控制台中查看命令输出

使用 Run Command 执行命令后，系统将返回命令列表。



Important

Amazon EC2 控制台将截断 2500 个字符后的所有命令输出。如果命令输出超过 2500 个字符，您可在 S3 存储桶中查看完整输出。

查看命令输出

1. 在 Amazon EC2 控制台中，选择列表中的一个命令。
2. 选择 Output 选项卡。
3. 选择 View Output。

The screenshot shows the AWS Lambda console interface. At the top, there are buttons for "Run a command" and "Actions". Below that is a search bar labeled "Filter by attributes". A table lists three command executions:

Command ID	Instance ID	Document name	Status	Requested date	Comment
ca4b10c6-cee1-437...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	getting list of proce...
561e5f4a-27d2-419...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	ipconfig on the bo...
d5b589e6-ad94-4d...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	Getting services on...

Below the table, it says "Command ID: ca4b10c6-cee1-437b-9f70-9746da1477e7 Instance ID: i-d583f76a". There are tabs for "Description" and "Output", with "Output" being selected. The output section shows a table with one row:

Plugin name	Status	Response code	Start Time	Finish Time	Output
aws.runPower...	Success	0	October 20, 2015 at 4:15:58 PM...	October 20, 2015 at 4:15:59 PM...	View Output

4. 命令输出页面将显示命令执行的结果。

The screenshot shows a table titled "Output for aws:runPowerShellScript". The table has columns: Handles, NPM (K), PM (K), WS (K), VM (M), CPU (s), Id, and ProcessName. The data is as follows:

Handles	NPM (K)	PM (K)	WS (K)	VM (M)	CPU (s)	Id	ProcessName
40	4	612	2752	27	0.00	2900	conhost
194	11	1712	3776	46	0.06	520	csrss
86	8	1236	3576	43	0.08	584	csrss
209	11	1700	21036	66	2.06	880	csrss
173	14	10764	1608	88	0.03	872	dwm
208	25	23216	45228	164	0.58	2560	dwm
836	63	47216	21880	643	24.92	2276	Ec2Config
1344	64	52420	108976	495	11.92	2776	explorer
0	0	0	4	0		0	Idle
105	8	1196	4844	33	0.02	1176	LiteAgent
268	21	12692	24108	138	0.08	2148	LogonUI
797	18	4336	10892	40	0.72	688	lsass
159	12	2108	3760	41	0.02	2888	msdtc
362	23	56848	53412	593	0.30	3688	powershell
219	11	1976	9600	87	0.28	732	rdpclip
650	48	108564	105064	773	4.58	3472	ServerManager
209	10	2420	7148	25	2.27	680	services
55	2	276	1048	4	0.03	436	smss
424	23	4536	12124	91	1.94	1148	spoolsv

At the bottom of the table, it says "Output truncated".

创建 SSM 文档

在使用 Amazon EC2 Run Command 执行命令时，系统将从定义要运行的插件和要使用的参数的文档中读取要执行的操作。此文档称为 SSM 文档。首次从新的 SSM 文档执行命令时，系统将使用您的 AWS 账户存储此文档。

限制

在开始使用 SSM 文档时，请注意下列限制。

- 对于每个 AWS 账户，您最多可创建 200 个 SSM 文档。
- 您创建的 SSM 文档仅在其创建区域中可用。要添加其他区域中的文档，请复制内容并在新区域中重新创建文档。



Note

如果您需要创建超出最大数量的 SSM 文档，请联系 AWS Support。

在为用户提供对 Run Command 的访问权限时，最佳实践是从具有最小权限的策略开始。创建允许用户执行最低数量任务的其他 SSM 文档。例如，您可以创建支持用户执行以下类型的操作的 SSM 文档：安装特定应用程序、重置 Internet Information Services (IIS) 或查看正在运行的服务或进程的列表。有关更多信息，请参阅[示例 SSM 文档 \(p. 369\)](#)。

使用 Amazon EC2 控制台创建 SSM 文档

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Documents，然后选择 Create Document。
3. 输入文档的描述性名称，然后在 Content 字段中使用 JSON 格式指定插件和参数。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 中的 [SSM 插件](#)。
4. 选择 Create Document 以将文档保存在您的 AWS 用户账户中。

使用 Windows PowerShell 创建 SSM 文档

1. 在一个文件中指定插件和参数。使用描述性名称和 .json 文件扩展名保存此文档。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 中的 [SSM 插件](#)。
2. 使用适用于 Windows PowerShell 的 AWS 工具创建文档并将其保存在您的 AWS 用户账户中。

```
$json = Get-Content C:\your_file | Out-String  
New-SSMDocument -Name document_name -Content $json
```

使用 AWS CLI 创建 SSM 文档

1. 在一个文件中指定插件和参数。使用描述性名称和 .json 文件扩展名保存此文档。有关更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 中的 [SSM 插件](#)。
2. 使用 AWS CLI 创建文档并将其保存在 AWS 用户账户中。

```
aws ssm create-document --content file://c:\temp\your_file --name "document_name"
```

示例 SSM 文档

SSM 文档当前在 JavaScript 对象表示法 (JSON) 中受支持并且使用以下项：

- schemaVersion 1.2
- 使用一个或多个插件执行任务的 runtimeConfig。插件是特定于平台的，这意味着它们可在支持的 Microsoft Windows 或 Linux 版本上运行。有关插件的更多信息，请参阅 *Amazon EC2 Simple Systems Manager API Reference* 中的 [SSM 插件](#)。

使用以下示例作为基础来创建您自己的文档。

适用于 Windows 的限制性 SSM 文档

以下示例显示在 Windows 上使用 AWS-RunPowerShellScript 文档的高限制性 SSM 文档。用户只能运行 ipconfig 命令来检查实例的 IP 配置：

```
{  
    "schemaVersion": "1.2",  
    "description": "Run ipconfig on the instance.",  
    "parameters": {  
        },  
    "runtimeConfig": {  
        "aws:runPowerShellScript": {  
            "properties": [  
                {  
                    "id": "0.aws:runPowerShellScript",  
                    "runCommand": ["ipconfig"],  
                    "workingDirectory": "",  
                    "timeoutSeconds": ""  
                }  
            ]  
        }  
    }  
}
```

您可使用下列 JSON 模板创建您自己的 SSM 文档。这些模板基于 AWS 公有 SSM 文档。

AWS-RunPowerShellScript

```
{  
    "schemaVersion": "1.2",  
    "description": "Run a PowerShell script or specify the paths to scripts to run.",  
    "parameters": {  
        "commands": {  
            "type": "StringList",  
            "description": "(Required) Specify the commands to run or the paths to existing scripts on the instance.",  
            "minItems": 1,  
            "displayType": "textarea"  
        },  
        "workingDirectory": {  
            "type": "String",  
            "default": ""  
        }  
    }  
}
```

```
        "description": "(Optional) The path to the working directory on your
instance.",
        "maxChars": 4096
    },
    "executionTimeout": {
        "type": "String",
        "default": "3600",
        "description": "(Optional) The time in seconds for a command to be
completed before it is considered to have failed. Default is 3600 (1 hour).
Maximum is 28800 (8 hours).",
        "allowedPattern": "([1-9][0-9]{0,3})|(1[0-9]{1,4})|(2[0-7][0-
9]{1,3})|(28[0-7][0-9]{1,2})|(28800)"
    }
},
"runtimeConfig": {
    "aws:runPowerShellScript": {
        "properties": [
            {
                "id": "0.aws:runPowerShellScript",
                "runCommand": "{{ commands }}",
                "workingDirectory": "{{ workingDirectory }}",
                "timeoutSeconds": "{{ executionTimeout }}"
            }
        ]
    }
}
}
```

AWS-ConfigureCloudWatch

```
{
    "schemaVersion": "1.2",
    "description": "Export metrics and log files from your instances to Amazon
cloudWatch.",
    "parameters": {
        "status": {
            "type": "String",
            "default": "Enabled",
            "description": "(Optional) Enable or disable CloudWatch. Valid values:
Enabled | Disabled",
            "allowedValues": [
                "Enabled",
                "Disabled"
            ]
        },
        "properties": {
            "type": "String",
            "default": "",
            "description": "(Optional) The configuration for CloudWatch in JSON
format. Learn more at http://docs.aws.amazon.com/ssm/latest/APIReference/aws-
cloudWatch.html",
            "displayType": "textarea"
        }
    },
    "runtimeConfig": {
        "aws:cloudWatch": {
            "settings": {

```

```
        "startType": "{{ status }}"
    },
    "properties": "{{ properties }}"
}
}
```

AWS-JoinDirectoryServiceDomain

```
{
    "schemaVersion": "1.2",
    "description": "Join your instances to an AWS Directory Service domain.",
    "parameters": {
        "directoryId": {
            "type": "String",
            "description": "(Required) The ID of the AWS Directory Service directory."
        },
        "directoryName": {
            "type": "String",
            "description": "(Required) The name of the directory; for example, test.example.com"
        },
        "directoryOU": {
            "type": "String",
            "default": "",
            "description": "(Optional) The Organizational Unit (OU) and Directory Components (DC) for the directory; for example, OU=test,DC=example,DC=com"
        },
        "dnsIpAddresses": {
            "type": "StringList",
            "default": [
            ],
            "description": "(Optional) The IP addresses of the DNS servers in the directory. Required when DHCP is not configured. Learn more at ht tp://docs.aws.amazon.com/directoryservice/latest/simple-ad/join\_get\_dns\_addresses.html" ,
            "allowedPattern": "((25[0-5]|2[0-4][0-9]|0[1]?[0-9][0-9]?)\.\{3\}(25[0-5]|2[0-4][0-9]|0[1]?[0-9][0-9]?)"
        }
    },
    "runtimeConfig": {
        "aws:domainJoin": {
            "properties": {
                "directoryId": "{{ directoryId }}",
                "directoryName": "{{ directoryName }}",
                "directoryOU": "{{ directoryOU }}",
                "dnsIpAddresses": "{{ dnsIpAddresses }}"
            }
        }
    }
}
```

AWS-InstallPowerShellModule

```
{  
    "schemaVersion": "1.2",  
    "description": "Deploy and install PowerShell modules.",  
    "parameters": {  
        "workingDirectory": {  
            "type": "String",  
            "default": "",  
            "description": "(Optional) The path to the working directory on your instance.",  
            "maxChars": 4096  
        },  
        "source": {  
            "type": "String",  
            "description": "(Optional) The URL or local path on the instance to the application .zip file."  
        },  
        "sourceHash": {  
            "type": "String",  
            "default": "",  
            "description": "(Optional) The SHA256 hash of the zip file."  
        },  
        "commands": {  
            "type": "StringList",  
            "default": [  
            ],  
            "description": "(Optional) Specify PowerShell commands to run on your instance.",  
            "displayType": "textarea"  
        },  
        "executionTimeout": {  
            "type": "String",  
            "default": "3600",  
            "description": "(Optional) The time in seconds for a command to be completed before it is considered to have failed. Default is 3600 (1 hour). Maximum is 28800 (8 hours).",  
            "allowedPattern": "([1-9][0-9]{0,3})|(1[0-9]{1,4})|(2[0-7][0-9]{1,3})|(28[0-7][0-9]{1,2})|(28800)"  
        }  
    },  
    "runtimeConfig": {  
        "aws:psModule": {  
            "properties": [  
                {  
                    "id": "0.aws:psModule",  
                    "runCommand": "{{ commands }}",  
                    "source": "{{ source }}",  
                    "sourceHash": "{{ sourceHash }}",  
                    "workingDirectory": "{{ workingDirectory }}",  
                    "timeoutSeconds": "{{ executionTimeout }}"  
                }  
            ]  
        }  
    }  
}
```

AWS-InstallApplication

```
{  
    "schemaVersion": "1.2",  
    "description": "Install, repair, or uninstall an application using an .msi  
file.",  
    "parameters": {  
        "action": {  
            "type": "String",  
            "default": "Install",  
            "description": "(Optional) The type of action to perform. Valid  
values: Install | Repair | Uninstall",  
            "allowedValues": [  
                "Install",  
                "Repair",  
                "Uninstall"  
            ]  
        },  
        "parameters": {  
            "type": "String",  
            "default": "",  
            "description": "(Optional) The parameters for the installer."  
        },  
        "source": {  
            "type": "String",  
            "description": "(Required) The URL or local path on the instance to  
the application .msi file."  
        },  
        "sourceHash": {  
            "type": "String",  
            "default": "",  
            "description": "(Optional) The SHA256 hash of the .msi file."  
        }  
    },  
    "runtimeConfig": {  
        "aws:applications": {  
            "properties": [  
                {  
                    "id": "0.aws:applications",  
                    "action": "{{ action }}",  
                    "parameters": "{{ parameters }}",  
                    "source": "{{ source }}",  
                    "sourceHash": "{{ sourceHash }}"  
                }  
            ]  
        }  
    }  
}
```

共享 SSM 文档

您可私下或公开共享 Amazon EC2 Simple Systems Manager (SSM) 文档。要私下共享 SSM 文档，请修改文档权限并允许特定个人根据其 Amazon Web Services (AWS) ID 访问文档。要公开共享 SSM 文档，请修改文档权限并指定 All。



Warning

请仅使用从可信来源获取的共享 SSM 文档。使用任何共享文档时，请务必在使用前仔细查看文件内容，了解它会如何更改您的实例配置。有关共享文档最佳实践的更多信息，请参阅 [共享 SSM 文档的共享和使用指南 \(p. 374\)](#)。

限制

在开始使用 SSM 文档时，请注意下列限制。

- 仅所有者可共享文档。
- 您必须先停止共享文档，然后才能删除它。有关更多信息，请参阅 [如何修改共享文档的权限 \(p. 377\)](#)。
- 您最多可与 20 个 AWS 账户共享一个文档。
- 您可公开共享最多 5 个 SSM 文档。



Note

如果您需要与超出最大数量的 AWS 账户共享或共享超出最大数量的 SSM 文档，请联系 AWS Support。

本主题包括下列部分。

- [共享 SSM 文档的共享和使用指南 \(p. 374\)](#)
- [如何共享 SSM 文档 \(p. 375\)](#)
- [如何修改共享文档的权限 \(p. 377\)](#)
- [如何使用共享的 SSM 文档 \(p. 377\)](#)

共享 SSM 文档的共享和使用指南

在共享或使用共享文档之前，请阅读以下指南。

删除敏感信息

请仔细审查您的 SSM 文档并删除任何敏感信息。例如，请确保文档不包含您的 AWS 凭证。如果您与特定个人共享文档，这些用户可查看文档中的信息。如果您公开共享文档，则任何人都可查看文档中的信息。

使用 IAM 用户信任策略限制 Run Command 操作

为将有权访问文档的用户创建限制性 AWS Identity and Access Management (IAM) 用户策略。此 IAM 策略确定用户可在 Amazon EC2 控制台中查看或通过使用 AWS CLI 或适用于 Windows PowerShell 的 AWS 工具调用 `ListDocuments` 查看的 SSM 文档。该策略还限制用户可使用 SSM 文档执行的操作。您可创建限制性策略，以便用户只能使用特定文档。有关更多信息，请参阅 [委派对 Amazon EC2 Run Command 的访问权限 \(p. 338\)](#)。

在使用共享文档之前审查其内容

审查与您共享的每个文档（特别是公开文档）的内容，以了解将在您的实例上执行的命令。一个文档在运行后可能会有意或无意具有负面影响。如果文档引用外部网络，请在使用文档前审查外部源。

使用文档哈希发送命令

在共享文档时，系统将创建 Sha-256 哈希并将其分配给文档。系统还将保存文档内容的快照。使用共享文档发送命令时，您可在命令中指定哈希以确保下列条件为 true：

- 您正在从正确的 SSM 文档执行命令
- 在与您共享之后文档内容未更改。

如果哈希与指定文档不匹配，或者共享文档的内容已更改，则命令将返回 `InvalidDocument` 异常。请注意：哈希无法验证来自外部位置的文档内容。

如何共享 SSM 文档

您可通过使用 Amazon EC2 控制台或通过使用 AWS CLI、适用于 Windows PowerShell 的 AWS 工具或 AWS SDK，以编程方式调用 `ModifyDocumentPermission` API 操作来共享 SSM 文档。在共享文档之前，获取要与之共享文档的人的 AWS 账户 ID。您将在共享文档时指定这些账户 ID。

使用 Amazon EC2 控制台共享文档

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Documents。
3. 在文档列表中，选择要共享的文档。选择 Permissions 选项卡并确保您是文档所有者。只有文档所有者才可共享文档。
4. 选择 Edit。
5. 要公开共享命令，请选择 Public，然后选择 Save。要私下共享命令，请选择 Private，输入 AWS 账户 ID，选择 Add Permission，然后选择 Save。

使用 AWS CLI 共享文档

以下步骤需要您为您的 CLI 会话指定区域。目前，Run Command 在以下 SSM 区域提供。

1. 在本地计算机上打开 AWS CLI 并执行以下命令来指定凭证。

```
aws config

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

2. 使用以下命令列出可供您使用的所有 SSM 文档。此列表包括您已创建的文档和与您共享的文档。

```
aws ssm list-documents --document-filter-list key=Owner,value=all
```

3. 使用以下命令获取特定文档。

```
aws ssm get-document --name document name
```

4. 使用以下命令获取文档的描述。

```
aws ssm describe-document --name document name
```

5. 使用以下命令查看文档的权限。

```
aws ssm describe-document-permission --name document name --permission-type Share
```

6. 使用以下命令修改文档的权限并共享文档。您必须是文档的所有者才能编辑权限。此命令与特定个体基于其 AWS 账户 ID 私下共享文档。

```
aws ssm modify-document-permission --name document name --permission-type Share --account-ids-to-add AWS account ID
```

使用以下命令公开共享文档。

```
aws ssm modify-document-permission --name document name --permission-type Share --account-ids-to-add 'all'
```

使用适用于 Windows PowerShell 的 AWS 工具共享文档

以下步骤需要您为您的 PowerShell 会话指定区域。目前，Run Command 在以下 SSM 区域提供。

1. 在您的本地计算机上打开适用于 Windows PowerShell 的 AWS 工具并执行以下命令来指定凭证。

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

2. 使用以下命令为 PowerShell 会话设置区域。此示例使用 us-west-2 区域。

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

3. 使用以下命令列出可供您使用的所有 SSM 文档。此列表包括您已创建的文档和与您共享的文档。

```
Get-SSMDocumentList -DocumentFilterList (@{ "key" = "Owner" ; "value" = "All" })
```

4. 使用以下命令获取特定文档。

```
Get-SSMDocument -Name document name
```

5. 使用以下命令获取文档的描述。

```
Get-SSMDocumentDescription -Name document name
```

6. 使用以下命令查看文档的权限。

```
Get-SSMDocumentPermission -Name document name -PermissionType Share
```

7. 使用以下命令修改文档的权限并共享文档。您必须是文档的所有者才能编辑权限。此命令与特定个体基于其 AWS 账户 ID 私下共享文档。

```
Edit-SSMDocumentPermission -Name document name -PermissionType Share -AccountIdsToAdd AWS account ID
```

使用以下命令公开共享文档。

```
Edit-SSMDocumentPermission -Name document name -AccountIdsToAdd ('all') -PermissionType Share
```

如何修改共享文档的权限

如果您共享一条命令，则在您删除对 SSM 文档的访问权限或删除 SSM 文档之前，用户可查看和使用该命令。但是，只要文档已共享，您就无法删除它。您必须先停止共享，然后再删除它。

使用 Amazon EC2 控制台停止共享文档

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Documents。
3. 在文档列表中，选择要停止共享的文档。选择 Permissions 选项卡并确保您是文档所有者。只有文档所有者才可停止共享文档。
4. 选择 Edit。
5. 删除不应再具有此命令的访问权限的 AWS 账户 ID，然后选择 Save。

使用 AWS CLI 停止共享文档

在本地计算机上打开 AWS CLI，然后执行以下命令停止共享命令。

```
aws ssm modify-document-permission --name document name --permission-type Share  
--account-ids-to-remove 'AWS account ID'
```

使用适用于 Windows PowerShell 的 AWS 工具停止共享文档

在您的本地计算机上打开适用于 Windows PowerShell 的 AWS 工具并执行以下命令停止共享命令。

```
Edit-SSMDocumentPermission -Name document name -AccountIdsToRemove AWS account ID -PermissionType Share
```

如何使用共享的 SSM 文档

共享 SSM 文档时，系统将生成一个 Amazon 资源名称 (ARN) 并将其分配给命令。如果您从 Amazon EC2 控制台选择并执行共享文档，则不会看到此 ARN。但如果要从命令行应用程序执行共享 SSM 文档，则必须指定完整的 ARN。当您执行命令以列出文档时，将为您显示 SSM 文档的完整 ARN。



Note

您无需为 AWS 公有文档（以 AWS-* 开头的文档）或您拥有的命令指定 ARN。

本节包含有关如何通过 AWS CLI 和适用于 Windows PowerShell 的 AWS 工具查看和执行共享 SSM 文档的示例。

通过 AWS CLI 使用共享 SSM 文档

列出所有公有 SSM 文档

```
aws ssm list-documents --document-filter-list key=Owner,value=Public
```

列出已与您共享的私有 SSM 文档

```
aws ssm list-documents --document-filter-list key=Owner,value=Private
```

列出可供您使用的所有 SSM 文档

```
aws ssm list-documents --document-filter-list key=Owner,value>All
```

使用完整 ARN 通过共享 SSM 文档执行命令

```
aws ssm send-command --document-name FullARN/name
```

例如：

```
aws ssm send-command --document-name arn:aws:ssm:us-east-1:12345678912:document/highAvailabilityServerSetup --instance-ids i-12121212
```

通过适用于 Windows PowerShell 的 AWS 工具使用共享 SSM 文档

列出所有公有 SSM 文档

```
Get-SSMDocumentList -DocumentFilterList @(New-Object Amazon.SimpleSystemsManagement.Model.DocumentFilter("Owner", "Public"))
```

列出已与您共享的私有 SSM 文档

```
Get-SSMDocumentList -DocumentFilterList @(New-Object Amazon.SimpleSystemsManagement.Model.DocumentFilter("Owner", "Shared"))
```

获取有关已与您共享的 SSM 文档的信息

```
Get-SSMDocument -Name FullARN/name
```

例如：

```
Get-SSMDocument -Name arn:aws:ssm:us-east-1:12345678912:document/highAvailabilityServerSetup
```

获取已与您共享的 SSM 文档的描述

```
Get-SSMDocumentDescription -Name FullARN/name
```

例如：

```
Get-SSMDocumentDescription -Name arn:aws:ssm:us-east-1:12345678912:document/highAvailabilityServerSetup
```

使用完整 ARN 通过共享 SSM 文档执行命令

```
Send-SSMCommand -DocumentName FullARN/name -InstanceId IDs
```

例如：

```
Send-SSMCommand -DocumentName arn:aws:ssm:us-east-1:555450671542:document/highAvailabilityServerSetup -InstanceId @{"i-273d4e9e"}
```

Amazon EC2 Run Command 演练

以下示例或演练可帮助您了解如何使用 Run Command 从 Amazon EC2 控制台或适用于 Windows PowerShell 的 AWS 工具执行命令。



Caution

如果这是您第一次使用 Run Command，建议您对测试实例或未在生产环境中使用的实例执行命令。

内容

- [使用控制台的 Amazon EC2 Run Command 演练 \(p. 379\)](#)
- [使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)

使用控制台的 Amazon EC2 Run Command 演练

以下示例演练说明如何从 Amazon EC2 控制台中的 Command History 页面使用 Run Command 执行命令。此示例说明如何使用 AWS-RunPowerShellScript SSM JSON 文档执行命令。有关 PowerShell 示例，请参阅[使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)。

从控制台使用 Run Command 执行命令

1. 在 [Amazon EC2 控制台](#) 中，选择导航窗格中的 Command History，然后选择 Run a Command。

Command ID	Instance ID	Document name	Status	Requested date	Comment
ca4b10c6-cee1-437...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	getting list of th...
561e5f4a-27d2-419...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	ipconfig on th...
d5b589e6-ad94-4d...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	Getting serv...

2. 在 Command document 列表中，选择 AWS-RunPowerShellScript。

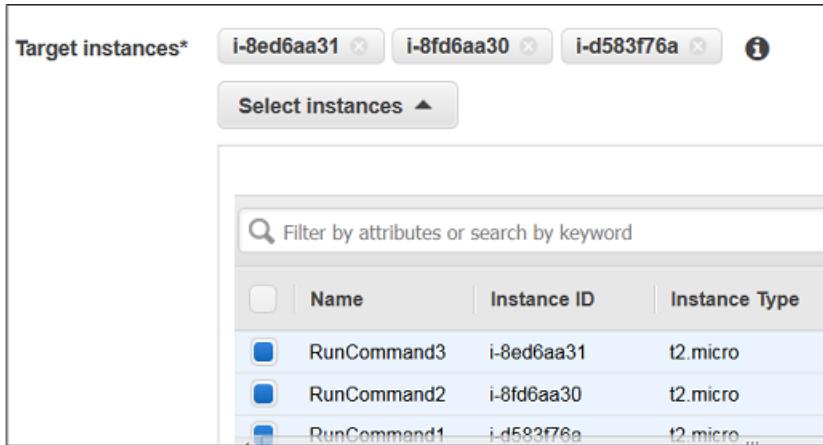
Run a command

A command document includes the information about the command you want to run. Select a command document from the dropdown menu.

Command document* AWS-RunPowerShellScript

Description Run a PowerShell script or specify the paths to scripts to run.

3. 选择 Select instances，然后选择要在其中执行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。



4. 在 Commands 字段中，键入有效的 PowerShell 命令或 PowerShell 脚本文件的路径。如果需要，您可以指定 Working Directory 和 Execution Timeout。Execution Timeout 是 EC2Config 服务在被视为已失败前将尝试运行命令的秒数。建议您在 Comments 字段中输入注释。注释将帮助您识别待处理命令列表中的命令并让查看输出变得更容易。

Commands*	Get-Service
Working Directory	
Execution Timeout	3600
Comment	Listing services on Run Command instances

5. 在 Timeout (seconds) 字段中，键入在实例被视为无法访问且命令执行失败之前，Run Command 应尝试连接实例的秒数。
6. 在 S3 bucket 字段中，键入要在其中存储命令输出的 Amazon S3 存储桶的名称。在 S3 key prefix 字段中，输入 Amazon S3 子文件夹。如果您正在对多个实例执行多个命令，子文件夹可帮助您组织输出。

Timeout (seconds)	600	i
S3 bucket	run-command-test	i
S3 key prefix	RC_Test_User	i

7. 选择 Run 同时对所选实例执行命令。Run Command 将显示一个状态屏幕。
8. 选择 View results。

Run a command

Success
We are running your command against the instances listed below.

Instance IDs i-8ed6aa31, i-8fd6aa30, i-d583f76a

Command ID 65555b90-ee60-4520-9dc3-e42e94445469

命令列表显示命令的三个调用，因为命令已发送到三个实例。每个调用拥有其自己的 Command ID 和状态。要查看状态，请选择一个调用，再选择该调用的 Output 选项卡，然后选择 View Output。

	Command ID	Instance ID	Document name	Status	Requested date	Comments
<input checked="" type="checkbox"/>	65555b90-ee60-45...	i-8fd6aa30	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	65555b90-ee60-45...	i-d583f76a	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	65555b90-ee60-45...	i-8ed6aa31	AWS-RunPowerSh...	Success	October 21, 2015 at...	Listing
<input type="checkbox"/>	ca4b10c6-cee1-437...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	getting
<input type="checkbox"/>	561ef5fa-27d2-419...	i-d583f76a	AWS-RunPowerSh...	Success	October 20, 2015 at...	ipconfi

Command ID: 65555b90-ee60-4520-9dc3-e42e94445469 Instance ID: i-8fd6aa30

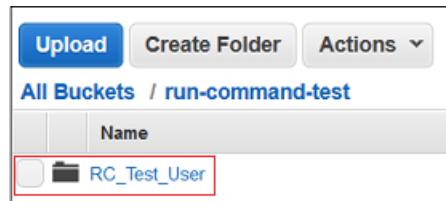
Description Output

Command ID	65555b90-ee60-4520-9dc3-e42e94445469	Instance
Document name	AWS-RunPowerShellScript	Status
Date requested	October 21, 2015 at 3:56:59 PM UTC-7	Comments
Output S3 bucket	run-command-test	Document parameters

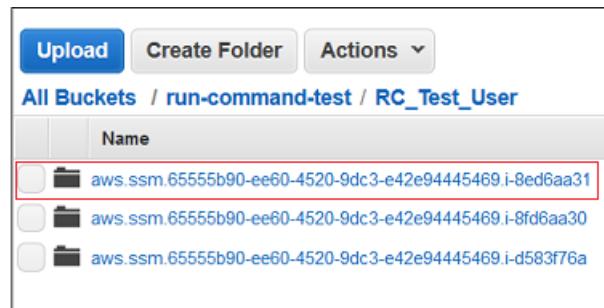
系统将在浏览器中显示输出。如果输出超过 2500 个字符，则仅显示前 2500 个字符，其余字符将被截断。

Commands > Output		
Output for aws:runPowerShellScript		
Status	Name	DisplayName
Stopped	AeLookupSvc	Application Experience
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	AudioEndpointBu...	Windows Audio Endpoint Builder
Stopped	Audiosrv	Windows Audio
Running	AWSLiteAgent	AWS Lite Guest Agent
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Ser...
Running	BrokerInfrastru...	Background Tasks Infrastructure Ser...
Stopped	Browser	Computer Browser
Running	CertPropSvc	Certificate Propagation
Stopped	cfn-hup	CloudFormation cfn-hup
Stopped	COMSysApp	COM+ System Application
Running	CryptSvc	Cryptographic Services
Running	DcomLaunch	DCOM Server Process Launcher
Stopped	defragsvc	Optimize drives
Stopped	DeviceAssociati...	Device Association Service
Stopped	DeviceInstall	Device Install Service
Running	Dhcp	DHCP Client
-----Output truncated-----		

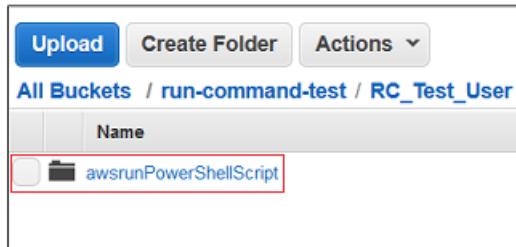
9. 在 Amazon S3 中查看完整命令输出。打开 [Amazon S3 控制台](#) 并选择 Amazon S3 存储桶。



10. 选择 *Command-ID*。要查看其命令输出的 *Instance-ID*。



11. 选择 awsrunShellScript 子文件夹。



12. 选择 stdout.txt 文件。S3 显示完整命令输出。



使用适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练

以下示例说明如何使用 Windows PowerShell 工具 查看有关命令和命令参数的信息、如何执行命令以及如何查看这些命令的状态。本演练为每个预定义的 SSM 文档包含了一个示例。



Tip

控制台中的 Command History 页面包含一个名为 AWS Command Line Interface command 的部分。此部分显示了根据您输入的参数生成的有用 CLI 脚本。

配置适用于 Windows PowerShell 的 AWS 工具 会话设置

在本地计算机上打开 适用于 Windows PowerShell 的 AWS 工具 并执行以下命令来指定凭证。您必须具有要配置的实例的管理员权限或必须已获得 IAM 中的适当权限。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。

```
Set-AWSCredentials -AccessKey key_name -SecretKey key_name
```

执行以下命令设置 PowerShell 会话的区域。该示例使用 us-east-1 区域。目前，Run Command 在以下 SSM 区域 提供。

```
Set-DefaultAWSRegion -Region us-east-1
```

列出所有可用文档

此命令列出对您的账户可用的所有文档：

```
Get-SSMDocumentList
```

运行 PowerShell 命令或脚本

利用 Run Command 和 AWS-RunPowerShell 文档，您可使用远程桌面在 EC2 实例上执行任何命令或脚本，就像您已登录到该实例一样。您可以发出命令或键入本地脚本的路径以执行命令。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-RunPowerShellScript"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-RunPowerShellScript" | select -ExpandProperty Parameters
```

使用 AWS-RunPowerShellScript 文档发送命令

以下命令在两个实例上显示 C:\Users 目录的内容和 C:\ 目录的内容。

```
$runPSCmd=Send-SSMCommand -InstanceId @('Instance-ID', 'Instance-ID')  
-DocumentName AWS-RunPowerShellScript -Comment 'Demo AWS-RunPowerShellScript  
with two instances' -Parameter @{'commands'=@( 'dir C:\Users', 'dir C:\')}
```

获取命令请求详细信息

以下命令使用命令 ID 获取两个实例上的命令执行的状态。此示例使用上一个命令中返回的命令 ID。

```
Get-SSMCommand -CommandId $runPSCmd.CommandId
```

此示例中命令的状态可以是 Success、Pending 或 InProgress。

获取每个实例的命令信息

以下命令使用来自上一命令的命令 ID 来获取每个实例的命令执行的状态。

```
Get-SSMCommandInvocation -CommandId $runPSCmd.CommandId
```

获取带有特定实例的响应数据的命令信息

以下命令返回特定实例的原始 Send-SSMCommand 的输出。

```
Get-SSMCommandInvocation -CommandId $runPSCmd.CommandId -Details $true -  
InstanceId Instance-ID | select -ExpandProperty CommandPlugins
```

取消命令

以下命令取消 AWS-RunPowerShellScript 文档的 Send-SSMComand。

```
$cancelCmdResponse=Send-SSMCommand -InstanceId @('Instance-ID', 'Instance-ID')  
-DocumentName AWS-RunPowerShellScript -Comment 'Demo AWS-RunPowerShellScript  
with two instances' -Parameter @{'commands'='Start-Sleep -Seconds 120; dir  
C:\'} Stop-SSMCommand -CommandId $cancelCmdResponse.CommandId Get-SSMCommand  
-CommandId $cancelCmdResponse.CommandId
```

查看命令状态

以下命令检查 Cancel 命令的状态

```
Get-SSMCommand -CommandId $cancelCommandResponse.CommandId
```

使用 AWS-InstallApplication 文档安装应用程序

借助 Run Command 和 AWS-InstallApplication 文档，您可以在实例上安装、修复或卸载应用程序。该命令需要 MSI 的路径或地址。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-InstallApplication"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-InstallApplication" | select -ExpandProperty Parameters
```

使用 AWS-InstallApplication 文档发送命令

以下命令将自动在您的实例上安装 Python 版本，并将输出记录在 C: 驱动器上的本地文本文件中。

```
$installAppCommand=Send-SSMCommand -InstanceId Instance-ID -DocumentName AWS-InstallApplication -Parameter @{'source'='https://www.python.org/ftp/python/2.7.9/python-2.7.9.msi'; 'parameters'='/norestart /quiet /log c:\pythoninstall.txt'}
```

获取每个实例的命令信息

以下命令使用命令 ID 获取命令执行的状态

```
Get-SSMCommandInvocation -CommandId $installAppCommand.CommandId -Details $true
```

获取带有特定实例的响应数据的命令信息

以下命令返回 Python 安装的结果。

```
Get-SSMCommandInvocation -CommandId $installAppCommand.CommandId -Details $true -InstanceId Instance-ID | select -ExpandProperty CommandPlugins
```

使用 AWS-InstallPowerShellModule JSON 文档安装 PowerShell 模块

可使用 Run Command 在 EC2 实例上安装 PowerShell 模块。有关 PowerShell 模块的更多信息，请参阅 [Windows PowerShell 模块](#)。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-InstallPowerShellModule"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-InstallPowerShellModule" | select -Expand  
Property Parameters
```

安装 PowerShell 模块

以下命令下载 EZOut.zip 文件，安装该文件，然后运行另一个命令来安装 XPS Viewer。最后，此命令的输出将上传到一个名为 demo-ssm-output-bucket 的 Amazon S3 存储桶中。

```
$installPSCmd=Send-SSMCommand -InstanceId Instance-ID -DocumentName AWS-  
InstallPowerShellModule -Parameter @{'source'='https://gallery.technet.mi-  
crosoft.com/EZOut-33ae0fb7/file/110351/1/EZOut.zip'; 'commands'=@( 'Add-WindowsFea-  
ture -name XPS-Viewer -restart' )} -OutputS3BucketName demo-ssm-output-bucket
```

获取每个实例的命令信息

以下命令使用命令 ID 获取命令执行的状态。

```
Get-SSMCommandInvocation -CommandId $installPSCmd.CommandId -Details $true
```

获取具有实例的响应数据的命令信息

以下命令返回特定命令 ID 的原始 Send-SSMCommand 的输出。

```
Get-SSMCommandInvocation -CommandId $installPSCmd.CommandId -Details $true  
| select -ExpandProperty CommandPlugins
```

使用 AWS-JoinDirectoryServiceDomain JSON 文档将实例加入域

借助 Run Command，您可以将实例快速加入 AWS Directory Service 域。在执行此命令前，您必须[创建目录](#)。还建议您了解有关 AWS Directory Service 的更多信息。有关更多信息，请参阅[什么是 AWS Directory Service？](#)。

目前，您只能将一个示例加入域。无法从域中删除实例。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-JoinDirectoryServiceDomain"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-JoinDirectoryServiceDomain" | select -  
ExpandProperty Parameters
```

将实例加入域

以下命令将实例加入给定的 AWS Directory Service 域，并将任何生成的输出上传到 Amazon S3 存储桶中。

```
$domainJoinCommand=Send-SSMCommand -InstanceId Instance-ID -DocumentName AWS-  
JoinDirectoryServiceDomain -Parameter @{'directoryId'='d-9067386b64'; 'direct-  
oryName'='ssm.test.amazon.com'; 'dnsIpAddresses'=@('172.31.38.48',  
'172.31.55.243')} -OutputS3BucketName demo-ssm-output-bucket
```

获取每个实例的命令信息

以下命令使用命令 ID 获取命令执行的状态。

```
Get-SSMCommandInvocation -CommandId $domainJoinCommand.CommandId -Details $true
```

获取具有实例的响应数据的命令信息

此命令返回特定命令 ID 的原始 Send-SSMCommand 的输出。

```
Get-SSMCommandInvocation -CommandId $domainJoinCommand.CommandId -Details $true  
| select -ExpandProperty CommandPlugins
```

使用 AWS-ConfigureCloudWatch 文档将 Windows 指标发送到 Amazon CloudWatch

您可以将应用程序、系统、安全和 Windows 事件跟踪 (ETW) 日志中的 Windows Server 消息发送到 Amazon CloudWatch 日志。在首次启用日志记录时，SSM 会发送从您开始上传该应用程序、系统、安全和 ETW 日志时起 1 分钟内生成的所有日志。其中不包括在此时间之前产生的日志。如果您禁用日志记录并在以后再次启用日志记录，则 SSM 会从其上次停止的时间继续发送日志。对于任何自定义日志文件和 Internet Information Services (IIS) 日志，SSM 会从头读取日志文件。此外，SSM 还可以将性能计数器数据发送到 Amazon CloudWatch。

如果您先前在 EC2Config 中启用了 CloudWatch 集成，则 SSM 设置会覆盖实例本地在 C:\Program Files\Amazon\EC2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json 文件中存储的任何设置。有关使用 EC2Config 在一个实例上管理性能计数器和日志的更多信息，请参阅[将性能计数器发送到 CloudWatch 并将日志发送到 CloudWatch 日志](#)。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-ConfigureCloudWatch"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-ConfigureCloudWatch" | select -ExpandProperty Parameters
```

将应用程序日志发送到 CloudWatch

以下命令配置实例并将 Windows 应用程序日志移至 CloudWatch。

```
$cloudWatchCommand=Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-ConfigureCloudWatch' -Parameter @{'properties'='{"engineConfiguration": {"PollInterval": "00:00:15", "Components": [{"Id": "ApplicationEventLog", "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent", "AWS.EC2.Windows.CloudWatch", "Parameters": {"LogName": "Application", "Levels": "7"}, {"Id": "CloudWatch", "FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput", "AWS.EC2.Windows.CloudWatch", "Parameters": {"Region": "us-east-1", "LogGroup": "My-Log-Group", "LogStream": "i-1234567890abcdef0"}}], "Flows": [{"Flows": ["ApplicationEventLog", "CloudWatch"]}]}}}'
```

获取每个实例的命令信息

以下命令使用命令 ID 获取命令执行的状态。

```
Get-SSMCommandInvocation -CommandId $cloudWatchCommand.CommandId -Details $true
```

获取每个实例的命令信息

以下命令使用命令 ID 获取命令执行的状态。

```
Get-SSMCommandInvocation -CommandId $cloudWatchCommand.CommandId -Details $true
```

获取带有特定实例的响应数据的命令信息

以下命令返回 Amazon CloudWatch 配置的结果。

```
Get-SSMCommandInvocation -CommandId $cloudWatchCommand.CommandId -Details $true  
-InstanceId Instance-ID | select -ExpandProperty CommandPlugins
```

使用 AWS-ConfigureCloudWatch 文档将性能计数器发送到 CloudWatch

以下演示命令将性能计数器数据上传到 CloudWatch。有关更多信息，请参阅 [Amazon CloudWatch 文档](#)。

```
$cloudWatchMetricsCommand=Send-SSMCommand -InstanceId Instance-ID -DocumentName  
'AWS-ConfigureCloudWatch' -Parameter @{'properties'='{"engineConfiguration":  
{"PollInterval":"00:00:15", "Components": [{"Id":"PerformanceCounter", "Full  
Name":"AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCoun  
terInputComponent,AWS.EC2.Windows.CloudWatch", "Parameters": {"Category  
Name":"Memory", "CounterName":"Available MBytes", "InstanceName": "", "Metric  
Name":"AvailableMemory", "Unit":"Megabytes", "DimensionName": "", "Dimension  
Value":""}}, {"Id":"CloudWatch", "FullName":"AWS.EC2.Windows.CloudWatch.Cloud  
Watch.CloudWatchOutputComponent,AWS.EC2.Windows.CloudWatch", "Parameters": {"Ac  
cessKey": "", "SecretKey": "", "Region": "us-east-1", "NameSpace": "Windows-De  
fault"}]}, "Flows": {"Flows": ["PerformanceCounter,CloudWatch"]}}}'}
```

使用 AWS-ConfigureWindowsUpdate 文档启用/禁用 Windows 自动更新

借助 Run Command 和 AWS-ConfigureWindowsUpdate 文档，可以在 Windows 实例上启用或禁用自动 Windows 更新。此命令将 Windows 更新代理配置为在您指定的日期和时间下载并安装 Windows 更新。如果更新需要重启，计算机将在安装更新 15 分钟后自动重启。利用此命令，您还可以将 Windows 更新配置为检查更新但不安装更新。AWS-ConfigureWindowsUpdate 文档可与 Windows Server 2008、2008 R2、2012 和 2012 R2 兼容。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-ConfigureWindowsUpdate"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-ConfigureWindowsUpdate" | select -Expand  
Property Parameters
```

启用 Windows 自动更新

以下命令将 Windows Update 配置为在每天晚上 10:00 自动下载和安装更新。

```
$configureWindowsUpdateCommand = Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-ConfigureWindowsUpdate' -Parameters @{'updateLevel'='InstallUpdatesAutomatically'; 'scheduledInstallDay'='Daily'; 'scheduledInstallTime'='22:00'}
```

查看用于启用 Windows 自动更新的命令状态

以下命令使用命令 ID 获取用于启用 Windows 自动更新的命令执行的状态。

```
Get-SSMCommandInvocation -Details $true -CommandId $configureWindowsUpdateCommand.CommandId | select -ExpandProperty CommandPlugins
```

禁用 Windows 自动更新

以下命令降低 Windows Update 通知级别，使系统检查更新但不自动更新实例。

```
$configureWindowsUpdateCommand = Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-ConfigureWindowsUpdate' -Parameters @{'updateLevel'='NeverCheckForUpdates'}
```

查看用于禁用 Windows 自动更新的命令状态

以下命令使用命令 ID 获取用于禁用 Windows 自动更新的命令执行的状态。

```
Get-SSMCommandInvocation -Details $true -CommandId $configureWindowsUpdateCommand.CommandId | select -ExpandProperty CommandPlugins
```

使用 AWS-UpdateEC2Config 文档更新 EC2Config

借助 Run Command 和 AWS-EC2ConfigUpdate 文档，可以更新正在 Windows 实例上运行的 EC2Config 服务。此命令可将 EC2Config 服务更新为最新版本或您指定的版本。

查看说明和可用参数

```
Get-SSMDocumentDescription -Name "AWS-UpdateEC2Config"
```

查看有关参数的更多信息

```
Get-SSMDocumentDescription -Name "AWS-UpdateEC2Config" | select -ExpandProperty Parameters
```

将 EC2Config 更新为最新版本

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName "AWS-UpdateEC2Config"
```

获取具有实例的响应数据的命令信息

此命令从上一个 Send-SSMCommand 返回指定命令的输出：

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

将 EC2Config 更新为特定版本

以下命令将 EC2Config 降级到较旧版本：

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName "AWS-UpdateEC2Config" -  
Parameter @{'version'='3.8.354'; 'allowDowngrade'='true'}
```

使用 Run Command 管理 Microsoft Windows 更新

Run Command 包含三个文档，可帮助您管理 Amazon EC2 Windows 实例的更新。

- AWS-FindWindowsUpdates - 扫描实例并确定缺少的更新。
- AWS-InstallMissingWindowsUpdates - 在 EC2 实例上安装缺少的更新。
- AWS-InstallSpecificUpdates - 安装特定更新。

以下示例演示如何执行指定的 Windows Update 管理任务。

搜索所有缺少的 Windows 更新

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-FindWindowsUpdates'  
-Parameters @{'UpdateLevel'='All'}
```

安装特定的 Windows 更新

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-InstallSpecificWindowsUpdates' -Parameters @{'KbArticleIds'='123456,KB567890,987654'}
```

安装缺少的重要 Windows 更新

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-InstallMissingWindowsUpdates' -Parameters @{'UpdateLevel'='Important'}
```

安装缺少的 Windows 更新（带特定排除内容）

```
Send-SSMCommand -InstanceId Instance-ID -DocumentName 'AWS-InstallMissingWindowsUpdates' -Parameters @{'UpdateLevel'='All'; 'ExcludeKbArticleIds'='KB567890,987654'}
```

取消命令

只要服务指明命令处于 Pending 或 Executing 状态，就可以尝试取消该命令。但是，即使命令仍处于其中某种状态，我们也无法保证该命令将终止并且基础流程将停止。

使用控制台取消命令

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择要取消的命令调用。
3. 选择 Actions，然后选择 Cancel command。

使用 AWS CLI 取消命令

使用以下命令。

```
aws ssm cancel-command --command-id "command ID" --instance-ids "instance ID"
```

有关已取消命令的状态的信息，请参阅[监控命令 \(p. 391\)](#)。

监控命令

可通过几种方式监控使用 Run Command 发送的命令的状态：

- 将 CloudWatch 事件 配置为记录状态更改。
- 将 Amazon SNS 配置为发送所有状态更改或特定状态（例如“失败”或“超时”）的通知。
- 单击 Amazon EC2 控制台中的 Command History 页面上的“刷新”图标。
- 使用命令行工具调用 ListCommand 或 ListCommandInvocation API。

此部分包括有关如何使用 CloudWatch 事件 和 SNS 通知自动化监控的信息。

在将一条命令同时发送给多个实例时，针对每个实例的命令的每个副本均为一个命令调用。例如，如果您使用 AWS-RunPowerShellScript JSON 文档并将一个 ipconfig 命令发送给 20 个实例，则该命令具有 20 个调用。利用 Run Command 监控选项，可以检查每个调用的详细信息，这可帮助您在命令失败时解决问题。

命令状态

每个命令调用都会单独报告状态。此外，每个 SSM 文档包含一个或多个名为插件的代码执行块。给定命令调用的插件也会单独报告状态。下表描述的是运行命令执行的状态。

有关插件的更多信息，请参阅 *Amazon EC2 Simple Systems Manager API Reference* 中的 [SSM 插件](#)。

状态	详细信息
Pending	SSM 尚未接受此命令。如果 SSM 代理在达到 Timeout(seconds) 参数指定的值前没有收到命令，该状态会更改为 Timed Out。
正在进行	该命令已由 SSM 代理接收，或者已开始在实例上执行。根据所有命令插件的结果，状态会变为成功、失败或超时。如果 SSM 代理在实例上不可用，命令状态会显示为 In Progress，直至 SSM 代理再次可用为止。状态将变为最终状态。
成功	该命令（包括所有插件）完成了在实例上的执行的任务。
已失败	一个或多个插件无法执行。为了帮助您标识和解决与命令相关的问题，如果插件失败，整个调用状态将变为 Failed。
超时	在达到 Timeout (seconds) 参数指定的值前，该命令未连接到实例上的 SSM 代理。或者，命令执行的时间长于允许的执行时间。命令执行的时间虽插件而有所不同。默认值从两小时到八小时不等。

状态	详细信息
正在取消	您已发送移除命令调用的口令。命令未达到最终状态 (Success、Failed 或 Timed Out)。如果 SSM 代理在 Timeout (seconds) 参数指定的时间范围内做出回应，那么状态就会改变，以反映最终状态。否则，状态会变为超时。
已取消	已成功取消您的命令。



Note

在 Amazon EC2 控制台中，单击右上角的“Refresh”符号可在命令执行时监视命令的状态。

有关如何使用 Windows PowerShell 查看命令状态的信息，请参阅[适用于 Windows PowerShell 的 AWS 工具的 Amazon EC2 Run Command 演练 \(p. 383\)](#)或[适用于 Windows PowerShell 的 AWS 工具参考](#)。有关如何使用 AWS CLI 查看命令状态的信息，请参阅[SSM CLI 参考](#)。

内容

- [在命令更改状态时接收 Amazon SNS 通知 \(p. 392\)](#)
- [记录 Run Command 的命令执行状态更改 \(p. 397\)](#)

在命令更改状态时接收 Amazon SNS 通知

Abstract

了解如何在使用 Run Command 发送的命令更改状态时从 Amazon SNS 接收电子邮件通知。

针对使用 Amazon EC2 Run Command 发送的命令，您可以将 Amazon Simple Notification Service (Amazon SNS) 配置为发送有关这些命令的状态的通知。Amazon SNS 协调并管理传输，或将通知发送到订阅客户端或终端节点。您可以在命令更改为新状态或特定状态（例如“失败”或“超时”）时接收通知。如果您将一条命令发送给多个实例，则可接收发送给特定实例的命令的每个副本的通知。每个副本称为一个调用。

Amazon SNS 能够以 HTTP 或 HTTPS POST 以及电子邮件（SMTP、纯文本或 JSON 格式）的方式传输通知，或者将通知作为消息发布到 Amazon Simple Queue Service (Amazon SQS) 队列。有关更多信息，请参阅 [Amazon Simple Notification Service 开发人员指南](#) 中的[什么是 Amazon SNS](#)。

例如，如果您将 Amazon SNS 配置为在命令状态更改为失败时发送通知，则 SNS 将发送包含命令执行的详细信息的电子邮件通知。



Note

如果您愿意，您可以使用 Amazon CloudWatch 事件 将目标配置为在命令更改状态时调用 AWS Lambda 函数。有关更多信息，请参阅 [记录 Run Command 的命令执行状态更改 \(p. 397\)](#)。

要设置命令更改状态时的 Amazon SNS 通知，您必须完成以下任务。

1. [配置账户权限 \(p. 394\)](#)
2. [为通知创建 IAM 角色 \(p. 394\)](#)
3. [配置 Amazon SNS \(p. 395\)](#)
4. [发送可返回状态通知的命令 \(p. 396\)](#)

为 SSM 配置 Amazon SNS 通知

对于进入以下状态的命令，Run Command 支持发送相应的 Amazon SNS 通知。有关导致命令进入以下状态之一的条件的信息，请参阅[监控命令 \(p. 391\)](#)。

- 正在进行
- 成功
- 已失败
- 超时
- 已取消



Note

使用 Run Command 发送的命令还报告“正在取消”和“正在挂起”状态。SNS 通知不会捕获这些状态。

如果您为 SNS 通知配置 Run Command，SNS 将发送包含以下信息的摘要消息：

字段	类型	说明
EventTime	字符串	触发事件的时间。由于 SNS 不保证消息传输顺序，因此时间戳很重要。示例：2016-04-26T13:15:30Z
DocumentName	字符串	用于执行此命令的 SSM 文档的名称。
CommandId	字符串	Run Command 在发送命令后生成的 ID。
ExpiresAfter	日期	如果达到此时间但命令尚未开始执行，则它将不会执行。
OutputS3BucketName	字符串	将命令执行响应存储到的 Amazon Simple Storage Service (Amazon S3) 存储桶。
OutputS3KeyPrefix	字符串	将命令执行响应存储到的存储桶中的 Amazon S3 目录路径。
RequestedDateTime	字符串	请求发送到此特定实例的日期和时间。
实例 ID	字符串	命令的目标实例。
状态	字符串	命令的命令状态。

如果您将一条命令发送给多个实例，则 Amazon SNS 可发送有关命令的每个副本或调用的消息，其中包含以下信息：

字段	类型	说明
EventTime	字符串	触发事件的时间。由于 SNS 不保证消息传输顺序，因此时间戳很重要。示例：2016-04-26T13:15:30Z

字段	类型	说明
DocumentName	字符串	用于执行此命令的 SSM 文档的名称。
RequestedDateTime	字符串	请求发送到此特定实例的日期和时间。
CommandId	字符串	Run Command 在发送命令后生成的 ID。
实例 ID	字符串	命令的目标实例。
状态	字符串	此调用的命令状态。

配置账户权限

在发送为通知配置的命令时，可指定服务角色 Amazon 资源名称 (ARN)。例如：
--service-role-arn=arn:aws:iam::123456789012:myrole。此服务角色供 SSM 用来触发 SNS 通知。

要从 Amazon SNS 服务接收通知，您必须将 iam:PassRole 策略附加到现有 AWS Identity and Access Management (IAM) 用户账户，或创建一个新的 IAM 账户并向其附加此策略。如果您创建新账户，则还必须附加 AmazonSSMFullAccess 策略，以便账户能够与 SSM API 进行通信。

使用以下过程可将 IAM 策略附加到您的用户账户。如果您需要创建新的用户账户，请参阅 *IAM 用户指南* 中的 [在您的 AWS 账户中创建 IAM 用户](#)。

将 iam:PassRole 策略附加到您的用户账户

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在左侧的导航窗格中，选择 Users，然后双击您的用户账户。
3. 在页面的顶部，将您的 User ARN 复制到剪贴板。
4. 在 Managed Policies 部分中，验证是否已列出 **AmazonSSMFullAccess** 策略或是否存在可向您授予对 SSM API 的权限的类似策略。
5. 选择 Inline Policies 旁边的向下箭头，然后选择 click here。
6. 在 Set Permissions 页面上，选择 Policy Generator，然后选择 Select。
7. 验证 Effect 是否已设置为 Allow。
8. 从 AWS Services 中，选择 AWS Identity and Access Management。
9. 从 Actions 中，选择 PassRole。
10. 在 Amazon Resource Name (ARN) 字段中，粘贴您的 ARN。
11. 选择 Add Statement，然后选择 Next。
12. 在 Review Policy 页面上，选择 Apply Policy。

为通知创建 IAM 角色

在上一个过程中，您已将 IAM 策略添加到用户账户，以便能发送用于返回通知的命令。在下面的过程中，您将创建一个角色，以使 SSM 服务能够在发送通知时代表您执行操作。

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中选择 Roles，然后选择 Create New Role。
3. 在 Step 1: Set Role Name 中，为通知输入用于将此角色标识为 Run Command 角色的名称。
4. 在 Step 2: Select Role Type 中，选择 Amazon EC2。系统会跳过 Step 3: Establish Trust，因为这是一个托管策略。

5. 在 Step 4: Attach Policy 中，选择 AmazonSNSFullAccess。
6. 选择 Next Step，然后选择 Create Role。系统将让您返回到 Roles 页。
7. 找到刚刚创建的角色，然后双击它。
8. 选择 Trust Relationships 选项卡，然后选择 Edit Trust Relationship。
9. 将 "ssm.amazonaws.com" 添加到现有策略，如以下代码段所示：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "ec2.amazonaws.com",  
                "Service": "ssm.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```



Note

您必须在现有条目后添加逗号。"Service": "sns.amazonaws.com"，否则 JSON 将不会验证。

10. 选择 Update Trust Policy。
11. 复制或记下 Role ARN。在发送配置为返回通知的命令时将指定此 ARN。

配置 Amazon SNS

要使用 Amazon SNS 发送电子邮件通知，必须先创建一个主题，然后用您的电子邮件地址订阅该主题。

创建一个 Amazon SNS 主题

Amazon SNS 主题是一个逻辑接入点，即 Run Command 用来发送通知的通信通道。您可通过为主题指定名称来创建主题。

有关更多信息，请参阅 *Amazon Simple Notification Service 开发人员指南* 中的[创建主题](#)。



Note

创建主题后，复制或记下 Topic ARN。在发送配置为返回状态通知的命令时将指定此 ARN。

订阅 Amazon SNS 主题

要接收 Run Command 发送到该主题的通知，必须让一个终端节点订阅该主题。在此过程中，为 Endpoint 指定要用来从 Run Command 接收通知的电子邮件地址。

有关更多信息，请参阅 *Amazon Simple Notification Service 开发人员指南* 中的[订阅主题](#)。

确认 Amazon SNS 订阅

Amazon SNS 向在上一步骤中指定的电子邮件地址发送确认电子邮件。

确保打开来自 AWS 通知的电子邮件，选择链接以确认订阅，然后继续执行下一步骤。

您将从 AWS 收到确认消息。Amazon SNS 现已配置为接收通知并将通知以电子邮件形式发送到您指定的电子邮件地址。

发送可返回状态通知的命令

此部分介绍如何使用 Amazon EC2 控制台或 AWS Command Line Interface (AWS CLI) 发送配置为返回状态通知的命令。

从 Amazon EC2 控制台发送可返回通知的命令

1. 打开 [Amazon EC2 控制台](#)，并在导航窗格中选择 Command History。
2. 选择 Run a Command。
3. 在 Command document 列表中，选择 SSM 文档。
4. 选择 Select target instances 以选择要在其中运行命令的实例。如果未看到实例的完整列表，则可能不会为 Run Command 正确配置缺少的实例。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。
5. 在 SSM 文档的必填字段中输入信息。在 SNS Notifications 部分中，选择 Enable SNS notifications。
6. 在 Role 字段中，键入或粘贴之前创建的 IAM 角色 ARN。
7. 在 SNS Topic 字段中，键入或粘贴之前创建的 Amazon SNS ARN。
8. 在 Notify me on 字段中，选择要接收其通知的事件。
9. 在 Notify me for 字段中，选择接收发送给多个实例（调用）或命令摘要的命令的每个副本的通知。
10. 选择 Run。
11. 检查来自 Amazon SNS 的电子邮件消息并打开电子邮件。Amazon SNS 发送电子邮件需要花费几分钟的时间。

从 AWS CLI 发送为通知配置的命令

1. 打开 AWS CLI。
2. 指定以下命令中的参数。

```
aws ssm send-command --instance-ids "ID-1, ID-2" --document-name "name" --parameters commands=date --service-role ServiceRole ARN --notification-config NotificationArn=SNS ARN
```

例如

```
aws ssm send-command --instance-ids "i-12345678, i-34567890" --document-name "AWS-RunPowerShellScript" --parameters commands=date --service-role arn:aws-cn:iam:: 123456789012:myrole --notification-config NotificationArn=arn:aws-cn:sns:cn-north-1:123456789012:test
```

3. 按 Enter。
4. 检查来自 Amazon SNS 的电子邮件消息并打开电子邮件。Amazon SNS 发送电子邮件需要花费几分钟的时间。

有关从命令行配置 Run Command 的更多信息，请参阅 [Amazon EC2 Simple Systems Manager API Reference](#) 和 [SSM AWS CLI 参考](#)。

记录 Run Command 的命令执行状态更改

可以使用 Amazon CloudWatch 事件 和简单 AWS Lambda 函数来记录命令执行状态更改。您可以创建一个规则，只要状态发生变换或者在变换到一个或多个感兴趣的状态时，就运行该规则。

Amazon EC2 Simple Systems Manager 事件类型

SSM 向 CloudWatch 事件 发送以下数据。

示例 1 - EC2 命令状态更改通知：此示例包含有关发送给多个实例的命令的执行状态更改的信息。

```
{  
    "version": "0",  
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",  
    "detail-type": "EC2 Run Command - Command Status change",  
    "source": "aws.ssm",  
    "account": "123456789012",  
    "time": "2016-03-14T18:43:48Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:instance/i-12345678",  
        "arn:aws:ec2:us-east-1:123456789012:instance/i-12345670",  
        "arn:aws:ec2:us-east-1:123456789012:instance/i-12345679"  
    ],  
    "detail": {  
        "command-id": "aws.ssm.12345678-1234-1234-1234-12345678",  
        "requested-date-time": "2016-03-14T18:43:48Z",  
        "expire-after": "2016-03-14T18:43:48Z",  
        "output-s3bucket-name": "mybucket",  
        "output-s3key-prefix": "test",  
        "parameters": "parameter",  
        "status": "Success"  
    }  
}
```

示例 2 - EC2 命令调用状态更改通知：此示例包含有关发送给多个实例的命令的信息，而事件仅显示一个实例或该命令的 调用 的信息。

```
{  
    "version": "0",  
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",  
    "detail-type": "EC2 Run Command - Command Invocation Status change",  
    "source": "aws.ssm",  
    "account": "123456789012",  
    "time": "2016-03-14T18:43:48Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:instance/i-12345678"  
    ],  
    "detail": {  
        "command-id": "aws.ssm.12345678-1234-1234-1234-12345678",  
        "instance-id": "i-12345678",  
        "requested-date-time": "2016-03-14T18:43:48Z",  
        "status": "Success"  
    }  
}
```

记录 SSM 命令执行状态更改

在以下示例方案中，您将创建一个简单 AWS Lambda 函数，将事件从 SSM 传送到该函数，然后测试方案以确保它已正确设置。

要记录 Run Command 的命令执行状态更改，您必须执行下列步骤。

1. 步骤 1：创建 AWS Lambda 函数 (p. 398)
2. 步骤 2：将事件传送到 AWS Lambda 函数 (p. 398)
3. 步骤 3：测试您的 Amazon CloudWatch 事件 规则 (p. 399)

步骤 1：创建 AWS Lambda 函数

创建 AWS Lambda 函数

1. 通过以下网址打开 AWS Lambda 控制台：<https://console.amazonaws.cn/lambda/>。
2. 选择 Create a Lambda function，然后在 Select blueprint 屏幕上选择 hello-world。
3. 在 Configure function 屏幕上的 Name 字段中，键入事件的名称。此示例使用 SomethingHappened。
4. 在 Lambda function code 部分中，编辑示例代码以匹配以下示例：

```
console.log('Loading function');

exports.handler = function(event, context, callback) {
    console.log('SomethingHappened()');
    console.log('Here is the event:', JSON.stringify(event, null, 2));
    callback(null, "Ready");
};
```

5. 在 Lambda function handler and role 下的 Role 字段中，选择 lambda_basic_execution_rule (如果有)。否则，创建新的基本执行角色。
6. 选择 Next，然后在 Review 屏幕上，选择 Edit 以进行任何更改。如果您对函数满意，请选择 Create function。

步骤 2：将事件传送到 AWS Lambda 函数

创建 CloudWatch 事件 规则

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 在导航窗格中，选择 Events。
3. 选择 Create rule，然后在 Event selector 下，选择 EC2 instance state-change notification。
4. 选择 Specific state(s)，然后从列表中选择 Running。
5. 执行以下任一操作：
 - 要使规则响应区域中的任一实例，请选择 Any instance。
 - 要使规则响应特定实例，请选择 Specific instance(s)，然后在文本框中输入实例 ID。
6. 在 Targets 下，选择 Add target。在 Select target type 列表中，选择 AWS Lambda function。
7. 在 Function 列表中，选择您在“步骤 1：创建 AWS Lambda 函数”中创建的函数。
8. 选择 Configure input，然后选择下列选项之一：
 - Matched event

- 将事件中的所有数据字段发送到 CloudWatch 日志。
 - Part of the matched event
 - 仅将事件的指定数据字段发送到 CloudWatch 日志。您可以使用以下格式的字符串指定事件部分：
`$first_parameter.second_parameter`
 - 例如，要只发送 Amazon EC2 实例 ID，请在字段中键入 `$.detail.state`。
 - Constant
 - 将指定的 JSON 格式的文本字符串发送到 CloudWatch 日志。例如，要发送事件的文本字符串，请键入 `{"Name": "MyInstance"}`。常量必须是有效的 JSON。
9. 选择 Configure details。在 Configure rule details 屏幕上的 Name 字段中，键入规则的名称。
 10. 在 Description 字段中，键入规则的简短描述，例如 Log command execution status changes。
 11. 如果您对规则满意，请选择 Create rule。

步骤 3：测试您的 Amazon CloudWatch 事件 规则

您可以使用 Run Command 执行命令来测试规则。在等待几分钟以便命令得到处理后，检查 Amazon CloudWatch 事件 控制台中的 AWS Lambda 指标，以验证您的函数是否已被调用。

使用控制台测试您的 CloudWatch 事件 规则

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Command History，然后对一个或多个实例执行命令。有关执行命令的更多信息，请参阅 [使用 Amazon EC2 Run Command 执行命令 \(p. 345\)](#)。
3. 要查看 AWS Lambda 指标，请打开 CloudWatch 控制台 <https://console.amazonaws.cn/cloudwatch/>。
4. 在导航窗格中，在 Metrics 下选择 Lambda 以查看由 Lambda 函数生成的指标。
5. 要查看您的函数的输出，请在导航窗格中，选择 Logs，然后在 Log Groups 列表中，选择包含数据的 /aws/lambda 日志组。
6. 在 Log Streams 下，选择日志流以查看有关命令执行状态更改的数据。

Amazon EC2 Run Command 疑难解答

使用以下信息来帮助解决与 Run Command 相关的问题。有关排查适用于 Linux 的 Run Command 的问题的信息，请参阅“Linux 用户指南”中的 [Run Command 疑难解答](#)。

我的实例在哪里？

如果您在选择 Select Target instances 后未看到预期的实例列表，则验证是否已使用可让实例与 SSM API 通信的 AWS Identity and Access Management (IAM) 角色来配置实例。此外，还验证您的用户账户是否具有一个允许您的账户与 SSM API 通信的 IAM 用户信任策略。以下过程介绍如何配置实例角色和用户信任策略。



Note

您在创建新实例时必须分配 IAM 实例角色。无法将角色分配给已在运行的实例。要将现有实例配置为使用 SSM 支持的角色，您必须创建实例映像，从该映像启动实例，并在启动实例时分配 IAM 角色。有关更多信息，请参阅 [创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

创建使用由 SSM 提供支持的角色的实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择支持的区域。
3. 选择 Launch Instance，然后选择一个 Windows Server 实例。
4. 选择实例类型，然后选择 Next: Configure Instance Details。
5. 在 IAM role 旁边，选择 Create new IAM role。此时将会打开 IAM 管理控制台。
 - a. 在 Step 2: Select Role Type 中，选择 Amazon EC2 Role for Simple Systems Manager。
 - b. 在 Step 3: Establish Trust 中，选择 AmazonEC2RoleforSSM。
 - c. 完成向导。
6. 在 EC2 管理控制台中，选择 Create New IAM role 旁边的 Refresh 按钮。
7. 在 IAM role 下拉列表中，选择您刚刚创建的角色。
8. 完成向导以创建并启动新实例。

向您的用户账户授予对 SSM 的访问权限

使用以下过程将 AmazonSSMFulAccess IAM 策略附加到您的用户账户。此策略向您授予对 SSM API 操作的完全访问权限。

为 EC2 实例创建 IAM 策略

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Policies。（如果这是您首次使用 IAM，请选择 Get Started，然后选择 Create Policy。）
3. 在 Filter 字段中，键入 AmazonSSMFulAccess 并按 Enter。
4. 选中 AmazonSSMFulAccess 旁边的复选框，然后依次选择 Policy Actions 和 Attach。



5. 在 Attach Policy 页面上，选择您的用户账户，然后选择 Attach Policy。

在附加策略后，查看您的实例是否在 EC2 控制台的 Select Target instances 部分中可见。如果这些实例不可见，则表示未满足一个或多个先决条件。有关更多信息，请参阅 [Amazon EC2 Run Command 先决条件 \(p. 333\)](#)。

使用 Health API 检查实例状态

您可以使用 Amazon EC2 Health API 快速确定以下有关 Amazon EC2 实例的信息：

- EC2Config 服务的版本
- 一个或多个实例的状态
- 操作系统
- EC2Config 服务的状态

- 该实例上次发送检测信号值的时间

使用以下命令可获取有关一个或多个实例的状态详细信息：

```
Get-SSMInstanceInformation -InstanceInformationFilterList @{Key="InstanceIds";ValueSet="instance-ID","instance-ID"}
```

使用以下不带筛选条件的命令可查看注册到您的账户的当前报告联机状态的所有实例。将 ValueSet="Online" 替换为 "ConnectionLost" 或 "Inactive" 可查看这些状态：

```
Get-SSMInstanceInformation -InstanceInformationFilterList @{Key="PingStatus";ValueSet="Online"}
```

使用以下命令可查看哪些实例正在运行 EC2Config 服务的最新版本。将 ValueSet="LATEST" 替换为特定版本（例如，3.0.54 或 3.10）可查看这些详细信息：

```
Get-SSMInstanceInformation -InstanceInformationFilterList @{Key="AgentVersion";ValueSet="LATEST"}
```

EC2Config 服务疑难解答

如果您在实例上执行命令时遇到问题，则 EC2Config 服务可能出现问题。此服务负责在实例上处理命令。如果您更改了网络配置，并且您的实例未显示在列表中，则需要重启 EC2Config Windows 服务。有关 EC2Config 服务问题排查的信息，请参阅[故障排除 \(p. 298\)](#)。

导入和导出虚拟机

Abstract

您可以从 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 等虚拟化平台中导入虚拟机，然后在 Amazon EC2 中启动该虚拟机。

您可以使用 Amazon Web Services (AWS) VM Import/Export 工具将虚拟机 (VM) 映像从您的本地环境导入到 AWS 中，然后将它们转换成准备就绪的 Amazon EC2 Amazon 系统映像 (AMI) 或实例。稍后，您可以将 VM 镜像作为实例导回至您的本地环境。使用 VM Import/Export，您可以利用为满足 IT 安全、配置管理和合规要求而已构建的 VM 中的现有投资，方式是将 VM 纳入到 Amazon Elastic Compute Cloud (Amazon EC2) 中作为准备就绪的 AMI 或实例。

VM Import/Export 与 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 虚拟化环境兼容。如果您使用的是 VMware vSphere，也可以使用 AWS Connector for vCenter 从 VMware 导出 VM，然后将其导入 Amazon EC2。有关更多信息，请参阅 [AWS Management Portal for vCenter 用户指南](#) 中的[使用 AWS Connector for vCenter 将您的虚拟机迁移至 Amazon EC2](#)。如果您使用的是 Microsoft Systems Center，则也可以使用 AWS Systems Manager for Microsoft SCVMM 来将 Windows VM 从 SCVMM 中导入到 Amazon EC2。有关更多信息，请参阅 [Amazon EC2 用户指南 \(适用于 Microsoft Windows 实例\)](#) 中的[使用 AWS Systems Manager for Microsoft SCVMM 导入虚拟机](#)。

VM Import/Export 可以用于迁移应用程序和工作负载，复制您的 VM 映像目录，或为 VM 映像创建灾难恢复存储库。

- 将现有应用程序和工作负载迁移至 Amazon EC2 - 您可以将基于 VM 的应用程序和工作负载迁移至 Amazon EC2 并保留其软件和配置设置。当您使用 VM Import 导入 VM 时，可将现有 VM 转换成 Amazon EC2 实例或可在 Amazon EC2 上运行的 Amazon 系统映像 (AMI)。当您从 VM 创建 AMI 时，可基于同

一导入的 VM 运行多个实例。您还可借助 AMI 使用 AMI 副本来复制您在全球的应用程序和工作负载。有关更多信息，请参阅 [复制 AMI \(p. 84\)](#)。

- 将您的 VM 映像目录导入到 Amazon EC2 - 您可以将现有 VM 映像目录导入到 Amazon EC2。如果您要维护批准的 VM 映像的目录，可以将您的映像目录复制到 Amazon EC2 并从导入的 VM 映像创建 AMI。您可以将现有软件（包括您已安装的产品，例如，反病毒软件、入侵检测系统等）与您的 VM 映像一起导入。您可将已创建的 AMI 用作您的 Amazon EC2 映像目录。
- 为 VM 映像创建灾难恢复存储库 - 您可以出于备份和灾难恢复目的将您的本地 VM 映像导入 Amazon EC2。您可导入您的 VM，然后将其存储为 AMI。创建的 AMI 将准备就绪，您可在需要时在 Amazon EC2 中启动它。如果您的本地环境发生任何事件，您可以快速启动实例来保持业务连续性，并将它们同步导出，以便重新构建本地基础设施。

内容

- [将 VM 作为镜像导入 Amazon EC2 \(p. 402\)](#)
- [将 VM 作为实例导入 Amazon EC2 \(p. 418\)](#)
- [导出 Amazon EC2 实例 \(p. 431\)](#)
- [对 VM Import/Export 进行故障排除 \(p. 434\)](#)

将 VM 作为镜像导入 Amazon EC2

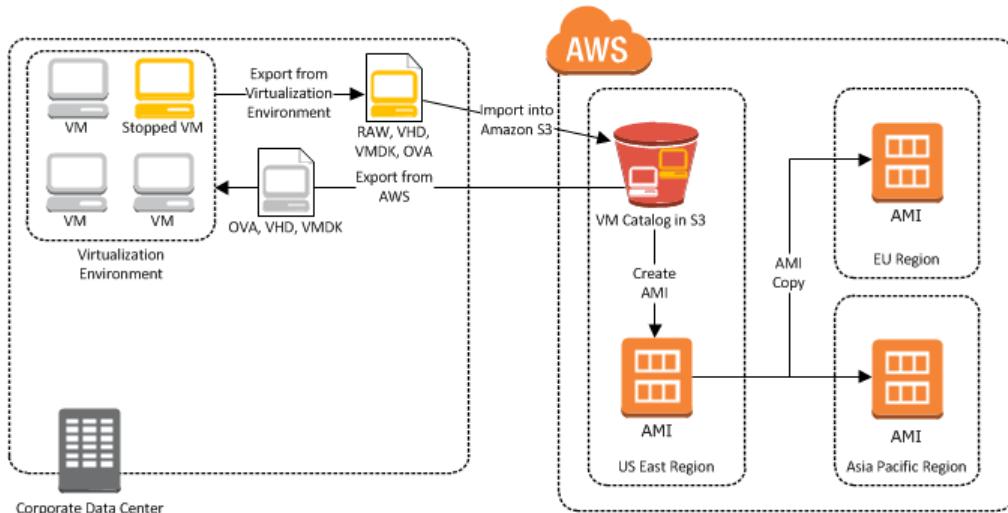
Abstract

使用 ImportImage API 从 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 虚拟化环境将 VM 作为镜像导入 Amazon EC2。

您可从您的虚拟化环境（例如，Citrix Xen、Microsoft Hyper-V 或 VMware vSphere）导入虚拟机（VM），然后将其作为 AMI 导入 Amazon EC2 中。有关如何从 AMI 启动 Amazon EC2 实例的更多信息，请参阅 [启动实例 \(p. 216\)](#)。

要在 Amazon EC2 中使用您的 VM，您必须首先将其从虚拟化环境中导出，然后使用 AWS Command Line Interface (AWS CLI) 或 API 工具将其导入 Amazon EC2。

下图显示将 VM 从您的本地虚拟化环境导出到 AWS 的过程。



无论使用 CLI 或 API，您将执行将 VM 或卷导入 Amazon EC2 的相同步骤。下面是使用 CLI 的过程。

将 VM 导入 Amazon EC2 中

1. 安装 AWS CLI。有关更多信息，请参阅 [步骤 1：安装 AWS CLI \(p. 409\)](#)。
2. 为 VM 导入 Amazon EC2 做准备。有关更多信息，请参阅 [步骤 2：准备您的 VM \(p. 410\)](#)。
3. 从虚拟化环境中导出 VM。有关更多信息，请参阅 [步骤 3：将您的 VM 从其虚拟化环境导出 \(p. 412\)](#)。
4. 将 VM 导入 Amazon EC2。有关信息，请参阅 [步骤 4：将您的 VM 导入 Amazon EC2 \(p. 412\)](#)。
5. 在 Amazon EC2 中启动实例。有关更多信息，请参阅 [步骤 5：在 Amazon EC2 中启动实例 \(p. 418\)](#)。

VM Import/Export 的先决条件

Abstract

在开始导入您的虚拟机之前查看基本信息和限制条件。

在您开始将 VM 从您的虚拟化环境导出或从 Amazon EC2 导入和导出 VM 之前，您必须了解 AWS 支持的操作系统和映像格式，还必须了解导出实例和卷的限制。

要从 Amazon EC2 导入或导出 VM，您还必须安装 CLI 工具：

- 有关安装 Amazon EC2 CLI 的更多信息，请参阅 [Amazon EC2 命令行参考](#)。
- 有关安装 AWS CLI 的更多信息，请参阅 [AWS Command Line Interface 用户指南](#)。有关 AWS CLI 中的 Amazon EC2 命令的更多信息，请参阅 [AWS Command Line Interface Reference](#) 中的 `ec2`。

内容

- [操作系统 \(p. 403\)](#)
- [映像格式 \(p. 405\)](#)
- [实例类型 \(p. 405\)](#)
- [卷类型和文件系统 \(p. 405\)](#)
- [Amazon S3 存储桶 \(p. 406\)](#)
- [VM Import 服务角色 \(p. 406\)](#)
- [IAM 权限 \(p. 407\)](#)
- [要求和限制 \(p. 408\)](#)

操作系统

以下操作系统可以在 Amazon EC2 中导入和导出。

Windows (32 和 64 位)

- 含 Service Pack 1 (SP1) 的 Microsoft Windows Server 2003 (标准版、数据中心版、企业版) 或更高版本 (32 位和 64 位)
- Microsoft Windows Server 2003 R2 (标准版、数据中心版、企业版) (32 位和 64 位)
- Microsoft Windows Server 2008 (标准版、数据中心版、企业版) (32 位和 64 位)
- Microsoft Windows Server 2008 R2 (标准版、数据中心版、企业版) (仅限 64 位)
- Microsoft Windows Server 2012 (标准版、数据中心版) (仅限 64 位)
- Microsoft Windows Server 2012 R2 (标准版、数据中心版) (仅限 64 位)
- Microsoft Windows 7 (专业版、企业版、旗舰版) (32 位和 64 位)



Note

VM Import 目前支持导入运行 Microsoft Windows 7 美国英语版（专业版、企业版、旗舰版）的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 8（专业版、企业版）（32 位和 64 位）



Note

VM Import 目前支持导入运行 Microsoft Windows 8 美国英语版（专业版、企业版）的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 8.1（专业版、企业版）（仅限 64 位）



Note

VM Import 目前支持导入运行 Microsoft Windows 8.1 美国英语版（专业版、企业版）的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 10（家庭版、专业版、企业版、教育版）（仅限 64 位）



Note

VM Import 目前支持导入运行 Microsoft Windows 10 美国英语版（家庭版、专业版、企业版、教育版）的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

Linux/Unix（64 位）



Note

导入的 Linux VM 应使用默认内核以获得最佳结果。使用自定义 Linux 内核的 VM 无法成功导入。

- Red Hat Enterprise Linux (RHEL) 5.1-5.11、6.1-6.6、7.0-7.1



Note

不支持 RHEL 6.0，因为它缺少在 Amazon EC2 上运行所需的驱动程序。

VM Import 支持 RHEL 实例的许可移植性。您的现有 RHEL 许可与它们的关联 RHEL 实例一同导入。有关对于 Red Hat Cloud Access 的资格的更多信息，请参阅 Red Hat 网站的[资格](#)。

- SUSE Linux Enterprise Server

- SUSE Linux Enterprise Server 11 Service Pack 1 - 2.6.32.12-0.7
- SUSE Linux Enterprise Server 11 Service Pack 2 - 3.0.13-0.27
- SUSE Linux Enterprise Server 11 Service Pack 3 - 3.0.76-0.11、3.0.101-0.8 和 3.0.101-0.15
- SUSE Linux Enterprise Server 11 Service Pack 4 - 3.0.101-63
- SUSE Linux Enterprise Server 12 - 3.12.28-4
- SUSE Linux Enterprise Server 12 Service Pack 1 - 3.12.49-11
- Ubuntu 12.04、12.10、13.04、13.10、14.04、14.10、15.04
- CentOS 5.1-5.11、6.1-6.6、7.0-7.2



Note

不支持 CentOS 6.0，因为它缺少在 Amazon EC2 上运行所需的驱动程序。

- Debian 6.0.0-6.0.8、7.0.0-7.8.0、8.0.0
- Oracle Linux 6.1-6.6、7.0-7.1
- Fedora Server 19-21

映像格式

以下格式可以导入 Amazon EC2 和从 Amazon EC2 中导出。

将映像格式导入 Amazon EC2

对于将磁盘和 VM 导入 Amazon EC2，AWS 支持下列映像格式：

- 用于导入磁盘和 VM 的 RAW 格式。
- 固定和动态虚拟硬盘 (VHD) 映像格式，该格式与 Microsoft Hyper-V 和 Citrix Xen 虚拟化产品兼容。目前不支持 VHDX 映像。



Note

VM Export 仅支持动态虚拟硬盘 (VHD)。不支持固定 VHD。

- 流优化型 ESX 虚拟机磁盘 (VMDK) 映像格式，该格式可与 VMware ESX 和 VMware vSphere 虚拟化产品兼容。



Note

您只能将通过 VMware 中的 OVF 导出过程创建的 VMDK 文件导入 Amazon EC2。

- 启动虚拟装置 (OVA) 映像格式，该格式支持将映像与多个硬盘一起导入。

实例类型

AWS 支持将 Windows 实例导入大多数实例类型。[Microsoft Windows BYOL](#) 实例必须作为 Microsoft Windows 的 [专用实例](#) 或 [专用主机](#) 启动，因此无法使用 t2 实例类型，因为它不支持专用实例。

您可以将 Linux 实例导入下列实例类型：

- 通用型: t2.micro | t2.small | t2.medium | m3.medium | m3.large | m3.xlarge | m3.2xlarge
- 计算优化: c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge | cc1.4xlarge
- 内存优化: r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge
- 存储优化: i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge

卷类型和文件系统

AWS 支持使用以下文件系统导入 Windows 和 Linux 实例：

Windows (32 和 64 位)

VM Import/Export 支持使用 NTFS 文件系统格式化并采用 MBR 分区的卷。不支持 GUID 分区表 (GPT) 分区的卷。

Linux/Unix (64 位)

VM Import/Export 支持使用 ext2、ext3、ext4、Btrfs、JFS 或 XFS 文件系统格式化并采用 MBR 分区的卷。不支持 GUID 分区表 (GPT) 分区的卷。

Amazon S3 存储桶

VM Import 需要 Amazon S3 存储桶来将您的磁盘映像存储在要导入 VM 的区域。有关创建 Amazon S3 存储桶的更多信息，请参阅 *Amazon Simple Storage Service 控制台用户指南* 中的[使用存储桶](#)。

VM Import 服务角色

VM Import 使用您的 AWS 账户中的角色执行特定操作（例如，从 Amazon S3 存储桶下载磁盘映像）。您必须利用以下策略和可信实体创建名为 `vmimport` 的角色。利用以下策略创建名为 `trust-policy.json` 的文件：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "vmie.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole",  
            "Condition": {  
                "StringEquals": {  
                    "sts:ExternalId": "vmimport"  
                }  
            }  
        }  
    ]  
}
```

使用 `aws iam create-role` 命令创建名为 `vmimport` 的角色，并向 VM Import/Export 提供对该角色的访问权。



Note

必须将外部 ID 命名为 `vmimport`。

```
aws iam create-role --role-name vmimport --assume-role-policy-document  
file://trust-policy.json
```



Note

您必须在策略文档名称前包含 `file://`（例如，`file://trust-policy.json`），否则该命令将返回错误“`A client error (MalformedPolicyDocument) occurred when calling the CreateRole operation: Syntax errors in policy.`”

为服务角色创建策略

利用以下策略创建名为 role-policy.json 的文件：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3>ListBucket",  
                "s3:GetBucketLocation"  
            ],  
            "Resource": [  
                "arn:aws:s3:::<disk-image-file-bucket>"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::<disk-image-file-bucket>/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:ModifySnapshotAttribute",  
                "ec2:CopySnapshot",  
                "ec2:RegisterImage",  
                "ec2:Describe*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

将 `<disk-image-file-bucket>` 替换为将磁盘文件存储到的适当的 Amazon S3 存储桶。运行以下命令可将策略挂载到上面创建的角色：

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

有关 IAM 角色的更多信息，请参阅 [IAM 用户指南](#) 中的 [IAM 角色（委托和联合）](#)。

IAM 权限

如果您以 AWS Identity and Access Management (IAM) 用户身份登录，那么您的 IAM 策略中需要以下权限才能导入或导出 VM：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:ModifySnapshotAttribute",  
                "ec2:CopySnapshot",  
                "ec2:RegisterImage",  
                "ec2:Describe*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
"Effect": "Allow",
"Action": [
    "s3>ListAllMyBuckets"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "s3>CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3>GetBucketLocation",
    "s3>GetObject",
    "s3>ListBucket",
    "s3>PutObject"
],
"Resource": [ "arn:aws:s3:::mys3bucket", "arn:aws:s3:::mys3bucket/*" ]
},
{
"Effect": "Allow",
"Action": [
    "ec2>CancelConversionTask",
    "ec2>CancelExportTask",
    "ec2>CreateImage",
    "ec2>CreateInstanceExportTask",
    "ec2>CreateTags",
    "ec2>DeleteTags",
    "ec2>DescribeConversionTasks",
    "ec2>DescribeExportTasks",
    "ec2>DescribeInstanceAttribute",
    "ec2>DescribeInstanceState",
    "ec2>DescribeInstances",
    "ec2>DescribeTags",
    "ec2>ImportInstance",
    "ec2>ImportVolume",
    "ec2>StartInstances",
    "ec2>StopInstances",
    "ec2>TerminateInstances",
    "ec2>ImportImage",
    "ec2>ImportSnapshot",
    "ec2>DescribeImportImageTasks",
    "ec2>DescribeImportSnapshotTasks",
    "ec2>CancelImportTask"
],
"Resource": "*"
}
]
```

有关 IAM 用户和策略的更多信息，请参阅[IAM 用户指南](#)中的 [IAM 用户和组](#)和[管理 IAM 策略](#)。

要求和限制

导入 AMI 和快照受下列限制：

- 在每个区域，您最多可以同时进行 20 个导入映像或快照任务。要请求增加此限制，请联系 AWS Support。任务必须自起始日期起的 7 日内完成。

- 已导入的 VM 创建使用硬件虚拟机 (HVM) 虚拟化的 Amazon EC2 AMI。不支持使用 VM Import 来创建使用半虚拟化 (PV) 的 AMI。导入的 VM 内支持 Linux PVHVM 驱动程序。
- 导入的 Red Hat Enterprise Linux (RHEL) VM 必须使用 Cloud Access (BYOL) 许可。
- 导入的 Linux VM 必须使用 64 位映像。不支持导入 32 位 Linux 映像。
- 导入的 Linux VM 应使用默认内核以获得最佳结果。使用自定义 Linux 内核的 VM 无法成功导入。
- 通常，您导入的是压缩版本的磁盘映像；展开的磁盘映像不能超过 1 TiB。
- 确保您拥有至少 250 MB 的可用磁盘空间才能在您希望将其导入到运行 Microsoft Windows 或 Linux 的 Amazon EC2 AMI 实例的任何 VM 上安装驱动程序和其他软件。
- 目前不支持多个网络接口。转换和导入后，您的 VM 会有一个虚拟 NIC，使用 DHCP 进行地址分配。
- 不支持 Internet 协议版本 6 (IPv6) IP 地址。
- 对于 vCenter 4.0 和 vSphere 4.0 用户，请从虚拟机中删除所有附加的 CD-ROM 映像或 ISO。
- Amazon EC2 VM Import 不支持因 P2V 转换而创建的虚拟机。通过在物理设备上通过执行 Linux 或 Windows 安装进程，然后将 Linux 或 Windows 安装导入虚拟机，从而创建磁盘映像，则会发生 P2V 转换。
- Amazon VM Import 不会安装单个根 I/O 虚拟化 (SR-IOV) 驱动程序，除非导入 Microsoft Windows Server 2012 R2 VM。除非您计划使用提供更高性能（每秒数据包）、更短延迟和更低抖动的增强联网，否则不需要这些驱动程序。要在导入您的 VM 后在 c3 或 i2 实例类型上启动增强联网，请查看 [Windows 上的增强联网 \(p. 630\)](#)。对于 Microsoft Windows Server 2012 R2 VM，会在导入过程中自动安装 SR-IOV 驱动程序。
- 结合使用您自己的 Microsoft 许可证（如通过 MSDN 或 [每用户 Windows 软件保障](#)）来通过自有许可 (BYOL) 模式在 AWS 上运行 Microsoft 软件：
 - 您的 BYOL 实例将以现行的 Amazon EC2 Linux 实例定价来进行定价（[Amazon EC2 实例购买选项](#) 中已说明），前提是您 (a) 运行专用实例（有关更多信息，请参阅[专用实例](#)）；(b) 使用 VM Import/Export 从源自您提供的软件二进制文件的 VM 中启动，这将受 VM Import/Export 的现时条款和功能的限制；(c) 将实例指定为 BYOL 实例（即在服务中声明适当的平台类型标志）；(d) 在指定的 AWS 区域内以及 AWS 提供 BYOL 模型的位置运行实例；以及 (e) 使用您提供的或您的密钥管理系统中使用的 Microsoft 密钥进行激活。
 - 您必须考虑的一个实际情况是，在启动某个 Amazon EC2 实例时，该实例可在可用区内的多台服务器中的任一服务器上运行。这意味着，每次启动 Amazon EC2 实例（包括停止/启动）时，该实例可在可用区内的不同服务器上运行。您还必须考虑有关 [Microsoft 产品和在线服务的批量许可](#) 中的 Microsoft 批量许可产品使用权利 (PUR)/产品条款 (PT) 中所述的许可重新分配的限制，或者查看您的特定使用权利来确定您的权利是否与此使用保持一致。
 - 您必须有资格在您与 Microsoft 签订的协议下（例如，在您的 MSDN 用户权利下或您的每用户 Windows 软件保障权利下）使用针对合适的 Microsoft 软件的 BYOL 计划。您单独负责获得所有所需的许可证并遵守所有适用的 Microsoft 许可要求，包括 PUR/PT。此外，您必须已接受 Microsoft 的最终用户许可协议 (Microsoft EULA)，并且一旦使用 BYOL 计划下的 Microsoft 软件，即表示您同意 Microsoft EULA。
 - AWS 建议您咨询您自己的法律顾问和其他顾问以了解并遵守适用的 Microsoft 许可要求。不授权也不允许在违反您与 Microsoft 签订的协议的情况下使用服务（包括使用 licenseType 参数和 BYOL 标志）。

步骤 1：安装 AWS CLI

Abstract

使用 Amazon EC2 命令行工具导入您的 Citrix、Microsoft Hyper-V 或 VMware vSphere 虚拟机。

您可以在 Amazon EC2 实例上安装 AWS CLI 以将您的 Citrix、Microsoft Hyper-V 或 VMware vSphere 虚拟机导入 Amazon EC2。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 命令行界面](#)。

您可以使用 AWS CLI 中的以下命令来以支持的格式导入 VM：

命令	说明
import-image	使用指定磁盘映像中的元数据创建新的导入映像任务并创建 Amazon 系统映像 (AMI)。
import-snapshot	使用指定磁盘映像中的元数据创建新的导入快照任务，并将快照导入 Amazon EBS 中。
describe-import-image-tasks	列出并描述您的导入任务。
describe-import-snapshot-tasks	列出并描述您的快照导入任务。
cancel-import-task	取消活动的导入任务。

步骤 2：准备您的 VM

Abstract

从虚拟化环境导出之前配置 VM。

在将 VM 从虚拟化环境中导出之前，请按照以下指南配置您的 VM。

- 审查前提条件。有关更多信息，请参阅 [VM Import/Export 的先决条件 \(p. 403\)](#)。
- 在您的 VM 上禁用任何反病毒软件或入侵检测软件。可在导入过程完成后重新启用上述服务。
- 从您的 VMware 虚拟机上卸载 VMware 工具。
- 断开连接任何 CD-ROM 驱动（虚拟或实际）。
- 将您的网络设置为 DHCP 而不是静态 IP 地址。如果您希望分配静态私有 IP 地址，请务必在您的 VPC 子网中使用非预留私有 IP 地址。Amazon Virtual Private Cloud (Amazon VPC) 保留了 VPC 子网中的前四个私有 IP 地址。
- 在从虚拟化环境导出您的 VM 之前先将其关闭。

Windows

- 启用 Remote Desktop (RDP) 以进行远程访问。
- 如果配置了主机防火墙（Windows 防火墙或类似防火墙），请确保该防火墙允许访问 RDP。否则在导入完成后，您将无法访问您的实例。
- 确保管理员账户和所有其他用户账户使用安全密码。所有账户均须有密码，否则导入可能失败。
- 确保您的 Windows VM 已安装 .NET Framework 3.5 或更高版本，如 [Amazon Windows EC2Config 服务](#) 所要求的一样。
- 在导入 Windows Server 2008 或 Windows Server 2012 VM 映像之前或之后，您可以在其上运行 System Preparation (Sysprep)。如果您在导入 VM 之前运行 Sysprep，则导入过程将在 VM 中添加一个回复文件，以自动接受最终用户许可协议 (EULA) 并将区域设置设为 EN-US。如果您选择导入后运行 Sysprep，我们建议您使用 Amazon EC2 配置服务运行 Sysprep。

要用您自己的回复文件替代默认回复文件 (unattend.xml)，请执行以下操作：

1. 复制以下示例文件 unattend.xml，并将 processorArchitecture 参数设置为 x86 或 amd64，具体取决于您的操作系统架构：

```
<?xml version='1.0' encoding='UTF-8'?>
<unattend xmlns:wcm='http://schemas.microsoft.com/WMIConfig/2002/State' xmlns='urn:schemas-microsoft-com:unattend'>
  <settings pass='oobeSystem'>
    <component versionScope='nonSxS' processorArchitecture='x86 or amd64' name='Microsoft-Windows-International-Core' publicKeyToken='31bf3856ad364e35'>
```

```
language='neutral'>
<InputLocale>en-US</InputLocale>
<SystemLocale>en-US</SystemLocale>
<UILanguage>en-US</UILanguage>
<UserLocale>en-US</UserLocale>
</component>
<component versionScope='nonSxS' processorArchitecture='x86 or amd64'
name='Microsoft-Windows-Shell-Setup' publicKeyToken='31bf3856ad364e35' lan-
guage='neutral'>
<OOBE>
<HideEULAPage>true</HideEULAPage>
<SkipMachineOOBE>true</SkipMachineOOBE>
<SkipUserOOBE>true</SkipUserOOBE>
</OOBE>
</component>
</settings>
</unattend>
```

2. 将文件保存在 C:\Windows\Panther 目录中，并命名为 unattend.xml。

3. 使用 /oobe 和 /generalize 选项运行 Sysprep。



Note

/oobe 和 /generalize 选项会从 Microsoft Windows 安装中删除所有唯一系统信息并提示您重置管理员密码。

4. 关闭 VM 并从您的虚拟环境中将其导出。

- 在您的 Windows VM 上禁用 Autologon。
- 打开 Control Panel > System and Security > Windows Update。在左窗格中，选择 Change settings。选择所需设置。请注意，如果选择 Download updates but let me choose whether to install them（默认值），则更新检查可能会临时占用实例上 50% 到 99% 的 CPU 资源。检查通常会在实例启动后的几分钟内执行。确保没有等待进行的 Microsoft 更新且计算机未设置成在重启时安装软件。
- 应用以下修补程序：
 - 如果 Windows 中启用了 RealTimelsUniversal 注册表项，那么您无法更改系统时间
 - Windows Server 2008、Windows 7 或 Windows Server 2008 R2 中 DST 转换期间的高 CPU 使用率
 - 启用 RealTimelsUniversal 注册表项。有关详细信息，请参阅 为 Windows 实例设置时间 (p. 292)。

Linux

- 启用安全外壳 (SSH) 以进行远程访问。
- 确保您的主机防火墙（例如 Linux iptables）允许访问 SSH。否则在导入完成后，您将无法访问您的实例。
- 确保您已配置了一个非根用户以使用基于密钥的公共 SSH 在导入您的实例后访问它。使用基于密码的 SSH 和通过 SSH 进行根登录均可行，但不推荐使用。推荐使用公共密钥和非根用户，因为它更安全。VM Import 不会在导入过程中配置 ec2-user 账户。
- 确保您的 Linux VM 将 GRUB（传统 GRUB）或 GRUB 2 作为其启动加载程序。
- 确保您的 Linux VM 使用下列根文件系统之一：EXT2、EXT3、EXT4、Btrfs、JFS 或 XFS。

步骤 3：将您的 VM 从其虚拟化环境导出

Abstract

从 Citrix、Microsoft Hyper-V 或 VMware vCenter 虚拟化环境导出 VM。

完成 VM 导出的准备工作后，您可以从您的虚拟化环境将其导出。有关如何从您的虚拟化环境中导出 VM 的信息，请参阅 Citrix、Microsoft Hyper-V 或 VMware vCenter 虚拟化环境的文档。

Citrix：有关更多信息，请参阅 Citrix 网站的[作为 OVF/OVA 导出 VM](#)。

Microsoft Hyper-V：有关更多信息，请参阅 Microsoft 网站上的[导出和导入虚拟机概述](#)。

VMware：有关更多信息，请参阅 VMware 网站的[导出 OVF 模板](#)。

步骤 4：将您的 VM 导入 Amazon EC2

Abstract

将 VM 导入 Amazon EC2。

从您的虚拟化环境导出您的 VM 后，您可以将其导入 Amazon EC2。无论 VM 来自哪里，导入过程都相同。

以下为需要您了解的有关 VM 实例的重要信息，以及一些安全和存储建议：

- Amazon EC2 将私有 DHCP IP 地址自动分配至您的实例。实例开始运行时，可通过 `ec2-describe-instances` 命令获得 DNS 名称和 IP 地址。出于安全原因，如果实例已导入到 VPC，它将不会获得公有 IP 地址，尽管子网已启用自动分配公有 IP。但是，您可以创建弹性 IP 地址 (EIP) 并将其附加到导入的实例。
- 您的实例将只有一个 Ethernet 网络接口。
- 我们建议您的 Windows 实例对于所有用户账户均包含强密码。我们建议您的 Linux 实例对 SSH 使用公钥。
- 对于 Windows 实例，我们建议您在将虚拟机导入到 Amazon EC2 中后，安装最新版本的 [Amazon Windows EC2Config 服务](#)。

以 OVA 格式将 VM 导入 Amazon EC2 中

您可使用所选的上传工具以 OVA 格式将 VM 上传到 Amazon S3 存储桶。将您的 VM 上传到 Amazon S3 后，您可使用 AWS CLI 导入 OVA 映像。这些工具接受 URL（公共 Amazon S3 文件，适用于私有 Amazon S3 文件的已签名的 GET URL）或 Amazon S3 存储桶和磁盘文件的路径。

使用 `aws ec2 import-image` 创建新的导入映像任务。

此命令的语法如下：

```
C:\> aws ec2 import-image --description "Windows 2008 OVA" --disk-containers file://containers.json
```

文件 `containers.json` 是包含有关映像的信息的 JSON 文档。`S3Key` 是要上传到 `S3Bucket` 的映像文件的名称。

```
[ {  
    "Description": "First CLI task",  
    "Format": "ova",  
    "UserBucket": {
```

```
        "S3Bucket": "my-import-bucket",
        "S3Key": "my-windows-2008-vm.ova"
    }
}]
```

响应示例

```
<ImportImageResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
<progress>2</progress>
<importTaskId>import-ami-fgxn195v</importTaskId>
<status>active</status>
<description>Windows 2008 OVA</description>
<snapshotTaskDetailSet>
    <item>
        <diskImageSize>0.0</diskImageSize>
        <userBucket>
            <s3Bucket>my-import-bucket</s3Bucket>
            <s3Key>my-windows-2008-vm.ova</s3Key>
        </userBucket>
    </item>
</snapshotTaskDetailSet>
<licenseType>AWS</licenseType>
<statusMessage>pending</statusMessage>
<requestId>1571e127-d6d8-4984-b4f1-3a21e9dbdc5</requestId>
</ImportImageResponse>
```

将具有多个显式磁盘的 VM 导入 Amazon EC2 中

在将您的 VM 磁盘映像上传到 Amazon S3 后，可使用 AWS CLI 导入您的磁盘映像或快照。这些工具接受 URL（公共 Amazon S3 文件，适用于私有 Amazon S3 文件的已签名的 GET URL）或 Amazon S3 存储桶和磁盘文件的路径。您还可以使用 Amazon EBS 快照作为 ImportImage API 的输入。

将 aws ec2 import-image 命令用于多个显式磁盘的示例

使用 aws ec2 import-image 命令创建新的导入映像任务。

```
C:\> aws ec2 import-image --description "Windows 2008 VMDKs" --disk-containers
file://containers.json
```

文件 containers.json 是包含有关映像的信息的 JSON 文档。S3Key 是要上传到 S3Bucket 的映像文件的名称。您可以通过指定 Amazon S3 存储桶的 URL、提供 Amazon S3 存储桶名称和密钥或通过提供 EBS 快照 ID 上传卷。有关更多信息，请参阅 [import-image](#)。

```
[ {
    "Description": "First CLI task",
    "Format": "vmdk",
    "UserBucket": {
        "S3Bucket": "my-import-bucket",
        "S3Key": "my-windows-2008-vm-disk1.vmdk"
    }
},
{
    "Description": "Second CLI task",
}
```

```
"Format": "vmdk",
"UserBucket": {
    "S3Bucket": "my-import-bucket",
    "S3Key": "my-windows-2008-vm-disk2.vmdk"
}
}]
```

响应示例

```
<ImportImageResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
<progress>2</progress>
<importTaskId>import-ami-fgxn591c</importTaskId>
<status>active</status>
<description>Windows 2008 VMDKs</description>
<snapshotTaskDetailSet>
    <item>
        <diskImageSize>0.0</diskImageSize>
        <userBucket>
            <s3Bucket>my-import-bucket</s3Bucket>
            <s3Key>my-windows-2008-vm-disk1.vmdk</s3Key>
        </userBucket>
    </item>
    <item>
        <diskImageSize>0.0</diskImageSize>
        <userBucket>
            <s3Bucket>my-import-bucket</s3Bucket>
            <s3Key>my-windows-2008-vm-disk2.vmdk</s3Key>
        </userBucket>
    </item>
</snapshotTaskDetailSet>
<licenseType>AWS</licenseType>
<statusMessage>pending</statusMessage>
<requestId>1571e127-d6d8-4984-b4f1-3a21e9dbdcb5</requestId>
</ImportImageResponse>
```

检查您的导入映像任务的状态

Abstract

使用 Amazon EC2 CLI 检查导入镜像任务的状态。

aws ec2 describe-import-image-tasks 命令会返回导入任务的状态。包括的状态值如下：

- active - 您的任务处于活动状态且当前正在进行中。
- deleting - 您的任务当前被取消。
- deleted - 您的任务已取消。
- completed - 您的任务已完成，并且 AMI 已准备就绪，可以随时使用。

检查您的导入任务的状态

使用 aws ec2 describe-import-image-tasks 命令返回任务的状态。此命令的语法如下：

使用 ec2 describe-import-image-tasks 命令的示例：

您可以在以下示例中查看您的导入任务的状态。

```
C:\> aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\": [\"import-ami-fgxn195v\"], \"NextToken\": \"abc\", \"MaxResults\": 10 } "
```

响应示例

以下响应显示了来自 `aws ec2 describe-import-image-tasks` 命令的输出。

```
<DescribeImportImageTasksResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
  <importImageTaskSet>
    <item>
      <platform>Windows</platform>
      <importTaskId>import-ami-fgs8im0c</importTaskId>
      <imageId>ami-4a6c2722</imageId>
      <status>completed</status>
      <description>Linux OVA</description>
      <architecture>x86_64</architecture>
      <snapshotTaskDetailSet>
        <item>
          <diskImageSize>3.115815424E9</diskImageSize>
          <deviceName>/dev/sda1</deviceName>
          <description>First CLI task</description>
          <format>VMDK</format>
          <url>https://mys3bucket/vms/my-linux-vm.ova?AWSAccessKeyId=myAccessKeyId&Expires=expirationDate&Signature=mySignature</url>
        </item>
      </snapshotTaskDetailSet>
      <licenseType>AWS</licenseType>
    </item>
  </importImageTaskSet>
  <requestId>377eclca-6a47-42f5-8b84-aa07ff87f7b0</requestId>
</DescribeImportImageTasksResponse>
```

将磁盘映像导入 Amazon EBS 中

Abstract

将您的数据存储导入 Amazon EBS 中，然后将其附加到您的某个现有 EC2 实例。

本部分介绍如何将磁盘导入 Amazon EBS 快照中，然后创建 Amazon EBS 卷。Amazon EC2 支持导入 RAW、虚拟硬盘 (VHD) 以及 ESX 虚拟机磁盘 (VMDK) 磁盘格式。

在您将您的虚拟机从虚拟化环境中导出之后，只需一步即可将卷导入 Amazon EBS 中。创建上传任务以将磁盘映像上传到 Amazon S3，然后创建导入任务以使用该卷。

将磁盘映像导入 Amazon EBS 中

1. 使用 `aws ec2 import-snapshot` 命令将您的卷上传到 Amazon EBS。您可以通过指定 Amazon S3 存储桶的 URL 或通过提供 Amazon S3 存储桶名称和密钥上传卷。有关更多信息，请参阅 [import-snapshot](#)。

使用 `aws ec2 import-snapshot` 命令的示例。

```
C:\> aws ec2 import-snapshot --description "Windows 2008 VMDK" --disk-container file://containers.json
```

文件 containers.json 是包含有关快照的信息的 JSON 文档。

```
[ {  
    "DryRun": false,  
    "Description": "First CLI snap",  
    "DiskContainer": {  
        "Description": "Windows 2008",  
        "Format": "vmdk",  
        "Url": "https://mys3bucket/vms/Win_2008_Server_Enterprise_R2_64-bit.vmdk?AWSAccessKeyId=myaccesskey&Expires=expirationdate&Signature=signature"  
    }  
}]
```

响应示例

```
<ImportSnapshotResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">  
  <snapshotTaskDetail>  
    <diskImageSize>0.0</diskImageSize>  
    <progress>3</progress>  
    <status>active</status>  
    <description>Windows 2008 VMDK</description>  
    <url>https://mys3bucket/vms/Win_2008_Server_Enterprise_R2_64-bit.vmdk?AWSAccessKeyId=myaccesskey&Expires=expirationdate&Signature=signature</url>  
    <statusMessage>pending</statusMessage>  
  </snapshotTaskDetail>  
  <importTaskId>import-snap-ffy5pvea</importTaskId>  
  <description>Windows 2008 VMDK</description>  
  <requestId>2ef5652d-6816-4c20-89b2-a4bbb0560190</requestId>  
</ImportSnapshotResponse>
```

2. 使用 aws ec2 describe-import-snapshot-tasks 命令可确认已成功导入快照。

使用 aws ec2 describe-import-snapshot-tasks 命令的示例

```
C:\> aws ec2 describe-import-snapshot-tasks --cli-input-json "{ \"ImportTaskIds\": [\"import-snap-fgr1mng7\"], \"NextToken\": \"abc\", \"MaxResults\": 10 }"
```

响应示例

```
<DescribeImportSnapshotTasksResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">  
  <importSnapshotTaskSet>  
    <item>  
      <snapshotTaskDetail>  
        <diskImageSize>3.115815424E9</diskImageSize>  
        <progress>22</progress>  
        <status>active</status>  
        <description>Windows 2008 VMDK</description>  
        <format>VMDK</format>  
        <url>https://mys3bucket/vms/Win_2008_Server_Enterprise_R2_64-bit.vmdk?AWSAccessKeyId=myaccesskey&Expires=expirationdate&Signature=signature</url>  
      </snapshotTaskDetail>  
    </item>  
  </importSnapshotTaskSet>  
</DescribeImportSnapshotTasksResponse>
```

```
<statusMessage>validated</statusMessage>
</snapshotTaskDetail>
<importTaskId>import-snap-fgr1mmg7</importTaskId>
<description>Windows 2008 VMDK</description>
</item>
</importSnapshotTaskSet>
<requestId>3ec7adc5-001a-454f-abc3-820c8a91c353</requestId>
</DescribeImportSnapshotTasksResponse>
```

此示例中的状态为 active，这表示导入仍在进行中。

3. 使用 aws ec2 create-volume 从 Amazon EBS 快照创建卷。以下示例从快照创建卷。确保您选择的是实例所在的可用区，以便将 Amazon EBS 卷挂载到 Amazon EC2 实例。

```
C:\> aws ec2 create-volume --availability-zone us-east-1a --snapshot-id snap-1234567890abcdef0
```

输出示例

```
{  
    "AvailabilityZone": "us-east-1a",  
    "VolumeId": "vol-1234567890abcdef0",  
    "State": "creating",  
    "SnapshotId": "snap-1234567890abcdef0"  
}
```

4. 使用 aws ec2 attach-volume 将 Amazon EBS 卷挂载到您的某个现有 Amazon EC2 实例。以下示例将卷 vol-1234567890abcdef0 挂载到设备 /dev/sdf 上的 i-1234567890abcdef0 实例。

```
C:\> aws ec2 attach-volume --volume-id vol-1234567890abcdef0 --instance-id i-1234567890abcdef0 --device /dev/sdf
```

输出示例

```
{  
    "AttachTime": "YYYY-MM-DDTHH:MM:SS.000Z",  
    "InstanceId": "i-1234567890abcdef0",  
    "VolumeId": "vol-1234567890abcdef0",  
    "State": "attaching",  
    "Device": "/dev/sdf"  
}
```

取消导入任务

Abstract

取消导入任务。

使用 aws ec2 cancel-import-task 命令取消活动的导入任务。任务可以是 AMI 或快照的导入。

取消导入任务

使用要通过 aws ec2 cancel-import-task 命令取消的导入的任务 ID。

使用 aws ec2 cancel-import-task 命令的示例

以下为取消与任务 ID import-ami-fg4z7c9h相关之上传的示例。

```
C:\> aws ec2 cancel-import-task --import-task-id "import-ami-fg4z7c9h"
```

响应示例

```
<CancelImportTaskResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
  <importTaskId>import-ami-fg4z7c9h</importTaskId>
  <state>active</state>
  <previousState>deleting</previousState>
  <requestId>1e5abd4c-b8de-4b3c-8cla-73d93b006clf</requestId>
</CancelImportTaskResponse>
```

步骤 5：在 Amazon EC2 中启动实例

Abstract

基于已导入的 VM 从 AMI 启动 Amazon EC2 实例。

完成 aws ec2 import-image 任务后，Amazon EC2 控制台中将显示您的 AMI。您可选择此 AMI，然后基于此 AMI 启动 Amazon EC2 实例。

基于您的 AMI 启动 Amazon EC2 实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 AMIs。
4. 在内容窗格中，选择此 AMI，然后单击 Launch。

将 VM 作为实例导入 Amazon EC2

Abstract

使用 ImportInstance API 从 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 虚拟化环境将 VM 作为实例导入 Amazon EC2。

您可以通过两种方式在 Amazon EC2 中启动实例。您可以从 Amazon 系统映像 (AMI) 启动实例，或者，您可以从您在 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 等虚拟化环境下导入的虚拟机 (VM) 启动实例。本节讲述导入 VM 并将其作为 Amazon EC2 实例启动。此方法仅支持具有单个卷的 VM。要导入具有多个卷的 VM，请参阅[将 VM 作为镜像导入 Amazon EC2 \(p. 402\)](#)。

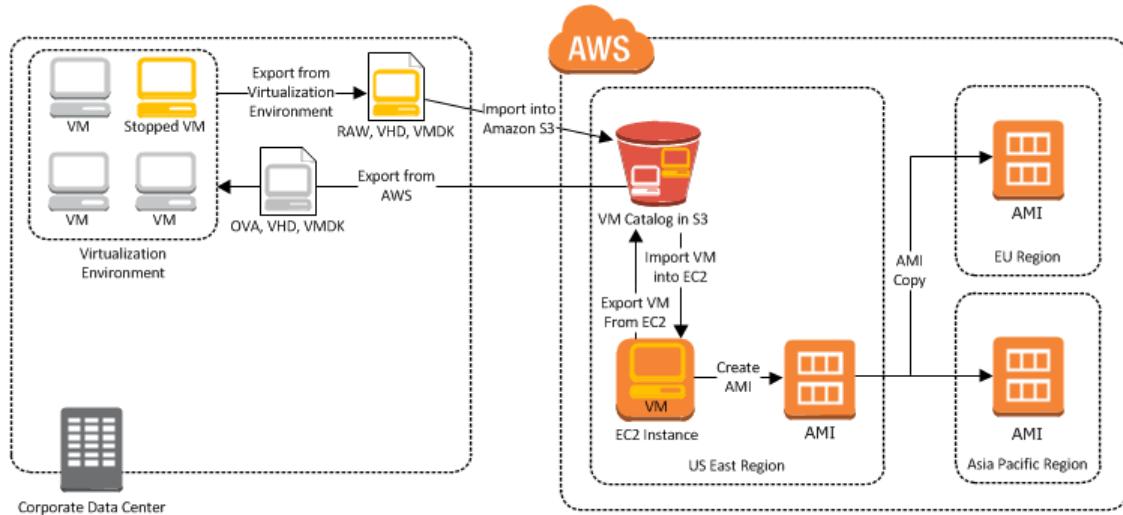
要在 Amazon EC2 中将您的 VM 作为实例使用，您必须首先将其从虚拟化环境中导出，然后使用 Amazon EC2 命令行界面 (CLI) 或 API 工具将其导入 Amazon EC2。如果您要从 VMware vCenter 导入 VM，您还可以使用 AWS Connector for vCenter 从 VMware 导出 VM，然后将其导入 Amazon EC2。有关更多信息，请参阅 [AWS Management Portal for vCenter 用户指南](#) 中的使用 AWS Connector for vCenter 将您的虚拟机迁移至 Amazon EC2。



Important

您不能使用 [ec2-import-instance](#) 导入使用自有许可 (BYOL) 模式的 Microsoft Windows 实例。要导入这些实例类型，请参阅[将 VM 作为镜像导入 Amazon EC2 \(p. 402\)](#)。

下图显示将 VM 从您的本地虚拟化环境导出到 AWS 的过程。



无论使用 CLI 或 API，您将执行将 VM 或卷导入 Amazon EC2 的相同步骤。下面是使用 CLI 的过程。

将 VM 导入 Amazon EC2 中

1. 安装 CLI。有关更多信息，请参阅 [步骤 1：安装 Amazon EC2 CLI \(p. 422\)](#)。
2. 为 VM 导入 Amazon EC2 做准备。有关更多信息，请参阅 [步骤 2：准备您的 VM \(p. 423\)](#)。
3. 从虚拟化环境中导出 VM。有关更多信息，请参阅 [步骤 3：将您的 VM 从其虚拟化环境导出 \(p. 424\)](#)。
4. 将 VM 导入 Amazon EC2。有关信息，请参阅 [步骤 4：将您的 VM 导入 Amazon EC2 \(p. 425\)](#)。
5. 在 Amazon EC2 中启动实例。有关更多信息，请参阅 [步骤 5：在 Amazon EC2 中启动实例 \(p. 431\)](#)。

VM Import/Export 的先决条件

Abstract

在开始导入您的虚拟机之前查看基本信息和限制条件。

在您开始将 VM 从您的虚拟化环境导出或从 Amazon EC2 导入和导出 VM 之前，您必须了解 AWS 支持的操作系统和映像格式，还必须了解导出实例和卷的限制。

要从 Amazon EC2 导入或导出 VM，您还必须安装 CLI 工具：

- 有关安装 Amazon EC2 CLI 的更多信息，请参阅 [Amazon EC2 命令行参考](#)。
- 有关安装 AWS CLI 的更多信息，请参阅 [AWS Command Line Interface 用户指南](#)。有关 AWS CLI 中的 Amazon EC2 命令的更多信息，请参阅 [AWS Command Line Interface Reference](#) 中的 `ec2`。

内容

- [操作系统 \(p. 420\)](#)
- [卷类型和文件系统 \(p. 421\)](#)
- [Amazon S3 存储桶 \(p. 421\)](#)
- [要求和限制 \(p. 421\)](#)

操作系统

以下操作系统可以在 Amazon EC2 中导入和导出。

Windows (32 和 64 位)

- 含 Service Pack 1 (SP1) 的 Microsoft Windows Server 2003 (标准版、数据中心版、企业版) 或更高版本 (32 位和 64 位)
- Microsoft Windows Server 2003 R2 (标准版、数据中心版、企业版) (32 位和 64 位)
- Microsoft Windows Server 2008 (标准版、数据中心版、企业版) (32 位和 64 位)
- Microsoft Windows Server 2008 R2 (标准版、数据中心版、企业版) (仅限 64 位)
- Microsoft Windows Server 2012 (标准版、数据中心版) (仅限 64 位)
- Microsoft Windows Server 2012 R2 (标准版、数据中心版) (仅限 64 位)
- Microsoft Windows 7 (专业版、企业版、旗舰版) (32 位和 64 位)



Note

VM Import 目前支持导入运行 Microsoft Windows 7 美国英语版 (专业版、企业版、旗舰版) 的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 8 (专业版、企业版) (32 位和 64 位)



Note

VM Import 目前支持导入运行 Microsoft Windows 8 美国英语版 (专业版、企业版) 的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 8.1 (专业版、企业版) (仅限 64 位)



Note

VM Import 目前支持导入运行 Microsoft Windows 8.1 美国英语版 (专业版、企业版) 的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

- Microsoft Windows 10 (家庭版、专业版、企业版、教育版) (仅限 64 位)



Note

VM Import 目前支持导入运行 Microsoft Windows 10 美国英语版 (家庭版、专业版、企业版、教育版) 的 VM。在导入这些操作系统时，您必须遵守 [要求和限制 \(p. 408\)](#)。

Linux/Unix (64 位)

- Red Hat Enterprise Linux (RHEL) 5.1-5.11、6.1-6.6、7.0-7.1



Note

导入的 Linux VM 应使用默认内核以获得最佳结果。使用自定义 Linux 内核的 VM 无法成功导入。

- Red Hat Enterprise Linux (RHEL) 5.1-5.11、6.1-6.6、7.0-7.1



Note

不支持 RHEL 6.0，因为它缺少在 Amazon EC2 上运行所需的驱动程序。

VM Import 支持 RHEL 实例的许可可移植性。您的现有 RHEL 许可与它们的关联 RHEL 实例一同导入。有关对于 Red Hat Cloud Access 的资格的更多信息，请参阅 Red Hat 网站的[资格](#)。

- SUSE Linux Enterprise Server
 - SUSE Linux Enterprise Server 11 Service Pack 1 - 2.6.32.12-0.7
 - SUSE Linux Enterprise Server 11 Service Pack 2 - 3.0.13-0.27
 - SUSE Linux Enterprise Server 11 Service Pack 3 - 3.0.76-0.11、3.0.101-0.8 和 3.0.101-0.15
 - SUSE Linux Enterprise Server 11 Service Pack 4 - 3.0.101-63
 - SUSE Linux Enterprise Server 12 - 3.12.28-4
 - SUSE Linux Enterprise Server 12 Service Pack 1 - 3.12.49-11
- Ubuntu 12.04、12.10、13.04、13.10、14.04、14.10、15.04
- CentOS 5.1-5.11、6.1-6.6、7.0-7.2



Note

不支持 CentOS 6.0，因为它缺少在 Amazon EC2 上运行所需的驱动程序。

- Debian 6.0.0-6.0.8、7.0.0-7.8.0、8.0.0
- Oracle Linux 6.1-6.6、7.0-7.1
- Fedora Server 19-21

卷类型和文件系统

AWS 支持使用以下文件系统导入 Windows 和 Linux 实例：

Windows (32 和 64 位)

VM Import/Export 支持使用 NTFS 文件系统格式化并采用 MBR 分区的卷。不支持 GUID 分区表 (GPT) 分区的卷。

Linux/Unix (64 位)

VM Import/Export 支持使用 ext2、ext3、ext4、Btrfs、JFS 或 XFS 文件系统格式化并采用 MBR 分区的卷。不支持 GUID 分区表 (GPT) 分区的卷。

Amazon S3 存储桶

VM Import 需要 Amazon S3 存储桶来将您的磁盘映像存储在要导入 VM 的区域。有关创建 Amazon S3 存储桶的更多信息，请参阅 *Amazon Simple Storage Service 控制台用户指南* 中的[使用存储桶](#)。

要求和限制

导入实例和卷受以下条件的限制：

- 在每个区域，您最多可以同时进行五个导入任务。要请求增加此限制，请联系 AWS Support。任务必须自起始日期起的 7 日内完成。
- 已导入的 VM 会创建使用硬件虚拟机 (HVM) 虚拟化的 EC2 实例。不支持使用 VM Import 来创建使用半虚拟化 (PV) 的实例。导入的 VM 内支持 Linux PVHVM 驱动程序。
- 导入的 Red Hat Enterprise Linux (RHEL) VM 必须使用 Cloud Access (BYOL) 许可。
- 导入的 Linux VM 必须使用 64 位映像。不支持导入 32 位 Linux 映像。
- 导入的 Linux VM 应使用默认内核以获得最佳结果。使用自定义 Linux 内核的 VM 无法成功导入。
- 通常，您导入的是压缩版本的磁盘映像；展开的磁盘映像不能超过 1 TiB。

- 确保您的 VM 仅使用一个磁盘。不支持使用多个磁盘导入 VM。对于 Linux VM，/boot 和 / 可位于不同分区中，但它们需要在同一磁盘上。

我们建议您只使用启动卷导入 VM，并使用 [ec2-import-volume](#) 命令导入任何其他磁盘。在完成 ImportInstance 任务后，可使用 [ec2-attach-volume](#) 命令将其他卷与您的实例关联。

- 虚拟硬盘 (VHD) 映像必须是动态的。
- 确保您拥有至少 250 MB 的可用磁盘空间才能在您希望将其导入运行 Microsoft Windows 或 Linux 的 Amazon EC2 实例的任何 VM 上安装驱动程序和其他软件。
- 导入的 VM 自动具有对 Amazon EC2 实例存储的访问权限，该存储是临时磁盘存储，位于以物理方式连接到主计算机的磁盘上。您不能在导入时禁用它。有关实例存储的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。
- 目前不支持多个网络接口。将您的实例转换和导入后，它会拥有一个使用 DHCP 的虚拟 NIC 以进行地址分配。
- 不支持 Internet 协议版本 6 (IPv6) IP 地址。
- 对于 vCenter 4.0 和 vSphere 4.0 用户，请从虚拟机中删除所有附加的 CD-ROM 映像或 ISO。
- Amazon VM Import 不会在 c3 和 i2 实例类型上安装单个根 I/O 虚拟化 (SR-IOV) 驱动程序，除非导入 Microsoft Windows Server 2012 R2 VM。除非您计划使用提供更高性能（每秒数据包）、更短延迟和更低抖动的增强联网，否则不需要这些驱动程序。要在导入您的 VM 后在 c3 或 i2 实例类型上启动增强联网，请查看 [Windows 上的增强联网 \(p. 630\)](#)。对于 Microsoft Windows Server 2012 R2 VM，会在导入过程中自动安装 SR-IOV 驱动程序。
- 您无法导入使用自有许可 (BYOL) 模型的 Microsoft Windows VM。要导入这些 VM，请参阅[将 VM 为镜像导入 Amazon EC2 \(p. 402\)](#)。

步骤 1：安装 Amazon EC2 CLI

Abstract

使用 Amazon EC2 命令行工具导入您的 Citrix、Microsoft Hyper-V 或 VMware vSphere 虚拟机。

您需要安装 Amazon EC2 CLI 才能将您的 Citrix、Microsoft Hyper-V 或 VMware vSphere 虚拟机导入 Amazon EC2 或将其从 Amazon EC2 导出。如果您尚未安装 Amazon EC2 CLI，请参阅[设置 Amazon EC2 工具](#)。

您将使用下列 Amazon EC2 命令导入或导出 VM。

命令	说明
ec2-import-instance	使用指定磁盘映像中的元数据创建新的导入实例任务，并将实例导入 Amazon EC2 中。
命令行中的	使用指定磁盘映像中的元数据创建新的导入卷任务，并将该卷导入 Amazon EC2 中。
ec2-resume-import	重新开始上传与导入实例或导入卷任务 ID 相关的磁盘映像。
ec2-describe-conversion-tasks	列出并描述您的导入任务。
ec2-cancel-conversion-task	取消活动的导入任务。任务可以是实例或卷的导入。
ec2-delete-disk-image	删除部分或全部上传的磁盘映像以便从 Amazon S3 存储桶导入。
ec2-create-image-export-task	将正在运行或停止的实例导出到 Amazon S3 存储桶。

命令	说明
ec2-cancel-export-task	取消活动的导出任务。
ec2-describe-export-tasks	列出并描述您的导出任务，包括最近取消和完成的任务。

有关上述命令和其他 Amazon EC2 命令的信息，请参阅 [Amazon EC2 命令行参考](#)。

步骤 2：准备您的 VM

Abstract

从虚拟化环境导出之前配置 VM。

在将 VM 从虚拟化环境中导出之前，请按照以下指南配置您的 VM。

- 审查前提条件。有关更多信息，请参阅 [VM Import/Export 的先决条件 \(p. 403\)](#)。
- 在您的 VM 上禁用任何反病毒软件或入侵检测软件。可在导入过程完成后重新启用上述服务。
- 从您的 VMware 虚拟机上卸载 VMware 工具。
- 断开连接任何 CD-ROM 驱动（虚拟或实际）。
- 将您的网络设置为 DHCP 而不是静态 IP 地址。如果您希望分配静态私有 IP 地址，请务必在您的 VPC 子网中使用非预留私有 IP 地址。Amazon Virtual Private Cloud (Amazon VPC) 保留了 VPC 子网中的前四个私有 IP 地址。
- 在导出前，请先关闭您的 VM。

Windows

- 启用 Remote Desktop (RDP) 以进行远程访问。
- 如果配置了主机防火墙（Windows 防火墙或类似防火墙），请确保该防火墙允许访问 RDP。否则在导入完成后，您将无法访问您的实例。
- 确保管理员账户和所有其他用户账户使用安全密码。所有账户均须有密码，否则导入可能失败。
- 确保您的 Windows VM 已安装 .NET Framework 3.5 或更高版本，如 [Amazon Windows EC2Config 服务](#) 所要求的一样。
- 在导入 Windows Server 2008 或 Windows Server 2012 VM 映像之前或之后，您可以在其上运行 System Preparation (Sysprep)。如果您在导入 VM 之前运行 Sysprep，则导入过程将在 VM 中添加一个回复文件，以自动接受最终用户许可协议 (EULA) 并将区域设置设为 EN-US。如果您选择导入后运行 Sysprep，我们建议您使用 Amazon EC2 配置服务运行 Sysprep。

要用您自己的回复文件替代默认回复文件 (unattend.xml)，请执行以下操作：

- 复制以下示例文件 unattend.xml，并将 processorArchitecture 参数设置为 x86 或 amd64，具体取决于您的操作系统架构：

```
<?xml version='1.0' encoding='UTF-8'?>
<unattend xmlns:wcm='http://schemas.microsoft.com/WMIConfig/2002/State' xmlns='urn:schemas-microsoft-com:unattend'>
    <settings pass='oobeSystem'>
        <component versionScope='nonSxS' processorArchitecture='x86 or amd64' name='Microsoft-Windows-International-Core' publicKeyToken='31bf3856ad364e35' language='neutral'>
            <InputLocale>en-US</InputLocale>
            <SystemLocale>en-US</SystemLocale>
            <UILanguage>en-US</UILanguage>
```

```
<UserLocale>en-US</UserLocale>
</component>
<component versionScope='nonSxS' processorArchitecture='x86 or amd64'
name='Microsoft-Windows-Shell-Setup' publicKeyToken='31bf3856ad364e35' lan
guage='neutral'>
<OOBE>
<HideEULAPage>true</HideEULAPage>
<SkipMachineOOBE>true</SkipMachineOOBE>
<SkipUserOOBE>true</SkipUserOOBE>
</OOBE>
</component>
</settings>
</unattend>
```

2. 将文件保存在 C:\Windows\Panther 目录中，并命名为 unattend.xml。
3. 使用 /oobe 和 /generalize 选项运行 Sysprep。



Note

/oobe 和 /generalize 选项会从 Microsoft Windows 安装中删除所有唯一系统信息并提示您重置管理员密码。

4. 关闭 VM 并从您的虚拟环境中将其导出。
- 在您的 Windows VM 上禁用 Autologon。
 - 确保没有等待进行的 Microsoft 更新且计算机未设置成在重启时安装软件。
 - 应用以下修补程序：
 - 如果 Windows 中启用了 RealTimelsUniversal 注册表项，那么您无法更改系统时间
 - Windows Server 2008、Windows 7 或 Windows Server 2008 R2 中 DST 转换期间的高 CPU 使用率
 - 启用 RealTimelsUniversal 注册表项。有关详细信息，请参阅 为 Windows 实例设置时间 (p. 292)。

Linux

- 启用安全外壳 (SSH) 以进行远程访问。
- 确保您的主机防火墙（例如 Linux iptables）允许访问 SSH。否则在导入完成后，您将无法访问您的实例。
- 确保您已配置了一个非根用户以使用基于密钥的公共 SSH 在导入您的实例后访问它。使用基于密码的 SSH 和通过 SSH 进行根登录均可行，但不推荐使用。推荐使用公共密钥和非根用户，因为它更安全。VM Import 不会在导入过程中配置 ec2-user 账户。
- 确保您的 Linux VM 将 GRUB（传统 GRUB）或 GRUB 2 作为其启动加载程序。
- 确保您的 Linux VM 使用下列根文件系统之一：EXT2、EXT3、EXT4、Btrfs、JFS 或 XFS。

步骤 3：将您的 VM 从其虚拟化环境导出

Abstract

从 Citrix、Microsoft Hyper-V 或 VMware vCenter 虚拟化环境导出 VM。

完成 VM 导出的准备工作后，您可以从您的虚拟化环境将其导出。有关如何从您的虚拟化环境中导出 VM 的信息，请参阅 Citrix、Microsoft Hyper-V 或 VMware vCenter 虚拟化环境的文档。

Citrix：有关更多信息，请参阅 Citrix 网站的[作为 OVF/OVA 导出 VM](#)。

Microsoft Hyper-V：有关更多信息，请参阅 Microsoft 网站上的[导出和导入虚拟机概述](#)。

VMware：有关更多信息，请参阅 VMware 网站的[导出 OVF 模板](#)。

步骤 4：将您的 VM 导入 Amazon EC2

Abstract

将 VM 导入 Amazon EC2。

从您的虚拟化环境导出您的 VM 后，您可以将其导入 Amazon EC2。无论 VM 来自哪里，导入过程都相同。

以下为需要您了解的有关 VM 实例的重要信息，以及一些安全和存储建议：

- Amazon EC2 将私有 DHCP IP 地址自动分配至您的实例。实例开始运行时，可通过 `ec2-describe-instances` 命令获得 DNS 名称和 IP 地址。要为您的实例指定私有 IP 地址，请将 `--private-ip-address` 选项与 `ec2-import-instance` 命令结合使用。
- 出于安全原因，如果将实例导入到 VPC，则您无法为其分配公有 IP 地址，即使子网已启用自动分配公有 IP 也是如此。但是，您可以创建弹性 IP 地址 (EIP) 并将其附加到导入的实例。此外，您也可以作为映像导入 VM，然后在启动 VM 时为其分配公有 IP 地址。有关作为映像导入 VM 的更多信息，请参阅[将 VM 作为镜像导入 Amazon EC2 \(p. 402\)](#)。
- 您的实例只有一个 Ethernet 网络接口。
- 若要在创建导入任务时指定要使用的子网，请使用带有 `--subnet subnet_id` 选项的 `ec2-import-instance` 命令；否则，您的实例将使用公有 IP 地址。我们建议您使用限制性安全组来控制对实例的访问。
- 我们建议您的 Windows 实例对于所有用户账户均包含强密码。我们建议您的 Linux 实例对 SSH 使用公钥。
- 对于 Windows 实例，我们建议您在将虚拟机导入到 Amazon EC2 中后，安装最新版本的 [Amazon Windows EC2Config 服务](#)。
- 如果未设置 `AWS_ACCESS_KEY` 和 `AWS_SECRET_KEY` 环境变量，则除了提供 `-o` 和 `-w` 选项以指定 Amazon S3 存储桶拥有者和私有密钥之外，您还必须包括 `-O` 和 `-W` 选项。

将 VM 导入 Amazon EC2 中

使用 `ec2-import-instance` 创建新的导入实例任务。

此命令的语法如下：

```
ec2-import-instance disk_image_filename -f file_format -t instance_type -a architecture -b s3_bucket_name -o owner -w secret_key -p platform_name -O your_access_key -W your_secret_key
```

如果 VM 的导入中断，您可以使用 `ec2-resume-import` 命令从其停止位置恢复导入。有关更多信息，请参阅[恢复上传 \(p. 429\)](#)。

示例 (Windows)

通过以下命令可以创建导入 Windows Server 2008 SP2 (32 位) VM 的实例任务。

```
C:\> ec2-import-instance ./WinSvr8-2-32-disk1.vmdk -f VMDK -t m1.small -a i386 -b myawsbucket -o AKIAIOSFODNN7EXAMPLE -w wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY -p Windows -o AKIAI44QH8DHBEXAMPLE -W je7MtGbC1wBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

此请求使用 VMDK 文件 WinSvr8-2-32-disk1.vmdk 创建导入任务。（请注意，可以选择使用 VHD 或 RAW 格式。）如果您没有使用 -s 参数指定请求卷的大小，则会使用基于磁盘映像文件的卷大小。输出类似于以下内容。

```
Requesting volume size: 25 GB
Disk image format: Stream-optimized VMDK
Converted volume size: 26843545600 bytes (25.00 GiB)
Requested EBS volume size: 26843545600 bytes (25.00 GiB)
TaskType      IMPORTINSTANCE TaskId import-i-fhbx6hua      ExpirationTime
              2011-09-09T15:03:38+00:00      Status active StatusMessage Pending In
stanceID      i-1234567890abcdef0
DISKIMAGE     DiskImageFormat VMDK      DiskImageSize 5070303744
VolumeSize    25      AvailabilityZone cn-north-1c      Approximate
BytesConverted 0      Status active StatusMessage Pending
Creating new manifest at testImport/9cba4345-b73e-4469-8106-
2756a9f5a077/Win_2008_R1_EE_64.vmdkmanifest.xml
Uploading the manifest file
Uploading 5070303744 bytes across 484 parts
0% |-----| 100%
|=====
Done
```

示例 (Linux)

以下示例创建一个导入 64 位 Linux VM 的导入实例任务。

```
$ ec2-import-instance rhel6.4-64bit-disk.vhd -f vhd -t m3.xlarge -a x86_64 -b
myawsbucket -o AKIAIOSFODNN7EXAMPLE -w wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
-p Linux
```

此请求使用 VHD 文件 rhel6.4-64bit-disk.vhd 创建导入任务。输出类似于以下内容。

```
Requesting volume size: 8 GB
TaskType      IMPORTINSTANCE TaskId import-i-ffnzq636      ExpirationTime
              2013-12-12T22:55:18Z      Status active StatusMessage Pending InstanceID
              i-1234567890abcdef0
DISKIMAGE     DiskImageFormat VHD      DiskImageSize 861055488
VolumeSize    8      AvailabilityZone cn-north-1d      ApproximateBytesCon
verted      0      Status active StatusMessage Pending
Creating new manifest at myawsbucket/b73bae14-7ec5-4122-8958-
4234028eld9f/rhel6.4-64bit-disk.vhdmanifest.xml
Uploading the manifest file
Uploading 861055488 bytes across 83 parts
0% |-----| 100%
|=====
Done

Average speed was 11.054 MBps

The disk image for import-i-ffnzq636 has been uploaded to Amazon S3 where it
is being converted into
an EC2 instance. You may monitor the progress of this task by running ec2-de
scribe-conversion-tasks.
When the task is completed, you may use ec2-delete-disk-image to remove the
image from S3.
```

检查您的导入任务的状态

Abstract

使用 Amazon EC2 CLI 检查导入任务的状态。

[ec2-describe-conversion-tasks](#) 命令返回导入任务的状态。包括的状态值如下：

- active – 您的实例或卷仍在导入中。
- cancelling – 您的实例或卷仍在取消中。
- cancelled – 您的实例或卷已被取消。
- completed – 您的实例或卷已做好使用准备。

已导入的实例处于停止状态。您可以使用[ec2-start-instance](#)启动实例。有关更多信息，请参阅 [Amazon EC2 命令行参考](#) 中的 [ec2-start-instances](#)。

检查您的导入任务的状态

使用 [ec2-describe-conversion-tasks](#) 返回任务状态。此命令的语法如下：

```
ec2-describe-conversion-tasks task_id
```

示例

您可以在以下示例中查看到您的导入实例任务之状态。

```
C:\> ec2-describe-conversion-tasks import-i-ffvko9js
```

响应 1

以下响应显示 IMPORTINSTANCE 状态为 active，且 893968896 个字节中的 73747456 个已被转换。

TaskType	IMPORTINSTANCE	TaskId	import-i-ffvko9js	ExpirationTime
2011-06-07T13:30:50+00:00	Status	active	StatusMessage	Pending
InstanceId	i-1234567890abcdef0			
DISKIMAGE	DiskImageFormat	VMDK	DiskImageSize	893968896
12	AvailabilityZone	cn-north-1	VolumeSize	ApproximateBytesConverted
73747456	Status	active	StatusMessage	Pending

响应 2

以下响应显示 IMPORTINSTANCE 状态为 active，进度为 7%，且 DISKIMAGE 已完成。

TaskType	IMPORTINSTANCE	TaskId	import-i-ffvko9js	ExpirationTime
2011-06-07T13:30:50+00:00	Status	active	StatusMessage	Progress: 7%
InstanceId	i-1234567890abcdef0			
DISKIMAGE	DiskImageFormat	VMDK	DiskImageSize	893968896
vol-1234567890abcdef0	VolumeSize	12	AvailabilityZone	cn-north-1
	ApproximateBytesConverted	893968896	Status	completed

响应 3

以下响应显示 IMPORTINSTANCE 状态为 completed。

TaskType	IMPORTINSTANCE	TaskId	import-i-ffvko9js	ExpirationTime
2011-06-07T13:30:50+00:00			Status completed	InstanceID i-1234567890abcdef0
DISKIMAGE	DiskImageFormat VMDK	DiskImageSize 893968896	VolumeId vol-1234567890abcdef0	VolumeSize 12 AvailabilityZone cn-north-1
	ApproximateBytesConverted 893968896	Status completed		



Note

IMPORTINSTANCE状态是您用于确定最终状态的状态。DISKIMAGE状态将会在IMPORTINSTANCE状态成为completed之前维持在completed一段时间。

现在，您可以使用ec2-stop-instance、ec2-start-instance、ec2-reboot-instance、ec2-terminate-instance等命令管理您的实例。有关更多信息，请参阅 [Amazon EC2 命令行参考](#)

将您的卷导入 Amazon EBS 中

Abstract

将您的数据存储导入 Amazon EBS 中，然后将其附加到您的某个现有 EC2 实例。

本节介绍如何将您的数据存储导入 Amazon EBS 中，然后将其附加到您的某个现有 EC2 实例。Amazon EC2 支持导入 RAW、虚拟硬盘 (VHD) 以及 ESX 虚拟机磁盘 (VMDK) 磁盘格式。



Important

我们建议使用 Amazon EC2 安全组限制对您的导入实例的网络访问。配置安全组，以仅允许可信 EC2 实例和远程主机连接到 RDP 和其他服务端口。有关安全组的更多信息，请参阅 [Amazon EC2 个安全组 \(对于 Windows 实例\) \(p. 515\)](#)。

在您将您的虚拟机从虚拟化环境中导出之后，只需一步即可将卷导入 Amazon EBS 中。您创建导入任务和上传卷。

要将卷导入 Amazon EBS 中

1. 使用 [ec2-import-volume](#) 创建允许您将卷上传到 Amazon EBS 中的任务。此命令的语法如下：

```
ec2-import-volume disk_image -f file_format -s volume_size -z availability_zone -b s3_bucket_name -o Amazon S3 bucket owner -w Amazon S3 bucket secret_access_key --region region_name -O your_access_key -W your_secret_key
```

下面的示例创建一个导入卷任务，将卷导入 d 可用区中的 cn-north-1 区域。

```
C:\> ec2-import-volume Win_2008_R1_EE_64.vmdk -f vmdk -s 25 -z cn-north-1d -b myawsbucket -o AKIAIOSFODNN7EXAMPLE -w wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY --region cn-north-1 -O AKIAI44QH8DHBEEXAMPLE -W je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

以下是一个示例响应。

```
Requesting volume size: 25 GB
Disk image format: Stream-optimized VMDK
Converted volume size: 26843545600 bytes (25.00 GiB)
Requested EBS volume size: 26843545600 bytes (25.00 GiB)
```

```
TaskType      IMPORTVOLUME   TaskId import-vol-ffut5xv4   ExpirationTime
              2011-09-09T15:22:30+00:00   Status active   StatusMessage Pending
DISKIMAGE     DiskImageFormat VMDK   DiskImageSize 5070303744
VolumeSize    25   AvailabilityZone cn-north-1d   Approxim
ateBytesConverted 0
Creating new manifest at myawsbucket/0fd8fcf5-04d8-44ae-981f-
3c9f56d04520/Win_2008_R1_EE_64.vmdkmanifest.xml
Uploading the manifest file
Uploading 5070303744 bytes across 484 parts
0% |-----| 100%
|=====
Done
```

Amazon EC2 返回您将在下一步中使用的任务 ID。在此示例中，ID 为 import-vol-ffut5xv4。

2. 使用 [ec2-describe-conversion-tasks](#) 确认您的卷已成功导入。

```
C:\> ec2-describe-conversion-tasks import-vol-ffut5xv4
TaskType      IMPORTVOLUME   TaskId import-vol-ffut5xv4   ExpirationTime
              2011-09-09T15:22:30+00:00   Status completed
DISKIMAGE     DiskImageFormat VMDK   DiskImageSize 5070303744
VolumeId     vol-1234567890abcdef0   VolumeSize 25   Available
ityZone       cn-north-1d   ApproximateBytesConverted 5070303744
```

此示例中的状态为 completed，这表示导入成功。

3. 使用 [ec2-attach-volume](#) 将 Amazon EBS 卷挂载到您的某个现有 EC2 实例中。以下为将卷 vol-1234567890abcdef0 附加到设备 /dev/sde 上的 i-1234567890abcdef0 实例中的示例。

```
C:\> ec2-attach-volume vol-1234567890abcdef0 -i i-1234567890abcdef0 -d xvde
ATTACHMENT vol-1234567890abcdef0 i-1234567890abcdef0 xvde attaching 2010-
03-23T15:43:46+00:00
```

恢复上传

Abstract

恢复上传。

连接发生问题会导致上传中断。当您恢复上传时，Amazon EC2 会从其停止位置自动开始上传。以下程序会带您一步步了解上传成功百分比和恢复上传的方法。

要恢复上传

使用任务 ID 及 [ec2-resume-import](#) 继续上传。命令使用 HTTP HEAD 操作决定恢复的位置。

```
ec2-resume-import disk_image -t task_id -o owner -w secret_key
```

示例

以下为恢复导入实例任务的示例。

```
C:\> ec2-resume-import Win_2008_R1_EE_64.vmdk -t import-i-ffni8aei -o AKIAIOS
FODNN7EXAMPLE -w wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

导入实例任务完成时显示下列输出内容：

```
Disk image size: 5070303744 bytes (4.72 GiB)
Disk image format: Stream-optimized VMDK
Converted volume size: 26843545600 bytes (25.00 GiB)
Requested EBS volume size: 26843545600 bytes (25.00 GiB)
Uploading 5070303744 bytes across 484 parts
0% |-----| 100%
|=====
Done
Average speed was 10.316 MBps
The disk image for import-i-ffni8aei has been uploaded to Amazon S3
where it is being converted into an EC2 instance. You may monitor the
progress of this task by running ec2-describe-conversion-tasks. When
the task is completed, you may use ec2-delete-disk-image to remove the
image from S3.
```

取消上传

Abstract

取消上传。

使用 [ec2-cancel-conversion-task](#) 取消活动的导入任务。任务可以是上传实例或卷。使用此命令会删除导入的所有项目，包括已上传的卷或实例。

如果导入已完成或仍在传输最后的磁盘映像，则命令失败且会返回类似于以下内容的例外情况：

```
Client.CancelConversionTask Error: Failed to cancel conversion task import-i-fh95npoc
```

取消上传任务

使用要删除的上传的任务 ID 及 [ec2-cancel-conversion-task](#)。

示例

以下为取消与任务 ID import-i-fh95npoc 相关之上传的示例。

```
C:\> ec2-cancel-conversion-task import-i-fh95npoc
```

成功的取消之输出类似于以下内容：

```
CONVERSION-TASK import-i-fh95npoc
```

您可以使用 [ec2-describe-conversion-tasks](#) 命令查看取消状态，如下面的示例所示：

```
C:\> ec2-describe-conversion-tasks import-i-fh95npoc
TaskType      IMPORTINSTANCE TaskId    import-i-fh95npoc      ExpirationTime
2010-12-20T18:36:39+00:00          Status    cancelled     InstanceID      i-
1234567890abcdef0
DISKIMAGE      DiskImageFormat VMDK      DiskImageSize   2671981568
VolumeSize    40      AvailabilityZone      cn-north-1c ApproximateBytesCon-
verted       0      Status    cancelled
```

在本示例中，状态为 `cancelled`。如果上传仍在进行，则状态为 `cancelling`。

上传后清除

Abstract

上传之后删除磁盘映像。

您可以使用 [ec2-delete-disk-image](#) 在映像文件上传后将其删除。如果您未删除文件，则会针对其在 Amazon S3 中的存储情况向您收费。

要删除磁盘映像

使用您想用 `ec2-delete-disk-image` 删除的磁盘映像的任务 ID。

示例

以下为删除与任务 ID `import-i-fh95npoc` 相关的磁盘映像的示例。

```
C:\> ec2-delete-disk-image -t import-i-fh95npoc
```

成功的取消之输出类似于以下内容：

```
DELETE-TASK import-i-fh95npoc
```

步骤 5：在 Amazon EC2 中启动实例

Abstract

启动从 VM 导入的实例。

在您将 VM 上传至 Amazon S3 后，VM Import 过程自动将其转换为 Amazon EC2 实例，并在 Amazon EC2 控制台中将其作为停止的实例进行启动。在您开始使用实例前，必须启动。有关使用 Amazon EC2 实例的更多信息，请参阅 [实例生命周期 \(p. 213\)](#)。

启动实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 Instances。
4. 在内容窗格中，右键单击实例，选择 Instance State (实例状态)，然后单击 Start (启动)。

导出 Amazon EC2 实例

Abstract

导出实例以将 Amazon EC2 实例的副本部署到您的现场虚拟化环境。

如果您之前已将实例导入 Amazon EC2 中，可以使用命令行工具将该实例导出到 Citrix Xen、Microsoft Hyper-V 或 VMware vSphere 中。当您想在您的现场虚拟化环境中部署您的 EC2 实例时，导出您之前导入的实例会很有用。

如果您使用的是 VMware vSphere，也可以使用 AWS Connector for vCenter 从 Amazon EC2 导出 VM。有关更多信息，请参阅 *AWS Management Portal for vCenter 用户指南* 中的 [导出迁移的 Amazon EC2 实例](#)。

内容

- [导出 VM 的先决条件 \(p. 432\)](#)
- [导出实例 \(p. 432\)](#)
- [取消或阻止实例的导出 \(p. 434\)](#)

导出 VM 的先决条件

在您开始从 Amazon EC2 导出 VM 之前，您必须了解 AWS 支持的操作系统和映像格式，还必须了解实例和卷的导出限制。

要从 Amazon EC2 导入或导出 VM，您还必须安装 CLI 工具：

- 有关安装 Amazon EC2 CLI 的更多信息，请参阅 [Amazon EC2 命令行参考](#)。
- 有关安装 AWS CLI 的更多信息，请参阅 [AWS Command Line Interface 用户指南](#)。有关 AWS CLI 中的 Amazon EC2 命令的更多信息，请参阅 [AWS Command Line Interface Reference](#) 中的 `ec2`。

从 Amazon EC2 导出 VM 的已知限制

导出实例和卷受下列限制：

- 在每个区域，您最多可以同时进行五个导出任务。
- 您无法导出 Amazon Elastic Block Store (Amazon EBS) 数据卷。
- 您不能导出具有多个虚拟磁盘的实例或 AMI。
- 您不能导出使用固定虚拟硬盘 (VHD) 的实例或 AMI。
- 您不能导出具有多个网络接口的实例或 AMI。
- 您不能从 Amazon EC2 导出实例或 AMI，除非之前从另一虚拟化环境中将其导入了 Amazon EC2。
- 如果您从另一 AWS 账户共享实例或 AMI，则不能从 Amazon EC2 导出它。

从 Amazon EC2 导出映像格式

对于从 Amazon EC2 导出卷和实例，AWS 支持下列映像格式。确保您将输出文件的格式转换为 VM 环境支持的格式：

- 启动虚拟装置 (OVA) 映像格式，该格式可与 VMware vSphere 版本 4 和 5 相兼容。
- 虚拟硬盘 (VHD) 映像格式，该格式可与 Citrix Xen 和 Microsoft Hyper-V 虚拟化产品兼容。
- 流优化型 ESX 虚拟机磁盘 (VMDK) 映像格式，该格式可与 VMware ESX 和 VMware vSphere 版本 4 和 5 虚拟化产品相兼容。

导出实例

您可以使用 Amazon EC2 CLI 导出实例。如果您尚未安装 CLI，请参阅[设置 Amazon EC2 工具](#)。

`ec2-create-instance-export-task` 命令可收集将实例正确导出到所选虚拟化格式所需的全部信息（例如，实例 ID；用于保存所导出映像的 Amazon S3 存储桶的名称；所导出映像的名称；VMDK、OVA 或 VHD 格式）。导出的文件保存在您指定的 Amazon S3 存储桶中。VM Export 支持导出动态虚拟硬盘 (VHD)。不支持固定 VHD。



Note

当您导出实例时，会针对您存储所导出 VM 所用的存储桶按照标准 Amazon S3 费率向您收费。此外，您的账单中还会出现反映 Amazon EBS 快照的临时使用情况的小额费用。有关 Amazon S3 定价的更多信息，请参阅 [Amazon Simple Storage Service \(S3\) 定价](#)。

要导出实例

1. 创建 Amazon S3 存储桶以存储导出的实例。Amazon S3 存储桶必须将上传/删除和查看权限授予 `vm-import-export@amazon.com` 账户。有关更多信息，请参阅 [Amazon Simple Storage Service 控制台用户指南](#) 中的 [创建存储桶和编辑存储桶权限](#)。



Note

您可使用区域特定的规范 ID，而不是使用 `vm-import-export@amazon.com` 账户。目标映像的 Amazon S3 存储桶必须存在，并且必须已向使用其规范 ID 的以下区域特定的账户授予 WRITE 和 READ_ACP 权限：

- 中国（北京）：`834baf86b15b6ca71074df0fd1f93d234b9d5e848a2cb31f880c149003ce36f`
- AWS GovCloud（美国）：
`af913ca13efe7a94b88392711f6fc8aa07c9d1454d4f190a624b126733a5602`

有关更多信息，请参阅 [AWS GovCloud \(US\) User Guide](#) 中的 [Amazon Elastic Compute Cloud \(Amazon EC2\)](#)。

- 所有其他区域：
`c4d8eabf8db69dbe46bfe0e517100c554f01200b104d59cd408e777ba442a322`

2. 在命令提示窗口中，键入以下命令：

```
ec2-create-instance-export-task instance_id -e target_environment -f  
disk_image_format -c container_format -b s3_bucket
```

instance_id

要导出的实例的 ID。

target_environment

VMware、Citrix 或 Microsoft。

disk_image_format

适用于 VMware 的 VMDK 或适用于 Microsoft Hyper-V 和 Citrix Xen 的 VHD。



Note

VM Export 仅支持动态虚拟硬盘 (VHD)。不支持固定 VHD。

container_format

可在导出至 VMware 时视需要设置为 OVA。

s3_bucket

您希望将实例导出到的 Amazon S3 存储桶的名称。

3. 若要监控实例的导出，请在命令提示符处键入以下命令，其中 `task_id` 是导出任务的 ID：

```
ec2-describe-export-tasks task_id
```

取消或阻止实例的导出

您可以使用 Amazon EC2 CLI 在完成之前取消或阻止实例的导出。[ec2-cancel-export-task](#) 命令会删除所有的导出项目，包括任何未完全创建的 Amazon S3 对象。如果导出任务完成或正在传输最后一个磁盘映像，则该命令将失败且会返回错误。

要取消或阻止导出实例

在命令提示符处键入以下命令，其中 *task_id* 是导出任务的 ID：

```
ec2-cancel-export-task task_id
```

对 VM Import/Export 进行故障排除

Abstract

在您将虚拟机导入 EC2 实例时排查问题。

导入或导出 VM 时，大多数错误是在您进行不受支持的尝试时发生。要避免这些错误，请在开始导入或导出之前阅读 [VM Import/Export 的先决条件 \(p. 403\)](#)。

错误

- [AWS Error Code: InvalidParameter, AWS Error Message: Parameter disk-image-size=0 has an invalid format. \(p. 435\)](#)
- [Client.NotExportable : 仅可导出已导入的实例。（服务：AmazonEC2；状态代码：400；错误代码：NotExportable；请求 ID：<RequestId>） \(p. 435\)](#)
- [Client.Unsupported : 未找到可启动的分区。（服务：AmazonEC2，状态代码：400，错误代码：Unsupported，请求 ID：<RequestId>） \(p. 435\)](#)
- [Client.UnsupportedOperation: This instance has multiple volumes attached.请删除额外的卷。 \(p. 435\)](#)
- [ClientError : Booter 联网故障/实例不可访问。请在安装 .Net framework 3.5 SP1 或更高版本后重试。 \(p. 435\)](#)
- [ClientError: Footers not identical \(ClientError: 页脚不同\) \(p. 436\)](#)
- [ClientError : 配置无效 - 无法读取 fstab。 \(p. 436\)](#)
- [ClientError: Uncompressed data has invalid length. \(p. 436\)](#)
- [ClientError : 配置不受支持 : 找到了多个目录。 \(p. 436\)](#)
- [ERROR: Bucket <MyBucketName> is not in the <RegionName> region, it's in <RegionName>. \(p. 436\)](#)
- [ERROR: File uses unsupported compression algorithm 0. \(p. 436\)](#)
- [Error starting instances: Invalid value <instance ID> for instanceId. Instance does not have a volume attached at root \(/dev/sda1\). \(p. 436\)](#)
- [S3 源位置无效 \(p. 437\)](#)
- [java.lang.OutOfMemoryError: Java heap space \(java.lang.OutOfMemoryError: Java 堆空间\) \(p. 437\)](#)
- [Service.InternalError: An internal error has occurred. Status Code: 500, AWS Service: AmazonEC2 \(状态代码: 500，AWS 服务: AmazonEC2\) \(p. 437\)](#)
- [调用 CreateRole 操作时出现客户端错误 \(MalformedPolicyDocument\) : 策略中的语法错误。 \(p. 437\)](#)
- [给定的 S3 存储桶不在该区域本地。 \(p. 437\)](#)
- [服务角色 <vmimport> 不存在或没有让服务继续的足够权限。 \(p. 437\)](#)
- [FirstBootFailure : 该导入请求失败的原因是 Windows 实例启动和建立网络连接失败。 \(p. 438\)](#)

- 请求的实例不支持 Linux (p. 439)

AWS Error Code: InvalidParameter, AWS Error Message: Parameter disk-image-size=0 has an invalid format.

不支持您使用的映像格式。

解决

使用受支持的映像格式重试：RAW、VHD 或 VMDK。

Client.NotExportable：仅可导出已导入的实例。（服务：
AmazonEC2；状态代码：400；错误代码：NotExportable；请
求 ID：`<RequestId>`）。

您只能导出之前已导入到 Amazon EC2 的实例或镜像。

解决

导出之前已导入到 Amazon EC2 的实例或镜像。

Client.Unsupported：未找到可启动的分区。（服务：
AmazonEC2，状态代码：400，错误代码：Unsupported，请求
ID：`<RequestId>`）

VM 具有 GUID 分区表 (GPT) 已分区的根卷。

解决

VM Import/Export 工具不支持 GPT 已分区的卷。将您的 VM 根卷转换为 MBR 分区，然后尝试重新导入
VM。

Client.UnsupportedOperation: This instance has multiple volumes
attached. 请删除额外的卷。

VM 有多个附加的磁盘。

解决

断开额外的驱动器并重试。如果您在其他卷上需要此数据，复制数据至根卷然后尝试再次导出 VM。

ClientError : Booter 联网故障/实例不可访问。请在安装 .Net
framework 3.5 SP1 或更高版本后重试。

Windows VM 需要支持 EC2 Config 服务的 Microsoft .NET Framework 3.5 Service Pack 1 或更高版本。

解决

先在 Windows VM 上安装 Microsoft .NET Framework 3.5 Service Pack 1 或更高版本，然后尝试导入
EC2 Config 服务。

ClientError: Footers not identical (ClientError: 页脚不同)

您尝试导入差异 VHD，或在创建 VHD 时出错。

解决

重新导出您的 VM，然后将其重新导入 Amazon EC2。

ClientError : 配置无效 - 无法读取 fstab。

不支持带有多个引导卷或多个 /etc 目录的 Linux VM。

解决

将 VM 配置为只有一个引导卷或 /etc 目录。

ClientError: Uncompressed data has invalid length.

VMDK 文件已损坏。

解决

您可以尝试维修或重新创建 VMDK 文件，或者为您的导入使用另一个 VMDK 文件。

ClientError : 配置不受支持 : 找到了多个目录。

不支持带有多个引导卷或多个 /etc 目录的 Linux VM。

解决

将 VM 配置为只有一个引导卷或 /etc 目录。

ERROR: Bucket <MyBucketName> is not in the <RegionName> region, it's in <RegionName>.

Amazon S3 存储桶与您希望导入的实例不在同一个区域。

解决

请尝试添加 --ignore-region-affinity 选项，它忽略了存储桶的区域是否与创建导入任务的区域相符。您也可以使用 Amazon Simple Storage Service 控制台创建 Amazon S3 存储桶并将区域设置为您希望导入 VM 的区域。再次运行命令并指定您刚创建的新存储桶。

ERROR: File uses unsupported compression algorithm 0.

使用 OVA 格式而非 OVF 格式创建 VMDK。

解决

以 OVF 格式创建 VMDK。

Error starting instances: Invalid value <instance ID> for instanceId. Instance does not have a volume attached at root (/dev/sda1).

您尝试在 VM Import 过程和所有转换任务完成之前启动实例。

解决

请等待 VM Import 过程和所有转换任务全部完成后再启动实例。

S3 源位置无效

命令语法或 Amazon S3 存储桶名称不正确。

解决

在仅用于 VM Import 的合适区域中创建新的 Amazon S3 存储桶，然后将 VM 文件上传到该存储桶的根。

`java.lang.OutOfMemoryError: Java heap space (java.lang.OutOfMemoryError: Java 堆空间)`

没有足够的虚拟内存启动 Java，或者您尝试导入的映像过大。

解决

如果您向 Java 分配额外内存，额外内容将仅适用于 JVM，但如果指定了此设置（明确针对 EC2 命令行工具），它将覆盖全局设置。例如，您可以使用下列命令向 Java“`set EC2_JVM_ARGS=-Xmx512m`”分配 512 MB 的额外内存。

`Service.InternalError: An internal error has occurred. Status Code: 500, AWS Service: AmazonEC2 (状态代码: 500 , AWS 服务: AmazonEC2)`

您尝试在未指定子网和可用性区域时导入没有默认 VPC 的实例。

解决

如果您正在导入没有默认 VPC 的实例，请确保指定子网和可用区。

调用 CreateRole 操作时出现客户端错误 (MalformedPolicyDocument)：策略中的语法错误。

您忘记在策略文档名称前包含 `file://`。

解决

在策略文档名称前包含 `file://`（例如，`file://trust-policy.json`）。

给定的 S3 存储桶不在该区域本地。

用于 VM Import 的 Amazon S3 存储桶必须位于您希望导入 VM 的同一 AWS 区域。

解决

在您希望导入 VM 的区域中创建 S3 存储桶。

服务角色 `<vmimport>` 不存在或没有让服务继续的足够权限。

VM Import Service 角色缺失或不正确。如果尝试开始导入的 IAM 用户没有对 Amazon EC2 资源的足够权限，您也可能收到此错误。

解决

请确保该服务角色存在且拥有所有适当权限。

FirstBootFailure : 该导入请求失败的原因是 Windows 实例启动和建立网络连接失败。

使用 `ec2-import-instance` 命令导入 VM 时，导入任务可能在完成之前停止，然后失败。若要调查问题原因，您可以使用 `ec2-describe-conversion-tasks` 命令描述实例。

当您收到 FirstBootFailure 错误消息时，意味着您的虚拟磁盘映像无法执行以下步骤之一：

- 启动并开始 Windows。
- 安装 Amazon EC2 联网和磁盘驱动程序。
- 使用一个 Dhcp 配置的网络接口接收 IP 地址。
- 使用 Amazon EC2 Windows 批量许可激活 Windows。

以下最佳实践可帮助您避免 Windows 首次启动失败：

- 禁用反病毒和反间谍软件和防火墙。这些类型的软件能够防止安装新 Windows 服务或防止运行未知的二进制文件。软件和防火墙可在导入后重新启用。
- 不要强化您的操作系统。安全配置（有时称为强化）可防止自动安装 Amazon EC2 驱动程序。还有其他 Windows 配置设置可防止导入。这些设置可在导入时重新使用。
- 禁用或删除多个可启动的分区。如果您的虚拟机启动并需要您选择使用的启动分区，导入可能会失败。

虚拟磁盘映像无法启动和建立网络连接可能是由于以下任一原因。

原因

- [TCP/IP 网络和 DHCP 未启用 \(p. 438\)](#)
- [虚拟机上丢失了 Windows 需要的卷 \(p. 438\)](#)
- [Windows 始终启动到 System Recovery Options \(p. 439\)](#)
- [虚拟机是利用 physical-to-virtual \(P2V\) 转换过程被创建的 \(p. 439\)](#)
- [Windows 激活失败 \(p. 439\)](#)
- [未找到可启动的分区 \(p. 439\)](#)

TCP/IP 网络和 DHCP 未启用

原因：对于所有 Amazon EC2 实例（包括 Amazon VPC 中的此类实例），必须启用 TCP/IP 网络和 DHCP。在 VPC 中，您在导入实例之前或之后都可以定义实例的 IP 地址。导出实例前，不要设置静态 IP 地址。

解决：确保 TCP/IP 网络已启用。有关更多信息，请参阅 Microsoft TechNet 网站的[设置 TCP/IP \(Windows Server 2003\)](#) 或 [配置 TCP/IP \(Windows Server 2008\)](#)。

确认 DHCP 已启用。有关更多信息，请参阅 Microsoft TechNet 网站的[什么是 DHCP](#)。

虚拟机上丢失了 Windows 需要的卷

原因：将 VM 导入 Amazon EC2 时只导入启动盘，必须断开所有其他磁盘，而且在导入虚拟机前 Windows 必须能够启动。例如，Active Directory 通常会将 Active Directory 数据库存储在 D:\ 驱动器上。如果 Active Directory 数据库丢失或无法访问时，域控制器无法启动。

解决：在导出前，断开所有连接到 Windows VM 的二级和网络磁盘。

将所有 Active Directory 数据库从辅助驱动或分区移至主要 Windows 分区。有关更多信息，请参阅 Microsoft Support 网站上的[启动基于 Windows 或基于 SBS 的域控制器时出现“Directory Services cannot start”（目录服务无法启动）错误消息](#)。

Windows 始终启动到 System Recovery Options

原因：Windows 可以出于多种原因启动到 System Recovery Options，包括将 Windows 从物理计算机推送至虚拟环境（也称为 P2V）。

解决：在导出或准备导入之前，确保 Windows 启动到登录提示。

不要导入来自物理设备的虚拟 Windows 实例。

虚拟机是利用 physical-to-virtual (P2V) 转换过程被创建的

原因：如果在物理计算机上执行 Windows 安装过程，然后将 Windows 安装的副本导入 VM，从而创建磁盘映像，则会发生 P2V 转换。Amazon EC2 VM Import 不支持作为 P2V 转换的结果而创建的 VM。Amazon EC2 VM Import 仅支持在源 VM 内本地安装的 Windows 映像。

解决：将 Windows 安装到虚拟化环境中，并将所安装的软件迁移至新的 VM。

Windows 激活失败

原因：在启动过程中，Windows 将检测硬件更改并尝试激活。在导入进程中，我们尝试将 Windows 中的授许可机制转换为 Amazon Web Services 提供的批量许可。但是，如果 Windows 激活过程失败，那么导入也会失败。

解决：确保要导入的 Windows 版本支持批量许可。Windows 测试版或预览版可能不会。

未找到可启动的分区

原因：在虚拟机导入期间，未能找到启动分区。

解决：确保要导入的磁盘有启动分区。我们不支持多磁盘导入。

请求的实例不支持 Linux

原因：只有特定实例类型才支持 Linux 导入。您尝试导入了一个不支持的实例类型。

解决：使用受支持的实例类型重试。[Microsoft Windows BYOL 实例必须作为 Microsoft Windows 的专用实例或专用主机启动](#)，因此无法使用 t2 实例类型，因为它不支持专用实例。

- 通用型: t2.micro | t2.small | t2.medium | m3.medium | m3.large | m3.xlarge | m3.2xlarge
- 计算优化: c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge | cc1.4xlarge
- 内存优化: r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge
- 存储优化: i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge

监控 Amazon EC2

Abstract

列出要进行监控，以保持 Amazon EC2 实例的可靠性、可用性以及性能的各个项目。

监控是保持 Amazon Elastic Compute Cloud (Amazon EC2) 实例和 AWS 解决方案的可靠性、可用性和性能的重要部分。您的 AWS 解决方案的所有组成部分都应收集监控数据，以便更轻松地调试出现的多点故障。但是，在开始监控 Amazon EC2 前，您应创建包括以下内容的监控计划：

- 您的监控目标是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

在定义监控目标并创建监控计划后，下一步是在您的环境中建立正常 Amazon EC2 性能的基准。您应该在不同时间和不同负载条件下测量 Amazon EC2 的性能。监控 Amazon EC2 时，您应存储所收集的监控数据的历史记录。您可将当前 Amazon EC2 性能与这些历史数据进行比较，这样可帮助您确定性能的正常模式和异常模式，找出解决问题的方法。例如，您可以监控 Amazon EC2 实例的 CPU 利用率、磁盘 I/O 和网络使用率。如果性能低于您所建立的基准，则您可能需要重新配置或优化实例以降低 CPU 使用率、改进磁盘 I/O 或减少网络流量。

要建立基准，您至少应监控以下各项：

要监控的项目	Amazon EC2 指标	监控脚本/CloudWatch Logs
CPU 利用率	CPU 利用率 (p. 453)	
内存利用率		(Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器 发送到 CW; , 将日志发送到 CloudWatch Logs

要监控的项目	Amazon EC2 指标	监控脚本/CloudWatch Logs
已用内存		(Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs
可用内存		(Linux 实例) 为 Amazon EC2 Linux 实例监控内存和磁盘指标 (Windows 实例) 将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs
网络使用率	网络输入 (p. 453) 网络输出 (p. 453)	
磁盘性能	磁盘读取操作 (p. 453) 磁盘写入操作 (p. 453)	
磁盘交换分区利用率 (仅限 Linux 实例) 使用的交换空间 (仅限 Linux 实例)		为 Amazon EC2 Linux 实例监控内存和磁盘指标
页面文件利用率 (仅限 Windows 实例) 使用的页面文件 (仅限 Windows 实例) 可用的页面文件 (仅限 Windows 实例)		将性能计数器发送到 CW; , 将日志发送到 CloudWatch Logs
磁盘读取/写入	磁盘读取字节数 (p. 453) 磁盘写入字节数 (p. 453)	
磁盘空间利用率 (仅限 Linux 实例)		为 Amazon EC2 Linux 实例监控内存和磁盘指标
使用的磁盘空间 (仅限 Linux 实例)		为 Amazon EC2 Linux 实例监控内存和磁盘指标
可用磁盘空间 (仅限 Linux 实例)		为 Amazon EC2 Linux 实例监控内存和磁盘指标

自动和手动监控

Abstract

配置 AWS 工具来监控您的 Amazon EC2 实例，其中一些工具自动执行，而一些工具需要手动干预。

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，但另一些工具需要手动干预。

主题

- [自动监控工具 \(p. 442\)](#)
- [手动监控工具 \(p. 442\)](#)

自动监控工具

您可以使用以下自动化监控工具来查看 Amazon EC2 并在出现错误时向您报告：

- System Status Checks (系统状态检查) - 监控使用您的实例所需的 AWS 系统，以确保这些系统正常工作。这些检查会检测出需要 AWS 参与修复的实例问题。当一个系统状态检查故障时，您可以等待 AWS 修复故障或者您也可以亲自解决该故障（例如，通过停止和重启或终止和替换实例）。导致系统状态检查出现故障的问题示例包括：
 - 网络连接丢失
 - 系统电源损耗
 - 物理主机上的软件问题
 - 物理主机上的硬件问题

有关更多信息，请参阅 [实例的状态检查 \(p. 444\)](#)。

- 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，一般需要都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 \(p. 444\)](#)。

- Amazon CloudWatch 警报 - 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。该操作是向 Amazon Simple Notification Service (Amazon SNS) 主题或 Auto Scaling 策略发送通知。警报只会调用操作进行持续的状态变更。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态，必须改变其状态并维持指定的若干个时间段。有关更多信息，请参阅 [使用 CloudWatch 监控您的实例 \(p. 452\)](#)。
- 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[监控日志文件](#)。
- Amazon EC2 监控脚本 – 可以使用 Perl 脚本在您的实例中监控内存、磁盘和页面/交换文件使用率。有关更多信息，请参阅 [Amazon EC2 Linux 实例监控内存和磁盘指标](#)。
- Microsoft System Center Operations Manager 的 AWS 管理包 - 链接 Amazon EC2 实例与其内部运行的 Microsoft Windows 或 Linux 操作系统。AWS 管理包是 Microsoft System Center Operations Manager 的一种扩展程序。它使用数据中心内的指定计算机（称为观察程序节点）和 Amazon Web Services API 远程发现并收集 AWS 资源的相关信息。有关更多信息，请参阅[AWS Management Pack for Microsoft System Center \(p. 771\)](#)。

手动监控工具

监控 Amazon EC2 的另一重要部分需要手动监控一些项目，监控脚本、状态检查和 CloudWatch 警报并不考察这些项目的指标。Amazon EC2 和 CloudWatch 控制台控制面板提供您的 Amazon EC2 环境状态的概览视图。

- Amazon EC2 控制面板显示：
 - 按区域显示服务运行状况和计划的事件
 - 实例状态
 - 状态检查
 - 警报状态
 - 实例指标详细信息（在导航窗格中，单击 Instances 选择一个实例，然后单击 Monitoring (监控) 选项卡）
 - 卷指标详细信息（在导航窗格中，单击 Volumes (卷) 选择一个卷，然后单击 Monitoring (监控) 选项卡）
- Amazon CloudWatch 控制面板显示：
 - 当前警报和状态
 - 警报和资源的图表
 - 服务运行状况

此外，您还可以使用 CloudWatch 执行以下操作：

- 将 Amazon EC2 监控数据绘制成为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

Abstract

介绍监控的最佳实践，帮助您执行 Amazon EC2 监控任务。

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

Abstract

您可以通过查看实例的状态检查和计划事件来监控您的 Amazon EC2 实例的状态。

您可以通过查看实例的状态检查和计划事件来监控您的实例状态。状态检查反映 Amazon EC2 自动检查的结果信息。这些自动检查会检测出指定的问题是否影响您的实例。该状态检查信息与 Amazon CloudWatch 提供的数据一起为您的每一个实例提供详细的操作可视性。

您也可以查看您的实例中指定的预定事件的状态。事件提供了关于活动日程信息，例如，根据每个事件预定的开始和结束时间，有计划的重启或指令引退您的实例。

内容

- [实例的状态检查 \(p. 444\)](#)
- [实例的计划事件 \(p. 448\)](#)

实例的状态检查

Abstract

使用状态检查监控实例，以确定 Amazon EC2 是否检测到实例的任何问题。

使用实例状态监控，您可以快速确定 Amazon EC2 是否已经检测到可能阻止您的实例运行应用程序的任何问题。Amazon EC2 将对运行的所有 EC2 实例执行自动检查以识别硬件和软件问题。您可以通过查看这些状态检查的结果来识别指定的和可检测的问题。这些数据扩充了 Amazon EC2 已提供的有关每个实例的预期状态（如 pending、running、stopping）的信息以及 Amazon CloudWatch 监控的利用率指标（CPU 利用率、网络流量和磁盘活动）。

状态检查每分钟进行一次并且每次都会返回一个通过或失败状态。如果所有的检查都通过，则实例的整体状态是OK。如果有一个或多个检查故障，则整体状态为受损。状态检查是内置到 Amazon EC2 中的，所以不能禁用或删除。但是，您可以创建或删除基于状态检查结果触发的警报。例如，您可以创建一个警报来提醒您在一个指定实例上的状态检查中返回了故障状态。有关更多信息，请参阅 [创建和编辑状态检查警报 \(p. 446\)](#)。

内容

- [状态检查的类型 \(p. 444\)](#)
- [查看状态检查 \(p. 445\)](#)
- [报告实例状态 \(p. 446\)](#)
- [创建和编辑状态检查警报 \(p. 446\)](#)

状态检查的类型

状态检查可分为两种类型：系统状态检查和实例状态检查。

系统状态检查

监控使用您的实例所需的 AWS 系统，以确保这些系统正常工作。这些检查会检测出需要 AWS 参与修复的实例问题。如果系统状态检查失败，您可以等待 AWS 修复问题，也可自行解决问题（例如，停止并启动实例，或终止并替换实例）。

以下可能导致系统状态检查失败的问题的示例：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题

实例状态检查

监控您的各个实例的软件和网络配置。这些检查检测需要您参与修复的问题。如果实例状态检查失败，一般需要您自行解决问题（例如，重启实例或更改实例配置）。

以下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
- 在实例重启期间或在一个 Windows 实例存储支持的实例正在进行捆绑时进行的状态检查将报告实例状态检查失败，直到该实例变得再次可用。

查看状态检查

Amazon EC2 为您提供了多种查看和使用状态检查的方法。

使用控制台查看状态

您可使用 AWS 管理控制台查看状态检查。

使用控制台查看状态检查

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 viewing status checks. At the top, there are tabs: Description, Status Checks (which is selected and highlighted in orange), Monitoring, and Tags. Below the tabs, a message states: "Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks." There are two main sections: "System Status Checks" and "Instance Status Checks".
System Status Checks: A green status bar indicates "System reachability check passed".
Instance Status Checks: A red status bar indicates "Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)".
Both sections include a "Create Status Check Alarm" button.

5. 如果您有一个实例出现过状态检查失败的情况，并且该实例无法访问的时间已超 20 分钟，请选择 AWS Support 提交帮助请求。

使用命令行或 API 查看状态

您可以使用 `describe-instance-status` (AWS CLI) 命令查看正在运行的实例的状态检查。

要查看所有实例的状态，请使用以下命令：

```
aws ec2 describe-instance-status
```

获取实例状态为 `impaired` 的所有实例的状态：

```
aws ec2 describe-instance-status --filters Name=instance-status.status,Values=impaired
```

要获取单一实例的状态，请使用以下命令：

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

或者，使用以下命令：

- [Get-EC2InstanceState](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeInstanceState](#) (Amazon EC2 查询 API)

报告实例状态

如果您的实例出现了问题但其状态并未显示为受损，或者您想要向 AWS 发送有关您遇到的受损实例相关问题的详细信息，可提供反馈。

我们利用报告的反馈来识别影响到多数客户的问题，但不会对单独的账户问题做出回应。提供反馈并不会改变您当前看到的实例状态检查结果。

使用控制台报告状态反馈

使用控制台报告实例状态

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。
4. 选择 Status Checks 选项卡，然后选择 Submit feedback。
5. 填写 Report Instance Status 表单，然后选择 Submit。

使用命令行或 API 报告状态反馈

使用以下 [report-instance-status](#) (AWS CLI) 命令发送有关受损实例状态的反馈：

```
aws ec2 report-instance-status --instances i-1234567890abcdef0 --status impaired  
--reason-codes code
```

或者，使用以下命令：

- [Send-EC2InstanceState.html](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ReportInstanceState](#) (Amazon EC2 查询 API)

创建和编辑状态检查警报

您可以创建实例状态和系统状态警报，以在实例的状态检查失败时向您发出通知。

使用控制台创建状态检查警报

您可以为现有实例创建状态检查警报，以监视实例状态或系统状态。您可以将警报配置为，当实例状态检查或系统状态检查失败时，通过电子邮件向您发出通知或停止、终止或恢复实例。

要创建状态检查警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。

4. 选择 Status Checks 选项卡，然后选择 Create Status Check Alarm。
5. 选择 Send a notification to。选择一个现有 SNS 主题，或单击 create topic 以创建新的主题。如果要创建新的主题，请在 With these recipients 中，输入您的电子邮件地址以及任何其他收件人的地址，中间用逗号隔开。
6. (可选) 选择 Take the action，然后选择要采取的操作。
7. 在 Whenever 中，选择想要获得通知的状态检查。



Note

如果您在上一步中选择的是 Recover this instance，则请选择 Status Check Failed (System)。

8. 在 For at least 中，设置所需的评估期间数量，然后在 consecutive periods 中，选择评估期间持续时间，此评估期间结束后才会触发警报并发送电子邮件。
9. (可选) 在 Name of alarm 中，将警报的默认名称替换为其他名称。
10. 选择 Create Alarm。



Important

如果您向收件人列表添加了电子邮件地址或创建了新的主题，则 Amazon SNS 将向每个新地址发送一封订阅确认电子邮件。每个收件人必须通过单击该邮件中包含的链接来确认订阅。警报通知仅发送至经过确认的地址。

在您需要更改实例状态警报时，您可以对其进行编辑。

要编辑状态检查警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例，选择 Actions，选择 CloudWatch Monitoring，然后选择 Add/Edit Alarms。
4. 在 Alarm Details 对话框中，选择警报的名称。
5. 在 Edit Alarm 对话框中，进行所需更改，然后选择 Save。

使用 AWS CLI 创建状态检查警报

在以下示例中，当实例的实例检查或系统状态检查在至少两个期间连续失败后，警报将向 SNS 主题 arn:aws:sns:us-west-2:111122223333:my-sns-topic 发送通知。指标为 StatusCheckFailed。

要使用 CLI 创建状态检查警报

1. 选择一个现有 SNS 主题或创建一个新的主题。有关更多信息，请参阅 *AWS Command Line Interface 用户指南* 中的 [将 Amazon SNS 与 AWS CLI 结合使用](#)。
2. 使用以下 `list-metrics` 命令查看 Amazon EC2 的可用 Amazon CloudWatch 指标：

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. 使用以下 `put-metric-alarm` 命令创建警报：

```
aws cloudwatch put-metric-alarm --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 --metric-name StatusCheckFailed --namespace AWS/EC2 --statistic Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 -
```

```
-unit Count --period 300 --evaluation-periods 2 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

注意

- `--period` 是收集 Amazon CloudWatch 指标的时间范围（秒）。此示例使用 300，这是 60 秒乘以 5 分钟得到的结果。
- `--evaluation-periods` 是必须将指标数值与阈值相比较的连续周期数。此示例使用 2。
- `--alarm-actions` 是要在此警报触发时执行的操作的列表。每个操作都被指定为一个 Amazon 资源名称 (ARN)。此示例将此警报配置为使用 Amazon SNS 发送电子邮件。

实例的计划事件

Abstract

监控实例的计划事件。

AWS 可为您的实例计划事件，例如重启、停止/启动或停用。这些事件不会频繁发生。如果您的一个实例将受某计划事件影响，则 AWS 将在该计划事件发生之前向与您的 AWS 账户关联的电子邮件地址发送电子邮件，其中包含有关该事件的详细信息，包括开始和结束日期。根据事件的不同，您也许能够采取操作来控制事件的发生时间。

要更新账户的联系人信息以确保获得有关计划事件的通知，请转至 [Account Settings](#) 页。

内容

- [计划事件的类型 \(p. 448\)](#)
- [查看计划的事件 \(p. 448\)](#)
- [使用计划停用的实例 \(p. 450\)](#)
- [使用计划为重启的实例 \(p. 450\)](#)
- [使用计划为维护的实例 \(p. 451\)](#)

计划事件的类型

Amazon EC2 为您的实例支持下列类型的计划事件：

- **实例停止**：实例将会停止。再次启动实例时，实例会迁移至新主机。仅适用于 Amazon EBS 支持的实例。
- **实例停用**：实例将停止或终止。
- **重启**：实例将重启（实例重启）或实例的主计算机将重启（系统重启）。
- **系统维护**：实例可能会因网络维护或电源维护受到暂时的影响。

查看计划的事件

除了通过电子邮件接收计划事件的通知外，您还可查看计划的事件。

使用控制台查看实例的计划事件

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在导航窗格中，单击 Events (事件)。将显示与事件关联的所有资源。您可按资源类型或按特定事件类型进行筛选。您可选择资源来查看详细信息。

The screenshot shows the AWS CloudWatch Events console. At the top, there are three dropdown filters: 'All resource types' (selected), 'All event types' (selected), and 'Ongoing and scheduled'. Below the filters is a table header row with columns: Resource Name, Resource Type, Resource Id, and Event Type. A single row is selected, showing 'my-instance' under Resource Name, 'instance' under Resource Type, 'i-c3870335' under Resource Id, and 'instance-stop' under Event Type. Below the table, the event details for 'Event: i-c3870335' are displayed. The details include: Availability Zone (us-west-2a), Event type (instance-stop), Event status (Scheduled), Description (The instance is running on degraded hardware), Start time (May 22, 2015 at 5:00:00 PM UTC-7), and End time.

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。

The screenshot shows the AWS EC2 Dashboard. The 'Scheduled Events' section is highlighted. It displays the message 'US West (Oregon): 1 instances have scheduled events'.

4. 请注意，还将显示受影响资源的事件。例如，在导航窗格中，选择 Instances，然后选择一个实例。如果所选实例具有关联事件，则关联事件将显示在底部窗格中。



使用命令行或 API 查看实例的计划事件

使用以下 AWS CLI 命令：

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

以下是显示实例停用事件的示例输出：

```
{
    "InstanceStatuses": [
        {
            "InstanceState": {
                "Status": "ok",
                "Details": [
                    {
                        "Status": "passed",
                        "Name": "reachability"
                    }
                ]
            },
            "AvailabilityZone": "us-west-2a",
            "InstanceId": "i-1234567890abcdef0",
            "Event": {
                "EventId": "e-1234567890abcdef1",
                "EventName": "instance-stop",
                "EventTime": "2015-05-22T17:00:00Z",
                "EventDetail": {
                    "Reason": "The instance is running on degraded hardware"
                }
            }
        }
    ]
}
```

```
"InstanceState": {  
    "Code": 16,  
    "Name": "running"  
},  
"SystemStatus": {  
    "Status": "ok",  
    "Details": [  
        {  
            "Status": "passed",  
            "Name": "reachability"  
        }  
    ]  
},  
"Events": [  
    {  
        "Code": "instance-stop",  
        "Description": "The instance is running on degraded hard  
ware",  
        "NotBefore": "2015-05-23T00:00:00.000Z"  
    }  
]  
}  
}
```

或者，使用以下命令：

- [Get-EC2InstanceState](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeInstanceStatus](#) (Amazon EC2 查询 API)

使用计划停用的实例

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 \(p. 231\)](#)。



Important

实例停止或终止之后，实例存储卷上存储的所有数据都将丢失。这包括连接到使用 EBS 卷作为根设备的实例的实例存储卷。在实例停止或终止之前，请务必保存实例存储卷中以后还将需要的数据。

Amazon EBS 支持的实例操作

您可等待实例按计划停止。您也可自行停止并启动实例，这会将实例迁移至新的主计算机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 [停止和启动您的实例 \(p. 227\)](#)。

实例存储支持的实例操作

建议您在实例按计划终止之前，从最新的 AMI 启动替代实例并将所有必需数据迁移至替代实例。然后，您可终止原始实例，或等待其按计划终止。

使用计划为重启的实例

当 AWS 需要执行安装更新或维护基础主机等任务时，它可计划实例或实例的基础主机进行重启。无论是否为任何现有实例计划了重启操作，新启动的实例都不需要重启，因为底层主机已应用更新。

您可确定重启事件为实例重启还是系统重启。

使用控制台查看计划重启事件的类型

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Instance resources，然后选择您的实例。
4. 在底部窗格中，找到 Event type。该值为 system-reboot 或 instance-reboot。

使用 AWS CLI 查看计划重启事件的类型

使用以下 `describe-instance-status` 命令：

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

针对实例重启的操作

您可等待重启在其计划的维护时段进行。您也可在方便时自行重启实例。有关更多信息，请参阅 [重启您的实例 \(p. 230\)](#)。

重启实例之后，会立即取消针对实例重启的计划事件，并且更新事件的描述。基础主计算机的所有挂起的维护都将完成，并且在您的实例完全启动后，您可再次开始使用您的实例。

针对系统重启的操作

您无需执行任何操作；系统重启将在其计划的维护时段进行。系统重启通常在几分钟内完成。要验证重启是否已进行，可查看实例是否不再有计划事件。建议您检查实例上的软件是否按预期运行。

使用计划为维护的实例

当 AWS 需要维护实例的基础主计算机时，它将计划实例进行维护。维护事件有两种：网络维护和电源维护。

在网络维护期间，计划的实例会在短时间内失去网络连接。在维护完成后，将恢复与实例的正常网络连接。

在电源维护期间，计划的实例将短时间脱机，然后重启。执行重启后，将保留您的所有实例的配置设置。

在实例重启后（这通常需要几分钟），验证您的应用程序是否按预期运行。此时，您的实例应该不再具有与之关联的计划事件，或者计划事件的描述应该以 [Completed] 开头。有时，此实例状态需要 1 个小时才能更新。已完成的维护事件将在 Amazon EC2 控制台面板上显示长达一周时间。

Amazon EBS 支持的实例操作

您可等待维护按计划进行。您也可停止并启动实例，这会将实例迁移至新的主计算机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 [停止和启动您的实例 \(p. 227\)](#)。

实例存储支持的实例操作

您可等待维护按计划进行。或者，如果您想在计划的维护时段保持正常操作，可从最新的 AMI 启动替代实例，并在计划的维护时段之前将所有必需数据迁移至替代实例，然后终止原始实例。

使用 CloudWatch 监控您的实例

Abstract

使用 Amazon CloudWatch 监控 Amazon EC2 实例，以便从实例收集原始数据，并将数据处理为易读的近乎实时的指标。

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两周，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 \(p. 452\)](#)。

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 开发者指南](#)。

内容

- [对您的实例启用或禁用详细监控 \(p. 452\)](#)
- [列出实例的可用 CloudWatch 指标 \(p. 453\)](#)
- [获取您的实例的指标的统计数据 \(p. 459\)](#)
- [绘制实例的指标图形 \(p. 474\)](#)
- [创建 CloudWatch 警报 \(p. 476\)](#)
- [创建停止、终止、重启或恢复实例的警报 \(p. 483\)](#)

对您的实例启用或禁用详细监控

Abstract

对 EC2 实例启用或禁用详细监控。

默认情况下，已对您的实例启用基本监控。您可以选择启用详细监控。当您启用详细监控后，Amazon EC2 控制台将以 1 分钟为间隔显示实例的监控图表。下表描述对实例的基本和详细监控。

类型	说明
基本	数据在 5 分钟期间内自动可用，无需收费。
明细	额外付费的情况下，每隔 1 分钟提供一次数据。要获得此级别的数据，您必须为实例专门启用此监视。对于您已启用详细监视的实例，您还可以跨组（相似实例所在组）获得聚合数据。 有关定价的信息，请参阅 Amazon CloudWatch 产品页 。

启用详细监控

在实例启动时或在实例运行或停止后，可对实例启用详细监控。

使用控制台对现有实例启用详细监控

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 Instances。
3. 选择一个实例，单击 Actions，选择 CloudWatch Monitoring，然后单击 Enable Detailed Monitoring。
4. 在“Enable Detailed Monitoring”对话框中，单击“Yes, Enable”。
5. 在“启用详细监视”确认对话框中，单击“关闭”。

在使用控制台启动实例时启用详细监控

在使用 AWS 管理控制台启动实例时，请在 Configure Instance Details 页面上选中 Monitoring 复选框。

使用 AWS CLI 对现有实例启用详细监控

使用以下 `monitor-instances` 命令对指定实例启用详细监控。

```
C:\> aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

在使用 AWS CLI 启动实例时启用详细监控

结合使用 `run-instances` 命令和 `--monitoring` 标志来启用详细监控。

```
C:\> aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

禁用详细监控

在实例启动时或在实例运行或停止后，可对实例禁用详细监控。

使用控制台禁用详细监控

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 Instances。
3. 选择一个实例，单击 Actions，选择 CloudWatch Monitoring，然后单击 Disable Detailed Monitoring。
4. 在“Disable Detailed Monitoring”对话框中，单击“Yes, Disable”。
5. 在“禁用详细监视”确认对话框中，单击“关闭”。

使用 AWS CLI 禁用详细监控

使用以下 `unmonitor-instances` 命令对指定实例禁用详细监控。

```
C:\> aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

列出实例的可用 CloudWatch 指标

Abstract

查看 Amazon EC2 发送到 CloudWatch 的指标，了解前 5 分钟内的活动的默认值。

Amazon EC2 将指标发送到 Amazon CloudWatch。可使用 AWS 管理控制台、AWS CLI 或 API 列出 Amazon EC2 发送到 CloudWatch 的指标。默认情况下，每个数据点中包含的是实例 5 分钟前的活动。如果您启用了详细监控，则每个数据点包含 1 分钟前的活动。

有关获取这些指标的统计数据的信息，请参阅 [获取您的实例的指标的统计数据 \(p. 459\)](#)。

实例指标

下表描述了您的实例的指标。有关为 EBS 卷提供的指标的信息，请参阅 [Amazon EBS 指标 \(p. 661\)](#)。有关为竞价型队列提供的指标的信息，请参阅 [竞价型队列的 CloudWatch 指标 \(p. 191\)](#)。

指标	说明
CPUCreditUsage	<p>(仅对 T2 实例有效) 在指定时段内消耗的 CPU 积分数量。</p> <p>这项指标标识了物理 CPU 在处理虚拟 CPU 分配给实例的指令时所花费的时间。</p> <p> Note</p> <p>CPU 积分指标每 5 分钟可用一次。</p> <p>单位 : 计数</p>
CPUCreditBalance	<p>(仅对 T2 实例有效) 实例累积的 CPU 积分数量。</p> <p>该指标用于确定实例在给定的速率下可以突增至超出基准性能水平的时长。</p> <p> Note</p> <p>CPU 积分指标每 5 分钟可用一次。</p> <p>单位 : 计数</p>
CPUUtilization	<p>当前正在实例上使用的已分配 EC2 计算单位的百分率。该指标确认在选定实例上运行一个应用程序需要的处理能力。</p> <p> Note</p> <p>根据实例类型，如果未向实例分配整个处理器核心，则操作系统中的工具显示的百分率可能低于 CloudWatch。</p> <p>单位 : 百分比</p>
DiskReadOps	<p>在指定时间段内从可供实例使用的所有实例存储卷完成的读取操作数。</p> <p> Note</p> <p>要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。</p> <p>单位 : 计数</p>

指标	说明
DiskWriteOps	<p>在指定时间段内向可供实例使用的所有实例存储卷完成的写入操作数。</p> <p> Note</p> <p>要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。</p> <p>单位：计数</p>
DiskReadBytes	<p>从可供实例使用的所有实例存储卷读取的字节数。</p> <p>该指标用来确定应用程序从实例的硬盘读取的数据量。它可以用来确定应用程序的速度。</p> <p>单位：字节</p>
DiskWriteBytes	<p>向可供实例使用的所有实例存储卷写入的字节数。</p> <p>该指标用来确定应用程序向实例的硬盘写入的数据量。它可以用来确定应用程序的速度。</p> <p>单位：字节</p>
NetworkIn	<p>实例在所有网络接口上收到的字节数。该指标确认单个实例上向应用程序传入的网络流量。</p> <p>单位：字节</p>
NetworkOut	<p>实例在所有网络接口上发送的字节数。该指标确认单个实例上向应用程序传出的网络流量。</p> <p>单位：字节</p>
NetworkPacketsIn	<p>实例在所有网络接口上收到的数据包的数量。此指标依据单个实例上的数据包数量来标识传入流量的量。此指标仅对基本监控可用。</p> <p>单位：计数</p> <p>统计数据：Minimum、Maximum、Average</p>
NetworkPacketsOut	<p>实例在所有网络接口上发送的数据包的数量。此指标依据单个实例上的数据包数量标识传出流量的量。此指标仅对基本监控可用。</p> <p>单位：计数</p> <p>统计数据：Minimum、Maximum、Average</p>

指标	说明
StatusCheckFailed	<p>报告两种状况检查之一是否失败的 StatusCheckFailed_Instance 和 StatusCheckFailed_System 组合。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p> Note</p> <p>状况检查指标每 1 分钟可用一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p>单位：计数</p>
StatusCheckFailed_Instance	<p>报告实例在上 1 分钟内是否通过了 Amazon EC2 实例状况检查。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p> Note</p> <p>状况检查指标每 1 分钟可用一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p>单位：计数</p>
StatusCheckFailed_System	<p>报告实例在上一分钟内是否通过了 EC2 系统状况检查。该指标的值为 0 (零) 或者 1 (一)。“零”表示状况检查已通过。“一”表示状况检查失败。</p> <p> Note</p> <p>状况检查指标每 1 分钟提供一次。对于新启动的实例，状况检查指标仅在实例已完成了初始化状态后可用。状况检查指标将在实例处于运行状态中的几分钟之内可用。</p> <p>单位：计数</p>

Amazon EC2 维度

您可以用下表中的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。

维度	说明
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

您可以按类别查看指标。指标首先按命名空间进行分组，然后按各命名空间内的各种维度组合进行分组。例如，您可以查看由 Amazon EC2 提供的所有指标或按实例 ID、实例类型、映像 (AMI) ID 或 Auto Scaling 组分组的指标。

按类别查看可用指标

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category 窗格中的 EC2 Metrics 下，选择 Per-Instance Metrics。

The screenshot shows the CloudWatch Metrics by Category interface. At the top, it displays a summary: "Your CloudWatch metric summary has loaded. Total metrics: 1,014". Below this, there are several categories of metrics:

- Billing Metrics:** 35
 - Total Estimated Charge: 1
 - By Service: 13
 - By Linked Account: 3
 - By Linked Account and Service: 18
- EC2 Metrics:** 272
 - Per-Instance Metrics: 181
 - By Auto Scaling Group: 56
 - By Image (AMI) Id: 14
 - Aggregated by Instance Type: 14
 - Across All Instances: 7
- DynamoDB Metrics:** 4
 - Table Metrics: 4
- EBS Metrics:** 80
 - Per-Volume Metrics: 80
- ELB Metrics:** 95
 - Per-LB Metrics: 29
 - Per LB, per AZ Metrics: 37
 - By Availability Zone: 20
 - Across All LBs: 9
- ElastiCache Metrics:** 87
 - Cache Node Metrics: 87
- OpsWorks Metrics:** 45
 - Instance Metrics: 15
 - Layer Metrics: 15
 - Stack Metrics: 15
- RDS Metrics:** 104
 - Per-Database Metrics: 52
 - By Database Class: 26
 - By Database Engine: 13
 - Across All Databases: 13
- Redshift Metrics:** 26
 - Node Metrics: 13
 - Aggregated by Cluster: 13

5. 在上方窗格中，向下滚动以查看完整指标列表。

The screenshot shows the EC2 > Per-Instance Metrics list view. It includes columns for InstanceId, InstanceName, and Metric Name. The InstanceId column lists several instance IDs, and the Metric Name column lists CPUUtilization, DiskReadBytes, DiskReadOps, and DiskWriteBytes. At the bottom, there is a search bar with placeholder text "Select a metric above to view graph" and a time range selector.

InstanceId	InstanceName	Metric Name
<input type="checkbox"/> i-0314eff14c446eb49		CPUUtilization
<input type="checkbox"/> i-0314eff14c446eb49		DiskReadBytes
<input type="checkbox"/> i-0314eff14c446eb49		DiskReadOps
<input type="checkbox"/> i-0314eff14c446eb49		DiskWriteBytes

Select a metric above to view graph
Click a checkbox to select a metric
Click on text to add to search

Time Range
Relative Absolute UTC (GMT)
From: 12 hours ago
To: 0 minutes ago
Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w

使用 AWS CLI 列出指标

使用 [list-metrics](#) 命令列出实例的 CloudWatch 指标。

列出所有实例可用的指标

指定 AWS/EC2 命名空间以将结果限制为由 Amazon EC2 发送的指标。

```
C:\> aws cloudwatch list-metrics --namespace AWS/EC2
```

下面是示例输出：

```
...
{
    "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": "NetworkIn"
},
...
...
```

列出指定实例的可用指标

指定 AWS/EC2 命名空间和 `InstanceId` 维度以将结果限制为由 Amazon EC2 发送的指定实例的指标。

```
C:\> aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions Name=InstanceId,Value=i-1234567890abcdef0
```

列出跨所有实例的指标

指定 AWS/EC2 命名空间和指标名称以将结果限制为由 Amazon EC2 发送的指定指标。

```
C:\> aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

获取您的实例的指标的统计数据

Abstract

介绍如何使用 Amazon CloudWatch 控制台或命令行命令获得指标统计数据的各种场景。

以下方案演示如何获取您实例的 CloudWatch 指标的统计数据。

内容

- [获取指定 实例的统计数据 \(p. 459\)](#)
- [聚合多实例统计数据 \(p. 462\)](#)
- [通过 Auto Scaling 组聚合统计数据 \(p. 467\)](#)
- [通过映像 \(AMI\) ID 聚合统计数据 \(p. 469\)](#)

获取指定 实例的统计数据

Abstract

此场景介绍如何获得特定 EC2 实例的统计数据。

以下场景演示了如何使用 AWS 管理控制台或 `get-metric-statistics` 命令来确定特定 EC2 实例的最大 CPU 利用率。



Note

开始和结束时间必须在最近 14 天内。

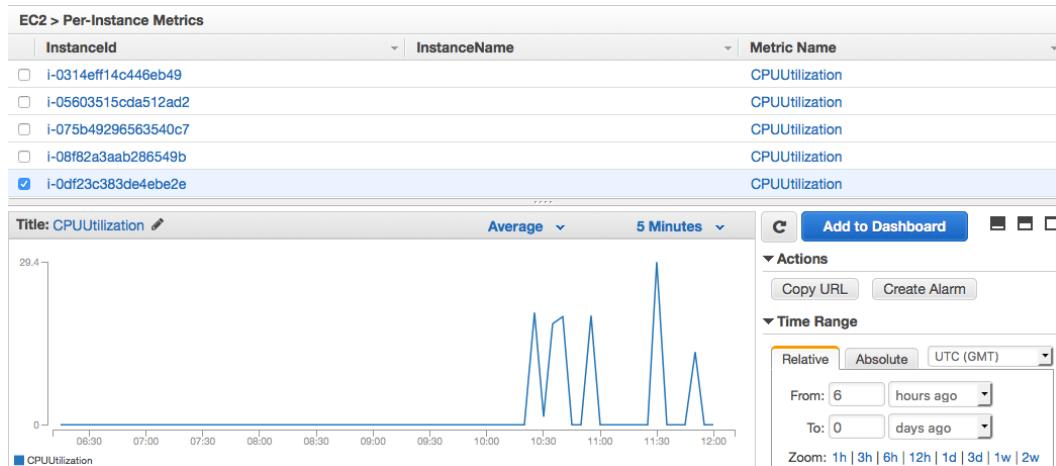
对于此例，我们假定您拥有一个 EC2 实例 ID。您可以通过 AWS 管理控制台或 `describe-instances` 命令来获取活动 EC2 实例的 ID。

AWS 管理控制台

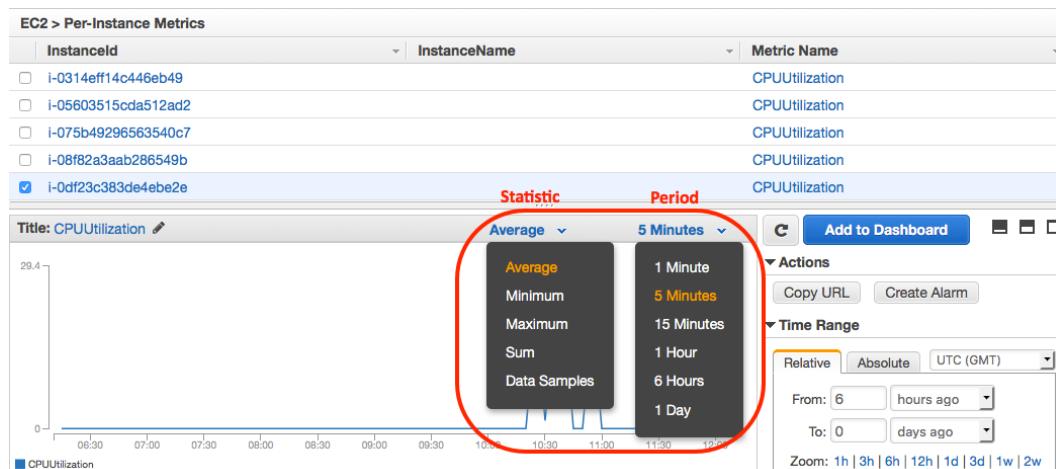
使用控制台显示特定实例的 CPU 利用率

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中，选择 EC2: Metrics (EC2: 指标)。
5. 选择包含特定实例的 CPUUtilization 的行，这将显示此实例指标的图表。

Amazon Elastic Compute Cloud Microsoft Windows 实例用
户指南
获取指标的统计数据



6. 要更改指标的统计数据或周期，请从列表中选择不同的值。



AWS Command Line Interface

使用 AWS CLI 获取特定实例的 CPU 利用率

使用以下 [get-metric-statistics](#) 命令。

```
C:\> aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 --statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --start-time 2014-02-18T23:18:00 --end-time 2014-02-19T23:18:00
```

返回的统计信息是以请求的 2 天时间为间隔的 6 分钟数值。每个数值代表一个 EC2 实例的最大 CPU 利用率百分比。下面是示例输出：

```
{  
    "Datapoints": [  
        {  
            "Timestamp": "2014-02-19T00:18:00Z",  
            "Value": 29.4  
        }  
    ]  
}
```

```
        "Maximum": 0.33000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T03:18:00Z",
        "Maximum": 99.670000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T07:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T12:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T02:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T01:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T17:18:00Z",
        "Maximum": 3.3900000000000001,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T13:18:00Z",
        "Maximum": 0.33000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-18T23:18:00Z",
        "Maximum": 0.6700000000000004,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T06:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T11:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
    {
        "Timestamp": "2014-02-19T10:18:00Z",
        "Maximum": 0.34000000000000002,
        "Unit": "Percent"
    },
}
```

```
{  
    "Timestamp": "2014-02-19T19:18:00Z",  
    "Maximum": 8.0,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T15:18:00Z",  
    "Maximum": 0.34000000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T14:18:00Z",  
    "Maximum": 0.34000000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T16:18:00Z",  
    "Maximum": 0.34000000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T09:18:00Z",  
    "Maximum": 0.34000000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T04:18:00Z",  
    "Maximum": 2.0,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T08:18:00Z",  
    "Maximum": 0.6800000000000005,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T05:18:00Z",  
    "Maximum": 0.3300000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2014-02-19T18:18:00Z",  
    "Maximum": 6.669999999999999,  
    "Unit": "Percent"  
}  
],  
"Label": "CPUUtilization"  
}
```

聚合多实例统计数据

Abstract

此场景介绍如何跨实例和区域获取并聚集统计数据。

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。因此指标在各地区间彼此独立。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。此场景展示了如何通过 AWS 管理控制台、get-metric-statistics API 或 GetMetricStatistics 命令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。要获取其他指标的统计数据，请参阅 [Amazon CloudWatch 命名空间、维度和指标参考](#)。



Important

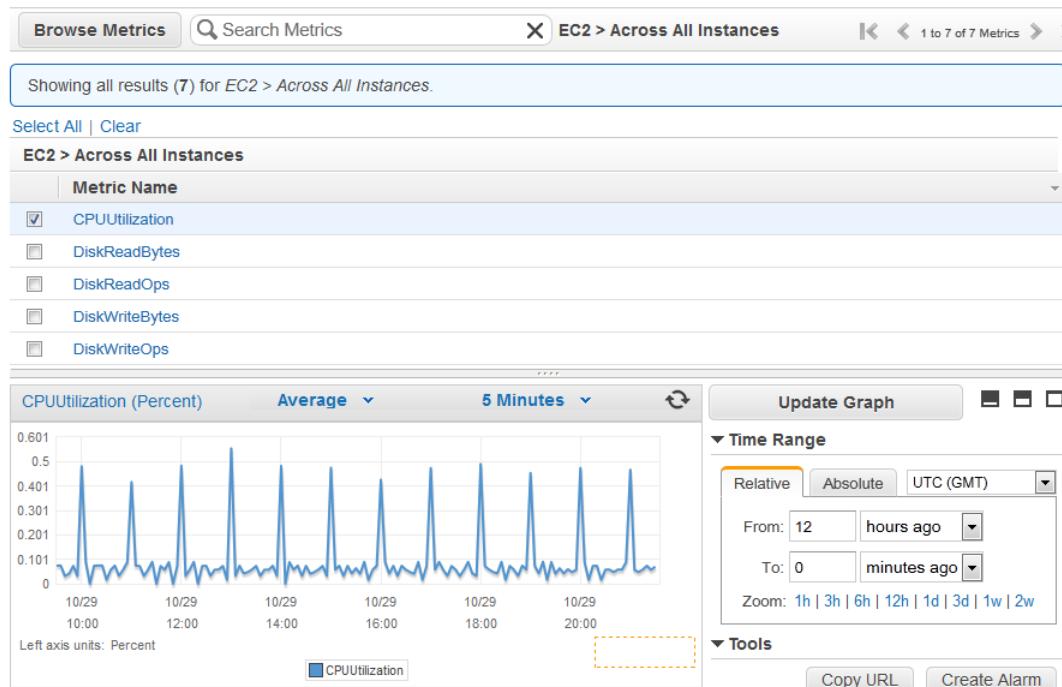
此方法可以在 AWS 命名空间中检索所有维度，但不适用于发布到 Amazon CloudWatch 的自定义命名空间。对于自定义命名空间，必须指定与任意给定数据关联的完整的维度组，以检索包含数据点的统计数据。

AWS 管理控制台

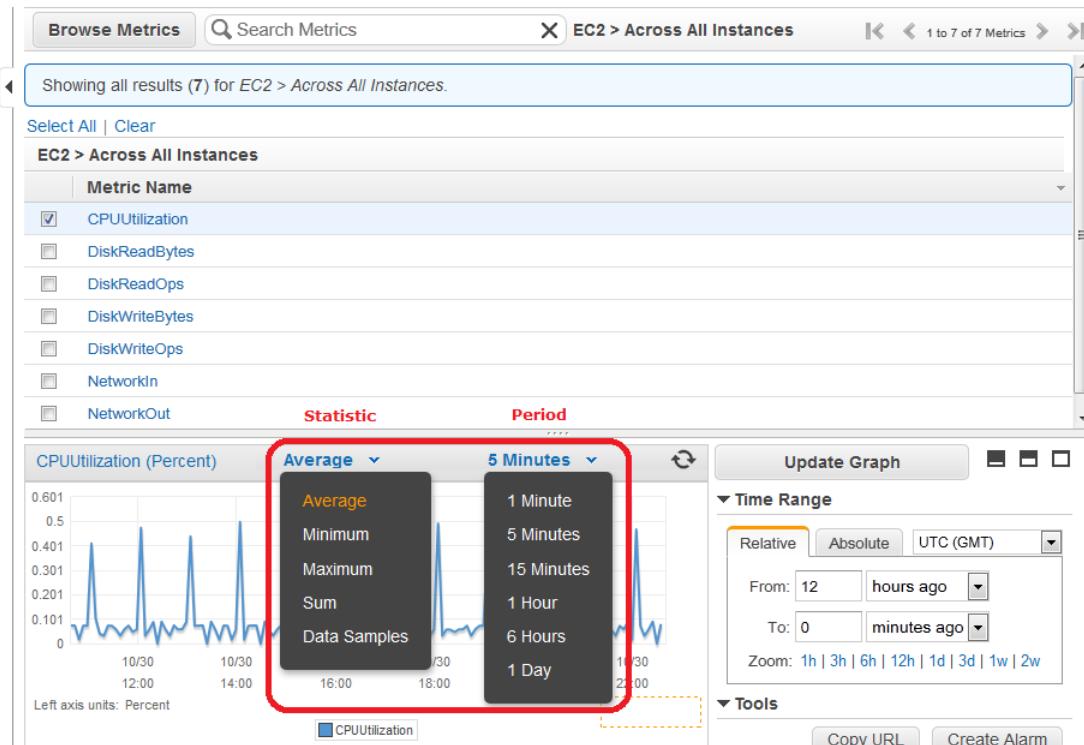
显示实例的平均 CPU 利用率

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中的 EC2 Metrics (EC2 指标) 下，选择 Across All Instances (跨所有实例)。
5. 在上方窗格中，选择包含 CPUUtilization (CPU 利用率) 的行。

详细信息窗格中会出现一个显示 EC2 实例的 CPUUtilization 的图表。



6. 要更改指标的统计数据或周期，请从列表中选择不同的值。



AWS Command Line Interface

要获取实例的平均 CPU 利用率，请执行以下步骤：

使用 [get-metric-statistics](#) 命令，如下所示。

```
C:\> aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 --statistics "Average" "SampleCount" --start-time 2014-02-11T23:18:00 --end-time 2014-02-12T23:18:00
```

下面是示例输出：

```
{  
    "Datapoints": [  
        {  
            "SampleCount": 238.0,  
            "Timestamp": "2014-02-12T07:18:00Z",  
            "Average": 0.038235294117647062,  
            "Unit": "Percent"  
        },  
        {  
            "SampleCount": 240.0,  
            "Timestamp": "2014-02-12T09:18:00Z",  
            "Average": 0.16670833333333332,  
            "Unit": "Percent"  
        },  
        {  
            "SampleCount": 238.0,
```

```
"Timestamp": "2014-02-11T23:18:00Z",
"Average": 0.041596638655462197,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T16:18:00Z",
"Average": 0.039458333333333345,
"Unit": "Percent"
},
{
"SampleCount": 239.0,
"Timestamp": "2014-02-12T21:18:00Z",
"Average": 0.041255230125523033,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T01:18:00Z",
"Average": 0.04458333333333336,
"Unit": "Percent"
},
{
"SampleCount": 239.0,
"Timestamp": "2014-02-12T18:18:00Z",
"Average": 0.043054393305439344,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T13:18:00Z",
"Average": 0.03945833333333345,
"Unit": "Percent"
},
{
"SampleCount": 238.0,
"Timestamp": "2014-02-12T15:18:00Z",
"Average": 0.041260504201680689,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T19:18:00Z",
"Average": 0.037666666666666668,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T06:18:00Z",
"Average": 0.037541666666666675,
"Unit": "Percent"
},
{
"SampleCount": 240.0,
"Timestamp": "2014-02-12T20:18:00Z",
"Average": 0.03933333333333338,
"Unit": "Percent"
},
```

```
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T08:18:00Z",  
    "Average": 0.039250000000000014,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 239.0,  
    "Timestamp": "2014-02-12T03:18:00Z",  
    "Average": 0.037740585774058588,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T11:18:00Z",  
    "Average": 0.039500000000000007,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 238.0,  
    "Timestamp": "2014-02-12T02:18:00Z",  
    "Average": 0.039789915966386563,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 238.0,  
    "Timestamp": "2014-02-12T22:18:00Z",  
    "Average": 0.039705882352941181,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T14:18:00Z",  
    "Average": 0.08245833333333328,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T05:18:00Z",  
    "Average": 0.0428750000000001,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T17:18:00Z",  
    "Average": 0.03945833333333345,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 240.0,  
    "Timestamp": "2014-02-12T10:18:00Z",  
    "Average": 0.08341666666666667,  
    "Unit": "Percent"  
},  
{  
    "SampleCount": 236.0,  
    "Timestamp": "2014-02-12T00:18:00Z",  
    "Average": 0.036567796610169498,
```

```
        "Unit": "Percent"
    },
{
    "SampleCount": 240.0,
    "Timestamp": "2014-02-12T12:18:00Z",
    "Average": 0.03954166666666676,
    "Unit": "Percent"
},
{
    "SampleCount": 240.0,
    "Timestamp": "2014-02-12T04:18:00Z",
    "Average": 0.043000000000000003,
    "Unit": "Percent"
}
],
"Label": "CPUUtilization"
}
```

通过 Auto Scaling 组聚合统计数据

Abstract

此场景介绍如何根据 Auto Scaling 组获取聚合的统计数据。

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。因此指标在各地区间彼此独立。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。

此场景展示了如何通过 *DiskWriteBytes* 指标使用 AWS 管理控制台、*GetMetricStatistics* 命令或 *get-metric-statistics* API 来检索某个 Auto Scaling 组的磁盘写入总字节数。总数以 1 分钟为周期 24 小时为间隔针对指定 *AutoScalingGroupName* 中的所有 EC2 实例计算得出。



Note

开始和结束时间必须在最近 14 天内。

在此例中，假定有一个 EC2 应用程序正在运行，且该应用程序包含一个名为 *test-group-1* 的 Auto Scaling 组。

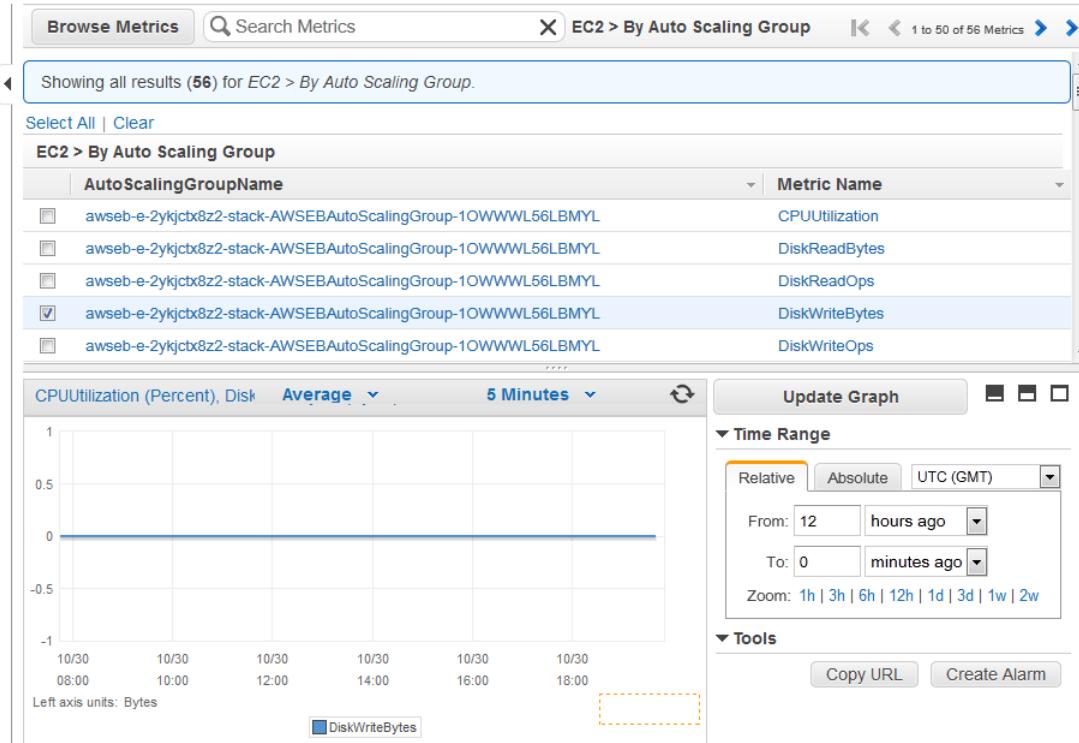
AWS 管理控制台

显示自动扩展的应用程序的 DiskWriteByte 总数

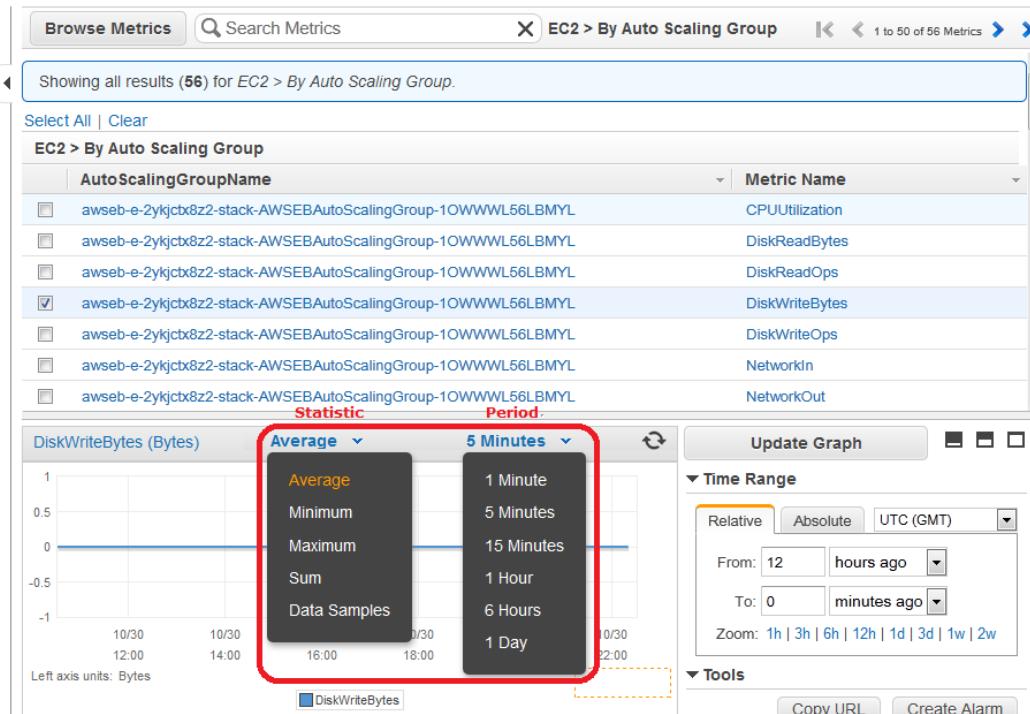
1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中的 EC2 Metrics (EC2 指标) 下，选择 By Auto Scaling Group (按 Auto Scaling 组)。
5. 选择包含 *DiskWriteBytes* 的行。

详细信息窗格中将出现一个显示所有 EC2 实例的 *DiskWriteBytes* 的图表。

Amazon Elastic Compute Cloud Microsoft Windows 实例用
户指南
获取指标的统计数据



6. 要更改指标的统计数据或周期，请从列表中选择不同的值。



AWS Command Line Interface

获取 Auto-Scaled 应用程序的写入磁盘总字节数

使用 `get-metric-statistics` 命令，如下所示。

```
C:\> aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes --period 360 --statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-group --start-time 2014-02-16T23:18:00 --end-time 2014-02-18T23:18:00
```

下面是示例输出：

```
{  
    "Datapoints": [  
        {  
            "SampleCount": 18.0,  
            "Timestamp": "2014-02-19T21:36:00Z",  
            "Sum": 0.0,  
            "Unit": "Bytes"  
        },  
        {  
            "SampleCount": 5.0,  
            "Timestamp": "2014-02-19T21:42:00Z",  
            "Sum": 0.0,  
            "Unit": "Bytes"  
        }  
    ],  
    "Label": "DiskWriteBytes"  
}
```

通过映像 (AMI) ID 聚合统计数据

Abstract

此场景介绍如何根据映像 ID 获取聚合的统计数据。

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。因此指标在各地区间彼此独立。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。

此场景展示了如何使用 AWS 管理控制台、`get-metric-statistics` 命令或 `GetMetricStatistics` API 来确定符合给定映像 ID 的所有实例的平均 CPU 利用率。平均值以 60 秒为时间间隔 1 天为周期。



Note

开始和结束时间必须在最近 14 天内。

在此场景中，EC2 实例运行 ID 为 `ami-c5e40dac` 的映像。

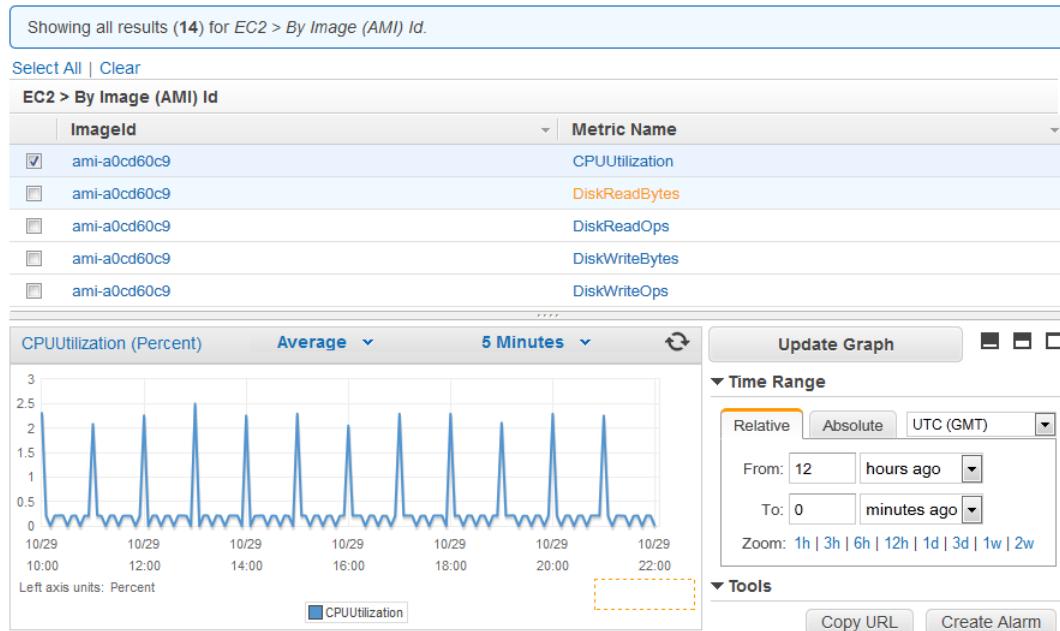
AWS 管理控制台

要显示映像 ID 的平均 CPU 利用率

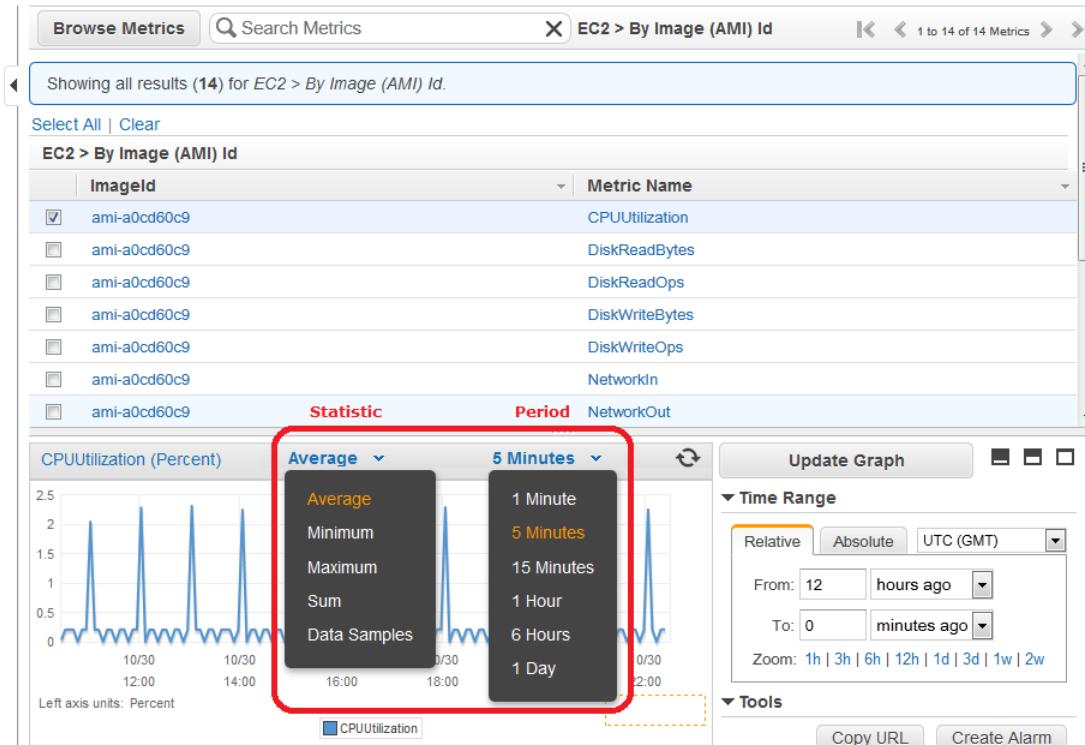
1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。

3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中的 EC2 Metrics (EC2 指标) 下，选择 By Image (AMI) Id (按映像 (AMI) ID)。
5. 选择包含 CPUUtilization (CPU 利用率) 和映像 ID 的行。

详细信息窗格中将出现一个显示基于 CPUUtilization 映像 ID 的所有 EC2 实例的平均 ami-c5e40dac 的图表。



6. 要更改指标的统计数据或周期，请从列表中选择不同的值。



AWS Command Line Interface

要获取映像 ID 的平均 CPU 利用率，请执行以下步骤：

使用 `get-metric-statistics` 命令，如下所示。

```
C:\> aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 --statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-time 2014-02-10T00:00:00 --end-time 2014-02-11T00:00:00
```

下面是示例输出：

```
{  
    "Datapoints": [  
        {  
            "Timestamp": "2014-02-10T07:00:00Z",  
            "Average": 0.04100000000000009,  
            "Unit": "Percent"  
        },  
        {  
            "Timestamp": "2014-02-10T14:00:00Z",  
            "Average": 0.079579831932773085,  
            "Unit": "Percent"  
        },  
        {  
            "Timestamp": "2014-02-10T06:00:00Z",  
            "Average": 0.03600000000000011,  
            "Unit": "Percent"  
        }  
    ]  
}
```

```
        "Unit": "Percent"
    },
{
    "Timestamp": "2014-02-10T13:00:00Z",
    "Average": 0.037625000000000013,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T18:00:00Z",
    "Average": 0.042750000000000003,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T21:00:00Z",
    "Average": 0.039705882352941188,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T20:00:00Z",
    "Average": 0.039375000000000007,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T02:00:00Z",
    "Average": 0.04104166666666671,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T01:00:00Z",
    "Average": 0.04108333333333354,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T23:00:00Z",
    "Average": 0.038016877637130804,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T15:00:00Z",
    "Average": 0.03766666666666668,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T12:00:00Z",
    "Average": 0.03929166666666676,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T03:00:00Z",
    "Average": 0.03600000000000004,
    "Unit": "Percent"
},
{
    "Timestamp": "2014-02-10T04:00:00Z",
    "Average": 0.04266666666666672,
    "Unit": "Percent"
},
```

```
"Timestamp": "2014-02-10T19:00:00Z",
"Average": 0.038305084745762719,
"Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T22:00:00Z",
  "Average": 0.03929166666666676,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T09:00:00Z",
  "Average": 0.17126050420168065,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T08:00:00Z",
  "Average": 0.04116666666666678,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T11:00:00Z",
  "Average": 0.08237499999999962,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T17:00:00Z",
  "Average": 0.037625000000000013,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T10:00:00Z",
  "Average": 0.03945833333333345,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T05:00:00Z",
  "Average": 0.039250000000000007,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T00:00:00Z",
  "Average": 0.037625000000000013,
  "Unit": "Percent"
},
{
  "Timestamp": "2014-02-10T16:00:00Z",
  "Average": 0.041512605042016815,
  "Unit": "Percent"
}
],
"Label": "CPUUtilization"
}
```

操作返回的统计信息是以 1 天时间为间隔的 1 分钟数值。每个数值代表运行指定系统映像的 EC2 实例的平均 CPU 利用率。

绘制实例的指标图形

Abstract

查看实例的监控图形。

启动实例后，您可以转至 Amazon EC2 控制台查看实例的监视图表。当您在 EC2 控制面板中的“Instances”页面上选择实例时，会显示监视图像。“Monitoring”选项卡显示在实例的“Description”选项卡旁。可供使用图形如下：

- CPU 平均利用率（%）
- 平均读磁盘数（字节）
- 平均写磁盘数（字节）
- 最大网络输入（字节）
- 最大网络输出（字节）
- 读磁盘操作概括（计数）
- 写磁盘操作概括（计数）
- 状态概括（任意）
- 实例状态概括（计数）
- 系统状态概括（计数）

每个图表以一个可用的 Amazon EC2 指标为基础。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 \(p. 453\)](#)。

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，以便更轻松地查看当前的运行状况。您可以使用下列步骤在 CloudWatch 中绘制指标图表。

内容

- [绘制指标图表 \(p. 474\)](#)
- [绘制跨资源指标的图表 \(p. 475\)](#)

绘制指标图表

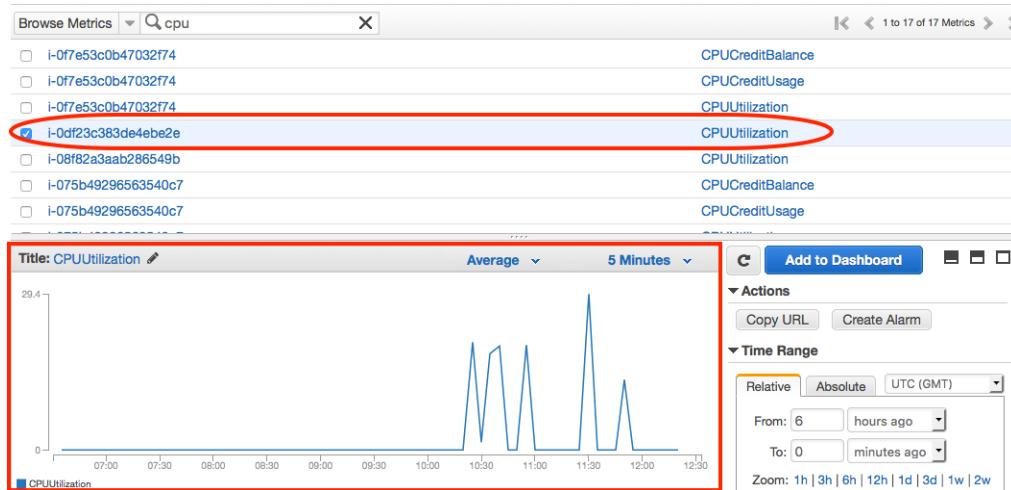
Abstract

此场景介绍如何在 CloudWatch 中选择指标和创建数据图表。

您可以选择一项指标，并在 CloudWatch 中创建数据的图表。例如，您可以选择一个 Amazon EC2 实例的 CPU 利用率指标，显示该实例的 CPU 利用率随着时间变化的图表。

绘制指标图表

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。
4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中，使用 Search Metrics (搜索指标) 框和类别，按指标名称、AWS 资源或其他元数据查找指标。
5. 使用指标列表上方的滚动条及上一页和下一页箭头来翻阅整个指标列表
6. 选择指标（例如 CPU 利用率）以进行查看。详细信息窗格中会显示相应图表。



7. 要保存此图表以在稍后进行访问，请在详细信息窗格中的 Tools (工具) 下，单击 Copy URL (复制 URL)，然后在 Copy Graph URL (复制图表 URL) 对话框中，选择该 URL，并将其粘贴到您的浏览器中。

绘制跨资源指标的图表

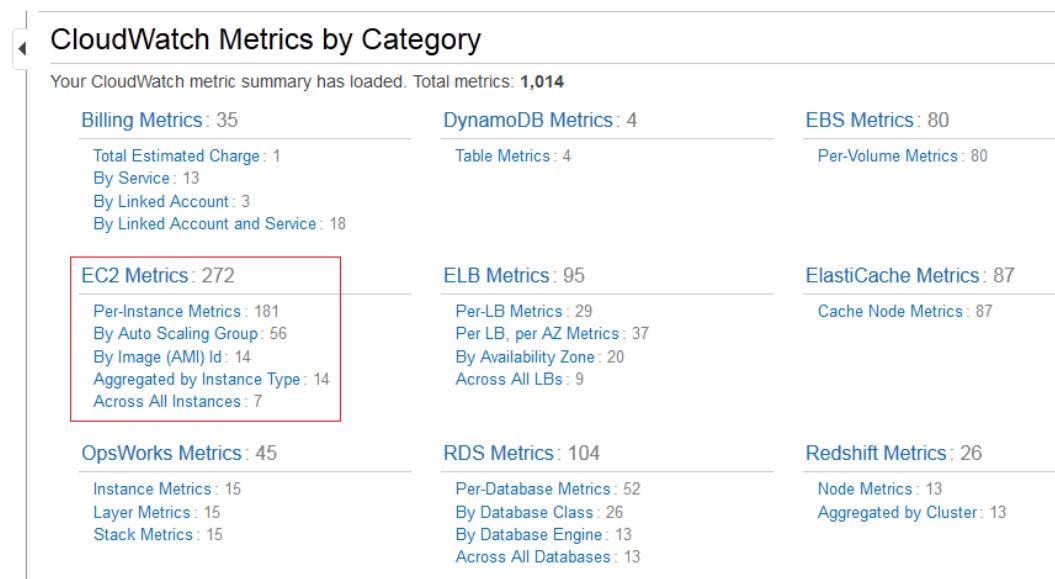
Abstract

此场景介绍如何跨所有资源选择一个指标并在 CloudWatch 中创建单个数据图表。

您可以为跨所有资源的指标绘制图表，以在一个图表中查看所有数据。例如，您可以在一个图表中绘制所有 Amazon EC2 实例的 CPU 利用率指标。

绘制跨资源指标的图表

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Metrics。



4. 在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中，选择一种指标类别。例如，在 EC2 Metrics (EC2 指标) 下，选择 Per-Instance Metrics (每个实例的指标)。

EC2 > Per-Instance Metrics

InstanceId	InstanceName	Metric Name
i-0314eff14c446eb49		CPUUtilization
i-0314eff14c446eb49		DiskReadBytes
i-0314eff14c446eb49		DiskReadOps
i-0314eff14c446eb49		DiskWriteBytes

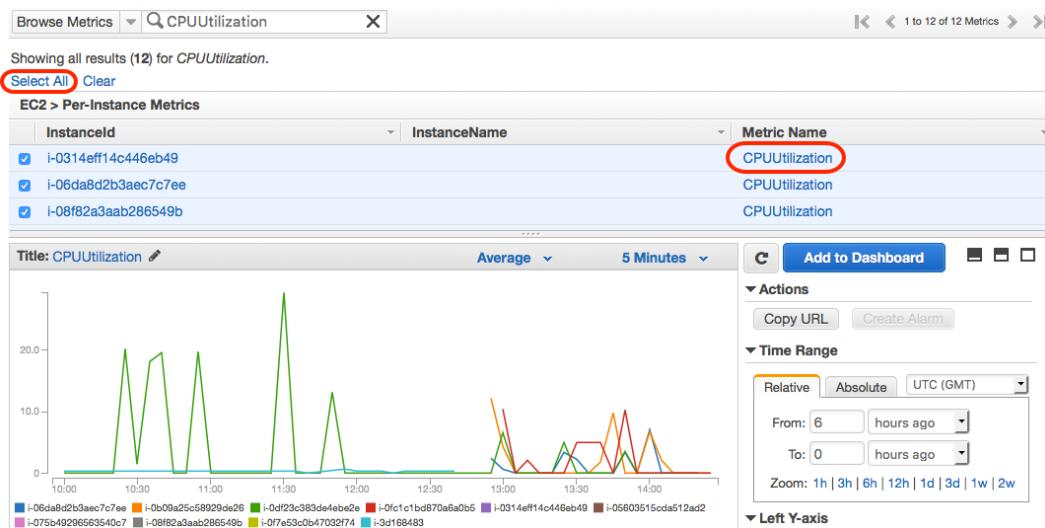
Select a metric above to view graph

Click a checkbox to select a metric
Click on text to add to search

Time Range: Relative, Absolute, UTC (GMT)
From: 12 hours ago, To: 0 minutes ago
Zoom: 1h, 3h, 6h, 12h, 1d, 3d, 1w, 2w

5. 在指标列表的 Metric Name (指标名称) 列中，单击一项指标。例如 CPUUtilization (CPU 利用率)。
6. 在指标列表的顶部，单击 Select All (全选)。

图表会显示所选指标的所有出现次数的全部数据。以下示例中显示了所有 Amazon EC2 实例的 CPU 利用率。



7. 要保存此图表以便稍后进行访问，请在详细信息窗格中的 Tools (工具) 下，单击 Copy URL (复制 URL)，然后在 Copy Graph URL (复制图表 URL) 对话框中，选择该 URL，并将其粘贴到您的浏览器中。

创建 CloudWatch 警报

Abstract

针对 CloudWatch 指标创建一个 CloudWatch 警报。

您可以创建 Amazon CloudWatch 警报来监控您的任一 Amazon EC2 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。您可以在 AWS 管理控制台的 Amazon EC2 控制台上创建 CloudWatch 警报，也可以使用 CloudWatch 控制台并配置更高级的选项。

内容

- [根据 CPU 利用率警报发送电子邮件 \(p. 477\)](#)
- [根据负载均衡器警报发送电子邮件 \(p. 479\)](#)
- [根据存储吞吐量警报发送电子邮件 \(p. 481\)](#)

根据 CPU 利用率警报发送电子邮件

Abstract

此场景介绍如何根据 CPU 使用率警报的状态创建发送电子邮件的警报。

此场景介绍如何使用 AWS 管理控制台或命令行界面创建一个 Amazon CloudWatch 警报，当警报状态从“正常”变为“警报”时，该警报会发送 Amazon Simple Notification Service 电子邮件。

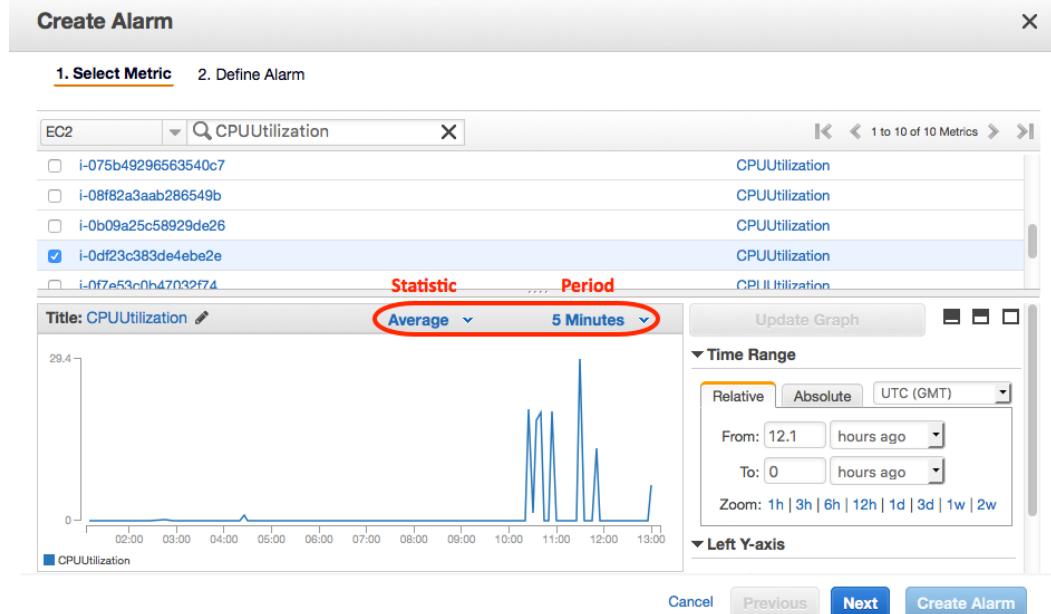
在此场景中，可以将警报配置为，当 EC2 实例的 CPU 利用率超过 70% 长达两个连续 5 分钟时间段时，更改为“警报”状态。

AWS 管理控制台

创建根据 CPU 利用率发送电子邮件的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 中，选择一个指标类别，例如 EC2 Metrics (EC2 指标)。
5. 在指标列表中，选择包含特定实例 ID 的 CPUUtilization (CPU 利用率) 的行。

一张显示单一实例平均 CPUUtilization 的图表会出现在下方窗格中。



6. 从 Statistic 下拉列表中选择 Average。
7. 从“Period”下拉列表中选择一个时间段，例如：5。
8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，为警报输入唯一名称，例如：myHighCpuAlarm。
9. 在 Description (描述) 字段中，输入警报的描述，例如：CPU 70%
10. 在 is 下拉列表中选择 >。
11. 在 is (条件) 下拉列表旁的框内，输入 70 并在 for (时间) 字段内输入 10。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，在 Whenever this alarm (每当此警报) 下拉列表中选择 State is ALARM (状态为“警报”)。
13. 在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新主题。
14. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。

在 Send notification to (发送通知到) 字段中，输入新 Amazon SNS 主题的名称，例如：myHighCpuAlarm，在 Email list (电子邮件列表) 字段中，输入警报变为 ALARM 状态时要通知的逗号分隔电子邮件地址列表。

15. 单击创建警报完成警报创建过程。

AWS Command Line Interface

在 CPU 利用率超过 70% 时发送 Amazon Simple Notification Service 电子邮件

1. 设置 Amazon Simple Notification Service 主题或检索要使用的主题的“主题资源名称”。有关设置 Amazon Simple Notification Service 主题的帮助，请参阅[设置 Amazon Simple Notification Service](#)。
2. 使用 `put-metric-alarm` 命令创建警报，如下所示。

```
C:\> aws cloudwatch put-metric-alarm --alarm-name cpu-mon --alarm-description "Alarm when CPU exceeds 70%" --metric-name CPUUtilization --namespace
```

```
AWS/EC2 --statistic Average --period 300 --threshold 70 --comparison-operator GreaterThanThreshold --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --evaluation-periods 2 --alarm-actions arn:aws:sns:cn-north-1:111122223333:MyTopic --unit Percent
```

3. 通过使用 `set-alarm-state` 命令强制改变警报状态对警报进行测试。

- a. 将警报状态从 `INSUFFICIENT_DATA` 更改为 `OK` :

```
C:\> aws cloudwatch set-alarm-state --alarm-name cpu-mon --state-reason "initializing" --state-value OK
```

- b. 将警报状态从 `OK` 更改为 `ALARM` :

```
C:\> aws cloudwatch set-alarm-state --alarm-name cpu-mon --state-reason "initializing" --state-value ALARM
```

- c. 查看是否已经收到电子邮件。

根据负载均衡器警报发送电子邮件

Abstract

此场景介绍如何根据警报的状态设置发送电子邮件的负载均衡器警报。

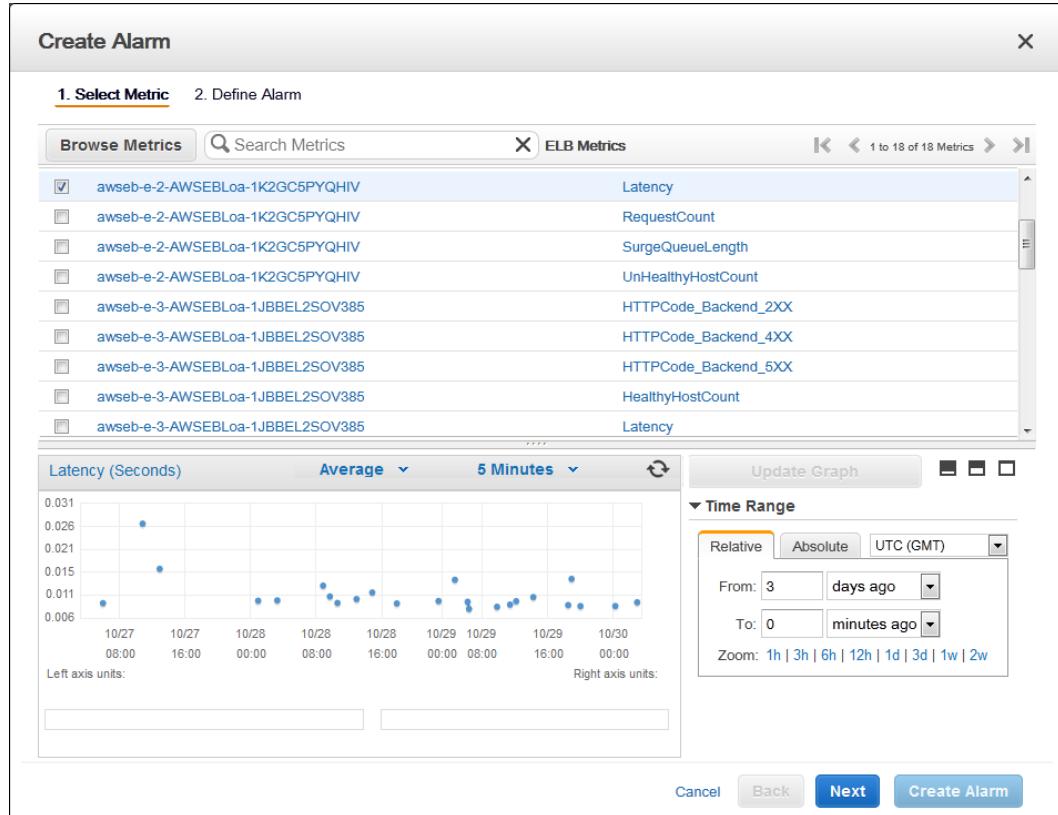
此场景介绍如何使用 AWS 管理控制台或命令行界面设置 Amazon Simple Notification Service 通知和配置警报，以监控超过 100 ms 的负载均衡器延迟。

AWS 管理控制台

创建发送电子邮件的负载均衡器警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中，选择一个指标类别，例如 ELB Metrics (ELB 指标)。
5. 在指标列表中，选择包含特定负载均衡器的 Latency (延迟) 的行。

下方窗格中会出现一个显示单个负载均衡器的平均 Latency 的图表。



6. 从 Statistic 下拉列表中选择 Average。
 7. 从“Period”下拉列表中选择“1 Minute”。
 8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，为警报输入唯一名称，例如：myHighCpuAlarm。
 9. 在 Description (描述) 字段中，输入警报的描述，例如：100ms。
 10. 在 is 下拉列表中选择 >。
 11. 在 is (条件) 下拉列表旁的框内，输入 0.1 并在 for (时间) 字段内输入 3。
 12. 在 Actions (操作) 下，在 Whenever this alarm (每当此警报) 下拉列表中选择 State is ALARM (状态为“警报”)。
 13. 在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新主题。
 14. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。
- 在 Send notification to (发送通知到) 字段中，输入新 Amazon SNS 主题的名称，例如：myHighCpuAlarm，在 Email list (电子邮件列表) 字段中，输入警报变为 ALARM 状态时要通知的逗号分隔电子邮件地址列表。
15. 单击创建警报完成警报创建过程。

AWS Command Line Interface

在负载均衡器延迟超过 100 毫秒时发送 Amazon Simple Notification Service 电子邮件

1. 创建一个 Amazon Simple Notification Service 主题。请参阅[设置 Amazon Simple Notification Service 中有关创建 Amazon SNS 主题的说明](#)。

2. 使用 [put-metric-alarm](#) 命令，如下所示。

```
C:\> aws cloudwatch put-metric-alarm --alarm-name lb-mon --alarm-description "Alarm when Latency exceeds 100ms" --metric-name Latency --namespace AWS/ELB --statistic Average --period 60 --threshold 100 --comparison-operator GreaterThanThreshold --dimensions Name=LoadBalancerName,Value=my-server --evaluation-periods 3 --alarm-actions arn:aws:sns:cn-north-1:1234567890:my-topic --unit Milliseconds
```

3. 测试警报。

- 将警报状态强制变为 ALARM：

```
C:\> aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value OK
```

```
C:\> aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value ALARM
```

- 检查您是否收到有关警报的电子邮件通知。

根据存储吞吐量警报发送电子邮件

Abstract

此场景介绍如何根据警报状态创建发送电子邮件的存储吞吐量警报。

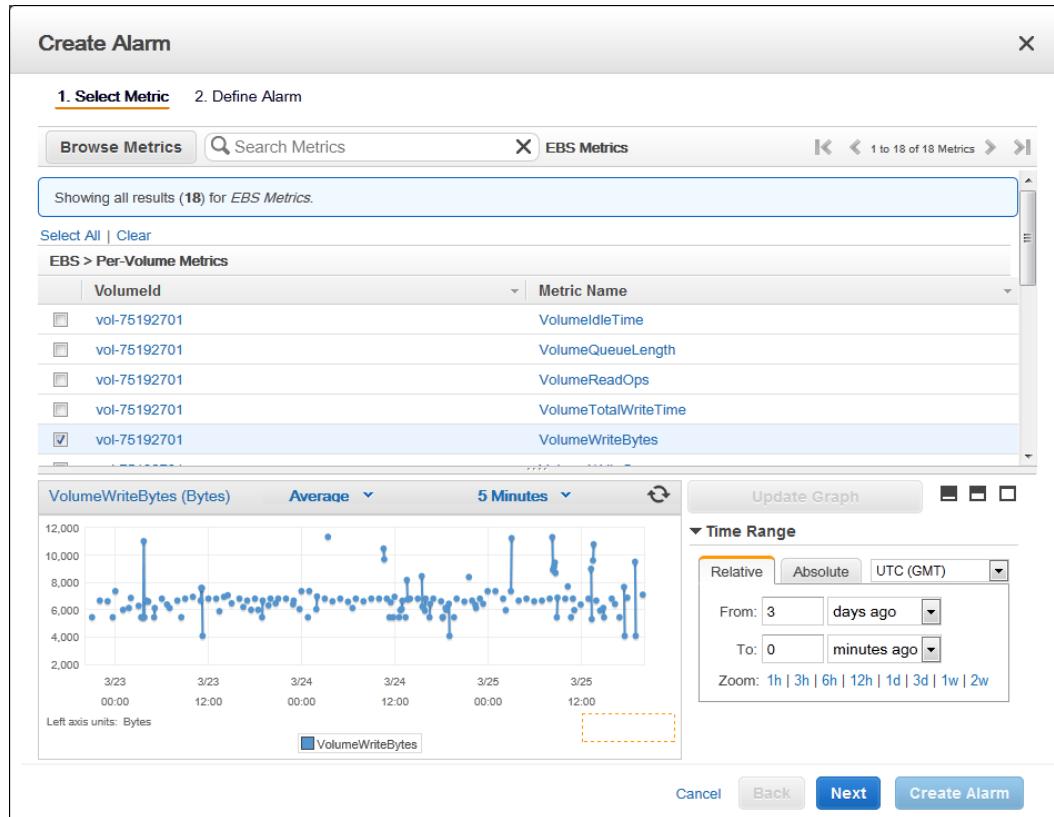
此场景介绍如何使用 AWS 管理控制台或命令行界面设置 Amazon Simple Notification Service 通知，以及配置当 EBS 超过 100 MB 吞吐量时发送电子邮件的警报。

AWS 管理控制台

创建发送电子邮件的存储吞吐量警报

- 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
- 如果需要，可从导航栏中更改区域以匹配实例所在的区域。
- 在导航窗格中，单击 Alarms (警报)。
- 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 窗格中，选择一个指标类别，例如 EBS Metrics (EBS 指标)。
- 在指标列表中，选择包含特定 VolumeId 的 VolumeWriteBytes (卷写入字节数) 的行。

下方窗格中会出现一个显示单个卷的平均 VolumeWriteBytes 的图表。



6. 从 Statistic 下拉列表中选择 Average。
7. 从 5 Minutes (周期) 下拉列表中选择 Period (5 分钟)。
8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，为警报输入唯一名称，例如：myHighWriteAlarm。
9. 在 Description (描述) 字段中，输入警报的描述，例如：VolumeWriteBytes 100000 KiB/s
10. 在 is 下拉列表中选择 >。
11. 在 is (条件) 下拉列表旁的框内，输入 100000 并在 for (时间) 字段内输入 15。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，在 Whenever this alarm (每当此警报) 下拉列表中选择 State is ALARM (状态为“警报”)。
13. 在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新主题。
14. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。

在 Send notification to (发送通知到) 字段中，输入新 Amazon SNS 主题的名称，例如：myHighCpuAlarm，在 Email list (电子邮件列表) 字段中，输入警报变为 ALARM 状态时要通知的逗号分隔电子邮件地址列表。

15. 单击创建警报完成警报创建过程。

AWS Command Line Interface

在 EBS 吞吐量超过 100 MB 时发送 Amazon Simple Notification Service 电子邮件

1. 创建一个 Amazon Simple Notification Service 主题。请参阅[设置 Amazon Simple Notification Service 中有关创建 Amazon SNS 主题的说明](#)。

2. 使用 [put-metric-alarm](#) 命令，如下所示。

```
C:\> aws cloudwatch put-metric-alarm --alarm-name ebs-mon --alarm-description "Alarm when EBS volume exceeds 100MB throughput" --metric-name VolumeRead Bytes --namespace AWS/EBS --statistic Average --period 300 --threshold 100000000 --comparison-operator GreaterThanThreshold --dimensions Name=VolumeId,Value=my-volume-id --evaluation-periods 3 --alarm-actions arn:aws:sns:cn-north-1:1234567890:my-alarm-topic --insufficient-data-actions arn:aws:sns:cn-north-1:1234567890:my-insufficient-data-topic
```

3. 测试警报。

- 将警报状态强制变为 ALARM。

```
C:\> aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value OK
```

```
C:\> aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value ALARM
```

```
C:\> aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value INSUFFICIENT_DATA
```

- 检查您是否收到有关警报的两份电子邮件通知。

创建停止、终止、重启或恢复实例的警报

Abstract

创建自动停止、终止、重启或恢复 Amazon EC2 实例的 CloudWatch 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 Amazon Elastic Compute Cloud (Amazon EC2) 实例的警报。当不再需要某个实例运行时，您可使用停止或终止操作来帮助您节省资金。如果发生了系统损害，您可使用重启和恢复操作自动重启这些实例或将它们恢复到新硬件上。

您创建的每个警报操作均使用警报操作 ARN。一组 ARN 更安全，因为它要求您的账户中有 EC2ActionsAccess IAM 角色。利用此 IAM 角色，您可执行停止、终止或重启操作 - 以前如果您使用的是 IAM 角色，则无法执行操作。使用以前的警报操作 ARN 的现有警报不需要此 IAM 角色，但建议您在编辑使用这些 ARN 的现有警报时更改 ARN 并添加此角色。

EC2ActionsAccess IAM 角色使 AWS 能够代表您执行警报操作。当您首次使用 Amazon EC2 或 Amazon CloudWatch 控制台创建警报操作时，AWS 将自动为您创建此角色。此外，您必须先使用任一控制台创建 EC2ActionsAccess 角色，然后才能通过 CLI 使用此角色。

在许多情况下，您可能需要自动终止或停止实例。例如，您可能拥有专用于批工资单处理工作或科学计算任务的实例，这些实例在运行一段时间后就完成了其工作。与其让这些实例空闲（并产生费用），不如将其停止或终止以节省开支。使用停止警报操作和终止警报操作的主要区别是，停止的警报可以在需要时轻松重启，还可以保留相同的实例 ID 和根卷。而终止的实例则无法重新启动。如此就必须启动一个新的实例。

您可以创建警报用于在实例受损（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 Amazon EC2 实例。导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题



Important

恢复操作仅受到以下项支持：

- C3、C4、M3、M4、R3、T2 和 X1 实例类型。
- VPC 中的实例。



Note

如果您的实例有公有 IP 地址，它会在恢复后保留相同的公有 IP 地址。

- 使用共享租赁的实例（实例的租赁属性设置为 default）。
- 完全使用 Amazon EBS 存储的实例。

目前，EC2-Classic 实例、专用租赁实例、在专用主机上运行的实例以及使用任何实例存储卷的实例不支持恢复操作。

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 InstanceId 值引用有效运行的 Amazon EC2 实例。

内容

- [向 Amazon CloudWatch 警报添加停止操作 \(p. 484\)](#)
- [向 Amazon CloudWatch 警报添加终止操作 \(p. 487\)](#)
- [向 Amazon CloudWatch 警报添加重启操作 \(p. 490\)](#)
- [向 Amazon CloudWatch 警报添加恢复操作 \(p. 493\)](#)
- [使用 Amazon CloudWatch 控制台查看已触发的警报和操作的历史记录 \(p. 496\)](#)
- [使用 CLI 或 API 创建警报以停止、终止、重启或恢复实例 \(p. 497\)](#)
- [Amazon CloudWatch 警报操作场景 \(p. 503\)](#)

向 Amazon CloudWatch 警报添加停止操作

您可使用 Amazon EC2 控制台、Amazon CloudWatch 控制台、Amazon CloudWatch 命令行界面 (CLI)、CloudWatch API 或 AWS 软件开发工具包配置停止警报操作。有关结合使用 Amazon CloudWatch API 和 AWS 开发工具包的信息，请参阅[示例代码和库](#)。

使用 Amazon EC2 控制台创建停止实例的警报

可以创建当达到一定阈值后停止 Amazon EC2 实例的警报。例如，您可能运行了开发或测试实例而偶尔忘记将其关闭。可以创建当平均 CPU 利用率低于 10% 达 24 小时时触发的警报，同时告知其为空闲并不再使用。可以根据需要调整阈值、时长和时间段，还可以添加 Amazon Simple Notification Service (Amazon SNS) 通知，以便您在触发警报后能够收到电子邮件。

可以停止或终止将 Amazon Elastic Block Store 卷用作根设备的 Amazon EC2 实例，但只能终止将实例存储用作根设备的实例。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- `ec2:DescribeInstanceStatus` 和 `ec2:DescribeInstances`，针对有关 Amazon EC2 实例状态指标的所有警报。
- `ec2:StopInstances`，针对包含停止操作的警报。
- `ec2:TerminateInstances`，针对包含终止操作的警报。
- `ec2:DescribeInstanceRecoveryAttribute` 和 `ec2:RecoverInstances`，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南中的权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 `EC2ActionsAccess` 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

要创建停止空闲实例的警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中的 INSTANCES 下，单击 Instances。
4. 在内容窗格中，右键单击一个实例，选择 CloudWatch Monitoring，然后单击 Add/Edit Alarms。

也可以选择该实例，然后在 Monitoring (监控) 选项卡上的下方窗格中单击 Create Alarm (创建警报)。
5. 在 Alarm Details for (以下项的警报详细信息) 对话框中，单击 Create Alarm (创建警报)。
6. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for (针对以下项创建警报) 对话框中的 Send a notification to (发送通知到) 框中选择一个现有 Amazon SNS 主题，或单击 Create Topic (创建主题) 创建新的主题。

- 如果创建新的主题，则请在“Send a notification to”方框中输入主题的名称，然后在“With these recipients”方框中输入收件人的电子邮件地址（以逗号隔开）。之后，待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可获得该主题的电子邮件。
7. 选中 Take the action 复选框，然后选择 Stop this instance 单选按钮。
 8. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。
 9. 在“Whenever”方框中，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”和“CPU Utilization”。
 10. 在“Is”方框中，定义指标的阈值。在此示例中，输入 10%。
 11. 在“For at least”方框中，选择警报的采样周期。在此示例中，输入 24 个连续 1 小时时时间段。
 12. 要更改警报的名称，在“Name this alarm”方框中，输入新的名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。



Note

可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

13. 单击 Create Alarm (创建警报)。

使用 Amazon CloudWatch 控制台创建停止实例的警报

可以创建当达到一定阈值后停止 Amazon EC2 实例的警报。例如，您可能运行了开发或测试实例而偶尔忘记将其关闭。可以创建当平均 CPU 利用率低于 10% 达 24 小时时触发的警报，同时告知其为空闲并不再使用。可以根据需要调整阈值、时长和时间段，还可以添加 Amazon Simple Notification Service (Amazon SNS) 通知，以便您在触发警报后能够收到电子邮件。

Amazon CloudWatch 警报操作可以停止由 EBS 支持的 Amazon EC2 实例，但无法停止由实例存储支持的 Amazon EC2 实例。但是，Amazon CloudWatch 警报操作可以终止这两种类型的 Amazon EC2 实例。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- ec2:DescribeInstanceStatus 和 ec2:DescribeInstances，针对有关 Amazon EC2 实例状态指标的所有警报。
- ec2:StopInstances，针对包含停止操作的警报。
- ec2:TerminateInstances，针对包含终止操作的警报。
- ec2:DescribeInstanceRecoveryAttribute 和 ec2:RecoverInstances，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 IAM 用户指南中的[权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

要创建停止空闲实例的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 中的 EC2 Metrics (EC2 指标) 下面，选择 Per-Instance Metrics (每个实例的指标)。
5. 在指标列表中，选择您要为其创建警报的实例和指标。还可以在搜索框中输入一个实例 ID 以便找到所需的实例。
6. 从 Statistic 下拉列表中选择 Average。

7. 从 Period (周期) 下拉列表中选择一个周期，例如：1。
8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，为警报输入唯一名称，例如：**stop EC2 instance**。
9. 在 Description (说明) 字段中输入警报描述，例如：**CPU EC2**
10. 在 is 下拉列表中选择 <。
11. 在 is (条件) 下拉列表旁的框内，输入 10 并在 for (时间) 字段内输入 1440。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，单击 EC2 Action (EC2 操作)。
13. 在 Whenever this alarm (每当此警报) 下拉列表中，选择 State is ALARM (状态为“警报”)。
14. 在 Take this action (请执行以下操作) 下拉列表中，选择 Stop this instance (停止此实例)。
15. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。
16. 单击 Notification (通知)，然后在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新的主题。
17. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。

在 Send notification to (发送通知到) 字段中，输入新 Amazon SNS 主题的名称，例如：**Stop_EC2_Instance**，在 Email list (电子邮件列表) 字段中，输入警报变为 ALARM 状态时要通知的电子邮件地址列表 (逗号分隔)。



Important

如果创建新主题或向现有主题添加电子邮件地址，则每个电子邮件地址会收到一封主题订阅确认电子邮件。必须点击其中包含的链接对订阅进行确认，方可让新的电子邮件地址接收通知。

18. 在导航窗格中，单击 Create Alarm (创建警报) 以完成警报创建过程。

向 Amazon CloudWatch 警报添加终止操作

您可使用 Amazon EC2 控制台、Amazon CloudWatch 控制台、Amazon CloudWatch 命令行界面 (CLI)、CloudWatch API 或 AWS 软件开发工具包配置终止警报操作。有关结合使用 Amazon CloudWatch API 和 AWS 开发工具包的信息，请参阅[示例代码和库](#)。

使用 Amazon EC2 控制台创建终止实例的警报

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[实例启用终止保护](#)。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- **ec2:DescribeInstanceStatus** 和 **ec2:DescribeInstances**，针对有关 Amazon EC2 实例状态指标的所有警报。
- **ec2:StopInstances**，针对包含停止操作的警报。
- **ec2:TerminateInstances**，针对包含终止操作的警报。
- **ec2:DescribeInstanceRecoveryAttribute** 和 **ec2:RecoverInstances**，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南中的权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

要创建终止空闲实例的警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中的 INSTANCES 下，单击 Instances。
4. 在上方窗格中，右键单击一个实例，选择 CloudWatch Monitoring (CloudWatch 监控)，然后单击 Add/Edit Alarms (添加/编辑警报)。

或者选择实例，然后在下方窗格中的“Monitoring”选项卡上单击“Create Alarm”。

5. 在 Alarm Details for (以下项的警报详细信息) 对话框中，单击 Create Alarm (创建警报)。
6. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for (针对以下项创建警报) 对话框中的 Send a notification to (发送通知到) 框中选择一个现有 Amazon SNS 主题，或单击 Create Topic (创建主题) 创建新的主题。

如果创建新的主题，则请在“Send a notification to”方框中输入主题的名称，然后在“With these recipients”方框中输入收件人的电子邮件地址（以逗号隔开）。之后，待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可获得该主题的电子邮件。

7. 选中 Take the action 复选框，然后选择 Terminate this instance 单选按钮。
8. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。
9. 在“Whenever”方框中，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”和“CPU Utilization”。
10. 在“Is”方框中，定义指标的阈值。在此示例中，输入 10%。
11. 在“For at least”方框中，选择警报的采样周期。在此示例中，输入 24 个连续 1 小时时时间段。
12. 要更改警报的名称，在“Name this alarm”方框中，输入新的名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。



Note

可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

13. 单击 Create Alarm (创建警报)。

使用 Amazon CloudWatch 控制台创建终止空闲实例的警报

在对 Amazon EC2 实例禁用终止保护后，可以创建当达到一定阈值时自动终止该实例的警报。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](#)。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- `ec2:DescribeInstanceStatus` 和 `ec2:DescribeInstances`，针对有关 Amazon EC2 实例状态指标的所有警报。
- `ec2:StopInstances`，针对包含停止操作的警报。
- `ec2:TerminateInstances`，针对包含终止操作的警报。
- `ec2:DescribeInstanceRecoveryAttribute` 和 `ec2:RecoverInstances`，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南](#) 中的 [权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 `EC2ActionsAccess` 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

要创建终止空闲实例的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 中的 EC2 Metrics (EC2 指标) 下面，选择 Per-Instance Metrics (每个实例的指标)。
5. 在指标列表中，选择您要为其创建警报的实例和指标。还可以在搜索框中输入一个实例 ID 以便找到所需的实例。
6. 从 Statistic 下拉列表中选择 Average。
7. 从 Period (周期) 下拉列表中选择一个周期，例如：1。
8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，输入警报的唯一名称，例如：`Terminate EC2 instance`。
9. 例如在 Description (说明) 字段中，输入警报描述，例如：`CPU EC2`
10. 在 is 下拉列表中选择 <。
11. 在 is (条件) 下拉列表旁的框内，输入 10 并在 for (时间) 字段内输入 1440。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，单击 EC2 Action (EC2 操作)。
13. 在 Whenever this alarm (每当此警报) 下拉列表中，选择 State is ALARM (状态为“警报”)。
14. 在 Take this action (请执行以下操作) 下拉列表中，选择 Terminate this instance (终止此实例)。
15. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。

16. 单击 Notification (通知) , 然后在 Send notification to (发送通知到) 下拉列表中 , 选择一个现有 Amazon SNS 主题或创建一个新的主题。
17. 要创建新 Amazon SNS 主题 , 请选择 New list (新建列表)。

在 Send notification to (发送通知到) 字段中 , 输入新 Amazon SNS 主题的名称 , 例如 : Terminate_EC2_Instance , 在 Email list (电子邮件列表) 字段中 , 输入警报变为 ALARM 状态时要通知的电子邮件地址列表 (逗号分隔)。



Important

如果创建新主题或向现有主题添加电子邮件地址 , 则每个电子邮件地址会收到一封主题订阅确认电子邮件。必须点击其中包含的链接对订阅进行确认 , 方可让新的电子邮件地址接收通知。

18. 在导航窗格中 , 单击 Create Alarm (创建警报) 以完成警报创建过程。

向 Amazon CloudWatch 警报添加重启操作

您可使用 Amazon EC2 控制台、Amazon CloudWatch 控制台、Amazon CloudWatch 命令行界面 (CLI)、CloudWatch API 或 AWS 软件开发工具包配置重启警报操作。有关结合使用 Amazon CloudWatch API 和 AWS 开发工具包的信息 , 请参阅 [示例代码和库](#)。

使用 Amazon EC2 控制台创建重启实例的警报

您可创建监控 Amazon EC2 实例并自动重启此实例的 Amazon CloudWatch 警报。在实例运行状况检查失败时 , 推荐重启警报操作 (与恢复警报操作相反 , 该操作适合系统运行状况检查失败的情况)。实例重启相当于操作系统重启。在许多情况下 , 只需要几分钟时间即可重启您的实例。重启实例时 , 其仍驻留在相同的物理主机上 , 因此您的实例将保留其公有 DNS 名称、私有 IP 地址及其实例存储卷上的任何数据。

重启实例不会启动新的实例计费时间 , 这与停止并重新启动您的实例不同。有关重启实例的更多信息 , 请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [重启您的实例](#)。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报 , 则必须拥有以下 Amazon EC2 权限 :

- ec2:DescribeInstanceStatus 和 ec2:DescribeInstances , 针对有关 Amazon EC2 实例状态指标的所有警报。
- ec2:StopInstances , 针对包含停止操作的警报。
- ec2:TerminateInstances , 针对包含终止操作的警报。
- ec2:DescribeInstanceRecoveryAttribute 和 ec2:RecoverInstances , 针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限 , 则仍然可以创建警报 , 但无法对 Amazon EC2 实例执行停止或终止操作。但是 , 如果您之后获得使用相关 Amazon EC2 API 的权限 , 将会执行之前创建的警报操作。有关 IAM 权限的更多信息 , 请参阅 [IAM 用户指南](#) 中的 [权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例 , 则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色 , 则无法停止、终止或重启实例。但是 , 您仍然可以查看警报状态和执行任何其他操作 , 如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

创建重启实例的警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中的 INSTANCES 下，单击 Instances。
4. 在上方窗格中，右键单击一个实例，选择 CloudWatch Monitoring (CloudWatch 监控)，然后单击 Add/Edit Alarms (添加/编辑警报)。

或者选择实例，然后在下方窗格中的“Monitoring”选项卡上单击“Create Alarm”。

5. 在 Alarm Details for (以下项的警报详细信息) 对话框中，单击 Create Alarm (创建警报)。
6. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for (针对以下项创建警报) 对话框中的 Send a notification to (发送通知到) 框中选择一个现有 Amazon SNS 主题，或单击 Create Topic (创建主题) 创建新的主题。

如果创建新的主题，则请在“Send a notification to”方框中输入主题的名称，然后在“With these recipients”方框中输入收件人的电子邮件地址（以逗号隔开）。之后，待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可获得该主题的电子邮件。

7. 选中 Take the action 复选框，然后选择 Reboot this instance 单选按钮。
8. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。
9. 在 Whenever 框中，选择“Status Check Failed (Instance)”。
10. 在 For at least 字段中，输入 2。
11. 在 consecutive period(s) of 框中，选择 1 minute。
12. 要更改警报的名称，可在 Name of alarm 框中键入新名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。

13. 单击 Create Alarm (创建警报)。

使用 Amazon CloudWatch 控制台创建重启实例的警报

您可创建监控 Amazon EC2 实例并自动重启此实例的 Amazon CloudWatch 警报。在实例运行状况检查失败时，推荐重启警报操作（与恢复警报操作相反，该操作适合系统运行状况检查失败的情况）。实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。重启实例时，其仍驻留在相同的物理主机上，因此您的实例将保留其公有 DNS 名称、私有 IP 地址及其实例存储卷上的任何数据。

重启实例不会启动新的实例计费时间，这与停止并重新启动您的实例不同。有关重启实例的更多信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [重启您的实例](#)。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- ec2:DescribeInstanceStatus 和 ec2:DescribeInstances，针对有关 Amazon EC2 实例状态指标的所有警报。
- ec2:StopInstances，针对包含停止操作的警报。
- ec2:TerminateInstances，针对包含终止操作的警报。
- ec2:DescribeInstanceRecoveryAttribute 和 ec2:RecoverInstances，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南中的权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

创建重启实例的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 中的 EC2 Metrics (EC2 指标) 下面，选择 Per-Instance Metrics (每个实例的指标)。
5. 在指标列表中，选择您要为其创建警报的实例和 StatusCheckFailed_Instance 指标。还可以在搜索框中输入一个实例 ID 以便找到所需的实例。
6. 从 Statistic 下拉列表中选择 Minimum (最小值)。



Note

这是当前唯一支持的统计数据。

7. 从 Period (周期) 下拉列表中选择一个周期，例如：1 Minute。
8. 单击 Next，然后在 Alarm Threshold 下的 Name 字段中，为警报输入唯一名称，例如：Reboot EC2 instance。
9. 在 Description 字段中，输入警报的描述，例如：Reboot EC2 instance when health checks fail。
10. 在 is 下拉列表中选择 >。
11. 在 is (条件) 下拉列表旁的框内，输入 0 并在 for (时间) 字段内输入 2。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，单击 EC2 Action (EC2 操作)。
13. 在 Whenever this alarm (每当此警报) 下拉列表中，选择 State is ALARM (状态为“警报”)。
14. 在 Take this action 下拉列表中，选择 Reboot this instance。
15. 单击 Notification (通知)，然后在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新的主题。
16. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。

在 Send notification to 字段中，为新的 Amazon SNS 主题输入名称，例如：Reboot_EC2_Instance，并在 Email list 字段中，输入警报变为 ALARM 状态时要通知的电子邮件地址的列表（以逗号分隔）。



Important

如果创建新主题或向现有主题添加电子邮件地址，则每个电子邮件地址会收到一封主题订阅确认电子邮件。必须点击其中包含的链接对订阅进行确认，方可让新的电子邮件地址接收通知。

17. 在导航窗格中，单击 Create Alarm (创建警报) 以完成警报创建过程。

向 Amazon CloudWatch 警报添加恢复操作

您可使用 Amazon EC2 控制台、Amazon CloudWatch 控制台、Amazon CloudWatch 命令行界面 (CLI)、CloudWatch API 或 AWS 软件开发工具包配置恢复警报操作。有关结合使用 Amazon CloudWatch API 和 AWS 开发工具包的信息，请参阅[示例代码和库](#)。

使用 Amazon EC2 控制台创建警报以恢复实例

您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。

当 StatusCheckFailed_System 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您会注意到，实例在已恢复的实例上重启。

导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题



Important

恢复操作仅受到以下项支持：

- C3、C4、M3、M4、R3、T2 和 X1 实例类型。
- VPC 中的实例。不支持专用实例或在专用主机上运行的实例。



Note

如果您的实例有公有 IP 地址，它会在恢复后保留相同的公有 IP 地址。

- 使用 EBS 支持的存储的实例。不支持实例存储。如果连接了任何实例存储，则实例的自动恢复会失败。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- ec2:DescribeInstanceStatus 和 ec2:DescribeInstances，针对有关 Amazon EC2 实例状态指标的所有警报。
- ec2:StopInstances，针对包含停止操作的警报。
- ec2:TerminateInstances，针对包含终止操作的警报。
- ec2:DescribeInstanceRecoveryAttribute 和 ec2:RecoverInstances，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南中的权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

创建用于恢复实例的警报

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中的 INSTANCES 下，单击 Instances。
4. 在上方窗格中，右键单击一个实例，选择 CloudWatch Monitoring (CloudWatch 监控)，然后单击 Add/Edit Alarms (添加/编辑警报)。

或者选择实例，然后在下方窗格中的“Monitoring”选项卡上单击“Create Alarm”。

5. 在 Alarm Details for (以下项的警报详细信息) 对话框中，单击 Create Alarm (创建警报)。
6. 如果您要在触发警报时接收电子邮件，请在 Create Alarm for (针对以下项创建警报) 对话框中的 Send a notification to (发送通知到) 框中选择一个现有 Amazon SNS 主题，或单击 Create Topic (创建主题) 创建新的主题。

如果创建新的主题，则请在“Send a notification to”方框中输入主题的名称，然后在“With these recipients”方框中输入收件人的电子邮件地址（以逗号隔开）。之后，待警报创建完成，您将收到一封订阅确认电子邮件，而您必须接受方可获得该主题的电子邮件。

7. 选中 Take the action 复选框，然后选择 Recover this instance 单选按钮。
8. 如果出现提示，请选中 Create IAM role: EC2ActionsAccess 复选框以自动创建 IAM 角色，以便 AWS 可在此警报触发时自动代表您停止实例。
9. 在 Whenever 框中，选择“Status Check Failed (System)”。
10. 在 For at least 字段中，输入 2。
11. 在 consecutive period(s) of 框中，选择 1 minute。
12. 要更改警报的名称，可在 Name of alarm 框中键入新名称。

如果不输入警报名称，则 Amazon CloudWatch 会自动为您创建一个。

13. 单击 Create Alarm (创建警报)。

使用 Amazon CloudWatch 控制台创建警报以恢复实例

您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 AWS 参与才能修复的问题）时自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。

当 StatusCheckFailed_System 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您会注意到，实例在已恢复的实例上重启。

导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上的硬件问题



Important

恢复操作仅受到以下项支持：

- C3、C4、M3、M4、R3、T2 和 X1 实例类型。
- VPC 中的实例。不支持专用实例或在专用主机上运行的实例。



Note

如果您的实例有公有 IP 地址，它会在恢复后保留相同的公有 IP 地址。

- 使用 EBS 支持的存储的实例。不支持实例存储。如果连接了任何实例存储，则实例的自动恢复会失败。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- `ec2:DescribeInstanceStatus` 和 `ec2:DescribeInstances`，针对有关 Amazon EC2 实例状态指标的所有警报。
- `ec2:StopInstances`，针对包含停止操作的警报。
- `ec2:TerminateInstances`，针对包含终止操作的警报。
- `ec2:DescribeInstanceRecoveryAttribute` 和 `ec2:RecoverInstances`，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 IAM 用户指南中的[权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 `EC2ActionsAccess` 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

创建用于恢复实例的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。

3. 在导航窗格中，单击 Alarms (警报)。
4. 单击 Create Alarm (创建警报)，然后在 CloudWatch Metrics by Category (按类别显示的 CloudWatch 指标) 中的 EC2 Metrics (EC2 指标) 下面，选择 Per-Instance Metrics (每个实例的指标)。
5. 在指标列表中，选择您要为其创建警报的实例和 StatusCheckFailed_System 指标。还可以在搜索框中输入一个实例 ID 以便找到所需的实例。
6. 从 Statistic 下拉列表中选择 Minimum (最小值)。



Note

这是当前唯一支持的统计数据。

7. 从 Period (周期) 下拉列表中选择一个周期，例如：1 Minute。
8. 单击 Next (下一步)，然后在 Alarm Threshold (警报阈值) 下的 Name (名称) 字段中，为警报输入唯一名称，例如：Recover EC2 instance。
9. 在 Description (描述) 字段中，输入警报的描述，例如：Recover EC2 instance when health checks fail。
10. 在 is 下拉列表中选择 >。
11. 在 is (条件) 下拉列表旁的框内，输入 0 并在 for (时间) 字段内输入 2。

Alarm Preview (警报预览) 下会显示阈值的图形表示。

12. 在 Actions (操作) 下，单击 EC2 Action (EC2 操作)。
13. 在 Whenever this alarm (每当此警报) 下拉列表中，选择 State is ALARM (状态为“警报”)。
14. 在 Take this action (请执行以下操作) 下拉列表中，选择 Recover this instance (恢复此实例)。
15. 单击 Notification (通知)，然后在 Send notification to (发送通知到) 下拉列表中，选择一个现有 Amazon SNS 主题或创建一个新的主题。
16. 要创建新 Amazon SNS 主题，请选择 New list (新建列表)。

在 Send notification to (发送通知到) 字段中，输入新 Amazon SNS 主题的名称，例如：Recover_EC2_Instance，在 Email list (电子邮件列表) 字段中，输入警报变为 ALARM 状态时要通知的电子邮件地址列表（逗号分隔）。



Important

如果创建新主题或向现有主题添加电子邮件地址，则每个电子邮件地址会收到一封主题订阅确认电子邮件。必须点击其中包含的链接对订阅进行确认，方可让新的电子邮件地址接收通知。

17. 在导航窗格中，单击 Create Alarm (创建警报) 以完成警报创建过程。

使用 Amazon CloudWatch 控制台查看已触发的警报和操作的历史记录

可以在 Amazon CloudWatch 控制台中查看警报和操作历史记录。Amazon CloudWatch 会保留最近两周的警报和操作历史记录。

要查看已触发的警报和操作的历史记录

1. 通过以下网址打开 CloudWatch 控制台：<https://console.amazonaws.cn/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏，选择实例运行所在的区域。有关更多信息，请参阅 [Regions and Endpoints](#)。
3. 在导航窗格中，单击 Alarms (警报)。

4. 在上方窗格中，选择包含您想要查看的历史记录的警报。
5. 在下方窗格中，Details (详细信息) 选项卡显示最近的状态转换以及时间和指标值。
6. 单击 History (历史记录) 选项卡可以查看最近的历史记录条目。

使用 CLI 或 API 创建警报以停止、终止、重启或恢复实例

如果您使用的是 AWS CLI 或 Amazon CloudWatch API，或者您将 AWS 软件开发工具包与 API 结合使用，则可以使用 Amazon EC2 每个实例的指标创建 CloudWatch 警报，然后使用该操作的专用 Amazon 资源名称 (ARN) 添加操作。可以向任何警报状态添加操作，同时可以指定每项操作的区域。地区必须与您发送 put-metric-alarm 请求的地区匹配。

操作	ARN (包含区域)	ARN (与 IAM 角色一起使用)
<i>Stop</i>	arn:aws:automate:cn-north-1:ec2:stop	arn:aws:swf:us-east-1:{ <i>custom-account</i> }:action/actions/AWS_EC2.InstanceId.Stop/1.0  Note 您必须使用 Amazon EC2 或 CloudWatch 控制台创建至少一个停止警报，然后才能创建 EC2ActionsAccess IAM 角色。在创建此 IAM 角色后，您可使用 CLI 创建停止警报。
<i>Terminate</i>	arn:aws:automate:cn-north-1:ec2:terminate	arn:aws:swf:us-east-1:{ <i>custom-account</i> }:action/actions/AWS_EC2.InstanceId.Terminate/1.0  Note 您必须使用 Amazon EC2 或 CloudWatch 控制台创建至少一个终止警报，然后才能创建 EC2ActionsAccess IAM 角色。在创建此 IAM 角色后，您可使用 CLI 创建终止警报。

操作	ARN (包含区域)	ARN (与 IAM 角色一起使用)
Reboot	无	arn:aws:swf:us-east-1:{custom-er-account}:action/actions/AWS_EC2.InstanceId.Reboot/1.0  Note 您必须使用 Amazon EC2 或 CloudWatch 控制台创建至少一个重启警报，然后才能创建 EC2ActionsAccess IAM 角色。在创建此 IAM 角色后，您可使用 CLI 创建重启警报。
Recover	arn:aws:automate:cn-north-1:ec2:recover	无

有关结合使用 Amazon CloudWatch API 和 AWS 开发工具包的信息，请参阅[示例代码和库](#)。



Note

如果您要使用 AWS Identity and Access Management (IAM) 账户创建或修改警报，则必须拥有以下 Amazon EC2 权限：

- ec2:DescribeInstanceStatus 和 ec2:DescribeInstances，针对有关 Amazon EC2 实例状态指标的所有警报。
- ec2:StopInstances，针对包含停止操作的警报。
- ec2:TerminateInstances，针对包含终止操作的警报。
- ec2:DescribeInstanceRecoveryAttribute 和 ec2:RecoverInstances，针对包含恢复操作的警报。

如果您拥有对 Amazon CloudWatch 而不是 Amazon EC2 的读/写权限，则仍然可以创建警报，但无法对 Amazon EC2 实例执行停止或终止操作。但是，如果您之后获得使用相关 Amazon EC2 API 的权限，将会执行之前创建的警报操作。有关 IAM 权限的更多信息，请参阅 [IAM 用户指南中的权限与策略](#)。

如果您想要通过警报操作来使用 IAM 角色停止、终止或重启实例，则只能使用 EC2ActionsAccess 角色。其他 IAM 角色不受支持。如果您正在使用其他 IAM 角色，则无法停止、终止或重启实例。但是，您仍然可以查看警报状态和执行任何其他操作，如 Amazon SNS 通知或 Auto Scaling 策略。

如果您使用的是用 AWS Security Token Service (AWS STS) 授予的临时安全凭据，则无法使用警报操作来恢复 Amazon EC2 实例。

要使用 CLI 创建停止实例的警报

可以使用 arn:aws:automate:cn-north-1:ec2:stop ARN 停止 Amazon EC2 实例。以下示例说明当平均 CPU 使用率低于 10% 的时间超过 24 小时时如何停止实例。

- 在命令提示符处，输入：

```
% aws cloudwatch put-metric-alarm --alarm-name my-Alarm --alarm-description "Stop the instance when it is idle for a day" --namespace "AWS/EC2" --dimensions Name=InstanceId,Value="i-1234567890abcdef0" --statistic Average --metric-name CPUUtilization --comparison-operator LessThanThreshold --threshold 10 --period 21600 --evaluation-periods 4 --alarm-actions arn:aws:automate:cn-north-1:ec2:stop
```

要使用 CLI 创建终止实例的警报

- 在命令提示符处，输入：

```
% aws cloudwatch put-metric-alarm --alarm-name my-Alarm --alarm-description "Terminate the instance when it is idle for a day" --namespace "AWS/EC2" --dimensions Name=InstanceId,Value="i-1234567890abcdef0" --statistic Average --metric-name CPUUtilization --comparison-operator LessThanThreshold --threshold 1 --period 21600 --evaluation-periods 4 --alarm-actions arn:aws:automate:cn-north-1:ec2:terminate
```

使用 CLI 创建重启实例的警报

- 在命令提示符处，输入：

```
% aws cloudwatch put-metric-alarm --alarm-name my-Alarm --alarm-description "Reboot the instance" --namespace "AWS/EC2" --dimensions Name=InstanceId,Value="i-1234567890abcdef0" --statistic Minimum --metric-name StatusCheckFailed_Instance --comparison-operator GreaterThanThreshold --threshold 0 --period 60 --evaluation-periods 2 --alarm-actions arn:aws:swf:cn-north-1:{customer-account}:action/actions/AWS_EC2.InstanceId.Reboot/1.0
```

使用 CLI 创建恢复实例的警报



Note

无法恢复终止的实例。

- 在命令提示符处，输入：

```
% aws cloudwatch put-metric-alarm --alarm-name my-Alarm --alarm-description "Recover the instance" --namespace "AWS/EC2" --dimensions Name=InstanceId,Value="i-1234567890abcdef0" --statistic Average --metric-name StatusCheckFailed_System --comparison-operator GreaterThanThreshold --threshold 0 --period 60 --evaluation-periods 2 --alarm-actions arn:aws:automate:cn-north-1:ec2:recover
```

使用 API 创建停止实例的警报

下面的示例请求说明如何创建停止 Amazon EC2 实例的警报：

- ```
http://monitoring.amazonaws.com/
?SignatureVersion=2
&Action=PutMetricAlarm
&Version=2009-05-15
&Namespace=AWS/EC2
&MetricName=CPUUtilization
&Dimension.member.1.Name=instance-id
&Dimension.member.1.Value=i-1234567890abcdef0
&Period=21600
&Statistic=Average
&AlarmName=Stop-EC2-Instance
&ComparisonOperator=LessThanThreshold
&Threshold=10
&EvaluationPeriods=4
&StartTime=2009-01-16T00:00:00
&EndTime=2009-01-16T00:02:00
&Timestamp=2009-01-08-18
&AWSAccessKeyId=XXX YOUR ACCESS KEY XXX
&Signature=%XXX YOUR SIGNATURE XXX%3D
&AlarmActions.member.1=arn:aws:automate:cn-north-1:ec2:stop
```

## 使用 API 创建终止实例的警报

下面的示例演示如何创建终止 Amazon EC2 实例的警报：

- ```
http://monitoring.amazonaws.com/
?SignatureVersion=2
&Action=PutMetricAlarm
&Version=2009-05-15
&Namespace=AWS/EC2
&MetricName=CPUUtilization
```

```
&Dimension.member.1.Name=instance-id  
&Dimension.member.1.Value=i-1234567890abcdef0  
&Period=21600  
&Statistic=Average  
&AlarmName=Terminate-EC2-Instance  
&ComparisonOperator=LessThanThreshold  
&Threshold=10  
&EvaluationPeriods=4  
&StartTime=2009-01-16T00:00:00  
&EndTime=2009-01-16T00:02:00  
&Timestamp=2009-01-08-18  
&AWSAccessKeyId=XXX YOUR ACCESS KEY XXX  
&Signature=%XXX YOUR SIGNATURE XXX%3D  
&AlarmActions.member.1=arn:aws:automate:cn-north-1:ec2:terminate
```

使用 API 创建重启实例的警报

以下示例请求演示如何创建重启 Amazon EC2 实例的警报：

- ```
http://monitoring.amazonaws.com/
?SignatureVersion=2
&Action=PutMetricAlarm
&Version=2009-05-15
&Namespace=AWS/EC2
&MetricName>StatusCheckFailed_Instance
&Dimension.member.1.Name=instance-id
&Dimension.member.1.Value=i-1234567890abcdef0
&Period=60
&Statistic=Average
&AlarmName=Reboot-EC2-Instance
```

```
&ComparisonOperator=GreaterThanThreshold
&Threshold=0
&EvaluationPeriods=2
&StartTime=2009-01-16T00:00:00
&EndTime=2009-01-16T00:02:00
&Timestamp=2009-01-08-18
&AWSAccessKeyId=XXX YOUR ACCESS KEY XXX
&Signature=%XXX YOUR SIGNATURE XXX%3D
&AlarmActions.member.1=arn:aws:aws:swf:cn-north-1:{customer-account} :ac
tion/actions/AWS_EC2.InstanceId.Reboot/1.0
```

## 使用 API 创建恢复实例的警报

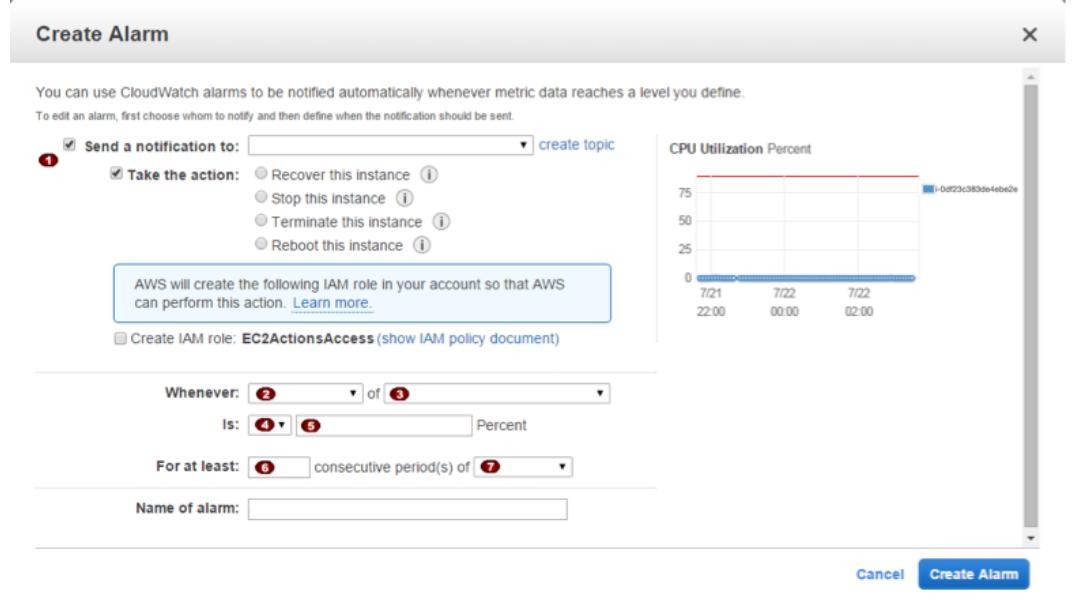
下面的示例演示如何创建恢复 Amazon EC2 实例的警报：

- `http://monitoring.amazonaws.com/  
?SignatureVersion=2  
&Action=PutMetricAlarm  
&Version=2009-05-15  
&Namespace=AWS/EC2  
&MetricName>StatusCheckFailed_System  
&Dimension.member.1.Name=instance-id  
&Dimension.member.1.Value=i-1234567890abcdef0  
&Period=60  
&Statistic=Average  
&AlarmName=Terminate-EC2-Instance  
&ComparisonOperator=GreaterThanThreshold  
&Threshold=0  
&EvaluationPeriods=2  
&StartTime=2009-01-16T00:00:00  
&EndTime=2009-01-16T00:02:00`

```
&Timestamp=2009-01-08-18
&AWSAccessKeyId=XXX YOUR ACCESS KEY XXX
&Signature=%XXX YOUR SIGNATURE XXX%3D
&AlarmActions.member.1=arn:aws:automate:cn-north-1:ec2:recover
```

## Amazon CloudWatch 警报操作场景

可以使用 Amazon Elastic Compute Cloud (Amazon EC2) 控制台创建当满足一定条件时停止或终止 Amazon EC2 实例的警报操作。在下方的控制台页面屏幕截图中，您设置了警报操作，我们对设置进行了编号。我们还对后续场景中的设置进行了编号，帮助您创建合适的操作。



### 场景 1：停止空闲开发与测试实例

创建当用于软件开发或测试的实例空闲达到至少 1 小时时停止该实例的警报。

| 设置                                  | 值    |
|-------------------------------------|------|
| <input checked="" type="checkbox"/> | Stop |

| 设置                                  | 值          |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | 最大值        |
| <input checked="" type="checkbox"/> | CPU 利用率    |
| <input checked="" type="checkbox"/> | <=         |
| <input checked="" type="checkbox"/> | 10%        |
| <input checked="" type="checkbox"/> | 60 minutes |
| <input checked="" type="checkbox"/> | 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              |
|-------------------------------------|----------------|
| <input checked="" type="checkbox"/> | Stop and email |
| <input checked="" type="checkbox"/> | 平均值            |
| <input checked="" type="checkbox"/> | CPU 利用率        |
| <input checked="" type="checkbox"/> | <=             |
| <input checked="" type="checkbox"/> | 5%             |
| <input checked="" type="checkbox"/> | 60 minutes     |
| <input checked="" type="checkbox"/> | 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          |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | 电子邮件       |
| <input checked="" type="checkbox"/> | 总计         |
| <input checked="" type="checkbox"/> | NetworkOut |
| <input checked="" type="checkbox"/> | >          |
| <input checked="" type="checkbox"/> | 10GB       |
| <input checked="" type="checkbox"/> | 1 天        |
| <input checked="" type="checkbox"/> | 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                 |
|-------------------------------------|-------------------|
| <input checked="" type="checkbox"/> | Stop and send SMS |
| <input checked="" type="checkbox"/> | 总计                |
| <input checked="" type="checkbox"/> | NetworkOut        |
| <input checked="" type="checkbox"/> | >                 |
| <input checked="" type="checkbox"/> | 1GB               |
| <input checked="" type="checkbox"/> | 1 小时              |
| <input checked="" type="checkbox"/> | 1                 |

#### 场景 5：停止出现内存泄漏的实例

创建当内存利用率达到或超过 90% 时停止实例的警报，让应用程序日志可以被检索用于故障排除。



Note

MemoryUtilization 指标是一种自定义指标。要使用 MemoryUtilization 指标，您必须为 Linux 实例安装 Perl 脚本。有关更多信息，请参阅[为 Amazon EC2 Linux 实例监控内存和磁盘指标](#)。

| 设置                                  | 值                 |
|-------------------------------------|-------------------|
| <input checked="" type="checkbox"/> | Stop              |
| <input checked="" type="checkbox"/> | 最大值               |
| <input checked="" type="checkbox"/> | MemoryUtilization |
| <input checked="" type="checkbox"/> | $\geq$            |
| <input checked="" type="checkbox"/> | 90%               |
| <input checked="" type="checkbox"/> | 1 minute          |
| <input checked="" type="checkbox"/> | 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                        |
|-------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | Stop                     |
| <input checked="" type="checkbox"/> | 平均值                      |
| <input checked="" type="checkbox"/> | StatusCheckFailed_System |
| <input checked="" type="checkbox"/> | $\geq$                   |
| <input checked="" type="checkbox"/> | 1                        |
| <input checked="" type="checkbox"/> | 15 分钟                    |
| <input checked="" type="checkbox"/> | 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            |
|-------------------------------------|--------------|
| <input checked="" type="checkbox"/> | Terminate    |
| <input checked="" type="checkbox"/> | Maximum      |
| <input checked="" type="checkbox"/> | 网络输出         |
| <input checked="" type="checkbox"/> | <=           |
| <input checked="" type="checkbox"/> | 100000 bytes |
| <input checked="" type="checkbox"/> | 5 minutes    |
| <input checked="" type="checkbox"/> | 1            |

还可以使用 Amazon CloudWatch 控制台执行上述场景。我们已对控制台上的设置进行编号，以将 Amazon EC2 控制台中已编号的设置与上面提到的场景相对应，以便您进行比较，并按照适当操作创建警报。

**Create Alarm**

**1. Select Metric** **2. Define Alarm**

Description:

Whenever: CPUUtilization  
is:  4  5  
for:  7 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

EC2 Action Delete

Whenever this alarm: State is ALARM

① Take this action:  Recover this instance i  
 Stop this instance i  
 Terminate this instance i  
 Reboot this instance i

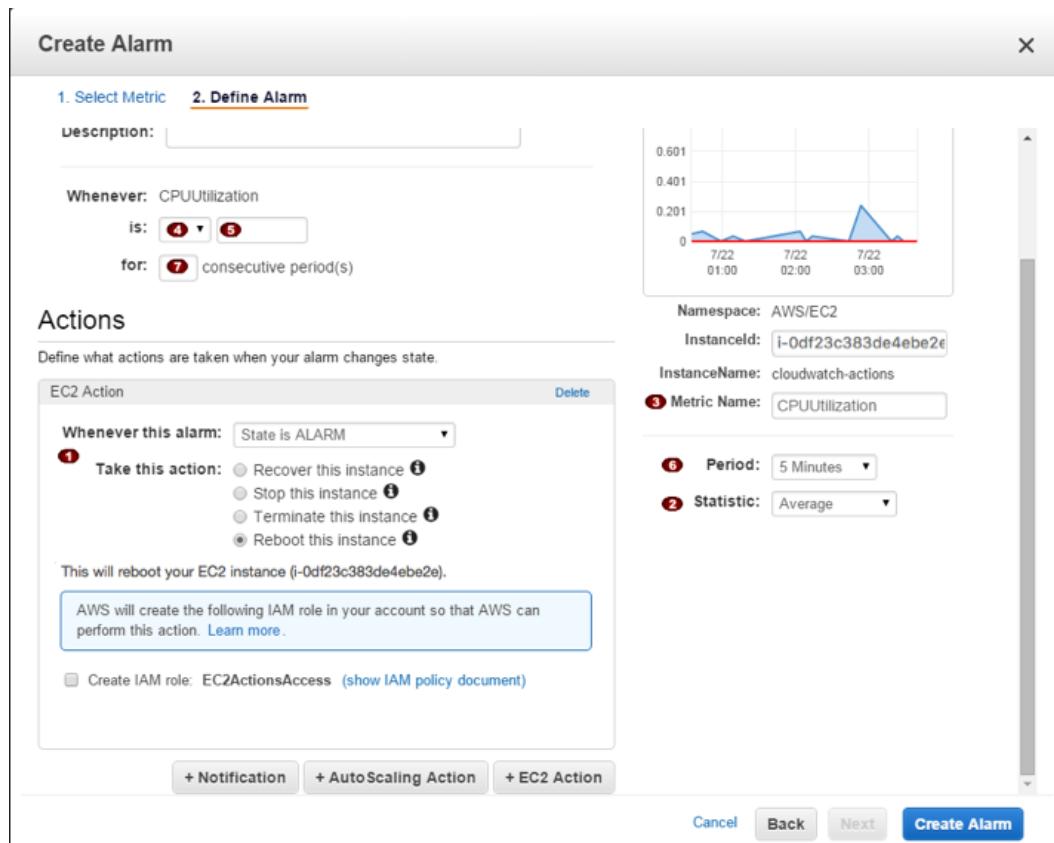
This will reboot your EC2 instance (i-0df23c383de4ebe2e).

AWS will create the following IAM role in your account so that AWS can perform this action. [Learn more](#).

Create IAM role: EC2ActionsAccess ([show IAM policy document](#))

**Cancel** **Back** **Next** **Create Alarm**

Namespace: AWS/EC2  
InstanceId: i-0df23c383de4ebe2e  
InstanceName: cloudwatch-actions  
③ Metric Name: CPUUtilization  
④ Period: 5 Minutes  
⑤ Statistic: Average



# 网络与安全性

---

## Abstract

了解 Amazon EC2 的网络和安全功能。

Amazon EC2 提供以下网络和安全功能。

### 特色

- [Amazon EC2 密钥对和 Windows 实例 \(p. 510\)](#)
- [Amazon EC2 个安全组 \(对于 Windows 实例\) \(p. 515\)](#)
- [控制对 Amazon EC2 资源的访问 \(p. 522\)](#)
- [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 572\)](#)
- [Amazon EC2 实例 IP 寻址 \(p. 597\)](#)
- [弹性 IP 地址 \(p. 606\)](#)
- [弹性网络接口 \(ENI\) \(p. 612\)](#)
- [置放群组 \(p. 624\)](#)
- [EC2 实例的网络最大传输单位 \(MTU\) \(p. 627\)](#)
- [Windows 上的增强联网 \(p. 630\)](#)

如果您使用命令行工具或 API 访问 Amazon EC2，则需要访问密钥 ID 和秘密访问密钥。有关更多信息，请参阅[如何获取安全证书？\(在 Amazon Web Services General Reference 中\)](#)。

您可以在以下两个平台之一中启动实例：EC2-Classic 或 EC2-VPC。在 EC2-Classic 或默认 VPC 中启动的实例自动分配有一个公有 IP 地址。在非默认 VPC 中启动的实例可在启动时分配有一个公有 IP 地址。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 577\)](#)。

实例可能会因为您不可控的原因失败或终止。如果一个实例失败了，您又启动了一个替代实例，则该替代实例的公有 IP 地址与原有实例不同。但是，如果您的应用程序需要一个静态 IP 地址，您可以使用[弹性 IP 地址](#)。

您可以使用安全组来控制您的实例的访问权限。这些安全组类似于一个传入网络防火墙，使您可以指定允许访问您的实例的协议、端口和源 IP 范围。您可以创建多个安全组，并给每个安全组指定不同的规则。然后您可以给每个实例分配一个或多个安全组，我们将按照这些规则确定允许哪些流量可访问实例。您可以配置一个安全组，以便只有特定的 IP 地址或特定的安全组可以访问实例。

# Amazon EC2 密钥对和 Windows 实例

## Abstract

使用公有密钥密码对为 Amazon EC2 实例加密和解密登录信息。

Amazon EC2 使用公有密钥密码术加密和解密登录信息。公有密钥密码术使用公有密钥加密某个数据（如一个密码），然后收件人可以使用私有密钥解密数据。公有和私有密钥被称为密钥对。

要登录您的实例，您必须创建一个密钥对，并在启动实例时指定密钥对的名称，然后使用私有密钥连接实例。对于 Windows 实例，您可以使用密钥对获得管理员密码，然后使用 RDP 登录实例。有关密钥对和 Linux 实例的更多信息，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的 [Amazon EC2 密钥对](#)。

### 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 \(p. 510\)](#)。

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 [将您自己的密钥对导入 Amazon EC2 \(p. 512\)](#)。

每个密钥对需要一个名称。切记选择一个容易记住的名称。Amazon EC2 会将公有密钥与您指定的密钥名称相关联。

Amazon EC2 只会存储公有密钥，您需要存储私有密钥。拥有您的私有密钥的任何人都可以解密您的登录信息，因此将您的私有密钥保存在一个安全的位置非常重要。

Amazon EC2 使用的密钥是 2048-bit SSH-2 RSA 密钥。对于每个区域，您可以拥有多达 5000 个密钥对。

### 启动并连接到您的实例

当您启动实例时，您应该指定计划用于连接到该实例的密钥对的名称。如果在启动实例时未指定现有密钥对的名称，您将无法连接到该实例。连接到实例时，您必须指定与启动该实例时指定的密钥对相对应的私有密钥。



### Note

#### 内容

- [使用 Amazon EC2 创建密钥对 \(p. 510\)](#)
- [将您自己的密钥对导入 Amazon EC2 \(p. 512\)](#)
- [在 Windows 上检索密钥对的公有密钥 \(p. 514\)](#)
- [验证您的密钥对指纹 \(p. 514\)](#)
- [删除您的密钥对 \(p. 514\)](#)

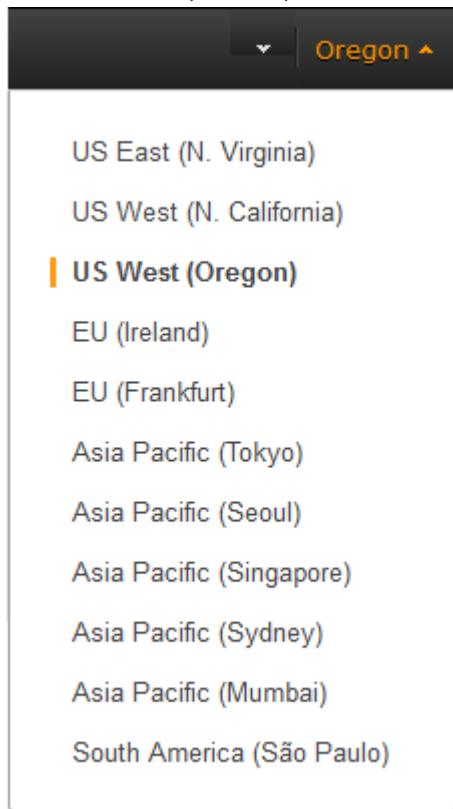
## 使用 Amazon EC2 创建密钥对

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。

### 使用控制台创建密钥对

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

- 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。这一项选择十分重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，而密钥对却不可以。例如，如果您在美国西部（俄勒冈）区域中创建密钥对，则无法在其他区域看到或使用该密钥对。



- 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；单击箭头扩展窗格。

- 选择 Create Key Pair。
- 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。
- 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。

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

## 将您自己的密钥对导入 Amazon EC2

正如前一部分所述，如果您使用 Amazon EC2 创建密钥对，则需要准备启动实例。如果不使用 Amazon EC2 创建密钥对，您可以使用第三方工具创建一个 RSA 密钥对，然后将公有密钥导入 Amazon EC2。举例来说，您可以使用 ssh-keygen（通过标准 OpenSSH 安装提供的工具）创建密钥对。或者，您可能使用 Java、Ruby、Python 和许多其他提供标准库的编程语言来创建 RSA 密钥对。

Amazon EC2 接受以下格式：

- OpenSSH 公有密钥格式
- Base64 编码的 DER 格式
- 如在[RFC4716](#)指定的 SSH 公有密钥文件格式

Amazon EC2 不接受 DSA 密钥。请确保您的密钥生成器被设置为创建 RSA 密钥。

支持的长度：1024、2048 和 4096。

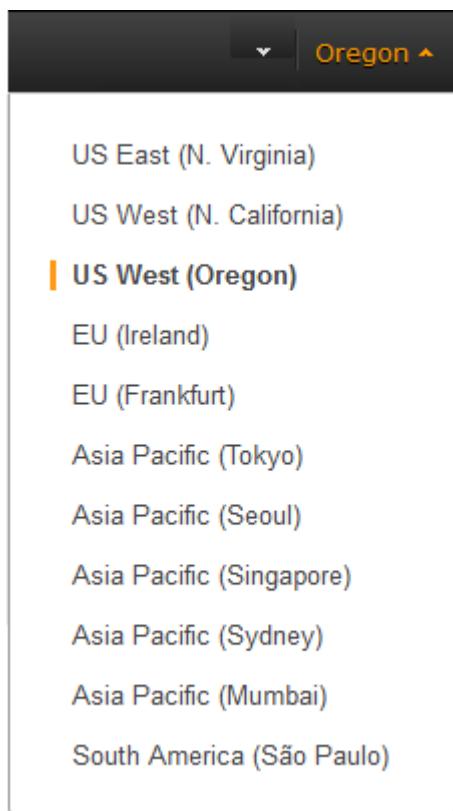
### 要使用第三方工具创建密钥对

1. 使用您选择的第三方工具生成密钥对。
2. 将公有密钥保存至本地文件。例如，`C:\keys\my-key-pair.pub`。此文件的文件扩展名并不重要。
3. 将私有密钥保存到扩展名为 `.pem` 的不同本地文件中。例如，`C:\keys\my-key-pair.pem`。将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

使用 Amazon EC2 控制台通过以下步骤导入密钥对。

### 导入公有密钥

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中，选择密钥对区域。这项选择非常重要，因为密钥对资源不能在区域之间共享。例如，如果将密钥对导入 美国西部（俄勒冈）区域，则不能在另一区域看到或使用该密钥对。



3. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
4. 选择 Import Key Pair。
5. 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 \(p. 3\)](#)。

- [import-key-pair \(AWS CLI\)](#)
- [Import-EC2KeyPair \(适用于 Windows PowerShell 的 AWS 工具\)](#)

在成功导入公有密钥文件后，您可以按照以下说明使用 Amazon EC2 控制台验证密钥对是否成功导入。

#### 验证密钥对是否已导入

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中，选择您在其中创建密钥对的区域。
3. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。
4. 验证您导入的密钥对是否在密钥对的显示列表中。

#### 使用命令行查看密钥对

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

- [describe-key-pairs \(AWS CLI\)](#)

- [Get-EC2KeyPair](#) (适用于 Windows PowerShell 的 AWS 工具)

## 在 Windows 上检索密钥对的公有密钥

在 Windows 上，您可以使用 PuTTYgen 获取密钥对的公有密钥。启动 PuTTYgen，单击 Load (加载)，然后选择 .ppk 或 .pem 文件。PuTTYgen 会显示公有密钥。

您在启动实例时指定的公有密钥也可以通过实例元数据使用。要查看您在启动实例时指定的公有密钥，请从您的实例中使用以下命令：

```
C:\> GET http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ITxCi+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItnckij7FbtXJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

有关更多信息，请参阅 [检索实例元数据 \(p. 239\)](#)。

## 验证您的密钥对指纹

在 Amazon EC2 控制台的 Key Pairs (密钥对) 页面上，Fingerprint (指纹) 列显示从您的密钥对生成的指纹。AWS 根据密钥对是由 AWS 还是第三方工具生成以不同方式计算指纹。如果您是使用 AWS 创建的密钥对，则会使用 SHA-1 哈希函数计算指纹。如果您使用第三方工具创建了密钥对并将公有密钥上传到 AWS，或者如果您从一个现有的 AWS 创建的私有密钥生成了一个新的公有密钥并将其上传到 AWS，则会使用 MD5 哈希函数计算指纹。

您可以使用 Key Pairs (密钥对) 页面上显示的指纹验证您本地计算机上的私有密钥是否与 AWS 中存储的公有密钥匹配。

如果您使用 AWS 创建了密钥对，那么您可以使用 OpenSSL 工具从私有密钥文件生成指纹：

```
C:\> openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -
nocrypt | openssl sha1 -c
```

如果您使用第三方工具创建了密钥对并将公有密钥上传到 AWS，则可以使用 OpenSSL 工具从您本地计算机上的私有密钥文件生成指纹。

```
C:\> openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

输出应与控制台中显示的指纹匹配。

## 删除您的密钥对

当您删除密钥对时，仅删除 Amazon EC2 的公有密钥副本。删除密钥对不影响您计算机上的私有密钥或是已使用该密钥对启动的任何实例上的公有密钥。您不能使用已删除的密钥对启动新实例，不过，只要您仍然有私有密钥 (.pem) 文件，就可以继续连接到使用已删除的密钥对启动的任何实例。



### Note

如果您使用的是 Auto Scaling 组（例如，在 Elastic Beanstalk 环境中），请确保您要删除的密钥对未在启动配置中指定。Auto Scaling 检测到运行不正常的实例时会启动替代实例；但是，如果找不到密钥对，实例将启动失败。

您可以使用 Amazon EC2 控制台或命令行删除密钥对。

#### 使用控制台删除密钥对

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## Amazon EC2 安全组（对于 Windows 实例）

### Abstract

使用安全组和安全组规则作为防火墙对一个或多个 EC2 实例控制流量。

安全组 起着虚拟防火墙的作用，可控制一个或多个实例的流量。在您启动实例时，将一个或多个安全组与该实例相关联。为每个安全组添加规则，规定流入或流出其关联实例的流量。您可以随时修改安全组的规则；新规则会自动应用于与该安全组相关联的所有实例。在决定是否允许流量到达实例时，我们会评估与实例相关联的所有安全组中的所有规则。

如果需要允许流量进入 Linux 实例，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [适用于 Linux 实例的 Amazon EC2 安全组](#)。

#### 主题

- [EC2-Classic 安全组 \(p. 515\)](#)
- [EC2-VPC 安全组 \(p. 516\)](#)
- [安全组规则 \(p. 516\)](#)
- [默认安全组 \(p. 518\)](#)
- [自定义安全组 \(p. 518\)](#)
- [正在创建安全组 \(p. 519\)](#)
- [描述您的安全组 \(p. 520\)](#)
- [向安全组添加规则 \(p. 520\)](#)
- [从安全组中删除规则 \(p. 521\)](#)
- [正在删除安全组 \(p. 521\)](#)
- [API 和命令概览 \(p. 521\)](#)

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。

## EC2-Classic 安全组

如果要使用 EC2-Classic，则必须使用为 EC2-Classic 专门创建的安全组。当您在 EC2-Classic 中启动实例时，您必须在实例所在的相同区域指定一个安全组。在 EC2-Classic 中启动实例时，您无法指定为 VPC 创建的安全组。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。但是，您可以向安全组添加或从中删除规则，并且这些更改会自动应用于与该安全组相关联的所有实例。



#### Note

在 EC2-Classic 中，您可将一个实例与最多 500 个安全组相关联，可向一个安全组添加最多 100 条规则。

## EC2-VPC 安全组

如果您正在使用 EC2-VPC，则必须使用专为 VPC 创建的安全组。在 VPC 中启动实例时，您必须为该 VPC 指定一个安全组。在 VPC 中启动实例时，您无法指定为 EC2-Classic 创建的安全组。

在 VPC 中启动实例后，您可以更改其安全组。安全组与网络接口关联。更改实例的安全组也会更改与主网络接口 (eth0) 关联的安全组。想要了解更多信息，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 [更改弹性网络接口的安全组 \(p. 621\)](#)。

您可以更改安全组的规则，并且这些更改会自动应用于与该安全组相关联的所有实例。



#### Note

在 EC2-VPC 中，您可将一个网络接口与最多 5 个安全组相关联，可向一个安全组添加最多 50 条规则。

在您将非默认 VPC 安全组指定到 CLI 或 API 操作时，必须使用安全组 ID 而非安全组名称来识别安全组。

EC2-VPC 安全组具有 EC2-Classic 安全组不支持的额外功能。有关 EC2-VPC 安全组的更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [您的 VPC 的安全组](#) 和 [EC2-Classic 和 EC2-VPC 安全组之间的差异](#)。

## 安全组规则

安全组规则可控制允许到达与安全组相关联的实例的入站流量以及允许离开实例的出站流量。

以下是您的安全组规则的特征：

- 默认情况下，安全组允许所有出站流量。
- 安全组规则始终是宽松的；您无法创建拒绝访问的规则。
- 您可以随时添加和删除规则。您无法更改 EC2-Classic 的出站规则。如果您使用的是 Amazon EC2 控制台，则可修改现有规则并可将规则从现有安全组复制到新的安全组。
- 当添加或删除规则时，您的更改会在较短的一段时间后自动应用于与安全组相关联的实例，具体取决于流量的连接跟踪。有关更多信息，请参阅 [连接跟踪 \(p. 517\)](#)。
- 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 \(p. 517\)](#)。



#### Note

如果您的实例（主机 A）发起到主机 B 的流量并使用 TCP、UDP 或 ICMP 之外的协议，则实例的防火墙将仅跟踪 IP 地址和协议编号以便允许来自主机 B 的响应流量。如果在原始请求或响应的 600 秒以内，主机 B 在单独的请求中发起到您的实例的流量，则无论入站安全组规则如何，您的实例都将接受该请求，因为该流量将被视为响应流量。对于 VPC 安全组，您可以通过将安全组的出站规则修改为仅允许某些类型的出站流量来控制这一点。或者，您可以使用您的子网的网络 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](#)。

对于每个规则，您可以指定以下内容：

- 允许的协议（例如 TCP、UDP 或 ICMP）
- TCP 和 UDP 或自定义协议：允许的端口范围
- ICMP：ICMP 类型和代码
- 适用于源（入站规则）或目标（出站规则）的以下选项之一：
  - 用 CIDR 表示法指定的单个 IP 地址。务必在 IP 地址后使用 /32 前缀；如果在 IP 地址后使用 /0 前缀，则会向任何人打开该端口。例如，指定 IP 地址 203.0.113.1 为 203.0.113.1/32。
  - 用 CIDR 表示法指定的 IP 地址范围（例如，203.0.113.0/24）。
- 安全组的名称 (EC2-Classic) 或 ID ( EC2-Classic 或 EC2-VPC )。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。（请注意，这不会将规则从源安全组添加到此安全组。）您可以指定以下安全组之一：
  - 当前安全组。
  - EC2-Classic：同一区域的另一个 EC2-Classic 安全组。
  - EC2-Classic：同一区域中另一个 AWS 账户的安全组（添加 AWS 账户 ID 作为前缀；例如，111122223333/sg-edcd9784）。
  - EC2-VPC：同一 VPC 或对等 VPC 的另一个安全组。

当您指定一个安全组为规则的源或目标时，该规则会影响与安全组相关联的所有实例。允许的传入流量基于与源安全组相关联的实例的私有 IP 地址（而不是公有 IP 或弹性 IP 地址）。有关 IP 地址的更多信息，请参阅 [Amazon EC2 实例 IP 寻址 \(p. 597\)](#)。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 3389 (RDP)，而另一条规则允许所有人访问 TCP 端口 3389，那么所有人都可以访问 TCP 端口 3389。

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。



#### Caution

由于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。

有关创建安全组规则以确保路径 MTU 发现可以正常工作的更多信息，请参阅 [路径 MTU 发现 \(p. 627\)](#)。

## 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响应通信的对应规则，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。

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 (0.0.0.0/0) 流入实例的规则，则会立即中断与该实例的现有 SSH 连接。

如果您希望确保在删除安全组规则后立即中断该流量，则可以为您的子网使用网络 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 账户在每个区域都自动拥有一个 EC2-Classic 默认安全组。创建 VPC 时，我们会自动创建 VPC 默认安全组。如果您在启动实例时没有指定其他安全组，实例会自动与相应的默认安全组相关联。

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初始设置：

- 仅允许来自其他与默认安全组相关联的实例的入站流量
- 允许从实例流出的所有出站流量

默认安全组在其入站规则中将其自身指定为源安全组。这就使与默认安全组相关联的实例可以和与默认安全组相关联的其他实例进行通信。

您可以更改默认安全组的规则。例如，您可以添加一条入站规则，以允许 RDP 连接，以便特定主机能够管理实例。

您无法删除默认安全组。如果您尝试删除 EC2-Classic 默认安全组，会显示以下错误：

`Client.InvalidGroup.Reserved: The security group 'default' is reserved.` 如果您尝试删除 VPC 默认安全组，会显示以下错误：`Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user.`

## 自定义安全组

如果您不希望所有的实例都使用默认安全组，您可以创建自己的安全组，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。有关可帮助您创建 Web 服务器和数据库服务器安全组的说明，请参阅 *Amazon VPC 用户指南* 中的[推荐安全组](#)。



### Note

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。在 EC2-VPC 中，您最多可以为每个 VPC 创建 500 个安全组。EC2-Classic 安全组不会根据 EC2-VPC 安全组限额来计数。

创建安全组时，您必须为其提供名称和描述。安全组的名称和描述最多 255 个字符，而且仅限于以下字符：

- EC2-Classic：ASCII 字符
- EC2-VPC：a-z、A-Z、0-9、空格和 \_-:/()#@[]+=&;!\$^\*

AWS 会为每个安全组分配一个形式为 sg-xxxxxxxx 的唯一 ID。以下是您创建的安全组的初始设置：

- 不允许入站流量
- 允许所有的出站流量

创建安全组后，您可以更改其入站规则，以反映您希望到达关联实例的入站流量的类型。在 EC2-VPC 中，您也可以更改其出站规则。

要允许具有相同安全组的不同实例相互通信，您必须明确添加实现此目的的规则。下表描述了为了使 EC2-Classic 中的实例能够相互通信而必须添加到安全组的规则。

| 入站     |      |           |                            |
|--------|------|-----------|----------------------------|
| 源      | 协议   | 端口范围      | 注释                         |
| 安全组 ID | ICMP | 全部        | 允许与该安全组相关联的其他实例的入站 ICMP 访问 |
| 安全组 ID | TCP  | 0 - 65535 | 允许与该安全组相关联的其他实例的入站 TCP 访问  |
| 安全组 ID | UDP  | 0 - 65535 | 允许与该安全组相关联的其他实例的入站 UDP 访问  |

下表描述了为了使 VPC 中的实例能够相互通信而必须添加到安全组的规则。

| 入站     |    |      |                      |
|--------|----|------|----------------------|
| 源      | 协议 | 端口范围 | 注释                   |
| 安全组 ID | 全部 | 全部   | 允许与该安全组相关联的其他实例的入站流量 |

## 正在创建安全组

### 创建新安全组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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。对于 VPC，选择 No VPC 以创建 EC2-Classic 的安全组，或选择 VPC ID 以创建该 VPC 的安全组。
5. 您可以开始添加规则，也可以选择 Create 以立即创建安全组（您可以在以后随时添加规则）。有关添加规则的更多信息，请参阅[向安全组添加规则 \(p. 520\)](#)。

### 复制安全组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择要复制的安全组，选择 Actions，然后选择 Copy to new。
4. Create Security Group (创建安全组) 对话框随即打开，其中预填充了现有安全组中的规则。为新的安全组指定名称和说明。在 VPC 列表中，选择 No VPC 以创建 EC2-Classic 的安全组，或选择 VPC ID 以创建该 VPC 的安全组。完成后，选择 Create。

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。在 VPC 中启动实例后，您可以更改其安全组。想要了解更多信息，请参阅 *Amazon VPC 用户指南* 中的[更改实例的安全组](#)主题。

## 描述您的安全组

### 描述您的 EC2-Classic 安全组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 从筛选列表中选择 Network Platforms，然后选择 EC2-Classic。
4. 选择一个安全组。我们将在 Description (描述) 选项卡中显示常规信息，并在 Inbound (入站) 选项卡中显示入站规则。

### 描述您的 EC2-VPC 安全组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 从筛选列表中选择 Network Platforms，然后选择 EC2-VPC。
4. 选择一个安全组。我们将在 Description (描述) 选项卡上显示常规信息，在 Inbound (入站) 选项卡上显示入站规则，并在 Outbound (出站) 选项卡上显示出站规则。

## 向安全组添加规则

当您向安全组添加规则时，这一新规则会自动应用于与该安全组相关联的任何实例。

### 向安全组添加规则

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择安全组。
4. 您可以允许 Web 服务器接收所有入站 HTTP 和 HTTPS 流量。在 Inbound 选项卡上，选择 Edit。在对话框中，选择 Add Rule。从 Type (类型) 列表中选择 HTTP，并将源保留为 Anywhere (任何位置) (0.0.0.0/0)。为 HTTPS 协议添加类似规则。
5. 若要连接到 Windows 实例，您需要允许 RDP 流量。选择 Add Rule，然后从 Type 列表中选择 RDP。

在 Source (源) 字段中，用 CIDR 表示法指定您计算机的公有 IP 地址。例如，如果您的 IP 地址为 203.0.113.25，请指定 203.0.113.25/32，以便用 CIDR 表示法列出此 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 203.0.113.0/24。您可以从 Source (源) 列表中选择 My IP (我的 IP) 以便自动使用您计算机的 IP 地址填充该字段。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。



### Caution

如果使用 0.0.0.0/0，则可以允许所有 IP 地址使用 RDP 访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产中，您将仅授权特定 IP 地址或地址范围访问您的实例。

6. 您可以允许所有与此安全组关联的实例彼此之间进行通信，或是在与其他安全组关联的实例和与此安全组关联的实例之间进行通信。选择 Add Rule，选择 All ICMP，然后开始在 Source 中输入安全组的 ID；这可为您提供安全组列表。从列表中选择安全组。对 TCP 和 UDP 协议重复这些步骤。完成后选择 Save。

| Type     | Protocol | Port Range | Source             |
|----------|----------|------------|--------------------|
| HTTP     | TCP      | 80         | Anywhere 0.0.0.0/0 |
| HTTPS    | TCP      | 443        | Anywhere 0.0.0.0/0 |
| All ICMP | ICMP     | 0 - 65535  | Custom sg-0bee2270 |
| All TCP  | TCP      | 0 - 65535  | Custom sg-0bee2270 |
| All UDP  | UDP      | 0 - 65535  | Custom sg-0bee2270 |

- 如果您正在创建 VPC 安全组，则还可以指定出站规则。有关示例，请参阅 *Amazon VPC 用户指南* 中的 [添加和删除规则](#)。

## 从安全组中删除规则

当您从安全组中删除规则时，此更改会自动应用于与该安全组相关联的任何实例。

### 要删除安全组规则

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 在导航窗格中，选择 Security Groups。
- 选择一个安全组。
- 选择 Edit，然后选择您需要删除的每个规则旁的 Delete ( 十字图标 )。
- 选择 Save。

## 正在删除安全组

您不能删除与实例相关联的安全组。您不能删除默认安全组。您不能删除由其他安全组中的规则引用的安全组。如果您的安全组由自己的一个规则引用，则必须先删除该规则，然后才能删除安全组。

### 删除安全组

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 在导航窗格中，选择 Security Groups。
- 选择一个安全组，然后选择 Delete。
- 选择 Yes, Delete。

## API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

### 创建安全组

- [create-security-group \(AWS CLI\)](#)

- [New-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

向安全组添加一个或多个传入规则

- [authorize-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

[EC2-VPC] 向安全组添加一个或多个传出规则

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

说明一个或多个安全组

- [describe-security-groups](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

[EC2-VPC] 修改实例的安全组

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

从安全组中删除一个或多个传入规则

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (适用于 Windows PowerShell 的 AWS 工具)

[EC2-VPC] 从安全组中删除一个或多个传出规则

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

删除安全组

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

## 控制对 Amazon EC2 资源的访问

### Abstract

通过设置安全组并使用 IAM 以 控制对 Amazon EC2 资源的访问。

您的安全证书使 AWS 中的服务可以识别您，并授予您对 AWS 资源（例如您的 Amazon EC2 资源）的无限制使用权限。您可以使用 Amazon EC2 和 AWS Identity and Access Management (IAM) 的功能，在不共享您的安全证书情况下允许其他用户、服务和应用程序使用您的 Amazon EC2 资源。您可以使用 IAM 控制其他用户对您 AWS 账户中资源的使用方式，并且您可以使用安全组来控制对您的 Amazon EC2 实例的访问。您可以选择授予 Amazon EC2 资源的完全使用或限制使用权限。

### 内容

- 网络访问您的实例 : ([p. 523](#))
- Amazon EC2 权限属性 ([p. 523](#))
- IAM 和 Amazon EC2 ([p. 523](#))
- Amazon EC2 的 IAM 策略 ([p. 525](#))
- 适用于 Amazon EC2 的 IAM 角色 ([p. 565](#))
- 为您的 Windows 实例授权入站流量 ([p. 570](#))

## 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 Windows 实例授权入站流量 \(p. 570\)](#)。

## Amazon EC2 权限属性

您的组织可拥有多个 AWS 账户。Amazon EC2 让您可以指定其他的 AWS 账户，能够使用您的Amazon 系统映像 (AMI) 和 Amazon EBS 快照。这些权限仅在 AWS 账户级别有效；您不能限制指定 AWS 账户内特定用户的权限。您指定的 AWS 账户中的所有用户均可使用 AMI 或快照。

每个 AMI 都拥有一个 `LaunchPermission` 属性，用于控制可以访问该 AMI 的 AWS 账户。有关更多信息，请参阅 [将 AMI 设为公用 \(p. 69\)](#)。

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 \(p. 681\)](#)。

## IAM 和 Amazon EC2

IAM 允许您执行以下操作：

- 在您的 AWS 账户下创建用户和组
- 为您的 AWS 账户下的每个用户分配唯一的安全证书
- 控制每个用户使用 AWS 资源执行任务的权限
- 允许另一 AWS 账户的用户共享 AWS 资源
- 创建 AWS 账户角色并定义可以担任这些角色的用户或服务
- 借助企业的现有身份验证，授予使用 AWS 资源执行任务的权限

通过将 IAM 与 Amazon EC2 配合使用，您可以控制组织中的用户能否使用特定的 Amazon EC2 API 操作执行任务，以及他们能否使用特定的 AWS 资源。

本主题有助于回答以下问题：

- 如何在 IAM 中创建组和用户？
- 如何创建策略？
- 在 Amazon EC2 中执行任务时我需要哪些 IAM 策略？
- 如何授予在 Amazon EC2 中执行操作的权限？
- 如何授予在 Amazon EC2 中对特定资源执行操作的权限？

## 创建 IAM 组和用户

### 创建 IAM 组

1. 登录到 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
3. 在 Group Name 框中，为您的组输入一个名称，然后选择 Next Step。
4. 在 Attach Policy 页面上，选择 AWS 管理的策略。例如，对于 Amazon EC2，下列 AWS 管理的策略之一可能符合您的需求：
  - PowerUserAccess
  - ReadOnlyAccess
  - AmazonEC2FullAccess
  - AmazonEC2ReadOnlyAccess
5. 选择 Next Step，然后选择 Create Group。

您的新组列在 Group Name (组名) 下方。

### 创建 IAM 用户，将该用户添加到您的组中，并为该用户创建密码

1. 在导航窗格中选择 Users，然后选择 Create New Users。
2. 在框 1 中，输入一个用户名，然后选择 Create。
3. 选择 Download Credentials 并将您的访问密钥保存在安全的位置。使用 AWS CLI、AWS SDK 或 HTTP API 以编程方式访问 AWS 时将会需要您的访问密钥。



#### Note

完成此步骤之后您将无法检索秘密访问密钥；如果放错了位置，则必须创建一个新的。

在您下载访问密钥后，选择 Close。

4. 在 User Name 下，选择您刚创建的用户的名称。
5. 在 Groups 选项卡中，选择 Add User to Groups。
6. 选择您之前创建的组，然后选择 Add to Groups。
7. 选择 Security Credentials，然后选择 Manage Password。
8. 选择 Assign a custom password，然后输入并确认密码。完成后，请选择 Apply。
9. 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 \(p. 525\)](#)
- [适用于 Amazon EC2 的 IAM 角色 \(p. 565\)](#)
- [Identity and Access Management \(IAM\)](#)
- [IAM 用户指南](#)

## Amazon EC2 的 IAM 策略

### Abstract

控制 IAM 用户可以查看、创建和修改的 Amazon EC2 资源。

默认情况下，IAM 用户没有创建或修改 Amazon EC2 资源或使用 Amazon EC2 API 执行任务的权限。（这意味着他们不能使用 Amazon EC2 控制台或 CLI 执行这些操作。）要允许 IAM 用户创建或修改资源和执行任务，您必须创建 IAM 策略以允许 IAM 用户使用他们所需的特定资源和 API 操作，然后将这些策略与需要这些权限的 IAM 用户或组关联起来。

当您将策略与一个用户或一组用户关联时，它会授权或拒绝用户使用指定资源执行指定任务。有关 IAM 策略的更多一般信息，请参阅 [IAM 用户指南中的权限与策略](#)。有关管理和创建自定义 IAM 策略的更多信息，请参阅[管理 IAM 策略](#)。

### 入门

IAM 策略必须授予或拒绝使用一个或多个 Amazon EC2 操作的权限。它还必须指定可以用于操作的资源（可以是所有资源，在某些情况下可以是特定资源）。策略还可以包含应用于资源的条件。

Amazon EC2 部分支持资源级权限。这意味着对于某些 EC2 API 操作，您无法指定允许用户为哪个资源使用该操作；而必须允许用户为所有资源使用该操作。

| 任务                      | 主题                                                    |
|-------------------------|-------------------------------------------------------|
| 了解策略的基本结构               | <a href="#">策略语法 (p. 526)</a>                         |
| 在策略中定义操作                | <a href="#">Amazon EC2 操作 (p. 526)</a>                |
| 在策略中定义特定资源              | <a href="#">适用于 Amazon EC2 的 Amazon 资源名称 (p. 527)</a> |
| 将条件应用于资源的使用             | <a href="#">Amazon EC2 的条件密钥 (p. 529)</a>             |
| 使用可用于 Amazon EC2 的资源级权限 | <a href="#">Amazon EC2 API 操作支持的资源级权限 (p. 532)</a>    |
| 测试策略                    | <a href="#">检查用户是否具有所需权限 (p. 531)</a>                 |
| 针对 CLI 或软件开发工具包的策略示例    | <a href="#">适用于 AWS CLI 或 AWS 开发工具包的策略示例 (p. 546)</a> |
| 针对 Amazon EC2 控制台的策略示例  | <a href="#">用于 Amazon EC2 控制台的策略示例。 (p. 556)</a>      |

## 策略结构

### Abstract

了解用于控制对 Amazon EC2 的访问的 IAM 策略结构。

以下主题说明 IAM 策略的结构。

### 主题

- [策略语法 \(p. 526\)](#)
- [Amazon EC2 操作 \(p. 526\)](#)
- [适用于 Amazon EC2 的 Amazon 资源名称 \(p. 527\)](#)
- [Amazon EC2 的条件密钥 \(p. 529\)](#)
- [检查用户是否具有所需权限 \(p. 531\)](#)

## 策略语法

IAM 策略是包含一个或多个语句的 JSON 文档。每个语句的结构如下：

```
{
 "Statement": [{
 "Effect": "effect",
 "Action": "action",
 "Resource": "arn",
 "Condition": {
 "condition": {
 "key": "value"
 }
 }
 }
]
```

组成语句的各个元素如下：

- Effect：此 *effect* 可以是 Allow 或 Deny。默认情况下 IAM 用户没有使用资源和 API 操作的权限，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- Action：*action* 是对其授予或拒绝权限的特定 API 操作。要了解有关指定 *action* 的信息，请参阅 [Amazon EC2 操作 \(p. 526\)](#)。
- Resource：操作影响的资源。有些 Amazon EC2 API 操作允许您在策略中包括该操作可以创建或修改的特定资源。要在语句中指定资源，您需要使用其 Amazon 资源名称 (ARN)。有关指定 *arn* 值的更多信息，请参阅 [适用于 Amazon EC2 的 Amazon 资源名称 \(p. 527\)](#)。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 \(p. 532\)](#)。如果 API 操作不支持 ARN，请使用 \* 通配符指定操作可以影响所有资源。
- Condition：条件是可选的。它们可以用于控制策略生效的时间。想要了解更多有关为 Amazon EC2 指定条件的信息，请参阅 [Amazon EC2 的条件密钥 \(p. 529\)](#)。

想要了解更多有关 Amazon EC2 的示例 IAM 策略语句的信息，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 546\)](#)。

## Amazon EC2 操作

在 IAM 策略语句中，您可以从支持 IAM 的任何服务中指定任何 API 操作。对于 Amazon EC2，请使用以下前缀为 API 操作命名：ec2：。例如：ec2:RunInstances 和 ec2>CreateImage。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": ["ec2:action1", "ec2:action2"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名称以单词“Describe”开头的所有操作，如下所示：

```
"Action": "ec2:Describe*"
```

要指定所有 Amazon EC2 API 操作，请使用 \* 通配符，如下所示：

```
"Action": "ec2:*
```

有关 Amazon EC2 操作的列表，请参阅 [Amazon EC2 API Reference](#) 中的[操作](#)主题。

## 适用于 Amazon EC2 的 Amazon 资源名称

每个 IAM 策略语句适用于您使用资源的 ARN 指定的资源。



### Important

当前，并不是所有 API 操作都支持各个 ARN；我们以后将为其他 API 操作添加支持以及为其他 Amazon EC2 资源添加 ARN。有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用以及每个 ARN 支持的条件密钥的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。

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，cn-north-1）。

*账户*

AWS 账户 ID，不包含连字符（例如，123456789012）。

*resourceType*

资源类型（例如，instance）。

*resourcePath*

识别资源的路径。您可以在路径中使用 \* 通配符。

例如，您可以使用特定实例 (i-1234567890abcdef0) 的 ARN 在语句中指定它，如下所示：

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

还可以使用 \* 通配符指定属于特定账户的所有实例，如下所示：

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

要指定所有资源，或者如果特定 API 操作不支持 ARN，请在 Resource 元素中使用 \* 通配符，如下所示：

```
"Resource": "*"
```

下表介绍了 Amazon EC2 API 操作使用的每种类型资源的 ARN。

| 资源类型                         | ARN                                                                            |
|------------------------------|--------------------------------------------------------------------------------|
| 所有 Amazon EC2 资源             | arn:aws:ec2:*                                                                  |
| 指定账户在指定地区拥有的所有 Amazon EC2 资源 | arn:aws:ec2:region:account:*                                                   |
| 客户网关                         | arn:aws:ec2:region:account:customer-gateway/cgw-id<br>其中 cgw-id 是 cgw-xxxxxxxx |

| 资源类型        | ARN                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP 选项集    | arn:aws:ec2:region:account:dhcp-options/dhcp-options- <i>id</i><br>其中 <i>dhcp-options-id</i> 是 dopt-xxxxxxxx                              |
| 图片          | arn:aws:ec2:region::image/ <i>image-id</i><br>其中 <i>image-id</i> 是 AMI、AKI 或 ARI 的 ID，而不使用 <i>account</i>                                 |
| 实例          | arn:aws:ec2:region:account:instance/ <i>instance-id</i><br>其中 <i>instance-id</i> 是 i-xxxxxxxx 或 i-xxxxxxxxxxxxxxxxxxxx                    |
| 实例配置文件      | arn:aws:iam::account:instance-profile/ <i>instance-profile-name</i><br>其中 <i>instance-profile-name</i> 是实例配置文件的名称，而不使用 <i>region</i>      |
| Internet 网关 | arn:aws:ec2:region:account:internet-gateway/igw- <i>id</i><br>其中 <i>igw-id</i> 是 igw-xxxxxxxx                                             |
| 密钥对         | arn:aws:ec2:region:account:key-pair/ <i>key-pair-name</i><br>其中 <i>key-pair-name</i> 是密钥对名称（例如，gsg-keypair）                               |
| 网络 ACL      | arn:aws:ec2:region:account:network-acl/nacl- <i>id</i><br>其中 <i>nacl-id</i> 是 acl-xxxxxxxx                                                |
| 网络接口        | arn:aws:ec2:region:account:network-interface/eni- <i>id</i><br>其中 <i>eni-id</i> 是 eni-xxxxxxxx                                            |
| 置放群组        | arn:aws:ec2:region:account:placement-group/placement-group- <i>name</i><br>其中 <i>placement-group-name</i> 是置放组名称（例如，my-cluster）           |
| 路由表         | arn:aws:ec2:region:account:route-table/route-table- <i>id</i><br>其中 <i>route-table-id</i> 是 rtb-xxxxxxxx                                  |
| 安全组         | arn:aws:ec2:region:account:security-group/security-group- <i>id</i><br>其中 <i>security-group-id</i> 是 sg-xxxxxxxx                          |
| 快照          | arn:aws:ec2:region::snapshot/ <i>snapshot-id</i><br>其中 <i>snapshot-id</i> 是 snap-xxxxxxxx 或 snap-xxxxxxxxxxxxxxxxxxxx，而不使用 <i>account</i> |
| 子网          | arn:aws:ec2:region:account:subnet/subnet- <i>id</i><br>其中 <i>subnet-id</i> 是 subnet-xxxxxxxx                                              |
| 卷           | arn:aws:ec2:region:account:volume/volume- <i>id</i><br>其中 <i>volume-id</i> 是 vol-xxxxxxxx 或 vol-xxxxxxxxxxxxxxxxxxxx                      |
| VPC         | arn:aws:ec2:region:account:vpc/vpc- <i>id</i><br>其中 <i>vpc-id</i> 是 vpc-xxxxxxxx                                                          |

| 资源类型     | ARN                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| VPC 对等连接 | <pre>arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id</pre> <p>其中 <i>vpc-peering connection-id</i> 是 pcx-xxxxxxxx</p> |

许多 Amazon EC2 API 操作涉及多种资源。例如，`AttachVolume` 将一个 Amazon EBS 卷挂载到一个实例，从而使 IAM 用户必须获得相应权限才能使用该卷和该实例。要在单个语句中指定多种资源，请使用逗号将它们隔开，如下所示：

```
"Resource": ["arn1", "arn2"]
```

更多有关 ARN 的一般信息，请参阅 *Amazon Web Services General Reference* 中的 [Amazon 资源名称 \(ARN\)](#) 和 [AWS 服务命名空间](#) 主题。有关 Amazon EC2 操作所创建或修改的资源以及可以在 IAM 策略语句中使用的 ARN 的更多信息，请参阅 *Amazon EC2 API Reference* 中的 [授予 IAM 用户所需的 Amazon EC2 资源使用权限](#) 主题。

## Amazon EC2 的条件密钥

在策略语句中，您可以选择性指定控制策略生效时间的条件。每个条件都包含一个或多个密钥值对。条件密钥不区分大小写。我们已经定义了 AWS 范围内的条件密钥以及其他特定于服务的条件密钥。

如果您指定了多个条件或在单一条件下指定了多个密钥，我们将通过逻辑 AND 操作对其进行评估。如果您在单一条件下指定了一个具有多个值的密钥，我们将通过逻辑 OR 操作对其进行评估。必须匹配所有条件才能授予权限。

在指定条件时，您也可使用占位符。例如，您可以授予 IAM 用户通过指定其 IAM 用户名的标签使用资源的权限。有关更多信息，请参阅 *IAM 用户指南* 中的 [策略变量](#)。

Amazon EC2 会实施 AWS 范围内的条件密钥（请参阅 [可用密钥](#)）以及以下服务特定的条件密钥。（我们将在以后为 Amazon EC2 添加其他服务特定的条件密钥支持。）



### Important

许多条件密钥是特定于某个资源的，而某些 API 操作会使用多个资源。如果您使用条件密钥编写策略，请使用语句的 `Resource` 元素指定要应用该条件密钥的资源。否则，该策略可能会完全阻止用户执行操作，因为针对未应用条件密钥的资源的条件检查失败。如果您不想指定资源，或者如果您已将策略的 `Action` 元素编写为包含多个 API 操作，则必须使用 `...IfExists` 条件类型以确保对不使用条件密钥的资源忽略条件密钥。有关更多信息，请参阅 *IAM 用户指南* 中的 [...IfExists 条件](#)。

| 条件密钥                              | 密钥/值对                                                                                                                                                                             | 评估类型       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>ec2:AccepterVpc</code>      | <pre>"ec2:AccepterVpc":"vpc-arn"</pre> <p>其中 <i>vpc-arn</i> 是对等 VPC 的 VPC ARN</p>                                                                                                 | ARN , Null |
| <code>ec2:AvailabilityZone</code> | <pre>"ec2:AvailabilityZone":"az-api-name"</pre> <p>其中 <i>az-api-name</i> 是可用区的名称（例如，<code>cn-north-1a</code>）</p> <p>要列出您的可用区，请使用 <a href="#">describe-availability-zones</a></p> | 字符串 , Null |

| 条件密钥                        | 密钥/值对                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 评估类型       |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ec2:EbsOptimized            | "ec2:EbsOptimized":"optimized-flag"<br><br>其中 <i>optimized-flag</i> 是 true   false                                                                                                                                                                                                                                                                                                                                                                                                                                           | 布尔值 , Null |
| ec2:ImageType               | "ec2:ImageType":"image-type-api-name"<br><br>其中 <i>image-type-api-name</i> 是 ami   aki   ari                                                                                                                                                                                                                                                                                                                                                                                                                                 | 字符串 , Null |
| ec2:InstanceProfile         | "ec2:InstanceProfile":"instance-profile-arn"<br><br>其中 <i>instance-profile-arn</i> 是实例配置文件 ARN                                                                                                                                                                                                                                                                                                                                                                                                                               | ARN , Null |
| ec2:InstanceType            | "ec2:InstanceType":"instance-type-api-name"<br><br>其中 <i>instance-type-api-name</i> 是实例类型名称 ( m1.small   m1.medium   m1.large   m1.xlarge   m3.xlarge   m3.2xlarge   c1.medium   c1.xlarge   c3.large   c3.xlarge   c3.2xlarge   c3.4xlarge   c3.8xlarge   cc2.8xlarge   m2.xlarge   m2.2xlarge   m2.4xlarge   r3.medium   r3.large   r3.xlarge   r3.2xlarge   r3.4xlarge   r3.8xlarge   cr1.8xlarge   hi1.4xlarge   hs1.8xlarge   i2.xlarge   i2.2xlarge   i2.4xlarge   i2.8xlarge   t1.micro   cg1.4xlarge   g2.2xlarge )。 | 字符串 , Null |
| ec2:Owner                   | "ec2:Owner":"account-id"<br><br>其中 <i>account-id</i> 是 amazon   aws-marketplace   aws-account-id                                                                                                                                                                                                                                                                                                                                                                                                                             | 字符串 , Null |
| ec2:ParentSnapshot          | "ec2:ParentSnapshot":"snapshot-arn"<br><br>其中 <i>snapshot-arn</i> 是快照 ARN                                                                                                                                                                                                                                                                                                                                                                                                                                                    | ARN , Null |
| ec2:ParentVolume            | "ec2:ParentVolume":"volume-arn"<br><br>其中 <i>volume-arn</i> 是卷 ARN                                                                                                                                                                                                                                                                                                                                                                                                                                                           | ARN , Null |
| ec2:Placement-Group         | "ec2:PlacementGroup":"placement-group-arn"<br><br>其中 <i>placement-group-arn</i> 是置放组 ARN                                                                                                                                                                                                                                                                                                                                                                                                                                     | ARN , Null |
| ec2:Placement-GroupStrategy | "ec2:PlacementGroupStrategy":"placement-group-strategy"<br><br>其中 <i>placement-group-strategy</i> 为 cluster                                                                                                                                                                                                                                                                                                                                                                                                                  | 字符串 , Null |
| ec2:ProductCode             | "ec2:ProductCode":"product-code"<br><br>其中 <i>product-code</i> 是产品代码                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 字符串 , Null |
| ec2:Public                  | "ec2:Public":"public-flag"<br><br>其中 AMI 的 <i>public-flag</i> 为 true   false                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 布尔值 , Null |
| ec2:Region                  | "ec2:Region":"region-name"<br><br>其中 <i>region-name</i> 是区域的名称 ( 例如 , cn-north-1 )。<br>要列出您的区域 , 请使用 <a href="#">describe-regions</a> 。                                                                                                                                                                                                                                                                                                                                                                                      | 字符串 , Null |

| 条件密钥                             | 密钥/值对                                                                                                                                                                              | 评估类型       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ec2:RequesterVpc                 | "ec2:RequesterVpc":" <i>vpc-arn</i> "<br><br>其中 <i>vpc-arn</i> 请求者 VPC 的 VPC ARN                                                                                                   | ARN , Null |
| ec2:Re-sourceTag/ <i>tag-key</i> | "ec2:ResourceTag/ <i>tag-key</i> ":" <i>tag-value</i> "<br><br>其中 <i>tag-key</i> 和 <i>tag-value</i> 是标签密钥对                                                                         | 字符串 , Null |
| ec2:RootDevice-Type              | "ec2:RootDeviceType":" <i>root-device-type-name</i> "<br><br>其中 <i>root-device-type-name</i> 是 ebs   instance-store                                                                | 字符串 , Null |
| ec2:Subnet                       | "ec2:Subnet":" <i>subnet-arn</i> "<br><br>其中 <i>subnet-arn</i> 是子网 ARN                                                                                                             | ARN , Null |
| ec2:Tenancy                      | "ec2:Tenancy":" <i>tenancy-attribute</i> "<br><br>其中 <i>tenancy-attribute</i> 是 default   dedicated   host                                                                         | 字符串 , Null |
| ec2:Volumelops                   | "ec2:Volumelops":" <i>volume-iops</i> "<br><br>其中 <i>volume-iops</i> 是每秒输入/输出操作 (IOPS)；其范围是从 100 到 20,000                                                                          | 数值 , Null  |
| ec2:VolumeSize                   | "ec2:VolumeSize":" <i>volume-size</i> "<br><br>其中 <i>volume-size</i> 是卷的大小 (以 GiB 为单位)                                                                                             | 数值 , Null  |
| ec2:VolumeType                   | "ec2:VolumeType":" <i>volume-type-name</i> "<br><br>其中， <i>volume-type-name</i> 对于通用型 SSD 卷是 gp2，对于 Provisioned IOPS 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":" <i>vpc-arn</i> "<br><br>其中 <i>vpc-arn</i> 是 VPC ARN                                                                                                                    | ARN , Null |

有关那个条件密钥可以与那些 Amazon EC2 资源一起使用的信息（根据操作流程），请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。有关适用于 Amazon EC2 的策略语句示例，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 546\)](#)。

## 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 --auth-dry-run 选项的 CLI 命令）。在这种情况下，调用会完成身份验证检查，但是不会完成该操作。例如，您可以检查用户能否终止特定实例，但不会真的终止它。如果测试用户具有所需的权限，请求会返回 DryRunOperation；否则，它会返回 UnauthorizedOperation。

如果策略未授予用户您所期望的权限，您可以根据需要调节策略并重新测试，直到您获得预期的结果。



### Important

在其生效之前，它需要几分钟时间将策略更改为适合状态。因此，我们建议您在测试策略更新前，等候五分钟的时间。

如果身份验证检查失败，该请求将返回一个带有诊断信息的代码消息。您可以使用 `DecodeAuthorizationMessage` 操作对消息进行解码。有关更多信息，请参阅 *AWS Security Token Service API Reference* 中的 [DecodeAuthorizationMessage](#)，以及 *AWS Command Line Interface Reference* 中的 [decode-authorization-message](#)。

## Amazon EC2 API 操作支持的资源级权限

### Abstract

了解当前支持资源级权限的 Amazon EC2 API 操作。

资源级权限 指的是能够指定允许用户对哪些资源执行操作的能力。Amazon EC2 部分支持资源级权限。这意味着对于某些 Amazon EC2 操作，您可以控制何时允许用户执行操作（基于必须满足的条件）或是允许用户使用的特定资源。例如，您可以向用户授予启动实例的权限，但是仅限特定类型的实例，并且只能使用特定的 AMI。

下表介绍当前支持资源级权限的 Amazon EC2 API 操作，以及每个操作支持的资源（及其 ARN）和条件密钥。指定 ARN 时，您可以在路径中使用 \* 通配符；例如，在无法或不希望指定确切资源 ID 的时候可以这样做。有关使用通配符的示例，请参阅 [适用于 AWS CLI 或 AWS 开发工具包的策略示例 \(p. 546\)](#)。



### Important

如果某一 Amazon EC2 API 操作在此表中没有列出，则它不支持资源级权限。如果 Amazon EC2 API 操作不支持资源级权限，那么，您可以向用户授予使用该操作的权限，但是必须为策略语句的资源元素指定 \*。有关如何执行此操作的示例，请参阅 [1：只读访问 \(p. 546\)](#)。我们将在以后为其他操作、ARN 和条件密钥添加支持。有关当前不支持资源级权限的 Amazon EC2 API 操作列表，请参阅 *Amazon EC2 API Reference* 中的 [不支持的资源级权限](#)。

| API 操作                     | 资源                                                                                                                    | 条件密钥                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| AcceptVpcPeeringConnection | VPC 对等连接<br><br>arn:aws:ec2:region:account:vpc-peering-connection/*                                                   | ec2:AcceptorVpc<br><br>ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:RequesterVpc |
|                            | arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id                                           |                                                                                          |
|                            | VPC<br><br>arn:aws:ec2:region:account:vpc/*<br><br>arn:aws:ec2:region:account:vpc/vpc-id<br><br>其中 vpc-id 是接受人拥有的 VPC | ec2:ResourceTag/tag-key<br><br>ec2:Region<br><br>ec2:Tenancy                             |
|                            |                                                                                                                       |                                                                                          |

| API 操作               | 资源                                                                                                                                                         | 条件密钥                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AttachClassicLinkVpc | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i>                                             | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |
|                      | 安全组<br><br>arn:aws:ec2:region:account:security-group/*<br><br>arn:aws:ec2:region:account:security-group/ <i>security-group-id</i><br><br>其中的安全组是 VPC 的安全组。 | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                                        |
|                      | VPC<br><br>arn:aws:ec2:region:account:vpc/*<br><br>arn:aws:ec2:region:account:vpc/ <i>vpc-id</i>                                                           | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Tenancy                                                                                                                                    |

| API 操作                         | 资源                                                                                                                                | 条件密钥                                                                                                                                                                                            |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AttachVolume                   | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i>                    | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |
|                                | 卷<br><br>arn:aws:ec2:region:account:volume/*<br><br>arn:aws:ec2:region:account:volume/ <i>volume-id</i>                           | ec2:AvailabilityZone<br>ec2:ParentSnapshot<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Volumelops<br>ec2:VolumeSize<br>ec2:VolumeType                                               |
| AuthorizeSecurity-GroupEgress  | 安全组<br><br>arn:aws:ec2:region:account:security-group/*<br><br>arn:aws:ec2:region:account:security-group/ <i>security-group-id</i> | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                                        |
| AuthorizeSecurityGroup-Ingress | 安全组<br><br>arn:aws:ec2:region:account:security-group/*<br><br>arn:aws:ec2:region:account:security-group/ <i>security-group-id</i> | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                                        |

| API 操作                     | 资源                                                                                                                 | 条件密钥                                                 |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| CreateVpcPeeringConnection | VPC<br>arn:aws:ec2:region:account:vpc/*<br>arn:aws:ec2:region:account:vpc/vpc-id<br>其中 <i>vpc-id</i> 是请求者的 VPC     | ec2:ResourceTag/tag-key<br>ec2:Region<br>ec2:Tenancy |
|                            | VPC 对等连接<br>arn:aws:ec2:region:account:vpc-peering-connection/*                                                    | ec2:AcceptorVpc<br>ec2:Region<br>ec2:RequesterVpc    |
| DeleteCustomerGateway      | 客户网关<br>arn:aws:ec2:region:account:customer-gateway/*<br>arn:aws:ec2:region:account:customer-gateway/cgw-id        | ec2:Region<br>ec2:ResourceTag/tag-key                |
| DeleteDhcpOptions          | DHCP 选项集<br>arn:aws:ec2:region:account:dhcp-options/*<br>arn:aws:ec2:region:account:dhcp-options/dhcp-options-id   | ec2:Region<br>ec2:ResourceTag/tag-key                |
| DeleteInternetGateway      | Internet 网关<br>arn:aws:ec2:region:account:internet-gateway/*<br>arn:aws:ec2:region:account:internet-gateway/igw-id | ec2:Region<br>ec2:ResourceTag/tag-key                |
| DeleteNetworkAcl           | 网络 ACL<br>arn:aws:ec2:region:account:network-acl/*<br>arn:aws:ec2:region:account:network-acl/nacl-id               | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc     |
| DeleteNetworkAclEntry      | 网络 ACL<br>arn:aws:ec2:region:account:network-acl/*<br>arn:aws:ec2:region:account:network-acl/nacl-id               | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc     |
| DeleteRoute                | 路由表<br>arn:aws:ec2:region:account:route-table/*<br>arn:aws:ec2:region:account:route-table/route-table-id           | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc     |

| API 操作                     | 资源                                                                                                                                                     | 条件密钥                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeleteRouteTable           | 路由表<br><br>arn:aws:ec2:region:account:route-table/*<br><br>arn:aws:ec2:region:account:route-table/route-table-id                                       | ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:Vpc                                                                                                                                                                |
| DeleteSecurityGroup        | 安全组<br><br>arn:aws:ec2:region:account:security-group/security-group-id                                                                                 | ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:Vpc                                                                                                                                                                |
| DeleteVolume               | 卷<br><br>arn:aws:ec2:region:account:volume/*<br><br>arn:aws:ec2:region:account:volume/volume-id                                                        | ec2:AvailabilityZone<br><br>ec2:ParentSnapshot<br><br>ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:VolumeLops<br><br>ec2:VolumeSize<br><br>ec2:VolumeType                                                       |
| DeleteVpcPeeringConnection | VPC 对等连接<br><br>arn:aws:ec2:region:account:vpc-peering-connection/*<br><br>arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id | ec2:AcceptorVpc<br><br>ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:RequesterVpc                                                                                                                                |
| DetachClassicLinkVpc       | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/instance-id                                                 | ec2:AvailabilityZone<br><br>ec2:EbsOptimized<br><br>ec2:InstanceProfile<br><br>ec2:InstanceType<br><br>ec2:PlacementGroup<br><br>ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:RootDeviceType<br><br>ec2:Tenancy |
|                            | VPC<br><br>arn:aws:ec2:region:account:vpc/*<br><br>arn:aws:ec2:region:account:vpc/vpc-id                                                               | ec2:Region<br><br>ec2:ResourceTag/tag-key<br><br>ec2:Tenancy                                                                                                                                                            |

| API 操作                | 资源                                                                                                             | 条件密钥                                                                                                                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DetachVolume          | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i> | ec2:AvailabilityZone<br><br>ec2:EbsOptimized<br><br>ec2:InstanceProfile<br><br>ec2:InstanceType<br><br>ec2:PlacementGroup<br><br>ec2:Region<br><br>ec2:ResourceTag/ <i>tag-key</i><br><br>ec2:RootDeviceType<br><br>ec2:Tenancy |
|                       | 卷<br><br>arn:aws:ec2:region:account:volume/*<br><br>arn:aws:ec2:region:account:volume/ <i>volume-id</i>        | ec2:AvailabilityZone<br><br>ec2:ParentSnapshot<br><br>ec2:Region<br><br>ec2:ResourceTag/ <i>tag-key</i><br><br>ec2:Volumelops<br><br>ec2:VolumeSize<br><br>ec2:VolumeType                                                       |
| DisableVpcClassicLink | VPC<br><br>arn:aws:ec2:region:account:vpc/*<br><br>arn:aws:ec2:region:account:vpc/vpc- <i>id</i>               | ec2:Region<br><br>ec2:ResourceTag/ <i>tag-key</i><br><br>ec2:Tenancy                                                                                                                                                            |
| EnableVpcClassicLink  | VPC<br><br>arn:aws:ec2:region:account:vpc/*<br><br>arn:aws:ec2:region:account:vpc/vpc- <i>id</i>               | ec2:Region<br><br>ec2:ResourceTag/ <i>tag-key</i><br><br>ec2:Tenancy                                                                                                                                                            |

| API 操作                     | 资源                                                                                                                                                             | 条件密钥                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GetConsoleScreenshot       | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i>                                                 | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |
| RebootInstances            | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i>                                                 | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |
| RejectVpcPeeringConnection | VPC 对等连接<br><br>arn:aws:ec2:region:account:vpc-peering-connection/*<br><br>arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection- <i>id</i> | ec2:AcceptorVpc<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RequesterVpc                                                                                                            |
| RevokeSecurityGroupEgress  | 安全组<br><br>arn:aws:ec2:region:account:security-group/*<br><br>arn:aws:ec2:region:account:security-group/ <i>security-group-id</i>                              | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                                        |
| RevokeSecurityGroupIngress | 安全组<br><br>arn:aws:ec2:region:account:security-group/*<br><br>arn:aws:ec2:region:account:security-group/ <i>security-group-id</i>                              | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                                        |

| API 操作       | 资源                                                                                                                                                        | 条件密钥                                                                                                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RunInstances | 图片<br><br>arn:aws:ec2: <i>region</i> ::image/*<br><br>arn:aws:ec2: <i>region</i> ::image/ <i>image-id</i>                                                 | ec2:ImageType<br><br>ec2:Owner<br><br>ec2:Public<br><br>ec2:Region<br><br>ec2:RootDeviceType<br><br>ec2:ResourceTag/ <i>tag-key</i>                                                      |
|              | 实例<br><br>arn:aws:ec2: <i>region</i> :account:instance/*                                                                                                  | ec2:AvailabilityZone<br><br>ec2:EbsOptimized<br><br>ec2:InstanceProfile<br><br>ec2:InstanceType<br><br>ec2:PlacementGroup<br><br>ec2:Region<br><br>ec2:RootDeviceType<br><br>ec2:Tenancy |
|              | 密钥对<br><br>arn:aws:ec2: <i>region</i> :account:key-pair/*<br><br>arn:aws:ec2: <i>region</i> :account:key-pair/ <i>key-pair-name</i>                       | ec2:Region                                                                                                                                                                               |
|              | 网络接口<br><br>arn:aws:ec2: <i>region</i> :account:network-interface/*<br><br>arn:aws:ec2: <i>region</i> :account:network-interface/ <i>eni-id</i>           | ec2:AvailabilityZone<br><br>ec2:Region<br><br>ec2:Subnet<br><br>ec2:ResourceTag/ <i>tag-key</i><br><br>ec2:Vpc                                                                           |
|              | 置放群组<br><br>arn:aws:ec2: <i>region</i> :account:placement-group/*<br><br>arn:aws:ec2: <i>region</i> :account:placement-group/ <i>placement-group-name</i> | ec2:Region<br><br>ec2:PlacementGroupStrategy                                                                                                                                             |
| 安全组          | 安全组<br><br>arn:aws:ec2: <i>region</i> :account:security-group/*                                                                                           | ec2:Region<br><br>ec2:ResourceTag/ <i>tag-key</i>                                                                                                                                        |
|              | arn:aws:ec2: <i>region</i> :account:security-group/ <i>security-group-id</i>                                                                              | ec2:Vpc                                                                                                                                                                                  |

| API 操作         | 资源                                                                                                                       | 条件密钥                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | 快照<br>arn:aws:ec2: <i>region</i> ::snapshot/*<br>arn:aws:ec2: <i>region</i> ::snapshot/ <i>snapshot-id</i>               | ec2:Owner<br>ec2:ParentVolume<br>ec2:Region<br>ec2:SnapshotTime<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:VolumeSize                                                                            |
|                | 子网<br>arn:aws:ec2: <i>region</i> :account:subnet/*<br>arn:aws:ec2: <i>region</i> :account:subnet/ <i>subnet-id</i>       | ec2:AvailabilityZone<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                                |
|                | 卷<br>arn:aws:ec2: <i>region</i> :account:volume/*                                                                        | ec2:AvailabilityZone<br>ec2:ParentSnapshot<br>ec2:Region<br>ec2:VolumeLops<br>ec2:VolumeSize<br>ec2:VolumeType                                                                                  |
| StartInstances | 实例<br>arn:aws:ec2: <i>region</i> :account:instance/*<br>arn:aws:ec2: <i>region</i> :account:instance/ <i>instance-id</i> | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |

| API 操作             | 资源                                                                                                             | 条件密钥                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StopInstances      | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i> | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |
| TerminateInstances | 实例<br><br>arn:aws:ec2:region:account:instance/*<br><br>arn:aws:ec2:region:account:instance/ <i>instance-id</i> | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:RootDeviceType<br>ec2:Tenancy |

## RunInstances 的资源级别权限

[RunInstances](#) API 操作可启动一个或多个实例，并创建和使用许多 Amazon EC2 资源。该操作需要一个 AMI 并创建一个实例；该实例必须与安全组关联。启动到 VPC 中需要子网，会创建网络接口。从由 Amazon EBS 支持的 AMI 启动将创建卷。用户必须具有使用这些资源的权限，因此必须在使用 `ec2:RunInstances` 操作的资源级别权限的任何策略的 `Resource` 元素中指定它们。如果您不打算对 `ec2:RunInstances` 操作使用资源级别权限，则可以在您的语句（而不是单个 ARN）的 `Resource` 元素中指定 \* 通配符。

如果您使用的是资源级别权限，下表介绍了使用 `ec2:RunInstances` 操作所需的最少资源。

| 启动类型                            | 需要的资源                                                     | 条件密钥                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用实例存储支持的 AMI 启动到 EC2-Classic 中 | arn:aws:ec2:region:account:instance/*                     | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:Tenancy |
|                                 | arn:aws:ec2:region::image/* ( 或特定 AMI ID )                | ec2:ImageType<br>ec2:Owner<br>ec2:Public<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:ResourceTag/ <i>tag-key</i>                                              |
|                                 | arn:aws:ec2:region:account:security-group/* ( 或特定安全组 ID ) | ec2:Region<br>ec2:ResourceTag/ <i>tag-key</i><br>ec2:Vpc                                                                                                     |

| 启动类型                                                      | 需要的资源                                      | 条件密钥                                                                                                                                                         |
|-----------------------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用 Amazon EBS 支持的 AMI 启动到 EC2-Classic 中                   | arn:aws:ec2:region:account:instance/*      | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:Tenancy |
|                                                           | arn:aws:ec2:region::image/* ( 或特定 AMI ID ) | ec2:ImageType<br>ec2:Owner<br>ec2:Public<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:ResourceTag/tag-key                                                      |
| arn:aws:ec2:region:account:security-group/* ( 或特定安全组 ID ) |                                            | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                                                             |
|                                                           | arn:aws:ec2:region:account:volume/*        | ec2:AvailabilityZone<br>ec2:ParentSnapshot<br>ec2:Region<br>ec2:VolumeIops<br>ec2:VolumeSize<br>ec2:VolumeType                                               |

| 启动类型                    | 需要的资源                                                         | 条件密钥                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用实例存储支持的 AMI 启动到 VPC 中 | arn:aws:ec2:region:account:instance/*                         | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:Tenancy |
|                         | arn:aws:ec2:region::image/* ( 或特定 AMI ID )                    | ec2:ImageType<br>ec2:Owner<br>ec2:Public<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:ResourceTag/tag-key                                                      |
|                         | arn:aws:ec2:region:account:security-group/* ( 或特定安全组 ID )     | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                                                             |
|                         | arn:aws:ec2:region:account:network-interface/* ( 或特定网络接口 ID ) | ec2:AvailabilityZone<br>ec2:Region<br>ec2:Subnet<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                       |
|                         | arn:aws:ec2:region:account:subnet/* ( 或特定子网 ID )              | ec2:AvailabilityZone<br>ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                                     |

| 启动类型                                                          | 需要的资源                                      | 条件密钥                                                                                                                                                         |
|---------------------------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用 Amazon EBS 支持的 AMI 启动到 VPC 中                               | arn:aws:ec2:region:account:instance/*      | ec2:AvailabilityZone<br>ec2:EbsOptimized<br>ec2:InstanceProfile<br>ec2:InstanceType<br>ec2:PlacementGroup<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:Tenancy |
|                                                               | arn:aws:ec2:region::image/* ( 或特定 AMI ID ) | ec2:ImageType<br>ec2:Owner<br>ec2:Public<br>ec2:Region<br>ec2:RootDeviceType<br>ec2:ResourceTag/tag-key                                                      |
| arn:aws:ec2:region:account:security-group/* ( 或特定安全组 ID )     |                                            | ec2:Region<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                                                             |
| arn:aws:ec2:region:account:network-interface/* ( 或特定网络接口 ID ) |                                            | ec2:AvailabilityZone<br>ec2:Region<br>ec2:Subnet<br>ec2:ResourceTag/tag-key<br>ec2:Vpc                                                                       |
| arn:aws:ec2:region:account:volume/*                           |                                            | ec2:AvailabilityZone<br>ec2:ParentSnapshot<br>ec2:Region<br>ec2:Volumelops<br>ec2:VolumeSize<br>ec2:VolumeType                                               |
| arn:aws:ec2:region:account:subnet/* ( 或特定子网 ID )              |                                            |                                                                                                                                                              |

| 启动类型 | 需要的资源 | 条件密钥                            |
|------|-------|---------------------------------|
|      |       | ec2:AvailabilityZone            |
|      |       | ec2:Region                      |
|      |       | ec2:ResourceTag/ <i>tag-key</i> |
|      |       | ec2:Vpc                         |

建议您还在策略中指定密钥对资源 — 即使不需要启动实例，但没有密钥对，您也无法连接到实例。有关对 `ec2:RunInstances` 操作使用资源级别权限的示例，请参阅[4：启动实例 \(RunInstances\) \(p. 549\)](#)。

有关 Amazon EC2 中资源级权限的更多信息，请参阅发布的以下 AWS 安全博客：[揭秘 EC2 资源级权限](#)。

## 适用于 AWS CLI 或 AWS 开发工具包的策略示例

### Abstract

了解如何创建策略语句来控制 IAM 用户对 Amazon EC2 拥有的权限。

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。 \(p. 556\)](#)。有关特定于 Amazon VPC 的 IAM 策略示例，请参阅[控制对 Amazon VPC 资源的访问](#)

- 1：只读访问 (p. 546)
- 2：使用实例 (p. 547)
- 3：使用卷 (p. 548)
- 4：启动实例 (RunInstances) (p. 549)
- 5. 使用 ClassicLink (p. 553)
- 6. 预留实例的使用 (p. 555)

### Example 1：只读访问

以下策略授权用户使用名称以 `Describe` 开头的所有 Amazon EC2 API 操作。`Resource` 元素使用通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 \* 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅[Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。

用户无权对资源执行任何操作（除非其他语句向用户授予执行此操作的权限），因为在默认情况下会对用户拒绝使用 API 操作的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:Describe*",
 "Resource": "*"
 }
]
}
```

## Example 2：使用实例

### a. 描述、启动、停止和终止所有实例

以下策略授权用户使用 Action 元素中指定的 API 操作。Resource 元素使用 \* 通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 \* 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。

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": "*"
 }
]
}
```

### b. 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 (cn-north-1) 中具有“purpose=test”资源标签的实例。

第一条语句为 Resource 元素使用 \* 通配符，以指示用户可以对操作指定所有资源；在本例中，用户可以列出所有实例。在 API 操作不支持资源级权限的情况下（在此情况下，为 ec2:DescribeInstances），也需要 \* 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。

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 (cn-north-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:cn-north-1:1234567890abcdef0:instance/i-0598c7d356eba48d7"
 }
]
}
```

```
],
"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"
 }
 }
}
]
```

### Example 3：使用卷

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:cn-north-1:123456789012:instance/*",
 "Condition": {
 "StringEquals": {
 "ec2:ResourceTag/department": "dev"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AttachVolume",
 "ec2:DetachVolume"
],
 "Resource": "arn:aws:ec2:cn-north-1:123456789012:volume/*",
 "Condition": {
 "StringEquals": {
 "ec2:ResourceTag/volume_user": "${aws:username}"
 }
 }
 }
]
}
```

```
 }
]
}
```

#### Example 4：启动实例 (RunInstances)

[RunInstances](#) API 操作启动一个或多个实例。RunInstances 需要一个 AMI 并创建实例；用户可以在请求中指定密钥对和安全组。启动到 EC2-VPC 中需要子网，会创建网络接口。从由 Amazon EBS 支持的 AMI 启动将创建卷。因此，用户必须拥有使用这些 Amazon EC2 资源的权限。发起人还可以使用 RunInstances 的可选参数配置实例，例如实例类型和子网。您可以创建要求用户指定可选参数或限制用户针对某个参数使用特定值的策略语句。本部分的示例展示了许多可能方法中的一部分，您可使用这些方法控制用户能够启动的实例的配置。

请注意，在默认情况下，用户没有描述、启动、停止或终止所生成实例的权限。授予用户管理所生成实例的权限的一种方法是：为每个实例创建一个特定标签，然后创建一个允许用户使用该标签管理实例的语句。有关更多信息，请参阅 [2：使用实例 \(p. 547\)](#)。

##### a. AMI

以下策略仅允许用户使用拥有与之关联的指定标签“department=dev”的 AMI 启动实例。用户无法使用其他 AMI 启动实例，因为第一条语句的 Condition 元素要求用户指定带有此标签的 AMI。用户也不能启动到子网中，因为该策略未授予子网和网络接口资源的权限。但是，用户可以启动到 EC2-Classic 中。第二条语句会使用通配符来允许用户创建实例资源，并要求用户指定密钥对 project\_keypair 和安全组 sg-1a2b3c4d。用户仍能够在没有密钥对的情况下启动实例。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region::image/ami-*"
],
 "Condition": {
 "StringEquals": {
 "ec2:ResourceTag/department": "dev"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:key-pair/project_keypair",
 "arn:aws:ec2:region:account:security-group/sg-1a2b3c4d"
]
 }
]
}
```

或者，以下策略仅允许用户使用指定的 AMI、ami-9e1670f7 和 ami-45cf5c3c 启动实例。用户无法使用其他 AMI 启动实例（除非其他语句授予执行此操作的用户权限），并且用户无法将实例启动到子网中。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region::image/ami-9e1670f7",
 "arn:aws:ec2:region::image/ami-45cf5c3c",
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:key-pair/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

另外，以下策略还允许用户从 Amazon 拥有的所有 AMI 启动实例。第一个语句的 Condition 元素测试 ec2:Owner 是不是 amazon。用户无法使用其他 AMI 启动实例（除非其他语句允许用户执行此操作）。用户能够将实例启动到子网中。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region::image/ami-*"
],
 "Condition": {
 "StringEquals": {
 "ec2:Owner": "amazon"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:subnet/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:network-interface/*",
 "arn:aws:ec2:region:account:key-pair/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

## b. 实例类型

以下策略仅允许用户使用 t2.micro 或 t2.small 实例类型启动实例，您也可以通过此操作控制成本。用户无法启动更大的实例，因为第一条语句的 Condition 元素会测试 ec2:InstanceType 是否是 t2.micro 或 t2.small。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:instance/*"
],
 "Condition": {
 "StringEquals": {
 "ec2:InstanceType": ["t2.micro", "t2.small"]
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region::image/ami-*",
 "arn:aws:ec2:region:account:subnet/*",
 "arn:aws:ec2:region:account:network-interface/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:key-pair/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

或者，您可以创建一个策略，对用户拒绝启动除 t2.micro 和 t2.small 实例类型之外的任何实例的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:instance/*"
],
 "Condition": {
 "StringNotEquals": {
 "ec2:InstanceType": ["t2.micro", "t2.small"]
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region::image/ami-*",
 "arn:aws:ec2:region:account:network-interface/*",
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:subnet/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:key-pair/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

```
]
 }
}
```

### c. 子网

以下策略仅允许用户使用指定子网 subnet-12345678 启动实例。组无法将实例启动到任何其他子网中（除非其他语句授予执行此操作的用户权限）。用户仍能够将实例启动到 EC2-Classic 中。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:subnet/subnet-12345678",
 "arn:aws:ec2:region:account:network-interface/*",
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:image/ami-*",
 "arn:aws:ec2:region:account:key-pair/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

或者，您可以创建一个策略，拒绝用户将实例启动到任何其他子网。该语句通过拒绝创建网络接口的权限来执行此操作，除非指定了子网 subnet-12345678。此拒绝会覆盖创建的任何其他策略以允许将实例启动到其他子网中。用户仍能够将实例启动到 EC2-Classic 中。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:account:network-interface/*"
],
 "Condition": {
 "ArnNotEquals": {
 "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:region:image/ami-*",
 "arn:aws:ec2:region:account:network-interface/*",
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:subnet/*",
 "arn:aws:ec2:region:account:volume/*",
 "arn:aws:ec2:region:account:key-pair/*",

```

```
 "arn:aws:ec2:region:account:security-group/*"
]
}
]
```

#### Example 5. 使用 ClassicLink

您可以为 VPC 启用 ClassicLink，然后将 EC2-Classic 实例链接到 VPC。您还可以查看启用了 ClassicLink 的 VPC 和所有链接到 VPC 的 EC2-Classic 实例。可以为 `ec2:EnableVpcClassicLink`、`ec2:DisableVpcClassicLink`、`ec2:AttachClassicLinkVpc` 和 `ec2:DetachClassicLinkVpc` 操作创建包含资源级权限的策略，以控制用户对这些操作的使用。`ec2:Describe*` 操作不支持资源级权限。

##### a. 使用 ClassicLink 的完全权限

以下策略授予用户以下权限：查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例，为 VPC 启用和禁用 ClassicLink，以及从启用了 ClassicLink 的 VPC 链接实例和取消与实例的链接。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeClassicLinkInstances", "ec2:DescribeVpcClassicLink",
 "ec2:EnableVpcClassicLink", "ec2:DisableVpcClassicLink",
 "ec2:AttachClassicLinkVpc", "ec2:DetachClassicLinkVpc"
],
 "Resource": "*"
 }
]
}
```

##### b. 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"
 }
 }
 }
]
}
```

##### c. 链接实例

以下策略向用户授予仅将 m3.large 类型的实例链接到 VPC 的权限。第二条语句允许用户使用 VPC 以及将实例链接到 VPC 所需的安全组资源。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:AttachClassicLinkVpc",
 "Resource": "arn:aws:ec2:region:account:instance/*",
 "Condition": {
 "StringEquals": {
 "ec2:InstanceType": "m3.large"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:AttachClassicLinkVpc",
 "Resource": [
 "arn:aws:ec2:region:account:vpc/*",
 "arn:aws:ec2:region:account:security-group/*"
]
 }
]
}
```

以下策略向用户授予权限，以仅允许用户将实例链接到特定 VPC (vpc-1a2b3c4d) 以及仅将 VPC 中的特定安全组与实例 ( sg-1122aabb 和 sg-aabb2233 ) 关联。用户不能将实例链接到任何其他 VPC，因此他们不能在请求中指定任何 VPC 其他安全组与实例关联。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:AttachClassicLinkVpc",
 "Resource": [
 "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",
 "arn:aws:ec2:region:account:instance/*",
 "arn:aws:ec2:region:account:security-group/sg-1122aabb",
 "arn:aws:ec2:region:account:security-group/sg-aabb2233"
]
 }
]
}
```

#### d. 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。第二条语句向用户授予权限以使用从 VPC 取消链接实例所需的 VPC 资源。

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

```
"Action": "ec2:DetachClassicLinkVpc",
"Resource": [
 "arn:aws:ec2:region:account:instance/*"
],
"Condition": {
 "StringEquals": {
 "ec2:ResourceTag/unlink": "true"
 }
}
{
 "Effect": "Allow",
 "Action": "ec2:DetachClassicLinkVpc",
 "Resource": [
 "arn:aws:ec2:region:account:vpc/*"
]
}
]
```

#### Example 6. 预留实例的使用

以下策略授予用户在您账户内查看、修改和购买预留实例的许可。

无法为单个预留实例设置资源级别的许可。此策略表示用户可以访问账户中的所有预留实例。

Resource元素使用的 \* 通配符可用于指示用户可以通过操作指定所有资源；在此情况下，他们可以列出并修改账户中的所有预留实例。他们也可以使用账户凭证购买预留实例。在 API 操作不支持资源级权限的情况下，也需要 \* 通配符。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
 "ec2:PurchaseReservedInstancesOffering", "ec2:DescribeAvailabilityZones",
 "ec2:DescribeReservedInstancesOfferings"
],
 "Resource": "*"
 }
]
}
```

允许用户查看和修改您账户中的预留实例，但是不能购买新的预留实例。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
 "ec2:DescribeAvailabilityZones"
],
 "Resource": "*"
 }
]
}
```



## 用于 Amazon EC2 控制台的策略示例。

### Abstract

了解如何向 IAM 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 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。

- 1 : 只读访问 (p. 557)
- 2 : 使用 EC2 启动向导 (p. 558)
- 3 : 使用卷 (p. 561)
- 4 : 使用安全组 (p. 562)
- 5 : 使用弹性 IP 地址 (p. 564)
- 6. 预留实例的使用 (p. 565)



### Note

为帮助您了解在控制台中执行任务所需的相应 API 操作，您可以使用 AWS CloudTrail 等服务。有关更多信息，请参阅 [AWS CloudTrail User Guide](#)。如果您的策略不授予创建或修改特定资源的权限，则控制台显示一个包含诊断信息的编码消息。您可以使用适用于 AWS STS 的 `DecodeAuthorizationMessage` API 操作或 AWS CLI 中的 `decode-authorization-message` 命令对该消息解码。

有关创建 Amazon EC2 控制台的策略的更多信息，请参阅发布的以下 AWS 安全博客：[授予用户在 Amazon EC2 控制台中工作的权限](#)。

### Example 1：只读访问

要允许用户在 Amazon EC2 控制台中查看所有资源，您可以使用与以下示例相同的策略：[1：只读访问 \(p. 546\)](#) 用户无法对这些资源执行任何操作或创建新资源（除非其他语句向用户授予执行此操作的权限）。

#### a. 查看实例、AMI 和快照

或者，您可以提供对资源子集的只读访问权限。为此，请对每个资源将 ec2:Describe API 操作中的 \* 通配符替换为特定 ec2:Describe 操作。以下策略允许用户在 Amazon EC2 控制台中查看所有实例、AMI 和快照。ec2:DescribeTags 操作允许用户查看公用 AMI。控制台需要标记信息来显示公用 AMI；但是，如果您只希望用户查看私有 AMI，则可以删除此操作。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeInstances", "ec2:DescribeImages",
 "ec2:DescribeTags", "ec2:DescribeSnapshots"
],
 "Resource": "*"
 }
]
}
```



#### Note

当前，Amazon EC2 ec2:Describe\* API 操作不支持资源级权限，因此您无法控制用户可以在控制台中查看的单个资源。因此，在以上语句的 Resource 元素中需要 \* 通配符。想要了解更多有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用的信息，请参阅 [Amazon EC2 API 操作支持的资源级权限 \(p. 532\)](#)。

#### b. 查看实例和 CloudWatch 指标

以下策略允许用户在 Amazon EC2 控制台中查看实例，以及在 Instances 页面的 Monitoring 选项卡中查看 CloudWatch 警报和指标。Amazon EC2 控制台使用 CloudWatch API 显示警报和指标，因此您必须向用户授予对 cloudwatch:DescribeAlarms 和 cloudwatch:GetMetricStatistics 操作的使用权。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeInstances",
 "cloudwatch:DescribeAlarms",
 "cloudwatch:GetMetricStatistics"
],
 "Resource": "*"
 }
]
}
```

## Example 2：使用 EC2 启动向导

Amazon EC2 启动向导是一系列屏幕，其中包含用于配置和启动实例的选项。您的策略必须包含允许用户使用向导选项的 API 操作使用权限。如果您的策略不包含使用这些操作的权限，则向导中的一些项目无法正确加载，用户无法完成启动。

### a. 基本启动向导访问

要成功完成启动，必须向用户授予使用 `ec2:RunInstances` API 操作以及至少以下 API 操作的权限：

- `ec2:DescribeImages`：查看并选择 AMI。
- `ec2:DescribeVPCs`：查看可用网络选项，即 EC2-Classic 和 VPC 列表。即使您不在 VPC 中启动也需要此操作。
- `ec2:DescribeSubnets`：如果在 VPC 中启动，请查看所选 VPC 的所有可用子网。
- `ec2:DescribeSecurityGroups`：查看向导中的安全组页面。用户可以选择现有安全组。
- `ec2:DescribeKeyPairs` 或 `ec2>CreateKeyPair`：选择现有密钥对或创建新密钥对。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeInstances", "ec2:DescribeImages",
 "ec2:DescribeKeyPairs", "ec2:DescribeVpc", "ec2:DescribeSubnets",
 "ec2:DescribeSecurityGroups"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": "*"
 }
]
```

您可以向策略添加 API 操作以便为用户提供更多选项，例如：

- `ec2:DescribeAvailabilityZones`：如果启动到 EC2-Classic，请查看并选择特定可用区。
- `ec2:DescribeNetworkInterfaces`：如果启动到 VPC，请查看并选择所选子网的现有网络接口。
- `ec2:CreateSecurityGroup` 创建新安全组；如创建向导推荐的 `launch-wizard-x` 安全组。但是，此操作仅单独创建安全组；不添加或修改任何规则。要添加入站规则，必须向用户授予使用 `ec2:AuthorizeSecurityGroupIngress` API 操作的权限。要向 VPC 安全组添加出站规则，必须向用户授予使用 `ec2:AuthorizeSecurityGroupEgress` API 操作的权限。要修改或删除现有规则，必须向用户授予使用相关 `ec2:RevokeSecurityGroup*` API 操作的权限。
- `ec2:CreateTags`：将标签添加到实例。默认情况下，启动向导尝试向实例添加一个键为 `Name` 的标签。无权使用此操作的用户会遇到一个警告，提示此标签不能应用于实例；但是，这不影响启动的成功，因此仅当绝对必要时，您才应向用户授予使用此操作的权限。



### Important

向用户授予使用 `ec2:CreateTags` 操作的权限时请小心谨慎。这会限制您使用 `ec2:ResourceTag` 条件密钥限制其他资源的使用的能力；用户可以更改资源的标签以便绕过这些限制。

当前，Amazon EC2 `Describe*` API 操作不支持资源级权限，因此您无法限制用户可以在启动向导中查看的单个资源。但是，您可以对 `ec2:RunInstances` API 操作应用资源级权限，以限制用户可以用于启动实例的资源。如果用户选择未授权他们使用的选项，则启动会失败。

b. 限制对特定实例类型、子网和区域的访问

以下策略允许用户使用 Amazon 拥有的 AMI 启动 `m1.small` 实例，并且仅在特定子网 (`subnet-1a2b3c4d`) 中启动。用户只能在 `sa-east-1` 区域中启动。如果用户在启动向导中选择不同区域或选择不同实例类型、AMI 或子网，则启动会失败。

第一条语句向用户授予查看启动向导中的选项的权限，如上例所示。第二条语句向用户授予将网络接口、卷、密钥对、安全组和子网资源（在 VPC 中启动实例需要这些资源）用于 `ec2:RunInstances` 操作的权限。有关使用 `ec2:RunInstances` 操作的更多信息，请参阅 [4：启动实例 \(RunInstances\) \(p. 549\)](#)。第三和第四条语句分别向用户授予使用实例（仅当实例是 `m1.small` 实例时）和 AMI 资源（仅当 AMI 由 Amazon 所有时）的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeInstances", "ec2:DescribeImages",
 "ec2:DescribeKeyPairs", "ec2:DescribeVpcs", "ec2:DescribeSubnets",
 "ec2:DescribeSecurityGroups"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
 "arn:aws:ec2:sa-east-1:111122223333:volume/*",
 "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
 "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
 "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
]
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:sa-east-1:111122223333:instance/*"
],
 "Condition": {
 "StringEquals": {
 "ec2:InstanceType": "m1.small"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": "ec2:RunInstances",
 "Resource": [
 "arn:aws:ec2:sa-east-1::image/ami-*"
],
 "Condition": {
 "StringEquals": {
 "ec2:Owner": "amazon"
 }
 }
 }
]
}
```

### Example 3：使用卷

以下策略向用户授予查看和创建卷以及将卷与特定实例连接和断开的权限。

用户可以将任何卷连接到具有标签“purpose=test”的实例，也可以从这些实例断开卷。要使用 Amazon EC2 控制台连接卷，用户有权使用 `ec2:DescribeInstances` 操作会很有帮助，因为这可以让他们从 Attach Volume (连接卷) 对话框的预填充列表中选择实例。但是，这也会允许用户在控制台的 Instances 页面上查看所有实例，因此，您可以省略此操作。

在第一条语句中，需要 `ec2:DescribeVolumeStatus` 和 `ec2:DescribeAvailabilityZones` 操作以确保卷在控制台中正确显示。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeVolumes", "ec2:DescribeVolumeStatus",
 "ec2:DescribeAvailabilityZones", "ec2>CreateVolume",
 "ec2:DescribeInstances"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AttachVolume",
 "ec2:DetachVolume"
],
 "Resource": "arn:aws:ec2:region:111122223333:instance/*",
 "Condition": {
 "StringEquals": {
 "ec2:ResourceTag/purpose": "test"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AttachVolume",
 "ec2:DetachVolume"
],
 "Resource": "arn:aws:ec2:region:111122223333:volume/*"
 }
]
```

#### Example 4：使用安全组

##### a. 查看安全组以及添加和删除规则

以下策略为用户授予的权限可在 Amazon EC2 控制台中查看安全组，并为具有标签 Department=Test 的现有安全组添加和删除入站和出站规则。



##### Note

您无法为 EC2-Classic 安全组修改出站规则。有关安全组的更多信息，请参阅 [Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。

在第一条语句中，`ec2:DescribeTags` 操作允许用户在控制台中查看标签，这样，用户更易于识别自己可修改的安全组。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeSecurityGroups", "ec2:DescribeTags"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",
 "ec2:AuthorizeSecurityGroupEgress", "ec2:RevokeSecurityGroupEgress"
],
 "Resource": [
 "arn:aws:ec2:region:111122223333:security-group/*"
],
 "Condition": {
 "StringEquals": {
 "ec2:ResourceTag/Department": "Test"
 }
 }
 }
]
```

##### b. 使用 Create Security Group 对话框

您可以创建一个策略，以允许用户使用 Amazon EC2 控制台中的 Create Security Group (创建安全组) 对话框。要使用此对话框，必须向用户授予使用至少以下 API 操作的权限：

- `ec2:CreateSecurityGroup`: 创建新安全组。
- `ec2:DescribeVpcs` 查看 VPC 列表中的现有 VPC 列表。即使您不为 VPC 创建安全组，也需要此操作。

借助这些权限，用户可以成功创建新安全组，但是他们不能向其中添加任何规则。要在 Create Security Group (创建安全组) 对话框中使用规则，您可以向策略添加以下 API 操作：

- `ec2:AuthorizeSecurityGroupIngress`：添加入站规则。

- `ec2:AuthorizeSecurityGroupEgress`：向 VPC 安全组添加出站规则。
- `ec2:RevokeSecurityGroupIngress`：修改或删除现有入站规则。如果您要允许用户使用控制台中的 `Copy to new` (复制到新项目) 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。如果用户创建的安全组具有无效规则，则控制台首先创建该安全组，然后尝试向其中添加规则。失败之后，会删除安全组。用户停留在 `Create Security Group` (创建安全组) 对话框中，其中会显示一个错误。规则仍会列出，因此用户可以更正无效规则并尝试再次创建安全组。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，用户更容易识别自己可添加入站规则的安全组。此策略还向用户授予删除与 VPC `vpc-1a2b3c4d` 关联的安全组的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeSecurityGroups", "ec2:CreateSecurityGroup", "ec2:De
 scribeVpcs"
],
 "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"
 }
 }
 }
]
```

#### Example 5：使用弹性 IP 地址

以下策略授予用户在 Amazon EC2 控制台中查看弹性 IP 地址的权限。该控制台使用 `ec2:DescribeInstances` 操作，来显示与弹性 IP 地址关联实例的相关信息。如果用户未获得使用该操作的权限，则弹性 IP 地址页面无法正确加载。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeAddresses", "ec2:DescribeInstances"
],
 "Resource": "*"
 }]
}
```

要允许用户使用弹性 IP 地址，可将以下操作添加到您策略中

- `ec2:AllocateAddress`：分配可在 VPC 或 EC2-Classic 中使用的地址。
- `ec2:ReleaseAddress`：解除弹性 IP 地址。
- `ec2:DescribeNetworkInterfaces`：使用 Associate Address (关联地址) 对话框。该对话框显示可将弹性 IP 地址关联到的可用网络接口，如果未授予用户使用此操作的权限，则该对话框不会打开。但这仅适用于 EC2-VPC；对于将弹性 IP 地址关联到 EC2-Classic 中的实例，无需执行此操作。
- `ec2:AssociateAddress`：将弹性 IP 地址与实例或网络接口关联。
- `ec2:DisassociateAddress`：取消弹性 IP 地址与实例或网络接口的关联，

### Example 6. 预留实例的使用

以下策略可以附加到 IAM 用户。它可让用户查看和修改您账户中的预留实例，同时也能在 AWS 管理控制台内购买新的预留实例。

该策略允许用户查看账户内的所有预留实例和按需实例。无法为单个预留实例设置资源级别的许可。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:DescribeReservedInstances", "ec2:ModifyReservedInstances",
 "ec2:PurchaseReservedInstancesOffering", "ec2:DescribeInstances",
 "ec2:DescribeAvailabilityZones", "ec2:DescribeReservedInstancesOfferings"
],
 "Resource": "*"
 }
]
}
```

必须进行 ec2:DescribeAvailabilityZones 操作才能确保 Amazon EC2 控制台可以显示有关您能够购买预留实例的可用区的信息。ec2:DescribeInstances 操作不是必须的，但是请确保用户可查看账户内的实例并且能够购买预留实例，以匹配正确的规格。

您可以调整 API 操作，以限制用户访问，例如移除 ec2:DescribeInstances，而 ec2:DescribeAvailabilityZones 表示用户有只读形式的访问权。

## 适用于 Amazon EC2 的 IAM 角色

### Abstract

通过创建 IAM 角色并将它们分配给 EC2 实例，允许应用程序发出安全的 API 请求。

应用程序必须通过 AWS 证书签署 API 请求。因此，如果您是应用程序开发人员，您需要一个策略来为 EC2 实例上运行的应用程序管理证书。例如，您可以安全地将您的 AWS 证书分配至实例，从而允许这些实例上运行的应用程序使用您的证书签署请求，并保护其免受其他用户的影响。但是，要将凭证安全地分配至每项实例有一定难度，尤其是 AWS 以您的名义创建的实例，例如竞价型实例或 Auto Scaling 组中的实例。当您更换 AWS 证书时，您还必须能够更新每项实例上的证书。

我们设计了 IAM 角色，以便您的应用程序能够安全地从实例发出 API 请求，而无需管理应用程序使用的安全证书。您可以使用 IAM 角色委托授权以发出 API 请求，而不用创建并分配您的 AWS 证书，如下所示：

1. 创建一个 IAM 角色。
2. 定义能够担任此角色的账户或 AWS 服务。
3. 定义担任角色后应用程序可以使用的 API 操作和资源。
4. 当您启动您的实例时，指定该角色。
5. 让应用程序检索一组临时证书并使用它们。

例如，您可以使用 IAM 角色为在实例上运行的应用程序授予使用 Amazon S3 中的存储桶的权限。



### Note

Amazon EC2 使用实例配置文件作为 IAM 角色的容器。使用控制台创建 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 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。要启动带有 IAM 角色的实例，请指定其实例配置文件的名称。使用 Amazon EC2 控制台启动实例时，您可以选择角色与实例关联；但是，显示的列表实际上是实例配置文件名称的列表。有关更多信息，请参阅 [IAM 用户指南 中的实例配置文件](#)。

您可以通过创建 JSON 格式的策略为 IAM 角色指定权限。这些类似于您为 IAM 用户创建的策略。如果您对某个角色进行了更改，系统会将此更改传播到所有实例，从而简化证书管理。



### Note

您不将角色分配给现有实例；只能在启动新实例时指定角色。

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](#)。

#### 主题

- [通过实例元数据检索安全证书 \(p. 566\)](#)
- [允许 IAM 用户启动带有 IAM 角色的实例 \(p. 567\)](#)
- [使用控制台创建 IAM 角色 \(p. 567\)](#)
- [使用控制台启动带有 IAM 角色的实例 \(p. 568\)](#)
- [使用 AWS CLI 创建 IAM 角色 \(p. 568\)](#)
- [使用 AWS CLI 通过 IAM 角色启动实例 \(p. 570\)](#)

## 通过实例元数据检索安全证书

实例上的应用程序通过实例元数据条目 `iam/security-credentials/role-name` 检索角色提供的安全证书。该应用程序具有使用您通过与角色关联的安全证书为其定义的操作和资源的权限。这些安全证书是临时的，我们会自动更换它们。我们在旧证书过期前至少五分钟提供可用的新证书。



### Warning

如果您使用的服务采用了带有 IAM 角色的实例元数据，请确保服务代表您进行 HTTP 调用时不会泄露您的证书。可能泄露您的证书的服务类型包括 HTTP 代理、HTML/CSS 验证程序服务和支持 XML 包含的 XML 处理程序。

以下命令检索名为 `s3access` 的 IAM 角色的安全证书。

```
C:\> curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

以下为输出示例。

{

```
"Code" : "Success",
"LastUpdated" : "2012-04-26T16:39:16Z",
"Type" : "AWS-HMAC",
"AccessKeyId" : "AKIAIOSFODNN7EXAMPLE",
"SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY",
"Token" : "token",
```

```
{ "Expiration" : "2012-04-27T22:39:16Z"
```

对于实例上运行的应用程序、AWS CLI 和 Windows PowerShell 工具 命令，您不必显式获取临时安全凭证 - AWS 软件开发工具包、AWS CLI 和 Windows PowerShell 工具 会自动从 EC2 实例元数据服务获取凭证并使用这些凭证。要使用临时安全凭证在实例外部发出调用（例如，为了测试 IAM 策略），您必须提供访问密钥、私有密钥和会话令牌。有关更多信息，请参阅 *IAM 用户指南* 中的[使用临时安全凭证以请求对 AWS 资源的访问权限](#)。

有关实例元数据的更多信息，请参阅 [实例元数据和用户数据 \(p. 239\)](#)。

## 允许 IAM 用户启动带有 IAM 角色的实例

要允许 IAM 用户启动带有 IAM 角色的实例，您必须授权用户将角色传递到实例。

例如，以下 IAM 策略将授权用户启动带有名为 s3access 的 IAM 角色的实例。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::123456789012:role/s3access"
 }
]
}
```

或者，您可以在策略中指定资源为“\*”，以授权 IAM 用户访问所有角色。但是，要考虑启动带有您的角色（现有的或您即将创建的）的实例的用户是否会被授予不需要或不应该有的权限。

有关更多信息，请参阅 *IAM 用户指南* 中的[在 Amazon EC2 中使用角色所需的权限](#)。

## 使用控制台创建 IAM 角色

您必须先创建一个 IAM 角色，才能启动带有该角色的实例。

### 使用 IAM 控制台创建 IAM 角色

1. 登录到 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
2. 在导航窗格中选择 Roles，然后选择 Create New Role。
3. 在 Set Role Name 页面上，输入角色的名称，然后选择 Next Step。
4. 在 Select Role Type 页面上，选择 Amazon EC2 旁的 Select。
5. 在 Attach Policy 页面上，选择 AWS 管理的策略。例如，对于 Amazon EC2，下列 AWS 管理的策略之一可能符合您的需求：
  - PowerUserAccess
  - ReadOnlyAccess
  - AmazonEC2FullAccess
  - AmazonEC2ReadOnlyAccess
6. 检查角色信息，根据需要编辑角色，然后选择 Create Role。

## 使用控制台启动带有 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

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 选择 AMI，然后选择实例类型并选择 Next: Configure Instance Details。
4. 在 Configure Instance Details 页面上，从 IAM role 列表中选择您创建的 IAM 角色。



### Note

IAM role (IAM 角色) 列表显示您在创建 IAM 角色时创建的实例配置文件的名称。如果您是使用控制台创建的 IAM 角色，则为您创建了实例配置文件，并提供了与角色相同的名称。如果使用 AWS CLI、API 或 AWS 开发工具包创建了 IAM 角色，则可能对实例配置指定了不同名称。

5. 配置其他详细信息，然后按照向导的其余说明操作，或选择 Review and Launch 接受默认设置并直接转到 Review Instance Launch 页面。
6. 检查设置，然后选择 Launch 以选择密钥对并启动实例。
7. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 AWS 安全证书，并使用它们签署请求。请注意，此操作由 AWS 开发工具包为您执行。

```
C:\> curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

## 使用 AWS CLI 创建 IAM 角色

您必须先创建一个 IAM 角色，才能启动带有该角色的实例。

### 使用 AWS CLI 创建 IAM 角色

- 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。

```
C:\> aws iam create-role --role-name s3access --assume-role-policy-document file://ec2-role-trust-policy.json
{
 "Role": {
 "AssumeRolePolicyDocument": {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "sts:AssumeRole",
 "Effect": "Allow",
 "Principal": {
 "Service": "ec2.amazonaws.com"
 }
 }
]
 },
 "RoleId": "AROAIIZKPBKS2LEXAMPLE",
 "CreateDate": "2013-12-12T23:46:37.247Z",
 "RoleName": "s3access",
 "Path": "/",
 "Arn": "arn:aws:iam::123456789012:role/s3access"
 }
}
```

- c. 创建访问策略并将其保存在名为 ec2-role-access-policy.json 的文本文件中。例如，此策略向在实例上运行的应用程序授予针对 Amazon S3 管理员权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["s3:*"],
 "Resource": ["*"]
 }
]
}
```

- d. 向角色附加访问策略。

```
C:\> 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。

```
C:\> 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。

```
C:\> aws iam add-role-to-instance-profile --instance-profile-name s3ac-
cess-profile --role-name s3access
```

想要了解更多有关这些命令的信息，请参阅 *AWS Command Line Interface Reference* 中的 [create-role](#)、[put-role-policy](#) 和 [create-instance-profile](#)。

## 使用 AWS CLI 通过 IAM 角色启动实例

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](#)。

### 使用 AWS CLI 启动带有 IAM 角色的实例

1. 使用实例配置文件启动实例。以下示例演示如何使用实例配置启动实例。

```
C:\> 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
```

想要了解更多有关信息，请参阅 *AWS Command Line Interface Reference* 中的 [run-instances](#)。

2. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 AWS 安全证书，并使用它们签署请求。请注意，此操作由 AWS 开发工具包为您执行。

```
C:\> curl http://169.254.169.254/latest/meta-data/iam/security-creden-
tials/role_name
```

## 为您的 Windows 实例授权入站流量

### Abstract

创建安全组以控制可以到达 Amazon EC2 实例的网络流量。

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 RDP 访问您的实例。如果您的实例为 Web 服务器，那么您可以允许所有 IP 地址通过 HTTP 访问您的实例，以便外部用户能够浏览您的 Web 服务器上的内容。

若要启用对实例的网络访问，您必须允许该实例的入站流量。要为入站流量打开端口，您需要在启动实例时向与实例关联的安全组添加规则。

要连接到您的实例，您必须设置规则以向来自您计算机的公有 IP 地址的 RDP 流量授权。若要允许来自其他 IP 地址范围的 RDP 流量，请为需要授权的每个范围另外添加规则。

如果您需要启用对 Linux 实例的网络访问，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的[为 Linux 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。在这种情况下，我们会使用您本地系统的公有 IP 地址。您可以通过一项服务来获取本地计算机的公有 IP 地址。例如，我们提供以下服务：<http://checkip.amazonaws.com>。要查找另一项可提供您的 IP 地址的服务，请使用搜索短语“what is my IP address”。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。



### Caution

如果使用 0.0.0.0/0，则可以允许所有 IP 地址使用 RDP 访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产中，您将仅授权特定 IP 地址或地址范围访问您的实例。

有关安全组的更多信息，请参阅 [Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。

## 针对发送到 Windows 实例的入站 RDP 流量添加规则

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须在安全组中添加规则，以便能够使用 RDP 从您的 IP 地址连接到 Windows 实例。

### 使用控制台在安全组中为入站 RDP 流量添加规则

1. 在 Amazon EC2 控制台的导航窗格中，选择 Instances。选择实例并查看 Description (描述) 选项卡；Security groups (安全组) 列出了与该实例关联的安全组。选择 view rules，以显示对实例生效的规则列表。
2. 在导航窗格中，选择 Security Groups。选择与您的实例相关联的一个 安全组。
3. 在详细信息窗格中的 Inbound 选项卡上，选择 Edit。在对话框中，选择 Add Rule，然后从 Type 列表中选择 RDP。
4. 在 Source (源) 字段中，用 CIDR 表示法指定您计算机的公有 IP 地址。例如，如果您的 IP 地址为 203.0.113.25，请指定 203.0.113.25/32，以便用 CIDR 表示法列出此 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 203.0.113.0/24。

有关查找 IP 地址的信息，请参阅[在您开始之前 \(p. 571\)](#)。

5. 选择 Save。

### 使用命令行向安全组添加规则

您可以使用以下任一命令。请确保此命令在您的本地系统中运行，而不是针对实例本身。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [authorize-security-group-ingress \(AWS CLI\)](#)
- [Grant-EC2SecurityGroupIngress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 向实例分配安全组

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。在 VPC 中启动实例后，您可以更改其安全组。想要了解更多有关信息，请参阅 [Amazon VPC 用户指南中的更改实例的安全组主题](#)。

# Amazon EC2 和 Amazon Virtual Private Cloud

## Abstract

在 VPC 中启动您的 EC2 实例，获取实例的高级功能。

通过 Amazon Virtual Private Cloud (Amazon VPC)，您可以在 AWS 云内您自己的逻辑隔离区域中定义虚拟网络，我们称之为 *Virtual Private Cloud (VPC)*。您可将 AWS 资源（如实例）启动到 VPC 中。您的 VPC 与您可能在自己的数据中心运行的传统网络极其相似，但同时可为您提供利用 AWS 的可扩展基础设施的优势。您可以配置您的 VPC；您可以选择它的 IP 地址范围、创建子网并配置路由表、网关和安全设置。现在您可以将您的 VPC 中的实例连接到 Internet。您可以将 VPC 连接到自己的企业数据中心，利用 AWS 云扩展您的数据中心。要保护各个子网中的资源，您可以利用多种安全层，包括安全组和网络访问控制列表。有关更多信息，请参阅 [Amazon VPC 用户指南](#)。

根据各区域的不同条件，您的账户可能同时支持 EC2-VPC 和 EC2-Classic 平台。如果您的账户是在 2013 年 12 月 4 日之后创建的，则它仅支持 EC2-VPC。要查明您的账户支持的平台，请参阅 [支持的平台 \(p. 577\)](#)。如果您的账户仅支持 EC2-VPC，我们会为您创建一个默认 VPC。默认 VPC 是已配置好可供您使用的 VPC。您可以立即在您的默认 VPC 内启动实例。有关更多信息，请参阅 [Amazon VPC 用户指南 中的您的默认 VPC 和子网](#)。如果您的账户支持 EC2-Classic 和 EC2-VPC，则可以在任一平台中启动实例。不论您的账户支持哪种平台，您都可以创建自己的非默认 VPC 并根据需要对其进行配置。

## 内容

- [使用 VPC 的优势 \(p. 572\)](#)
- [EC2-Classic 与 EC2-VPC 的区别 \(p. 573\)](#)
- [在 EC2-Classic 与 EC2-VPC 之间共享和访问资源 \(p. 575\)](#)
- [实例类型仅在 VPC 中可用 \(p. 576\)](#)
- [Amazon VPC 文档 \(p. 577\)](#)
- [支持的平台 \(p. 577\)](#)
- [ClassicLink \(p. 578\)](#)
- [从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例 \(p. 588\)](#)

## 使用 VPC 的优势

通过将实例启动到 VPC（而不是 EC2-Classic），您能够：

- 为启动和停止时保持不变的实例分配静态私有 IP 地址。
- 为您的实例分配多个 IP 地址
- 定义网络接口，并将一个或多个网络接口连接到您的实例
- 在实例运行时更改其安全组成员身份
- 控制您的实例的入站流量（入站筛选）和出站流量（出站筛选）
- 以网络访问控制列表 (ACL) 的方式为您的实例添加额外的访问控制层
- 在单租户硬件上运行您的实例

## EC2-Classic与 EC2-VPC 的区别

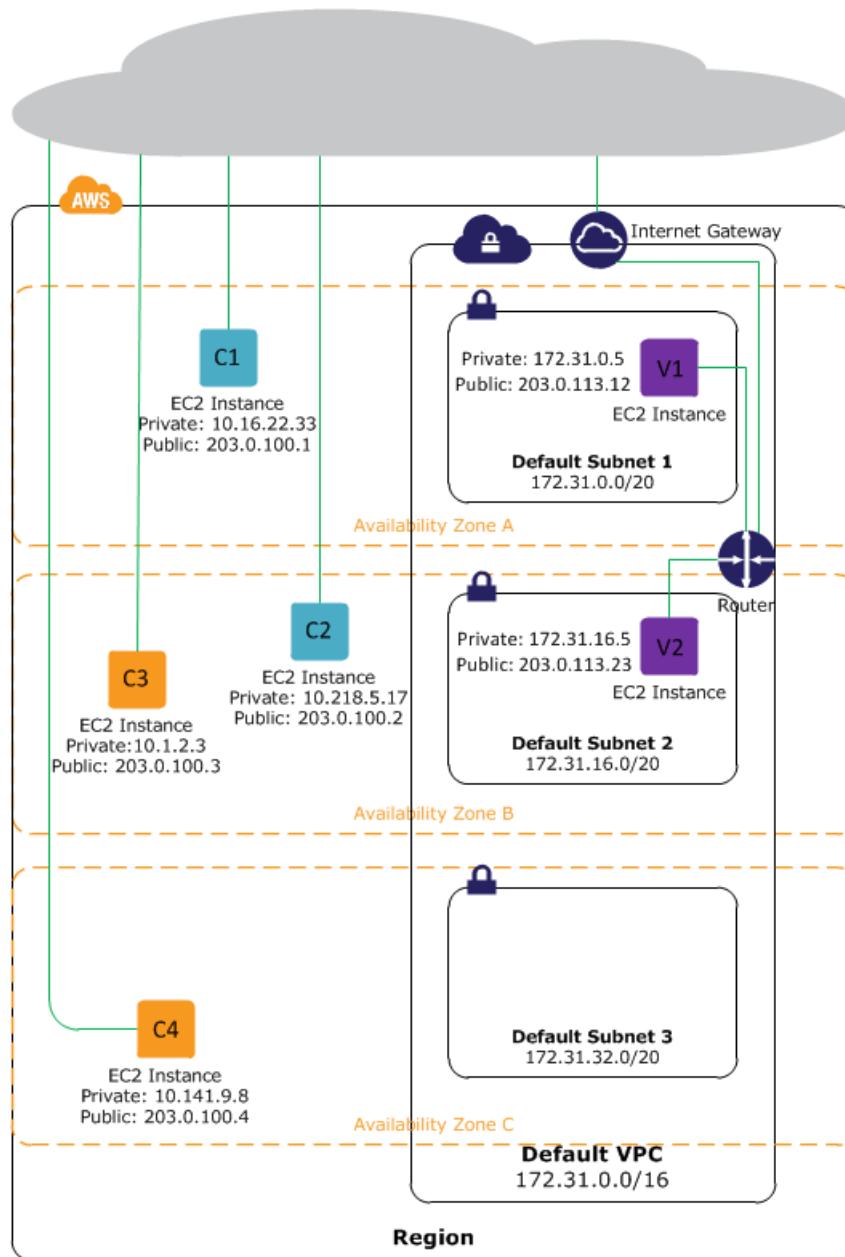
下表总结了在 EC2-Classic、默认 VPC 以及非默认 VPC 这三种平台中启动的实例之间的区别。

| 性能                                   | EC2-Classic                                                                                                                                              | 默认 VPC                                                         | 非默认 VPC                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------|
| 公有 IP 地址<br>( 来自 Amazon 的公有 IP 地址池 ) | 您的实例会收到一个公有 IP 地址。                                                                                                                                       | 默认情况下，在默认子网中启动的实例会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。 | 默认情况下，您的实例不会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。 |
| 私有 IP 地址                             | 您的实例会在每次启动时收到一个来自 EC2-Classic 范围的私有 IP 地址。                                                                                                               | 您的实例会收到一个来自您的默认 VPC 地址范围的静态私有 IP 地址。                           | 您的实例会收到一个来自您的 VPC 地址范围的静态私有 IP 地址。                       |
| 多个私有 IP 地址                           | 我们会为您的实例选择一个私有 IP 地址；不支持多个 IP 地址。                                                                                                                        | 您可以为实例分配多个私有 IP 地址。                                            | 您可以为实例分配多个私有 IP 地址。                                      |
| 弹性 IP 地址                             | 当您停止实例时，EIP 会取消与该实例的关联。                                                                                                                                  | 当您停止实例时，EIP 会保持与该实例的关联。                                        | 当您停止实例时，EIP 会保持与该实例的关联。                                  |
| DNS 主机名                              | DNS 主机名默认处于启用状态。                                                                                                                                         | DNS 主机名默认处于启用状态。                                               | DNS 主机名默认处于禁用状态。                                         |
| 安全组                                  | 安全组可以引用属于其他 AWS 账户的安全组。<br><br>您最多可以为每个区域创建 500 个安全组。                                                                                                    | 安全组只能引用您的 VPC 的安全组。<br><br>您最多可以为每个 VPC 创建 100 个安全组。           | 安全组只能引用您的 VPC 的安全组。<br><br>您最多可以为每个 VPC 创建 100 个安全组。     |
| 安全组关联                                | 启动实例时，您可以为其分配无限数量的安全组。<br><br>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。<br><br>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。<br><br>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。<br><br>您最多可以为一个安全组添加 100 条规则。                                                                                                              | 您可以为入站和出站流量添加规则。<br><br>您最多可以为一个安全组添加 50 条规则。                  | 您可以为入站和出站流量添加规则。<br><br>您最多可以为一个安全组添加 50 条规则。            |
| 租期                                   | 您的实例在共享硬件上运行。                                                                                                                                            | 您可以在共享硬件或单租户硬件上运行您的实例。                                         | 您可以在共享硬件或单租户硬件上运行您的实例。                                   |

| 性能            | EC2-Classic                                                       | 默认 VPC                                                                                             | 非默认 VPC                                                                          |
|---------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 正在访问 Internet | 您的实例可以访问 Internet。您的实例会自动接收公有 IP 地址，并且可以直接通过 AWS 网络边界访问 Internet。 | 默认情况下，您的实例可以访问 Internet。您的实例默认会接收一个公有 IP 地址。一个 Internet 网关连接到您的默认 VPC，并且您的默认子网有一个到 Internet 网关的路由。 | 默认情况下，您的实例不能访问 Internet。您的实例默认不会接收公有 IP 地址。您的 VPC 可能有一个 Internet 网关，具体取决于它的创建方式。 |

下图展示了每个平台中的实例。请注意以下几点：

- 实例 C1、C2、C3、和 C4 在 EC2-Classic 平台中。C1 和 C2 由一个账户启动，C4 和 C3 由不同的账户启动。这些实例可相互通信，并且可以直接访问 Internet。
- 实例 V1 和 V2 在 EC2-VPC 平台同一 VPC 内的不同子网中。它们的启动账户拥有 VPC；其他账户无法在此 VPC 内启动实例。这些实例可相互通信并且可访问 EC2-Classic 中的实例以及通过 Internet 网关访问 Internet。



## 在 EC2-Classic 与 EC2-VPC 之间共享和访问资源

AWS 账户中的一些资源和功能可以在 EC2-Classic 与 EC2-VPC 平台之间共享或访问（例如，通过 ClassicLink）。有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 578\)](#)。

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 Windows 实例迁移到 VPC 中的 Windows 实例 \(p. 588\)](#)。

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          | 您可将弹性 IP 地址从 EC2-Classic 迁移至 EC2-VPC。您无法将本来分配为在 VPC 中使用的弹性 IP 地址迁移至 EC2-Classic。有关更多信息，请参阅 <a href="#">将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 608)</a> 。                                                                                       |
| 实例                | EC2-Classic 实例可以使用公有 IP 地址与 VPC 中的实例通信，或者您可以使用 ClassicLink 通过私有 IP 地址实现通信。<br><br>您不能将实例从 EC2-Classic 迁移到 VPC。不过，您可以将应用程序从 EC2-Classic 中的实例迁移到 VPC 中的实例。有关更多信息，请参阅 <a href="#">从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例 (p. 588)</a> 。 |
| 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。<br><br>您不能将负载均衡器从 EC2-Classic 迁移到 VPC。您不能将 VPC 中的实例注册到 EC2-Classic 中的负载均衡器注册。                                                                           |
| 置放群组              |                                                                                                                                                                                                                                                |
| Reserved Instance | 可以将预留实例的网络平台从 EC2-Classic 更改为 EC2-VPC。                                                                                                                                                                                                         |
| 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。<br><br>您不能将安全组从 EC2-Classic 迁移到 VPC。您可以将规则从 EC2-Classic 中的安全组复制到 VPC 中的安全组。有关更多信息，请参阅 <a href="#">正在创建安全组 (p. 519)</a> 。                                 |
| 快照                |                                                                                                                                                                                                                                                |

以下资源不能在 EC2-Classic 与 VPC 之间共享或移动：

- 竞价型实例

## 实例类型仅在 VPC 中可用

EC2-Classic 中不支持以下实例类型的实例，它们必须在 VPC 中启动：

- C4
- M4
- T2
- X 1

如果您的账户支持 EC2-Classic，但您尚未创建非默认 VPC，您可以执行以下操作之一来启动仅 VPC 实例：

- 在请求中指定子网 ID 或网络接口 ID，以便创建非默认 VPC 并将您的仅 VPC 实例启动至该 VPC。请注意，如果您没有默认 VPC 并且使用 AWS CLI、Amazon EC2 API 或 AWS 开发工具包来启动仅限 VPC 的实例，则必须创建非默认 VPC。有关更多信息，请参阅 [创建 Virtual Private Cloud \(VPC\) \(p. 16\)](#)。
- 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。请注意，该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 IP 地址属性设置为 `true`，以便该实例可接收公有 IP 地址。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [您的 VPC 中的 IP 地址](#)。
  - 一个 Internet 网关，以及一个将 VPC 中的流量路由到该 Internet 网关的主路由表。这使您在 VPC 中启动的实例可以在 Internet 上通信。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [Internet 网关](#)。
  - VPC 的默认安全组和与每个子网关联的默认网络 ACL。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [您的 VPC 中的安全性](#)。

如果您在 EC2-Classic 中有其他资源，则可以采取措施将它们迁移到 EC2-VPC。有关更多信息，请参阅 [从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例 \(p. 588\)](#)。

## Amazon VPC 文档

有关 Amazon VPC 的更多信息，请参阅以下文档。

| 指南                                 | 说明                         |
|------------------------------------|----------------------------|
| <a href="#">Amazon VPC 入门指南</a>    | 提供关于 Amazon VPC 的实践经验介绍。   |
| <a href="#">Amazon VPC 用户指南</a>    | 提供有关如何使用 Amazon VPC 的详细信息。 |
| <a href="#">Amazon VPC 网络管理员指南</a> | 帮助网络管理员配置您的客户网关。           |

## 支持的平台

### Abstract

在您 AWS 账户支持的平台上启动实例。

Amazon EC2 支持以下平台。根据各区域的情况，您的 AWS 账户可以在两个平台或只能在 EC2-VPC 中启动。

| 平台          | 引入版本             | 说明                                                        |
|-------------|------------------|-----------------------------------------------------------|
| EC2-Classic | Amazon EC2 的初始版本 | 您的实例会在一个可与其他客户共享的扁平化网络中运行。                                |
| EC2-VPC     | Amazon VPC 的初始版本 | 您的实例会在一个“逻辑上”与 AWS 账户分离的 Virtual Private Cloud (VPC) 中运行。 |

有关您的账户中任何一个平台的可用性的详细信息，请参阅 *Amazon VPC 用户指南* 中的 [可用性](#)。（有关 EC2-Classic 和 EC2-VPC 之间区别的更多信息，请参阅[EC2-Classic与 EC2-VPC 的区别 \(p. 573\)](#)。

## 在 Amazon EC2 控制台中的所支持的平台

Amazon EC2 控制台会显示在所选区域中您可以启动实例的平台，以及在该区域您是否拥有默认 VPC。

检查您要使用的区域已在导航栏中选定。在 Amazon EC2 控制台控制面板上，从 Account Attributes (账户属性) 下找到 Supported Platforms (支持的平台)。如果有两个值 EC2 和 VPC，您可以将实例启动到两个中的任何一个平台中。如果有一个值 VPC，您只能将实例启动到 EC2-VPC 中。

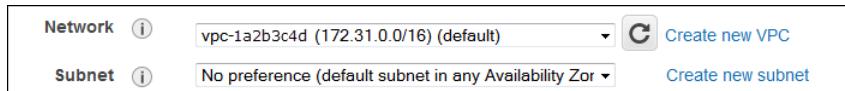
如果您只能将实例启动为 EC2-VPC，我们会为您创建一个默认 VPC。之后，当您启动实例时，我们会将其启动为默认 VPC，除非您创建了非默认 VPC 并在启动实例时对其进行指定。

### EC2-VPC

控制面板在 Account Attributes (账户属性) 下方显示以下内容，表示该账户仅支持 EC2-VPC 平台，且具有一个标识符为 vpc-1a2b3c4d 的默认 VPC。

Supported Platforms  
VPC  
  
Default VPC  
vpc-1a2b3c4d

如果您的账户仅支持 EC2-VPC，则可以在使用启动向导启动实例时，从 Network (网络) 列表中选择 VPC，从 Subnet (子网) 列表中选择子网。



### EC2-Classic、EC2-VPC

控制面板在 Account Attributes (账户属性) 下显示以下内容，表示该账户同时支持 EC2-Classic 和 EC2-VPC 平台。

Supported Platforms  
EC2  
VPC

如果您的账户支持 EC2-Classic 和 EC2-VPC，通过从 Network (网络) 列表中选择 Launch into EC2-Classic (在 EC2-Classic 中启动)，可以使用启动向导在 EC2-Classic 中启动。要启动到 VPC，您可以选择从 Network (网络) 列表中选择 VPC，并从 Subnet (子网) 列表中选择子网。

### 相关主题

有关如何区分您可以将实例启动到哪个平台的更多信息，请参阅 *Amazon VPC 用户指南* 中[检测支持的平台](#)。

## ClassicLink

### Abstract

使用 ClassicLink 允许您的 EC2-Classic 实例通过私有 IP 与 VPC 中的实例通信。

ClassicLink 允许将您的 EC2-Classic 实例链接到您账户中位于同一区域内的 VPC。因此，您可以将 VPC 安全组与 EC2-Classic 实例相关联，从而允许 EC2-Classic 实例与 VPC 中的实例使用私有 IP 地址进行

通信。通过 ClassicLink，无需使用公有 IP 地址或弹性 IP 地址即可在这里平台中的实例之间进行通信。有关私有 IP 地址和公有 IP 地址的更多信息，请参阅[您的 VPC 中的 IP 地址](#)。

ClassicLink 可用于账户支持 EC2-Classic 平台的所有用户，并且可以与任何 EC2-Classic 实例一起使用。要查明您的账户支持的平台，请参阅[支持的平台 \(p. 577\)](#)。有关使用 VPC 的好处的更多信息，请参阅[Amazon EC2 和 Amazon Virtual Private Cloud \(p. 572\)](#)。有关将资源迁移到 VPC 的更多信息，请参阅[从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例 \(p. 588\)](#)。

使用 ClassicLink 不收取任何额外费用。采用标准的数据传输和实例使用小时数计费方式。

#### 主题

- [ClassicLink 基本知识 \(p. 579\)](#)
- [ClassicLink 限制 \(p. 581\)](#)
- [使用 ClassicLink \(p. 582\)](#)
- [API 和 CLI 概述 \(p. 585\)](#)
- [示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 \(p. 586\)](#)

## ClassicLink 基本知识

使用 ClassicLink 将 EC2-Classic 实例链接到 VPC 分两步进行。首先，您必须为 VPC 启用 ClassicLink。默认情况下，您账户中的所有 VPC 都未启用 ClassicLink，目的是保持其隔离状态。为 VPC 启用 ClassicLink 之后，您可以将账户中位于同一区域的任何运行的 EC2-Classic 实例链接到该 VPC。链接实例的过程中，要从将与您的 EC2-Classic 实例关联的 VPC 中选择安全组。在您链接实例之后，只要 VPC 安全组允许，实例可以使用其私有 IP 地址与您的 VPC 中的实例通信。EC2-Classic 实例在链接到 VPC 时不会丢失其私有 IP 地址。



#### Note

将实例链接到 VPC 有时称为连接实例。

链接的 EC2-Classic 实例可以与 VPC 中的实例通信，但它并不构成 VPC 的一部分。如果您列出自己的实例并按 VPC 筛选，例如，通过 `DescribeInstances` API 请求或使用 Amazon EC2 控制台中的 `Instances` 屏幕执行此操作，则结果不会返回任何链接到 VPC 的 EC2-Classic 实例。有关如何查看链接的 EC2-Classic 实例的更多信息，请参阅[查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例 \(p. 583\)](#)。

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 \(p. 584\)](#)。

如果您不再需要实例与 VPC 之间的 ClassicLink 连接，可以从 VPC 取消与 EC2-Classic 实例的链接。这将断开 VPC 安全组与 EC2-Classic 实例的连接。链接的 EC2-Classic 实例一旦停止，会自动取消与 VPC 的链接。从 VPC 取消链接的所有 EC2-Classic 实例的链接后，您可以为 VPC 禁用 ClassicLink。

## 使用启用 ClassicLink 的 VPC 中的其他 AWS 服务

链接的 EC2-Classic 实例可以访问 VPC 中的以下 AWS 服务：Amazon Redshift、Amazon ElastiCache、Elastic Load Balancing 和 Amazon RDS。但是，VPC 中的实例无法通过 ClassicLink 访问 EC2-Classic 平台预配置的 AWS 服务。

如果您在 VPC 中使用 Elastic Load Balancing，那么只要实例位于您的 VPC 具有子网的可用区中，便可以向负载均衡器注册您的链接的 EC2-Classic 实例。当您终止链接的 EC2-Classic 实例时，负载均衡器会取消注册该实例。有关在 VPC 中使用负载均衡器的更多信息，请参阅 *Elastic Load Balancing 用户指南* 中的 [Amazon VPC 中的 Elastic Load Balancing](#)。

如果您使用 Auto Scaling，则可以创建一个 Auto Scaling 组，其中包含在启动时自动链接到启用了 ClassicLink 的指定 VPC 的实例。有关更多信息，请参阅 *Auto Scaling 用户指南* 中的[将 EC2-Classic 实例链接到 VPC](#)。

如果您在 VPC 中使用 Amazon RDS 实例或 Amazon Redshift 群集，并且它们可以公开访问（可通过 Internet 访问），则您用于从链接的 EC2-Classic 实例定位这些资源的终端节点会默认解析为公有 IP 地址。如果这些资源不可公开访问，则终端节点会解析为私有 IP 地址。要使用 ClassicLink 通过私有 IP 定位可公共访问的 RDS 实例或 Redshift 群集，您必须使用其私有 IP 地址或私有 DNS 主机名，或者必须对 VPC 启用 ClassicLink DNS 支持。

如果使用私有 DNS 主机名或私有 IP 地址对 RDS 实例寻址，则链接的 EC2-Classic 实例将无法使用多可用区部署可用的故障转移支持。

您可以使用 Amazon EC2 控制台查找 Amazon Redshift、Amazon ElastiCache 或 Amazon RDS 资源的私有 IP 地址。

#### 查找您的 VPC 中的 AWS 资源的私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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“Details (详细信息)”窗格中，从 Primary private IP (主要私有 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 \(p. 525\)](#)。

有关使用 ClassicLink 的策略的更多信息，请参阅以下示例：[5. 使用 ClassicLink \(p. 553\)](#)。

### ClassicLink 中的安全组

将 EC2-Classic 实例链接到 VPC 不会对您的 EC2-Classic 安全组造成影响。它们会继续控制实例的所有传入和传出流量。这不包括 VPC 中传入和传出实例的流量，这些流量由与 EC2-Classic 实例关联的 VPC 安全组控制。链接到同一 VPC 的 EC2-Classic 实例无论是否与同一 VPC 安全组关联，都不能通过该 VPC 相互通信。EC2-Classic 实例之间的通信由与这些实例关联的 EC2-Classic 安全组控制。有关安全组配置的示例，请参阅[示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 \(p. 586\)](#)。

在您将实例链接到 VPC 之后，不可再更改与该实例关联的 VPC 安全组。要将不同安全组与您的实例关联，必须先取消实例链接，然后再将其链接到 VPC 并选择所需的安全组。

### ClassicLink 路由

在您为 VPC 启用 ClassicLink 时，会向所有 VPC 路由表添加一个静态路由，其目的地为 10.0.0.0/8，目标为 local。这允许 VPC 中的实例与后来链接到该 VPC 的任意 EC2-Classic 实例之间进行通信。如果您向启用了 ClassicLink 的 VPC 添加自定义路由表，则会自动添加一个静态路由，其目的地为 10.0.0.0/8，目标为 local。在您为 VPC 禁用 ClassicLink 时，会从所有 VPC 路由表中自动删除此路由。

可以为处于 10.0.0.0/16 和 10.1.0.0/16 IP 地址范围内的 VPC 启用 ClassicLink，但仅当这些 VPC 的路由表中没有任何 10.0.0.0/8 IP 地址范围内的现有静态路由时才能如此，并且在创建 VPC 时自动

添加的本地路由除外。同样，如果您已经为 VPC 启用了 ClassicLink，那么您不能在路由表中再添加 10.0.0.0/8 IP 地址范围内的任何其他特定路由。



#### Important

如果您的 VPC CIDR 块为公共可路由 IP 地址范围，则在您将 EC2-Classic 实例链接到 VPC 之前，应考虑安全方面的问题。例如，如果链接的 EC2-Classic 实例从处于 VPC IP 地址范围内的源 IP 地址收到传入的拒绝服务 (DoS) 请求洪流攻击，则响应流量将发送到您的 VPC。我们强烈建议您使用私有 IP 地址范围创建 VPC，具体说明见 [RFC 1918](#)。

有关 VPC 中的路由表和路由的更多信息，请参阅 *Amazon VPC 用户指南* 中的 [路由表](#)。

### 为 ClassicLink 启用 VPC 对等连接

如果您在两个 VPC 之间有 VPC 对等连接，而且存在一个或多个 EC2-Classic 实例（这些实例通过 ClassicLink 链接到这两个 VPC 中的一个或两个），则可以扩展 VPC 对等连接以启用 EC2-Classic 实例与 VPC 对等连接另一端的 VPC 中的实例之间的通信。这将使 EC2-Classic 实例和 VPC 中的实例能够使用私有 IP 地址进行通信。为此，您可允许本地 VPC 与对等 VPC 中链接的 EC2-Classic 实例通信，也可允许本地链接的 EC2-Classic 实例与对等 VPC 中的实例通信。

如果您允许本地 VPC 与对等 VPC 中的链接 EC2-Classic 实例通信，则将自动向您的路由表添加一个静态路由（目的地为 10.0.0.0/8，目标为 local）。

有关更多信息和示例，请参阅 *Amazon VPC Peering Guide* 中的 [使用 ClassicLink 进行配置](#)。

### ClassicLink 限制

要使用 ClassicLink 功能，您需要了解以下限制：

- EC2-Classic 实例一次只能链接到一个 VPC。
- 如果您停止链接的 EC2-Classic 实例，它会自动取消与 VPC 的链接，并且 VPC 安全组不再与实例关联。您可以在重新启动之后，再次将实例链接到 VPC。
- 不能将 EC2-Classic 实例链接到不同区域或不同 AWS 账户中的 VPC。
- 对于配置用于专用租赁的 VPC，无法启用 ClassicLink。您可以联系 AWS Support，申请允许为您的专用租期 VPC 启用 ClassicLink。



#### Important

EC2-Classic 实例运行在共享硬件上。如果您因法规或安全要求已将 VPC 租赁设置为 dedicated，那么将 EC2-Classic 实例链接到 VPC 可能并不符合这些要求，因为您可以利用共享的租赁资源，使用私有 IP 地址直接对隔离的资源进行寻址。如果您希望为专用 VPC 启用 ClassicLink，请在 AWS Support 请求中提供这么做的详细原因。

- 路由与 EC2-Classic 私有 IP 地址范围 10/8 冲突的 VPC 不能启用 ClassicLink。这不包括在路由表中已有本地路由的 10.0.0.0/16 和 10.1.0.0/16 IP 地址范围的 VPC。有关更多信息，请参阅 [ClassicLink 路由 \(p. 580\)](#)。
- 您不能将 VPC 弹性 IP 地址与链接的 EC2-Classic 实例关联。
- 您可以将运行的竞价型实例链接到 VPC。要在竞价型实例请求中指定实例应当在请求执行时链接到 VPC，您必须使用 Amazon EC2 控制台中的启动向导。
- ClassicLink 不支持 VPC 外的传递关系。链接的 EC2-Classic 实例不能访问与 VPC 关联的任何 VPN 连接、VPC 端点或 Internet 网关。同样，VPN 连接或 Internet 网关另一端的资源也不能访问链接的 EC2-Classic 实例。
- 您不能使用 ClassicLink 将一个 VPC 实例链接到另一个 VPC 或 EC2-Classic 资源。要在 VPC 之间建立私有连接，可以使用 VPC 对等连接。有关更多信息，请参阅 *Amazon VPC 用户指南* 中的 [VPC 对等](#)。

- 如果您将 EC2-Classic 实例链接到 172.16.0.0/16 范围中的某个 VPC，并在该 VPC 中的 172.16.0.23/32 IP 地址上运行了一个 DNS 服务器，那么您所链接的 EC2-Classic 实例将无法访问 VPC DNS 服务器。要解决此问题，请在该 VPC 中的其他 IP 地址上运行您的 DNS 服务器。

## 使用 ClassicLink

您可以通过 Amazon EC2 和 Amazon VPC 控制台使用 ClassicLink 功能。您可以为 VPC 启用或禁用 ClassicLink，也可以将 EC2-Classic 实例链接到 VPC 或取消其链接。



### Note

ClassicLink 功能仅显示在支持 EC2-Classic 的账户和区域的控制台中。

#### 主题

- 为 VPC 启用 ClassicLink (p. 582)
- 将实例链接到 VPC (p. 582)
- 创建启用了 ClassicLink 的 VPC (p. 583)
- 在启动时将 EC2-Classic 实例链接到 VPC (p. 583)
- 查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例 (p. 583)
- 启用 ClassicLink DNS 支持 (p. 584)
- 禁用 ClassicLink DNS 支持 (p. 584)
- 从 VPC 取消与 EC2-Classic 实例的链接 (p. 584)
- 对 VPC 禁用 ClassicLink (p. 585)

## 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 \(p. 580\)](#)。

### 为 VPC 启用 ClassicLink

- 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/vpc/>。
- 在导航窗格中，选择 Your VPCs。
- 选择一个 VPC，然后选择 Actions、Enable ClassicLink。
- 在确认对话框中，选择 Yes, Enable。

## 将实例链接到 VPC

为 ClassicLink 启用 VPC 后，您可以将 EC2-Classic 实例与其链接。



### Note

您只能将正在运行的 EC2-Classic 实例链接到 VPC。您无法链接处于 stopped 状态的实例。

## 将实例链接到 VPC

- 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
- 在导航窗格中，选择 Instances。
- 选择正在运行的 EC2-Classic 实例，然后选择 Actions、ClassicLink、Link to VPC。您可以选择多个实例，将其链接到同一 VPC。

4. 在显示的对话框中，从列表中选择一个 VPC。此处仅显示已启用 ClassicLink 的 VPC。
5. 选择要与您的实例关联的一个或多个 VPC 安全组。完成操作后，选择 Link to VPC。

## 创建启用了 ClassicLink 的 VPC

您可以使用 Amazon VPC 控制台中的 VPC 向导创建新 VPC 并立即为其启用 ClassicLink。

### 创建启用了 ClassicLink 的 VPC

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/vpc/>。
2. 从 Amazon VPC 控制面板上，选择 Start VPC Wizard。
3. 选择一个 VPC 配置选项并选择 Select。
4. 在向导的下一页上，对 Enable ClassicLink 选择 Yes。完成向导中的剩余步骤创建您的 VPC。有关使用 VPC 向导的更多信息，请参阅 *Amazon VPC 用户指南* 中的 *Amazon VPC 情景*。

## 在启动时将 EC2-Classic 实例链接到 VPC

您可以在 Amazon EC2 控制台中使用启动向导启动 EC2-Classic 实例，然后立即将其链接到启用了 ClassicLink 的 VPC。

### 在启动时将实例链接到 VPC

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从 Amazon EC2 控制面板中，选择 Launch Instance。
3. 选择 AMI，然后选择实例类型。在 Configure Instance Details (配置实例详细信息) 页面上，确保从 Network (网络) 列表中选择 Launch into EC2-Classic (在 EC2-Classic 中启动)。



#### Note

某些实例类型（如 T2 实例类型）只能在 VPC 中启动。请确保您选择的实例类型可以在 EC2-Classic 中启动。

4. 在 Link to VPC (ClassicLink) 部分，从 Link to VPC 中选择一个 VPC。将只显示启用了 ClassicLink 的 VPC。从 VPC 中选择要与实例关联的安全组。完成页面上的其他配置选项，然后完成向导中的剩余步骤启动您的实例。有关如何使用启动向导的更多信息，请参阅 [从 AMI 启动实例 \(p. 217\)](#)。

## 查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例

您可以在 Amazon VPC 控制台中查看启用了 ClassicLink 的所有 VPC，在 Amazon EC2 控制台中查看链接的 EC2-Classic 实例。

### 查看启用了 ClassicLink 的 VPC

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/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-Classical 实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择一个 EC2-Classical 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-Classical 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-Classical 实例和 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。要使此功能起作用，必须对您的 VPC 启用 DNS 主机名和 DNS 解析。



#### Note

如果您对 VPC 启用 ClassicLink DNS 支持，您关联的 EC2 经典版实例可以访问与 VPC 相关的所有私有托管区域。有关更多信息，请参阅 [Amazon Route 53 开发人员指南中的私有托管区域的使用](#)。

### 启用 ClassicLink DNS 支持

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/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.amazonaws.cn/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions、Edit ClassicLink DNS Support。
4. 选择 No 禁用 ClassicLink DNS 支持，然后选择 Save。

### 从 VPC 取消与 EC2-Classical 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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 在 Actions 列表中，选择 ClassicLink，然后选择 Unlink Instance。您可以选择多个实例，将其从同一 VPC 取消链接。
4. 在确认对话框中选择 Yes。

### 对 VPC 禁用 ClassicLink

如果您不再需要 EC2-Classic 实例与 VPC 之间的连接，可以禁用 VPC 的 ClassicLink。您必须先取消链接到 VPC 的所有链接的 EC2-Classic 实例的链接。

#### 为 VPC 禁用 ClassicLink

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions、Disable ClassicLink。
4. 在确认对话框中，选择 Yes, Disable。

## API 和 CLI 概述

您可以使用命令行或查询 API 执行此页面上所述的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

#### 为 VPC 启用 ClassicLink

- [enable-vpc-classic-link](#) (AWS CLI)
- [Enable-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [EnableVpcClassicLink](#) (Amazon EC2 查询 API )

#### 将 EC2-Classic 实例链接（连接）到 VPC

- [attach-classic-link-vpc](#) (AWS CLI)
- [Add-EC2ClassicLinkVpc](#) (适用于 Windows PowerShell 的 AWS 工具)
- [AttachClassicLinkVpc](#) (Amazon EC2 查询 API )

#### 从 VPC 取消链接（断开）EC2-Classic 实例

- [detach-classic-link-vpc](#) (AWS CLI)
- [Dismount-EC2ClassicLinkVpc](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DetachClassicLinkVpc](#) (Amazon EC2 查询 API )

#### 为 VPC 禁用 ClassicLink

- [disable-vpc-classic-link](#) (AWS CLI)
- [Disable-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DisableVpcClassicLink](#) (Amazon EC2 查询 API )

### 描述 VPC 的 ClassicLink 状态

- [describe-vpc-classic-link](#) (AWS CLI)
- [Get-EC2VpcClassicLink](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcClassicLink](#) ( Amazon EC2 查询 API )

### 阐述链接的 EC2-Classical 实例

- [describe-classic-link-instances](#) (AWS CLI)
- [Get-EC2ClassicLinkInstance](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeClassicLinkInstances](#) ( Amazon EC2 查询 API )

### 为 ClassicLink 启用 VPC 对等连接

- [modify-vpc-peering-connection-options](#) (AWS CLI)
- [Edit-EC2VpcPeeringConnectionOption](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ModifyVpcPeeringConnectionOptions](#) ( Amazon EC2 查询 API )

### 对 VPC 启用 ClassicLink DNS 支持

- [enable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Enable-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [EnableVpcClassicLinkDnsSupport](#) ( Amazon EC2 查询 API )

### 对 VPC 禁用 ClassicLink DNS 支持

- [disable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Disable-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DisableVpcClassicLinkDnsSupport](#) ( Amazon EC2 查询 API )

### VPC 的 ClassicLink DNS 支持说明

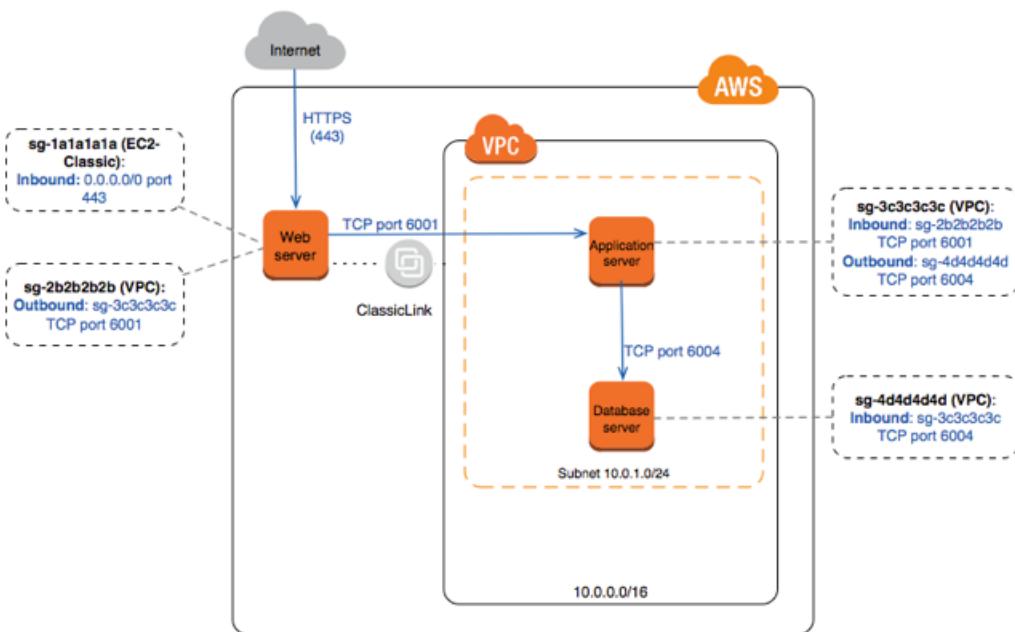
- [describe-vpc-classic-link-dns-support](#) (AWS CLI)
- [Get-EC2VpcClassicLinkDnsSupport](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcClassicLinkDnsSupport](#) ( Amazon EC2 查询 API )

## 示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置

在此示例中，您有具有以下三个实例的应用程序：面向公众的 Web 服务器、应用程序服务器和数据库服务器。您的 Web 服务器接收来自 Internet 的 HTTPS 流量，然后通过 TCP 端口 6001 与应用程序服务器通信。然后，您的应用程序服务器通过 TCP 端口 6004 与数据库服务器通信。您正在进行将整个应用程序迁移到账户中的 VPC 的过程。已将您的应用程序服务器和数据库服务器迁移到 VPC。您的 Web 服务器仍在 EC2-Classical 中而且已通过 ClassicLink 链接到 VPC。

您需要一个安全组配置，该配置仅允许流量在这些实例间流动。您具有 4 个安全组：其中两个安全组用于 Web 服务器 (`sg-1a1a1a1a` 和 `sg-2b2b2b2b`)、一个安全组用于应用程序服务器 (`sg-3c3c3c3c`)，一个安全组用于数据库服务器 (`sg-4d4d4d4d`)。

下图显示了实例的架构及其安全组配置。



#### 适用于 Web 服务器的安全组 (sg-1a1a1a1a 和 sg-2b2b2b2b)

您的一个安全组位于 EC2-Classic 中，另一个安全组位于 VPC 中。当通过 ClassicLink 将您的 Web 服务器实例链接到 VPC 时，是将 VPC 安全组与该实例关联。VPC 安全组使您能够控制从 Web 服务器到应用程序服务器的出站流量。

以下是适用于 EC2-Classic 安全组的安全组规则 (sg-1a1a1a1a)。

| 入站        |       |      |                             |
|-----------|-------|------|-----------------------------|
| 源         | Type  | 端口范围 | 注释                          |
| 0.0.0.0/0 | HTTPS | 443  | 允许 Internet 流量到达您的 Web 服务器。 |

以下是适用于 VPC 安全组的安全组规则 (sg-2b2b2b2b)。

| 出站          |      |      |                                                               |
|-------------|------|------|---------------------------------------------------------------|
| 目的地         | Type | 端口范围 | 注释                                                            |
| 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。

| 入站 |
|----|
|----|

| 源             | Type | 端口范围 | 注释                                                       |
|---------------|------|------|----------------------------------------------------------|
| sg-2b2b2b2b   | TCP  | 80   | 允许来自 Web 服务器（或与 sg-2b2b2b2b 关联的任何其他实例）的指定类型的流量到达应用程序服务器。 |
| 出站            |      |      |                                                          |
| 目的地           | Type | 端口范围 | 注释                                                       |
| sg-4d4d4d4d4d | TCP  | 3306 | 允许从应用程序服务器到数据库服务器（或到与 sg-4d4d4d4d4d 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-4d4d4d4d4d)

以下是适用于与您的数据库服务器关联的 VPC 安全组的安全组规则。

| 入站          |      |      |                                                        |
|-------------|------|------|--------------------------------------------------------|
| 源           | Type | 端口范围 | 注释                                                     |
| sg-3c3c3c3c | TCP  | 6004 | 允许来自应用程序服务器（或与 sg-3c3c3c3c 关联的任何其他实例）的指定类型的流量到达数据库服务器。 |

## 从 EC2-Classic 中的 Windows 实例迁移到 VPC 中的 Windows 实例

### Abstract

从 EC2-Classic 迁移到 EC2-VPC。

根据您创建账户的时间以及您使用的区域，您的 AWS 账户可能同时支持 EC2-Classic 和 EC2-VPC。有关更多信息以及要查明您账户支持的平台，请参阅 [支持的平台 \(p. 577\)](#)。有关使用 VPC 的好处以及 EC2-Classic 与 EC2-VPC 之间的差异的更多信息，请参阅 [Amazon EC2 和 Amazon Virtual Private Cloud \(p. 572\)](#)。

您在 AWS 账户中创建和使用资源。一些资源和功能（如增强联网和 T2 实例）只能在 VPC 中使用。一些资源可在 EC2-Classic 和 VPC 之间共享，另一些则不能。有关更多信息，请参阅 [在 EC2-Classic 与 EC2-VPC 之间共享和访问资源 \(p. 575\)](#)。

如果您的账户支持 EC2-Classic，您可能已经设置在 EC2-Classic 中使用的资源。如果您要从 EC2-Classic 迁移到 VPC，则必须在 VPC 中重新创建这些资源。

有两种方式可迁移到 VPC。您可以执行完整迁移，也可以随时间推移执行增量迁移。您选择的方法取决于 EC2-Classic 中的应用程序的大小和复杂性。例如，如果您的应用程序仅由一两个运行静态网站的实例构成，并且您可以承受短时间的停机，那么您可以一次完成迁移。如果您的应用程序是包含不可中断进程

的多层应用程序，则可以使用 ClassicLink 执行增量迁移。通过这种方式，您可以按每次一个组件的方式转移功能，直到应用程序完全在 VPC 中运行。

如果需要迁移 Linux 实例，请参阅 *Amazon EC2 用户指南（适用于 Linux 实例）* 中的[将 Linux 实例从 EC2-Classic 迁移至 VPC](#)。

#### 内容

- [完整迁移到 VPC \(p. 589\)](#)
- [使用 ClassicLink 增量迁移到 VPC \(p. 594\)](#)

## 完整迁移到 VPC

完成以下任务可将应用程序从 EC2-Classic 完整迁移到 VPC。

#### 任务

- [步骤 1：创建 VPC \(p. 589\)](#)
- [步骤 2：配置安全组 \(p. 589\)](#)
- [步骤 3：从您的 EC2-Classic 实例创建 AMI \(p. 590\)](#)
- [步骤 4：在 VPC 中启动实例 \(p. 591\)](#)
- [示例：迁移简单的 Web 应用程序 \(p. 592\)](#)

### 步骤 1：创建 VPC

要开始使用 VPC，请确保您在账户中有 VPC。可以使用下列方法之一创建一个 VPC：

- 使用新的仅限 EC2-VPC 的 AWS 账户。仅限 EC2-VPC 的账户在每个区域中有一个默认 VPC，可供您使用。默认情况下，您启动的实例会在此 VPC 中启动，除非您另行指定。有关默认 VPC 的更多信息，请参阅[您的默认 VPC 和子网](#)。如果您不想自己设置 VPC，或是如果您的 VPC 配置无需特定要求，请使用此选项。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并使用 VPC 向导创建新 VPC。有关更多信息，请参阅[Amazon VPC 情景](#)。如果您要使用向导中的可用配置集之一在现有 EC2-Classic 账户中快速设置 VPC，请使用此选项。您将在每次启动实例时指定此 VPC。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并根据您的要求设置 VPC 的组件。有关更多信息，请参阅[您的 VPC 和子网](#)。如果您对 VPC 有特定要求（如特定数量的子网），请使用此选项。您将在每次启动实例时指定此 VPC。



#### Note

T2 实例类型必须在 VPC 中启动。如果您在 EC2-Classic 账户中没有任何 VPC，并且您使用 Amazon EC2 控制台中的启动向导启动 T2 实例，则该向导会为您创建一个非默认 VPC。有关 T2 实例类型的更多信息，请参阅[T2 实例 \(p. 113\)](#)。您的 T2 实例将无法与使用私有 IP 地址的 EC2-Classic 实例通信。请考虑使用本主题中概述的方法将您的现有实例迁移到相同 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[Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。

#### 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.amazonaws.cn/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[Amazon EC2 个安全组（对于 Windows 实例）\(p. 515\)](#)。



### Note

如果您在 EC2-Classic 安全组中定义了引用其他安全组的规则，则您将无法在 VPC 安全组中使用相同规则。请将该规则修改为引用同一 VPC 中的安全组。

6. 选择 Create。

## 步骤 3：从您的 EC2-Classic 实例创建 AMI

AMI 是用于启动实例的模板。您可以基于现有 EC2-Classic 实例创建自己的 AMI，然后使用该 AMI 在 VPC 中启动实例。

用于创建 AMI 的方法取决于您的实例的根设备类型，以及实例运行时所在的操作系统平台。要查明您实例的根设备类型，请转到 Instances 页面，选择您的实例，然后在 Description (说明) 选项卡上的 Root device type (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。

| 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 <a href="#">创建 Amazon EBS 支持的 Windows AMI (p. 76)</a> 。           |
| 实例存储    | 捆绑您的实例，然后从捆绑过程中生成的清单创建由实例存储提供支持的 AMI。有关更多信息，请参阅 <a href="#">创建实例存储支持的 Windows AMI (p. 78)</a> 。 |

#### ( 可选 ) 在 Amazon EBS 卷上存储您的数据

您可以创建Amazon EBS 卷并使用它备份和存储实例中的数据（如同使用物理硬盘驱动器一样）。Amazon EBS 卷可以与同一可用区中的任何实例连接和断开。您可以断开卷与 EC2-Classic 中实例的连接，并将它连接到在同一可用区内的 VPC 中启动的新实例。

有关 Amazon EBS 卷的更多信息，请参阅以下主题：

- [Amazon EBS 卷 \(p. 640\)](#)

- [创建 Amazon EBS 卷 \(p. 652\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)

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 \(p. 676\)](#)
- [创建 Amazon EBS 快照 \(p. 677\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 655\)](#)

## 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.amazonaws.cn/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (选择一个Amazon 系统映像) 页面上，选择 My AMIs (我的 AMI) 类别，然后选择您创建的 AMI。
4. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择您的 VPC。从 Subnet (子网) 列表中选择所需子网。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
6. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。
7. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 216\)](#)。

### 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.amazonaws.cn/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

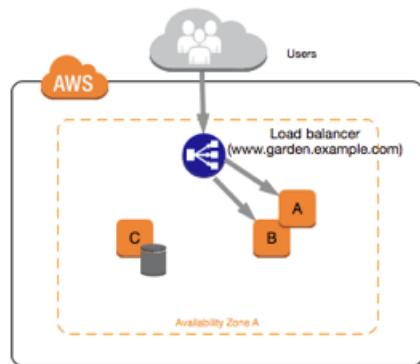
1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 切换到您的新 AWS 账户。
3. 在导航窗格中，选择 AMIs。
4. 在 Filter (筛选条件) 列表中，选择 Private images (私有映像)。选择您从 EC2-Classic 账户共享的 AMI，然后选择 Launch。
5. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
6. 在 Configure Instance Details (配置实例详细信息) 页面上，应在 Network (网络) 中选择默认 VPC。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
7. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。
8. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

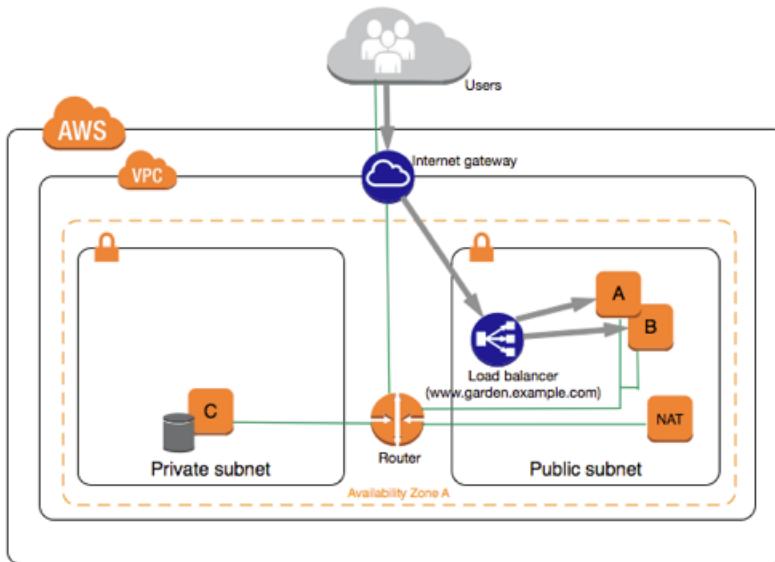
有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 216\)](#)。

## 示例：迁移简单的 Web 应用程序

在此示例中，您使用 AWS 托管您的园艺网站。为了管理您的网站，您在 EC2-Classic 中有三个正在运行的实例。实例 A 和 B 托管面向公众的 Web 应用程序，您使用 Elastic Load Balancer 对这些实例之间的流量进行负载均衡。您向实例 A 和 B 分配了弹性 IP 地址，从而可将静态 IP 地址用于这些实例上的配置和管理任务。实例 C 存储您网站的 MySQL 数据库。您注册了域名 [www.garden.example.com](http://www.garden.example.com)，并且使用 Amazon Route 53 创建了一个托管区域，该区域具有与负载均衡器的 DNS 名称关联的别名记录集。



第一部分往 VPC 的迁移决定了适合您需要的 VPC 架构类型。在此情况中，您做出了以下决定：将一个公有子网用于您的 Web 服务器，而将一个私有子网用于您的数据库服务器。随着您网站的发展，您可以向子网添加更多 Web 服务器和数据库服务器。默认情况下，私有子网中的实例无法访问 Internet；但是，您可以通过公有子网中的网络地址转换 (NAT) 设备启用 Internet 访问。您可能需要设置 NAT 设备，以通过 Internet 为数据库服务器提供定期更新和补丁。您将您的弹性 IP 地址迁移到 EC2-VPC，并在公有子网中创建弹性负载均衡器来对 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 \(p. 590\)](#)。
- 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 \(p. 589\)](#)。



#### 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 \(p. 591\)](#)。
- 配置您的 NAT 设备：如果您使用的是 NAT 实例，则必须为其创建安全组，以便允许来自您的私有子网的 HTTP 和 HTTPS 流量。有关更多信息，请参阅 [NAT 实例](#)。如果您使用的是 NAT 网关，则会自动允许来自您的私有子网的流量。
- 配置您的数据库：在 EC2-Classic 中从数据库服务器创建 AMI 时，该实例中存储的所有配置信息都已复制到 AMI。您可能必须连接到新数据库服务器并更新配置详细信息；例如，如果您将数据库配置为向 EC2-Classic 中的 Web 服务器授予完全读取、写入和修改权限，则您必须更新配置文件以改为向新 VPC Web 服务器授予相同权限。
- 配置您的 Web 服务器：您的 Web 服务器将具有与 EC2-Classic 中的实例相同的配置设置。例如，如果您将 Web 服务器配置为使用 EC2-Classic 中的数据库，请将您 Web 服务器的配置设置更新为指向您的新数据库实例。



#### Note

默认情况下，不会向在非默认子网中启动的实例分配公有 IP 地址，除非您在启动时另行指定。您的新数据库服务器可能没有公有 IP 地址。在这种情况下，您可以更新您 Web 服务器的配置文件以使用新数据库服务器的私有 DNS 名称。同一 VPC 中的实例通过私有 IP 地址互相通信。

- **迁移您的弹性 IP 地址**：在 EC2-Classic 中从您的 Web 服务器取消与弹性 IP 地址的关联，然后将这些地址迁移到 EC2-VPC。迁移这些地址后，您可在 VPC 中将其与您的新 Web 服务器关联。有关更多信息，请参阅 [将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC \(p. 608\)](#)。
- **创建新负载均衡器**：要继续使用 Elastic Load Balancing 对发送到实例的流量进行负载均衡，请确保您了解 VPC 中负载均衡器的各种配置。有关更多信息，请参阅 [Amazon VPC 中的 Elastic Load Balancing](#)。
- **更新您的 DNS 记录**：在公有子网中设置了负载均衡器之后，请确保 www.garden.example.com 域指向您的新负载均衡器。为此，您需要更新您的 DNS 记录并更新 Amazon Route 53 中的别名记录集。有关使用 Amazon Route 53 的更多信息，请参阅 [Amazon Route 53 入门](#)。
- **关闭您的 EC2-Classic 资源**：验证了您的 Web 应用程序是否正在 VPC 架构内运行之后，可以关闭 EC2-Classic 资源以使它们停止产生费用。终止 EC2-Classic 实例，并释放 EC2-Classic 弹性 IP 地址。

## 使用 ClassicLink 增量迁移到 VPC

### Abstract

使用 ClassicLink 从 EC2-Classic 迁移到 EC2-VPC。

通过 ClassicLink 功能可以更容易地管理到 VPC 的增量迁移。ClassicLink 允许您将 EC2-Classic 实例链接到您账户中位于同一区域的 VPC，从而允许新的 VPC 资源使用私有 IP 地址与 EC2-Classic 实例通信。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 \(p. 578\)](#)。

### 主题

- [步骤 1：准备迁移序列 \(p. 594\)](#)
- [步骤 2：创建 VPC \(p. 594\)](#)
- [步骤 3：为 VPC 启用 ClassicLink \(p. 595\)](#)
- [步骤 4：从您的 EC2-Classic 实例创建 AMI \(p. 595\)](#)
- [步骤 5：在 VPC 中启动实例 \(p. 596\)](#)
- [步骤 6：将 EC2-Classic 实例链接到 VPC \(p. 596\)](#)
- [步骤 7：完成 VPC 迁移 \(p. 596\)](#)

### 步骤 1：准备迁移序列

要有效地使用 ClassicLink，您必须先确定必须迁移到 VPC 的应用程序组件，然后确认迁移功能的顺序。

例如，您的一个应用程序依赖于演示 Web 服务器、后端数据库服务器以及用于交易的身份验证逻辑。您可以决定从身份验证逻辑开始迁移过程，然后是数据库服务器，最后是 Web 服务器。

### 步骤 2：创建 VPC

要开始使用 VPC，请确保您在账户中有 VPC。可以使用下列方法之一创建一个 VPC：

- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并使用 VPC 向导创建新 VPC。有关更多信息，请参阅 [Amazon VPC 情景](#)。如果您要使用向导中的可用配置集之一在现有 EC2-Classic 账户中快速设置 VPC，请使用此选项。您将在每次启动实例时指定此 VPC。
- 在您的现有 AWS 账户中，打开 Amazon VPC 控制台并根据您的要求设置 VPC 的组件。有关更多信息，请参阅 [您的 VPC 和子网](#)。如果您对 VPC 有特定要求（如特定数量的子网），请使用此选项。您将在每次启动实例时指定此 VPC。

## 步骤 3：为 VPC 启用 ClassicLink

创建 VPC 之后，您可以为它启用 ClassicLink。有关 ClassicLink 的更多信息，请参阅[ClassicLink \(p. 578\)](#)。

### 为 VPC 启用 ClassicLink

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后从 Actions 列表中选择 Enable ClassicLink。
4. 在确认对话框中，选择 Yes, Enable。

## 步骤 4：从您的 EC2-Classic 实例创建 AMI

AMI 是用于启动实例的模板。您可以基于现有 EC2-Classic 实例创建自己的 AMI，然后使用该 AMI 在 VPC 中启动实例。

用于创建 AMI 的方法取决于您的实例的根设备类型，以及实例运行时所在的操作系统平台。要查明您实例的根设备类型，请转到 Instances 页面，选择您的实例，然后在 Description (说明) 选项卡上的 Root device type (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。

| 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 <a href="#">创建 Amazon EBS 支持的 Windows AMI (p. 76)</a> 。           |
| 实例存储    | 捆绑您的实例，然后从捆绑过程中生成的清单创建由实例存储提供支持的 AMI。有关更多信息，请参阅 <a href="#">创建实例存储支持的 Windows AMI (p. 78)</a> 。 |

### ( 可选 ) 在 Amazon EBS 卷上存储您的数据

您可以创建AmazonEBS卷并使用它备份和存储实例中的数据（如同使用物理硬盘驱动器一样）。Amazon EBS 卷可以与同一可用区中的任何实例连接和断开。您可以断开卷与 EC2-Classic 中实例的连接，并将它连接到在同一可用区内的 VPC 中启动的新实例。

有关 Amazon EBS 卷的更多信息，请参阅以下主题：

- [Amazon EBS 卷 \(p. 640\)](#)
- [创建 Amazon EBS 卷 \(p. 652\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)

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 \(p. 676\)](#)
- [创建 Amazon EBS 快照 \(p. 677\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 655\)](#)

## 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.amazonaws.cn/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (选择一个Amazon 系统映像) 页面上，选择 My AMIs (我的 AMI) 类别，然后选择您创建的 AMI。
4. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择您的 VPC。从 Subnet (子网) 列表中选择所需子网。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达 Configure Security Group 页面。
6. 选择 Select an existing group (选择现有组)，然后选择您之前创建的安全组。选择 Review and Launch。
7. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导每个步骤中可以配置的参数的更多信息，请参阅[启动实例 \(p. 216\)](#)。

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.amazonaws.cn/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 平台上使用的弹性 IP 地址迁移到 EC2-VPC 平台。有关更多信息，请参阅[将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC \(p. 608\)](#)。

完成此步骤并测试应用程序是否从 VPC 正常工作之后，您可以终止 EC2-Classic 实例并为 VPC 禁用 ClassicLink。您还可以清理所有可能不再需要的 EC2-Classic 资源以免它们产生费用。例如，您可以释放弹性 IP 地址，并删除之前与 EC2-Classic 实例关联的卷。

# Amazon EC2 实例 IP 寻址

## Abstract

了解 Amazon EC2 如何根据您是在 Amazon EC2 还是在 VPC 中启动了实例来为实例提供公有和私有 IP 地址及 DNS 主机名。

我们为您的实例提供 IP 地址和 DNS 主机名。这些会因实例的启动位置（EC2-Classic 平台或 Virtual Private Cloud (VPC) 中）而异。

有关 EC2-Classic 和 EC2-VPC 平台的信息，请参阅[支持的平台 \(p. 577\)](#)。有关 Amazon VPC 的信息，请参阅[Amazon VPC 是什么？\(在 Amazon VPC 用户指南中\)](#)。

### 内容

- [私有 IP 地址和内部 DNS 主机名 \(p. 597\)](#)
- [公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#)
- [弹性 IP 地址 \(p. 599\)](#)
- [Amazon DNS 服务器 \(p. 599\)](#)
- [EC2-Classic 和 EC2-VPC 之间的 IP 地址区别 \(p. 599\)](#)
- [确定您的公有、私有和弹性 IP 地址 \(p. 599\)](#)
- [分配公有 IP 地址 \(p. 601\)](#)
- [多个私有 IP 地址 \(p. 602\)](#)

## 私有 IP 地址和内部 DNS 主机名

私有 IP 地址是无法通过 Internet 访问的 IP 地址。您可以使用私有 IP 地址在同一网络（EC2-Classic 或 VPC）中实现实例之间的通信。有关私有 IP 地址标准和规范的更多信息，请转到[RFC 1918](#)。

当您启动实例时，我们会使用 DHCP 为实例分配私有 IP 地址。另外，还为每个实例指定了一个可解析为实例私有 IP 地址的内部 DNS 主机名，例如，`ip-10-251-50-12.ec2.internal`。您可以使用内部 DNS 主机名在同一网络中实现实例之间的通信，但我们无法解析实例所在网络之外的 DNS 主机名。

在 VPC 中启动的实例，将在子网地址范围内指定一个主要私有 IP 地址。有关更多信息，请参阅 *Amazon VPC 用户指南* 中的[子网大小调整](#)。如果您在启动实例时未指定主要私有 IP 地址，我们会在子网范围内为您选择可用的 IP 地址。VPC 中的每个实例都具有分配了主要私有 IP 地址的默认网络接口 (`eth0`)。您还可以指定其他私有 IP 地址，即[辅助私有 IP 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[多个私有 IP 地址 \(p. 602\)](#)。

对于在 EC2-Classic 中启动的实例，我们在实例停止或终止时释放私有 IP 地址。如果您重新启动已停止的实例，该实例会收到新的私有 IP 地址。

对于在 VPC 中启动的实例，私有 IP 地址会在实例停止并重新启动时保持与网络接口的关联，并在实例终止时释放。

如果您在 EC2-Classic 中创建自定义防火墙配置，那么必须在您的防火墙中创建规则，以允许来自 Amazon DNS 服务器地址的端口 53 (DNS)（目标端口在临时范围内）的入站流量，否则，实例的内部 DNS 解析会失败。如果您的防火墙无法自动允许 DNS 查询响应，那么您就需要允许来自 Amazon DNS 服务器的 IP 地址的流量。要获取 Amazon DNS 服务器的 IP 地址，请在您的实例中使用以下命令：

- Windows

```
ipconfig /all | findstr /c:"DNS Servers"
```

## 公有 IP 地址和外部 DNS 主机名

公有 IP 地址可从 Internet 访问。您可以使用公用 IP 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 主机名解析到实例所在网络外的该实例的公有 IP 地址和实例所在网络内的该实例的私有 IP 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。要了解更多有关 NAT 的信息，请转至：[RFC 1631: The IP Network Address Translator \(NAT\)](#) 部分。

当您在 EC2-Classic 中启动实例时，我们会自动从 EC2-Classic 公有 IP 地址池中为该实例分配一个公有 IP 地址。您不能修改此行为。当您在某个 VPC 中启动实例时，您子网的一个属性会确定在该子网中启动的实例是否从 EC2-VPC 公有 IP 地址池接收公有 IP 地址。默认情况下，我们会为在默认 VPC 中启动的实例分配公有 IP 地址，而不会为在非默认子网中启动的实例分配公有 IP 地址。

您可以通过执行以下操作，控制 VPC 中的实例是否接收公有 IP 地址：

- 修改子网的公有 IP 寻址属性。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [修改您子网的公有 IP 地址行为](#)。
- 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 [分配公有 IP 地址 \(p. 601\)](#)。

公有 IP 地址将从 Amazon 的公有 IP 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，该地址释放回公有 IP 地址池中，并且您无法重新使用该地址。

您不能从实例手动关联或取消关联公有 IP 地址。在某些情况下，我们会从您的实例释放公有 IP 地址，或为其分配新的地址：

- 当您的实例已停止或终止后，我们释放它的公有 IP 地址。已停止的实例在重新启动时会接收新的公有 IP 地址。
- 如果您将弹性 IP 地址与实例相关联，或在 VPC 中将弹性 IP 地址与实例的主要网络接口 (`eth0`) 相关联，我们会释放实例的公有 IP 地址。当您从实例取消与弹性 IP 地址的关联时，实例会收到新的公有 IP 地址。
- 如果 VPC 中的实例的公有 IP 地址已释放，则在多个网络接口与实例相连的情况下，该实例不会接收新地址。

如果您需要可根据需要关联到实例并从实例进行关联的永久公有 IP 地址，可改为使用弹性 IP 地址。例如，如果您使用动态 DNS 来将现有 DNS 名称映射到新实例的公有 IP 地址，则可能需要 24 小时，以便 IP 地址通过 Internet 进行传播。其结果是，新的实例可能无法接收流量，而已终止实例继续接收请求。要解决此问题，请使用弹性 IP 地址。您可以分配自己的弹性 IP 地址，并将其与您的实例相关联。有关更多信息，请参阅 [弹性 IP 地址 \(p. 606\)](#)。

如果您的实例在 VPC 中且分配有弹性 IP 地址，则在启用 DNS 主机名后，实例会收到一个 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

弹性 IP 地址即可以分配给您的账户的公有 IP 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 \(p. 606\)](#)。

## Amazon DNS 服务器

Amazon 提供了 DNS 服务器，可将 DNS 主机名解析为 IP 地址。在 EC2-Classic 中，此 Amazon DNS 服务器位于 172.16.0.23。在 EC2-VPC 中，Amazon DNS 服务器位于 VPC 网络范围起始地址 + 2 的位置。有关更多信息，请参阅 *Amazon VPC 用户指南* 中的 [Amazon DNS 服务器](#)。

## EC2-Classic 和 EC2-VPC 之间的 IP 地址区别

下表总结了在 EC2-Classic、默认子网和非默认子网中启动的实例 IP 地址之间的区别。

| 性能                                   | EC2-Classic                                | 默认子网                                                     | 非默认子网                                                              |
|--------------------------------------|--------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------|
| 公有 IP 地址<br>( 来自 Amazon 的公有 IP 地址池 ) | 您的实例会收到一个公有 IP 地址。                         | 默认情况下，您的实例不会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。 | 默认情况下，您的实例不会接收公有 IP 地址，除非您在启动过程中另行指定，或是您修改子网的公有 IP 地址属性。           |
| 私有 IP 地址                             | 您的实例会在每次启动时收到一个来自 EC2-Classic 范围的私有 IP 地址。 | 您的实例会收到一个来自您的默认子网地址范围的静态私有 IP 地址。                        | 您的实例会收到一个来自您的子网地址范围的静态私有 IP 地址。                                    |
| 多个 IP 地址                             | 我们会为您的实例选择一个私有 IP 地址；不支持多个 IP 地址。          | 您可以为实例分配多个私有 IP 地址。                                      | 您可以为实例分配多个私有 IP 地址。                                                |
| 网络接口                                 | IP 地址与实例相关联；不支持网络接口。                       | IP 地址与网络接口相关联。每个实例都有一个或多个网络接口。                           | IP 地址与网络接口相关联。每个实例都有一个或多个网络接口。                                     |
| 弹性 IP 地址                             | 当您停止实例时，弹性 IP 地址会取消与实例的关联。                 | 当您停止实例时，弹性 IP 地址会保持与实例的关联。                               | 当您停止实例时，弹性 IP 地址会保持与实例的关联。                                         |
| DNS 主机名                              | DNS 主机名默认处于启用状态。                           | DNS 主机名默认处于启用状态。                                         | 默认情况下 DNS 主机名为禁用状态，但有一种情况除外，即当您在 Amazon VPC 控制台中使用 VPC 向导创建 VPC 时。 |

## 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 IP 地址、公有 IP 地址和弹性 IP 地址。您还可以使用实例元数据，从实例内确定实例的公有 IP 地址和私有 IP 地址。有关更多信息，请参阅 [实例元数据和用户数据 \(p. 239\)](#)。

### 使用控制台确定实例的私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。

3. 选择实例。在“Details (详细信息)”窗格中，从 Private IPs (私有 IP) 字段中获取私有 IP 地址，从 Private DNS (私有 DNS) 字段中获取内部 DNS 主机名。
4. (仅限 VPC) 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 IP 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. (仅限 VPC) 或者，在“Navigation (导航)”窗格中，单击 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 IP (主要私有 IP) 字段中获取主要私有 IP 地址，从 Private DNS (私有 DNS) 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，那么可从 Secondary private IPs (辅助私有 IP) 字段中获取这些 IP 地址。

### 使用控制台确定实例的公有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择实例。在“Details (详细信息)”窗格中，从 Public IP (公有 IP) 字段中获取公有 IP 地址，从 Public DNS (公有 DNS) 字段中获取外部 DNS 主机名。
4. 如果弹性 IP 地址已与实例关联，则可从 Elastic IP (弹性 IP) 字段中获取弹性 IP 地址。



#### Note

如果您已将弹性 IP 地址与您的实例关联，则 Public IP 字段中也将显示弹性 IP 地址。

5. (仅限 VPC) 或者，在导航窗格中，选择 Network Interfaces，然后选择与您的实例关联的网络接口。
6. 从 Public IP (公有 IP) 字段获取公有 IP 地址。星号 (\*) 表示映射到主要私有 IP 地址的公有 IP 地址或弹性 IP 地址。



#### Note

公有 IP 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 IP 地址。因此，如果您检查实例网络接口的属性（例如，通过 ifconfig (Linux) 或 ipconfig (Windows)），则不会显示公有 IP 地址。要从实例内确定实例的公有 IP 地址，您可以使用实例元数据。

### 使用实例元数据确定实例的 IP 地址

1. 连接到您的实例。
2. 使用以下命令访问私有 IP 地址：
  - Linux

```
C:\> curl http://169.254.169.254/latest/meta-data/local-ipv4
```

- Windows

```
C:\> wget http://169.254.169.254/latest/meta-data/local-ipv4
```

3. 使用以下命令访问公有 IP 地址：
  - Linux

```
C:\> curl http://169.254.169.254/latest/meta-data/public-ipv4
```

- Windows

```
C:\> wget http://169.254.169.254/latest/meta-data/public-ipv4
```

请注意，如果弹性 IP 地址与实例相关联，则返回的值是弹性 IP 地址。

## 分配公有 IP 地址

如果在 EC2-Classic 中启动实例，则默认情况下，系统会为实例分配公有 IP 地址。您不能修改此操作。

在 VPC 中，所有子网都有一个属性可指定是否为子网中启动的实例分配公有 IP 地址。默认情况下，非默认子网的此属性设置为 false，默认子网的此属性设置为 true。如果您在 VPC 中启动实例，则可以通过公有 IP 寻址功能来控制是否为实例分配一个公有 IP 地址；您可以覆盖子网 IP 寻址属性的默认行为。公有 IP 地址从 Amazon 的公有 IP 地址池分配，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 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。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 \(p. 606\)](#)。

### 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.amazonaws.cn/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 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择一个 VPC。会显示一个 Auto-assign Public IP (自动分配公有 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，对于非默认子网，如果您为 eth0 指定了一个现有的网络接口，则不能自动分配公有 IP 地址。

5. 按照向导中后续页面中的步骤完成实例的设置。有关向导配置选项的更多信息，请参阅 [启动实例 \(p. 216\)](#)。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 Instances 页面中，选择新实例并在详细信息窗格的 Public IP (公有 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 \(p. 606\)](#)。您也可以修改您子网的公有 IP 地址行为。有关更多信息，请参阅 [修改您子网的公有 IP 地址行为](#)。

## 用于公有 IP 寻址的 API 和命令行工具

要启用或禁用公有 IP 地址分配功能，请使用下表中的一种方法。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

| 方法                              | 参数                                                                                                                                  |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| AWS CLI                         | 将 <code>--associate-public-ip-address</code> 或 <code>--no-associate-public-ip-address</code> 选项与 <code>run-instances</code> 命令结合使用。 |
| 适用于 Windows PowerShell 的 AWS 工具 | 将 <code>-AssociatePublicIp</code> 参数与 <code>New-EC2Instance</code> 命令结合使用。                                                          |
| 查询 API                          | 将 <code>NetworkInterface.n.AssociatePublicIpAddress</code> 参数与 <code>RunInstances</code> 请求结合使用。                                    |

## 多个私有 IP 地址

### Abstract

了解如何为 VPC 中的实例指定多个私有 IP 地址。

在 EC2-VPC 中，您可以为实例指定多个私有 IP 地址。您可以为实例指定的网络接口和私有 IP 地址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私有 IP 地址 \(p. 613\)](#)。

在执行以下操作时，为 VPC 中的实例分配多个私有 IP 地址会非常有帮助：

- 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私有 IP 地址的网络设备，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私有 IP 地址。

### 内容

- [多个 IP 地址如何工作 \(p. 602\)](#)
- [分配辅助私有 IP 地址 \(p. 603\)](#)
- [在您的实例上配置操作系统以识别辅助私有 IP 地址 \(p. 605\)](#)
- [将弹性 IP 地址与辅助私有 IP 地址关联 \(p. 605\)](#)
- [查看您的辅助私有 IP 地址 \(p. 605\)](#)
- [取消分配辅助私有 IP 地址 \(p. 605\)](#)

## 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 IP 地址。网络接口可与实例连接或断开。
- 您必须为网络接口选择一个子网 CIDR 块范围内的辅助私有 IP 地址。
- 安全组适用于网络接口，而不适用于 IP 地址。因此，IP 地址受在其中指定 IP 地址的网络接口的安全组约束。
- 可以将辅助私有 IP 地址分配给正在运行或已停止实例的弹性网络接口，也可以取消分配操作。
- 如果您明确允许，已分配到一个网络接口的辅助私有 IP 地址可以重新分配到其他网络接口。

- 当使用命令行工具或 API 将多个辅助私有 IP 地址分配给网络接口时，如果其中有一个辅助私有 IP 地址无法分配，整个操作都会失败。
- 当网络接口与实例断开或连接到其他实例时，主要私有 IP 地址、辅助私有 IP 地址以及任何相关的弹性 IP 地址将仍然属于此网络接口。
- 尽管您无法从实例移去主要网络接口，但是您可以将主要网络接口的辅助私有 IP 地址重新分配到另一个网络接口。
- 您可以将任何其他网络接口从一个实例移动到另一个。

下表说明了多个 IP 地址如何与弹性 IP 地址配合工作：

- 每个私有 IP 地址只能与一个弹性 IP 地址相关联，反之亦然。
- 当辅助私有 IP 地址重新分配到其他接口时，该私有 IP 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 IP 地址时，相关的弹性 IP 地址会自动取消与该辅助私有 IP 地址的关联。

## 分配辅助私有 IP 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 IP 地址。本节包括以下过程。

- 在 EC2-VPC 中启动实例时分配辅助私有 IP 地址 (p. 603)
- 使用命令行在启动期间分配辅助 IP 地址 (p. 604)
- 要向现有实例分配辅助私有 IP 地址 (p. 604)
- 使用命令行向现有实例分配辅助私有 IP (p. 604)

### 在 EC2-VPC 中启动实例时分配辅助私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 选择 Launch Instance。
3. 选择一个 AMI，然后选择实例类型并选择 Next: Configure Instance Details。
4. 在 Configure Instance Details (配置实例详细信息) 页面上，从 Network (网络) 列表中选择一个 VPC，并从 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：
  - a. 选择 Add Device 以添加另一个网络接口。当您启动实例时，控制台允许您指定最多两个网络接口。启动实例后，选择导航窗格中的 Network Interfaces 以添加其他网络接口。您可以连接的网络接口总数因实例类型而有所差异。有关更多信息，请参阅 [每个实例类型的每个网络接口的私有 IP 地址 \(p. 613\)](#)。



#### Important

当您添加另一个网络接口时，系统将无法再自动分配公有 IP 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 \(p. 608\)](#)。

- b. 对于每个网络接口，您都可以指定一个主要私有 IP 地址和一个或多个辅助私有 IP 地址。然而，在此示例接受了我们自动分配的 IP 地址。
- c. 在 Secondary IP addresses 下，选择 Add IP，然后输入子网范围内的私有 IP 地址，或接受默认设置 Auto-assign 以让我们选择一个地址。



### 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 IP 地址 \(p. 605\)](#)。

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: Tag Instance。
7. 在 Tag Instance 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。

### 使用命令行在启动期间分配辅助 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 \(p. 3\)](#)。

- 用于 `--secondary-private-ip-addresses` `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。

### 要向现有实例分配辅助私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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. 选择 Actions，然后选择 Manage Private IP Addresses。
4. 在 Manage Private IP Addresses (管理私有 IP 地址) 对话框中，执行以下操作：
  - a. 选择 Assign new IP。
  - b. 输入实例子网范围内的特定 IP 地址，或者将字段留空，系统将为您选择一个 IP 地址。
  - c. （可选）选择 Allow reassignment (允许重新分配)，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。
  - d. 选择 Yes, Update，然后选择 Close。

请注意，您也可以为实例分配辅助私有 IP 地址。在导航窗格中选择 Instances，选择实例，选择 Actions，选择 Networking，然后选择 Manage Private IP Addresses。您可以按上述步骤进行操作，在对话框中配置相同的内容。

### 使用命令行向现有实例分配辅助私有 IP

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 IP 地址

将辅助私有 IP 地址分配到实例后，您需要在实例上配置操作系统，以识别辅助私有 IP 地址。

有关配置 Windows 实例的信息，请参阅 *Amazon EC2 用户指南（适用于 Microsoft Windows 实例）中的为 VPC 中的 Windows 实例配置辅助私有 IP 地址 (p. 319)*。

## 将弹性 IP 地址与辅助私有 IP 地址关联

在 EC2-VPC 中将弹性 IP 地址与辅助私有 IP 地址关联

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Actions，然后选择 Associate Address。
4. 在 Associate Address 对话框中，从 Network Interface 下拉列表中选择网络接口，然后从 Private IP address 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 IP 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 IP 地址

在 EC2-VPC 中查看分配给网络接口的私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 (详细信息) 选项卡上，查看 Primary private IP (主要私有 IP) 和 Secondary private IPs (辅助私有 IP) 字段，了解分配到网络接口的主要私有 IP 地址和任何辅助私有 IP 地址。

要查看分配到实例的 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择您要查看其私有 IP 地址的实例。
4. 在详细信息窗口的 Description (描述) 选项卡上，检查通过实例的网络接口分配给实例的主要私有 IP 地址和任何辅助私有 IP 地址的 Private IPs (私有 IP) 和 Secondary private IPs (辅助私有 IP) 字段。

## 取消分配辅助私有 IP 地址

如果您不再需要辅助私有 IP 地址，则可以从实例或网络接口取消分配操作。当从弹性网络接口取消分配辅助私有 IP 地址后，此弹性 IP 地址（如果存在）也会断开相关联系。

要从实例取消分配辅助私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在导航窗格中，选择 Instances。
3. 选择一个实例，选择 Actions，选择 Networking，然后选择 Manage Private IP Addresses。
4. 在 Manage Private IP Addresses 对话框中，在要取消分配的辅助私有 IP 地址的旁边选择 Unassign。
5. 选择 Yes, Update，然后关闭对话框。

要从网络接口取消分配辅助私有 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择网络接口、Actions 和 Manage Private IP Addresses。
4. 在 Manage Private IP Addresses 对话框中，在要取消分配的辅助私有 IP 地址的旁边选择 Unassign。
5. 选择 Yes, Update，然后选择 Close。

使用命令行取消分配辅助私有 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 \(p. 3\)](#)。

- [unassign-private-ip-addresses \(AWS CLI\)](#)
- [Unregister-EC2PrivateIpAddress \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 弹性 IP 地址

### Abstract

您可以将弹性 IP 地址从一个实例快速重新映射到另一个实例，以处理实例或软件的问题。

弹性 IP 地址是专为动态云计算设计的静态 IP 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 IP 地址，可通过 Internet 访问。如果您的实例没有公有 IP 地址，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，从您的本地计算机连接到您的实例。

#### 主题

- [弹性 IP 地址基础信息 \(p. 606\)](#)
- [EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别 \(p. 607\)](#)
- [使用弹性 IP 地址 \(p. 608\)](#)
- [将反向 DNS 用于电子邮件应用程序 \(p. 612\)](#)
- [弹性 IP 地址限额 \(p. 612\)](#)

## 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 IP 地址（如果有）将释放回 Amazon 的公有 IP 地址池中。您无法重用公有 IP 地址。有关更多信息，请参阅 [公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。
- 您可以取消弹性 IP 地址与资源的关联，然后重新将此地址与其他资源关联。
- 取消关联的弹性 IP 地址保持分配到您的账户，直至您明确释放它。

- 为确保弹性 IP 地址的有效使用，如果弹性 IP 地址未与正在运行的实例关联，或者它已与停止的实例或未连接的网络接口关联，我们将强制收取小额的小时费用。当您的实例正在运行时，您无需为与该实例关联的某个弹性 IP 地址付费，但需为与该实例关联的所有其他弹性 IP 地址付费。有关更多信息，请参阅 [Amazon EC2 定价](#)。
- 弹性 IP 地址只能在一个特定区域中使用。
- 在将弹性 IP 地址与之前具有公共 IP 地址的实例关联时，实例的公共 DNS 主机名称将发生更改以匹配弹性 IP 地址。
- 我们会将公共 DNS 主机名解析为实例所在网络外部的该实例的公有 IP 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 IP 地址。

如果您的账户支持 EC2-Classic，则 EC2-Classic 与 EC2-VPC 的弹性 IP 地址的使用和行为可能有所不同。有关更多信息，请参阅 [EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别 \(p. 607\)](#)。

## EC2-Classic 与 EC2-VPC 的弹性 IP 地址的区别

如果您的账户支持 EC2-Classic，则其中一个弹性 IP 地址池可与 EC2-Classic 平台配合使用，而另一个可与 EC2-VPC 平台配合使用。您不能将已分配与 VPC 配合使用的弹性 IP 地址与 EC2-Classic 中的实例相关联，反之亦然。但是，您可将已分配在 EC2-Classic 平台中使用的弹性 IP 地址迁移至 EC2-VPC 平台。您不能将弹性 IP 地址迁移到另一个区域。有关 EC2-Classic 和 EC2-VPC 的更多信息，请参阅[支持的平台 \(p. 577\)](#)。

当您将弹性 IP 地址与 EC2-Classic（默认 VPC）中的实例或与您在启动时为 eth0 网络接口分配了公有 IP 的非默认 VPC 中的实例关联时，该实例的当前公有 IP 地址会释放回公有 IP 地址池。如果您从实例断开弹性 IP 地址，实例会在几分钟内自动分配到新的公有 IP 地址。但是，如果将第二个网络接口连接到 VPC 中的实例，则不会为该实例自动分配新的公有 IP 地址。有关公有 IP 地址的更多信息，请参阅[公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。

有关对 VPC 中的实例使用弹性 IP 地址的信息，请参阅 *Amazon VPC 用户指南* 中的[弹性 IP 地址](#)。

下表列出了 EC2-Classic 和 EC2-VPC 上的弹性 IP 地址之间的区别。有关私有 IP 地址和公有 IP 地址之间的区别的更多信息，请参阅 [EC2-Classic 和 EC2-VPC 之间的 IP 地址区别 \(p. 599\)](#)。

| 性能           | EC2-Classic                                                                                                                            | EC2-VPC                                                                                                                         |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 分配弹性 IP 地址   | 在分配弹性 IP 地址后，它将在 EC2-Classic 中使用；但是，您可将弹性 IP 地址迁移到 EC2-VPC 平台。有关更多信息，请参阅 <a href="#">将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 608)</a> 。 | 在分配弹性 IP 地址后，它将只能在 VPC 中使用。                                                                                                     |
| 分配弹性 IP 地址   | 将弹性 IP 地址与实例相关联。                                                                                                                       | 弹性 IP 地址是弹性网络接口 (ENI) 的一个属性。您可以通过更新连接到实例的 ENI，将弹性 IP 地址与实例关联起来。有关更多信息，请参阅 <a href="#">弹性网络接口 (ENI) (p. 612)</a> 。               |
| 取消关联弹性 IP 地址 | 如果您试图关联已与其他实例关联的弹性 IP 地址，该地址会自动与新实例关联。                                                                                                 | 如果您的账户仅支持 EC2-VPC，并且您尝试关联已与其他实例相关联的弹性 IP 地址，则该地址会自动与新实例关联。如果您在 EC2-Classic 账户中使用 VPC，并且您尝试关联已与其他实例相关联的弹性 IP 地址，则仅当您允许重新关联时才会成功。 |

| 性能         | EC2-Classic                                           | EC2-VPC                                                                                  |
|------------|-------------------------------------------------------|------------------------------------------------------------------------------------------|
| 停止实例       | 如果您停止某个实例，则其弹性 IP 地址将取消关联；在您重新启动该实例时，必须重新关联该弹性 IP 地址。 | 如果您停止某个实例，其弹性 IP 地址会保持关联。                                                                |
| 分配多个 IP 地址 | 实例仅支持一个私有 IP 地址和一个相应的弹性 IP 地址。                        | 实例支持多个 IP 地址，并且每个 IP 地址都可以拥有相应的弹性 IP 地址。有关更多信息，请参阅 <a href="#">多个私有 IP 地址 (p. 602)</a> 。 |

## 将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC

如果您的账户支持 EC2-Classic，则可将已分配为在 EC2-Classic 平台中使用的弹性 IP 地址迁移至同一区域中的 EC2-VPC 平台。这可帮助您将资源从 EC2-Classic 迁移到 VPC；例如，您可在 VPC 中启动新的 Web 服务器，然后将 EC2-Classic 中您的 Web 服务器所使用的弹性 IP 地址用于新的 VPC Web 服务器。

在将弹性 IP 地址迁移至 EC2-VPC 后，您将无法在 EC2-Classic 平台中使用该地址；不过，如果需要，您可以将该地址还原至 EC2-Classic。在将弹性 IP 地址还原至 EC2-Classic 后，您将无法在 EC2-VPC 中使用该地址，直至您重新迁移它。只能将弹性 IP 地址从 EC2-Classic 迁移至 EC2-VPC。不能将本来分配为在 EC2-VPC 中使用的弹性 IP 地址迁移至 EC2-Classic。

要迁移弹性 IP 地址，则不得将该地址与实例关联。有关解除弹性 IP 地址与实例的关联的更多信息，请参阅 [取消关联弹性 IP 地址，并将它与其他实例重新关联 \(p. 610\)](#)。

您可以迁移您账户中拥有的数量的 EC2-Classic 弹性 IP 地址。但是，在将弹性 IP 地址迁移到 EC2-VPC 时，该地址会计入 EC2-VPC 的弹性 IP 地址限制。如果某个弹性 IP 地址将导致您超出限制，则不能迁移该地址。同样，在将弹性 IP 地址还原到 EC2-Classic 时，该地址会计入 EC2-Classic 的弹性 IP 地址限制。有关更多信息，请参阅 [弹性 IP 地址限额 \(p. 612\)](#)。

您不能迁移在 24 小时之前分配给您的账户弹性 IP 地址。

有关更多信息，请参阅 [移动弹性 IP 地址 \(p. 610\)](#)。

## 使用弹性 IP 地址

以下部分介绍如何使用弹性 IP 地址。

### 主题

- [分配弹性 IP 地址 \(p. 608\)](#)
- [描述您的弹性 IP 地址 \(p. 609\)](#)
- [将弹性 IP 地址与正在运行的实例关联起来 \(p. 609\)](#)
- [取消关联弹性 IP 地址，并将它与其他实例重新关联 \(p. 610\)](#)
- [移动弹性 IP 地址 \(p. 610\)](#)
- [释放弹性 IP 地址 \(p. 611\)](#)

## 分配弹性 IP 地址

您可以使用 Amazon EC2 控制台或命令行分配弹性 IP 地址。如果您的账户支持 EC2-Classic，则可分配一个地址来在 EC2-Classic 或 EC2-VPC 中使用。

### 使用控制台分配用于 EC2-VPC 的弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate New Address。
4. (EC2-Classic 账户) 在 Allocate New Address 对话框中，从 EIP used in 中选择 VPC，然后选择 Yes, Allocate。关闭确认对话框。
5. (仅限 VPC 账户) 选择 Yes, Allocate，然后关闭确认对话框。

### 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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate New Address。
4. 依次选择 EC2 和 Yes, Allocate。关闭确认对话框。

### 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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 从“Resource Attribute (资源属性)”列表中选择筛选条件以开始搜索。可以在单个搜索中使用多个筛选条件。

### 使用命令行描述您的弹性 IP 地址

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

- [describe-addresses \(AWS CLI\)](#)
- [Get-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 将弹性 IP 地址与正在运行的实例关联起来

您可以使用 Amazon EC2 控制台或命令行将弹性 IP 地址关联到实例。

(仅限 VPC) 如果要将弹性 IP 地址与您的实例关联以启用与 Internet 的通信，您还必须确保您的实例在公有子网中。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 *Internet 网关*。

### 使用控制台将弹性 IP 地址与实例关联

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Associate Address。
4. 在 Associate Address 对话框中，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.amazonaws.cn/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. 当系统提示进行确认时，选择 Yes, Disassociate。
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. 在 Associate Address 对话框中，从 Instance 中选择新实例，然后选择 Associate。

#### 使用命令行取消关联弹性 IP 地址

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

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

#### 使用命令行关联弹性 IP 地址

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

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

## 移动弹性 IP 地址

目前，您只能使用 Amazon EC2 查询 API、AWS 软件开发工具包或 AWS CLI 来将弹性 IP 地址迁移至 EC2-VPC 或将其还原至 EC2-Classic。

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。

如果弹性 IP 地址处于移动状态超过 5 分钟，请联系 <http://www.amazonaws.cn/support-plans/>。

#### 使用 Amazon EC2 查询 API 或 AWS CLI 移动弹性 IP 地址

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

- [move-address-to-vpc](#) (AWS CLI)
- [MoveAddressToVpc](#) ( Amazon EC2 查询 API )
- [Move-EC2AddressToVpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 Amazon EC2 查询 API 或 AWS CLI 将弹性 IP 地址还原到 EC2-Classic

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

- [restore-address-to-classic](#) (AWS CLI)
- [RestoreAddressToClassic](#) ( Amazon EC2 查询 API )
- [Restore-EC2AddressToClassic](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 Amazon EC2 查询 API 或 AWS CLI 描述移动中的地址的状态

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

- [describe-moving-addresses](#) (AWS CLI)
- [DescribeMovingAddresses](#) ( Amazon EC2 查询 API )
- [Get-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

在 EC2-VPC 中检索已迁移的弹性 IP 地址的分配 ID

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

- [describe-addresses](#) (AWS CLI)
- [DescribeAddresses](#) ( Amazon EC2 查询 API )
- [Get-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

## 释放弹性 IP 地址

如果您不再需要弹性 IP 地址，我们建议您解除此弹性 IP 地址（地址不可与实例相关联）。对于已分配用于 EC2-Classic 但未与实例关联的所有弹性 IP 地址，您也需要承担相应费用。

您可以使用 Amazon EC2 控制台或命令行释放弹性 IP 地址。

使用控制台释放弹性 IP 地址

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 Yes, Release。

使用命令行释放弹性 IP 地址

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

- [release-address](#) (AWS CLI)
- [Remove-EC2Address](#) (适用于 Windows PowerShell 的 AWS 工具)

## 将反向 DNS 用于电子邮件应用程序

如果您打算从实例向第三方发送电子邮件，我们建议您调配一个或多个弹性 IP 地址，并将它们提供给我们。AWS 与 ISP 以及国际反垃圾电子邮件组织合作，减少从这些地址发送的电子邮件被标记为垃圾电子邮件的机率。

此外，还向您用于发送电子邮件的弹性 IP 地址分配了静态反向 DNS 记录，有助于避免电子邮件被一些反垃圾电子邮件组织标记为垃圾电子邮件。请注意，必须要先有指向您的弹性 IP 地址的对应的正向 DNS 记录（记录类型 A），然后我们才能创建反向 DNS 记录。

如果反向 DNS 记录与弹性 IP 地址关联，则该弹性 IP 地址将锁定到您的账户中且无法从您的账户中释放，直至删除记录。

要删除电子邮件发送限制，或向我们提供您的弹性 IP 地址和反向 DNS 记录，请前往[请求删除电子邮件发送限制](#)页面。

## 弹性 IP 地址限额

在默认情况下，所有 AWS 账户最多可拥有 5 个弹性 IP 地址，因为公有 (IPv4) Internet 地址是稀缺的公共资源。我们大大鼓励您主要使用弹性 IP 地址，以便在实例发生故障的情况下能够将该地址映射到另一实例，并能够将 DNS 主机名用于所有其他节点间通信。

如果您认为您的架构需要额外的弹性 IP 地址，请填写[Amazon EC2 弹性 IP 地址申请表](#)。我们会要求您描述您的使用案例，让我们能够了解您对额外地址的需求。

## 弹性网络接口 (ENI)

### Abstract

将弹性网络接口连接到您的实例，以指定其私有 IP 地址、弹性 IP 地址和安全组。

弹性网络接口 (ENI) 是一种虚拟网络接口，您可以将其连接至 VPC 中的实例。ENI 只可用于在 VPC 中运行的实例。

ENI 包含以下属性：

- 主要私有 IP 地址。
- 一个或多个次要私有 IP 地址。
- 每个私有 IP 地址一个弹性 IP 地址。
- 一个公有 IP 地址，该地址在您启动实例时可自动分配到 eth0 的弹性网络接口。有关更多信息，请参阅[网络接口的公有 IP 地址 \(p. 615\)](#)。
- 一个或多个安全组。
- MAC 地址。
- 源/目标检查标记。
- 描述。

您可以创建一个弹性网络接口，将其附加到一个实例上，然后将其与实例分离再附加到另一个实例上。弹性网络接口的属性会在该接口连接一个实例或断开与一个实例的连接并重新连接至另一实例时跟随该接口。当您将一个弹性网络接口从一个实例移动到另一个实例时，网络流量也会重定向到新的实例。

VPC 中的每个实例都有一个默认的弹性网络接口（主网络接口 eth0），并会被指定一个在您的 VPC 的 IP 地址范围内的私有 IP 地址。您无法从实例断开主网络接口。您可以创建并连接额外的弹性网络接口。您可以使用的弹性网络接口的最大数量根据实例类型而不同。有关更多信息，请参阅 [每个实例类型的每个网络接口的私有 IP 地址 \(p. 613\)](#)。

当您想执行以下操作时，将多个弹性网络接口连接至实例很有帮助：

- 创建管理网络。
- 在您的 VPC 中使用网络和安全性设备。
- 创建双归属实例，并在不同子网间分配工作负载/任务。
- 创建低预算、高可用性的解决方案。

#### 内容

- [每个实例类型的每个网络接口的私有 IP 地址 \(p. 613\)](#)
- [网络接口的公有 IP 地址 \(p. 615\)](#)
- [创建一个管理网络 \(p. 615\)](#)
- [使用您的 VPC 中的网络和安全设备 \(p. 616\)](#)
- [通过不同子网的工作负载/角色创建双主机实例。 \(p. 616\)](#)
- [创建一个低成本、高可用性解决方案 \(p. 616\)](#)
- [监控您的网络接口上的 IP 流量 \(p. 616\)](#)
- [有关配置弹性网络接口的最佳实践 \(p. 617\)](#)
- [创建弹性网络接口 \(p. 617\)](#)
- [删除弹性网络接口 \(p. 618\)](#)
- [查看有关弹性网络接口的详细信息 \(p. 618\)](#)
- [在启动实例时连接弹性网络接口 \(p. 618\)](#)
- [将弹性网络接口连接至已停止的实例或正在运行的实例 \(p. 619\)](#)
- [从实例中分离弹性网络接口 \(p. 620\)](#)
- [更改弹性网络接口的安全组 \(p. 621\)](#)
- [更改弹性网络接口的源/目标检查 \(p. 621\)](#)
- [将弹性 IP 地址与弹性网络接口相关联 \(p. 622\)](#)
- [解除弹性 IP 地址与弹性网络接口的关联 \(p. 622\)](#)
- [更改弹性网络接口的终止行为 \(p. 622\)](#)
- [添加或编辑弹性网络接口的描述 \(p. 623\)](#)
- [添加或编辑弹性网络接口的标签 \(p. 623\)](#)

## 每个实例类型的每个网络接口的私有 IP 地址

下表列出了每种实例类型的最大弹性网络接口 (ENI) 数，以及每个 ENI 的最大私有 IP 地址数。ENI 和多个私有 IP 地址仅适用于在 VPC 中运行的实例。有关更多信息，请参阅 [多个私有 IP 地址 \(p. 602\)](#)。

| 实例类型      | 最大弹性网络接口数 | 每个接口的 IP 地址 |
|-----------|-----------|-------------|
| c1.medium | 2         | 6           |
| c1.xlarge | 4         | 15          |
| c3.large  | 3         | 10          |
| c3.xlarge | 4         | 15          |

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
每个实例类型的每个网络接口的私有 IP 地址

---

| 实例类型         | 最大弹性网络接口数 | 每个接口的 IP 地址 |
|--------------|-----------|-------------|
| c3.2xlarge   | 4         | 15          |
| c3.4xlarge   | 8         | 30          |
| c3.8xlarge   | 8         | 30          |
| c4.large     | 3         | 10          |
| c4.xlarge    | 4         | 15          |
| c4.2xlarge   | 4         | 15          |
| c4.4xlarge   | 8         | 30          |
| c4.8xlarge   | 8         | 30          |
| cc2.8xlarge  | 8         | 30          |
| cg1.4xlarge  | 8         | 30          |
| crl1.8xlarge | 8         | 30          |
| d2.xlarge    | 4         | 15          |
| d2.2xlarge   | 4         | 15          |
| d2.4xlarge   | 8         | 30          |
| d2.8xlarge   | 8         | 30          |
| g2.2xlarge   | 4         | 15          |
| g2.8xlarge   | 8         | 30          |
| hi1.4xlarge  | 8         | 30          |
| hs1.8xlarge  | 8         | 30          |
| i2.xlarge    | 4         | 15          |
| i2.2xlarge   | 4         | 15          |
| i2.4xlarge   | 8         | 30          |
| i2.8xlarge   | 8         | 30          |
| m1.small     | 2         | 4           |
| m1.medium    | 2         | 6           |
| m1.large     | 3         | 10          |
| m1.xlarge    | 4         | 15          |
| m2.xlarge    | 4         | 15          |
| m2.2xlarge   | 4         | 30          |
| m2.4xlarge   | 8         | 30          |
| m3.medium    | 2         | 6           |

| 实例类型        | 最大弹性网络接口数 | 每个接口的 IP 地址 |
|-------------|-----------|-------------|
| m3.large    | 3         | 10          |
| m3.xlarge   | 4         | 15          |
| m3.2xlarge  | 4         | 30          |
| m4.large    | 2         | 10          |
| m4.xlarge   | 4         | 15          |
| m4.2xlarge  | 4         | 15          |
| m4.4xlarge  | 8         | 30          |
| m4.10xlarge | 8         | 30          |
| r3.large    | 3         | 10          |
| r3.xlarge   | 4         | 15          |
| r3.2xlarge  | 4         | 15          |
| r3.4xlarge  | 8         | 30          |
| r3.8xlarge  | 8         | 30          |
| t1.micro    | 2         | 2           |
| t2.nano     | 2         | 2           |
| t2.micro    | 2         | 2           |
| t2.small    | 2         | 4           |
| t2.medium   | 3         | 6           |
| t2.large    | 3         | 12          |
| x1.32xlarge | 8         | 30          |

## 网络接口的公有 IP 地址

在 VPC 中，所有子网都有一个属性可指定是否为子网中启动的实例分配公有 IP 地址。公有 IP 地址从 Amazon 的公有 IP 地址池进行分配，并分配给设备索引为 eth0 ( 主网络接口 ) 的网络接口。

默认情况下，在默认子网中启动的实例会自动分配一个公有 IP 地址，除非您在启动过程中另行指定，或者您修改了子网的公有 IP 地址属性，或者您在启动时指定了多个网络接口。默认情况下，在非默认子网中启动的实例不会自动分配一个公有 IP 地址，除非您在启动时另行指定，或者您修改了子网的公有 IP 地址属性。此外，对于非默认子网，公有 IP 地址仅可以自动分配给单个新的网络接口。

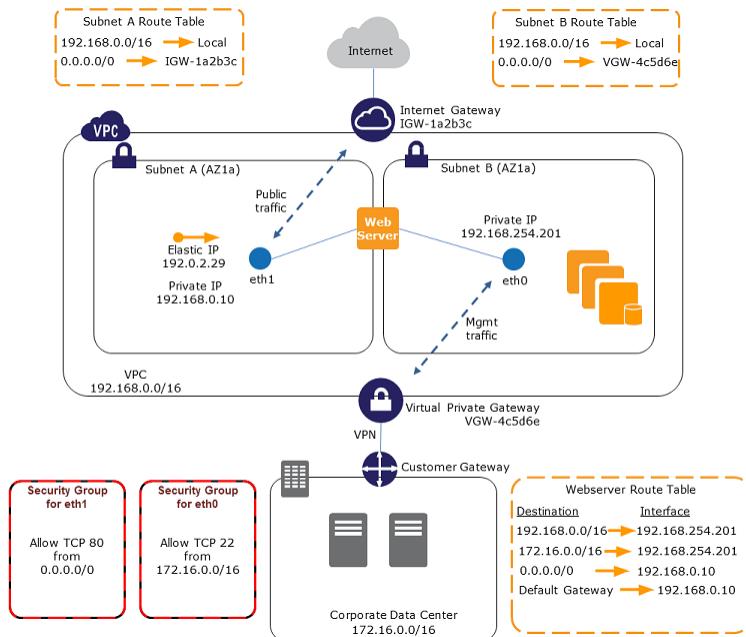
有关更多信息，请参阅 [公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#) 和 [分配公有 IP 地址 \(p. 601\)](#)。

## 创建一个管理网络

您可使用弹性网络接口创建管理网络。在这种情况下，实例上的辅助弹性网络接口处理面向公众的流量，主要弹性网络接口处理后端管理流量并与您的有较多限制性访问控制的 VPC 中单独的子网相连接。面向公众的接口可能在也有可能不在负载均衡器之后，它有一个相关安全组来实现通过 Internet 对服务器进行的访问（例如，允许 TCP 端口 80 和 443 通过 0.0.0.0/0 或负载均衡器访问），而面向私人的接口的

相关安全组只能确保通过 VPC 或 Internet 中允许的 IP 地址范围、VPC 或虚拟专用网关内的私有子网访问 RDP。

为确保故障转移功能，考虑针对弹性网络接口上的传入流量使用辅助私有 IP。实例失效时，您可以将接口和/或次要私有 IP 地址移动到备用实例中。



## 使用您的 VPC 中的网络和安全设备

负载均衡器、网络地址转换 (NAT) 服务器和代理服务器等网络和安全设备更偏向于配置多个弹性网络接口。您可以创建并连接辅助弹性网络接口至 VPC 中正在运行这些类型的应用程序的实例，并使用实例自己的公用和私有 IP 地址、安全组和源/目标检查配置其他接口。

## 通过不同子网的工作负荷/角色创建双主机实例。

您可以将弹性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，则其弹性网络接口可连接至一个针对同一种角色预配置的替代或热备用实例，以快速恢复服务。例如，您可以将 ENI 用作数据库实例或 NAT 实例等关键服务的主要或次要网络接口。如果实例失效，您（或更有可能时代表您运行的代码）可将 ENI 连接至热备用实例。由于接口保持其私有 IP 地址、弹性 IP 地址和 MAC 地址，网络流量在您一开始将 ENI 连接至替代实例时就会开始流向备用实例。在实例失效与 ENI 连接至备用实例这个时间期间内，用户会感到暂时失去连接，但不需要更改 VPC 路由表或您的 DNS 服务器。

## 监控您的网络接口上的 IP 流量

您可以在弹性网络接口上启用 VPC 流日志以捕获有关出入该接口的 IP 流量的信息。创建流日志后，您可以在 Amazon CloudWatch Logs 中查看和检索其数据。

有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [VPC 流日志](#)。

## 有关配置弹性网络接口的最佳实践

- 您可以在实例运行时（热连接）、实例停止时（暖连接）或实例启动时（冷连接）将弹性网络接口连接至实例。
- 您可以在实例运行时或停止时分离辅助 (ethN) 弹性网络接口。但您不能分离主要 (eth0) 接口。
- 您可以在同一个 VPC 中将一个子网中的弹性网络接口连接至另一个子网中的实例；但是，该弹性网络接口和实例必须在同一个可用区内。
- 通过 CLI 或 API 启动实例时，您可针对主要 (eth0) 弹性网络接口和额外弹性网络接口指定要连接至实例的弹性网络接口。
- 启动具有多个网络接口的 Amazon Linux 或 Microsoft Windows Server 实例会自动在该实例的操作系统上配置接口、私有 IP 地址和路由表。
- 额外弹性网络接口的暖连接或热连接可能需要您手动添加第二个接口、配置私有 IP 地址并相应修改路由表。运行 Amazon Linux 或 Microsoft Windows Server 的实例会自动识别暖挂载或热挂载，并自行进行配置。
- 将另一个弹性网络接口连接至实例并非是提高网络带宽或使与双主机实例相连接的网络带宽加倍的方法。
- 如果将来自同一子网的两个或多个网络接口连接到一个实例，可能会遇到非对称路由等联网问题。请尽可能在主网络接口上使用辅助私有 IP 地址。有关更多信息，请参阅 [分配辅助私有 IP 地址 \(p. 603\)](#)。如果需要使用多个网络接口，则必须将网络接口配置为使用静态路由。有关更多信息，请参阅 [配置辅助弹性网络接口 \(p. 323\)](#)。

## 创建弹性网络接口

您可使用 Amazon EC2 控制台或命令行创建弹性网络接口。

### 使用控制台创建弹性网络接口

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择 Create Network Interface。
4. 在 Create Network Interface 对话框中，提供弹性网络接口的以下信息，然后选择 Yes, Create。
  - a. 对于 Description，输入一个描述性名称。
  - b. 对于 Subnet，选择子网。请注意，您不能在创建弹性网络接口之后将其移动至另一子网，而且您只能将该接口连接至同一可用区中的实例。
  - c. 对于 Private IP，输入主私有 IP 地址。如果您未指定 IP 地址，我们将在所选子网中选择一个可用的私有 IP 地址。
  - d. 对于 Security groups，选择一个或多个安全组。

### 使用命令行创建弹性网络接口

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)

## 删除弹性网络接口

您必须先将弹性网络接口与实例分离，然后才能删除弹性网络接口。删除弹性网络接口之后，所有与该接口关联的属性都会被释放，而且所有私有 IP 地址或弹性 IP 地址也都会被释放以供另一个实例使用。

您可使用 Amazon EC2 控制台或命令行删除弹性网络接口。

使用控制台删除弹性网络接口

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择一个弹性网络接口，然后选择 Delete。
4. 在 Delete Network Interface 对话框中，选择 Yes, Delete。

使用命令行删除弹性网络接口

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)

## 查看有关弹性网络接口的详细信息

您可以使用 Amazon EC2 控制台或命令行描述弹性网络接口。

使用控制台描述弹性网络接口

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择弹性网络接口。
4. 在 Details (详细信息) 选项卡上查看详细信息。

使用命令行描述弹性网络接口

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)

使用命令行描述弹性网络接口属性

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)

## 在启动实例时连接弹性网络接口

启动实例时，您可以指定一个现有的网络接口或连接其他网络接口。您可以使用 Amazon EC2 控制台或命令行执行此操作。



#### Note

如果在将弹性网络接口连接至实例时发生错误，则会导致实例启动失败。

### 使用控制台在启动实例时连接弹性网络接口

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 Network Interfaces 部分，当您启动实例时，控制台允许您最多指定 2 个弹性网络接口（新接口和/或现有接口）。对于每个新接口，您还可以输入一个主要 IP 地址和一个或多个辅助 IP 地址。完成后，选择 Next: Add Storage。

启动实例后，您可以将更多网络接口添加到该实例。您可以连接的网络接口总数因实例类型而有所差异。有关更多信息，请参阅 [每个实例类型的每个网络接口的私有 IP 地址 \(p. 613\)](#)。



#### Note

如果您指定了多个网络接口，则无法将公有 IP 地址自动分配到您的实例。

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 Tag Instance。
7. 在 Tag Instance 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 页面上，您可以选择一个安全组，也可以创建新的安全组。选择 Review and Launch。



#### Note

如果您在第 5 步指定了一个现有网络接口，实例将与该网络接口的安全组关联，无论您在此步骤中选择哪个选项。

9. Review Instance Launch (查看实例启动) 页面上会显示有关主要网络接口和其他网络接口的详细信息。检查设置，然后选择 Launch 以选择密钥对并启动实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

### 使用命令行在启动实例时连接弹性网络接口

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)

## 将弹性网络接口连接至已停止的实例或正在运行的实例

您可通过 Amazon EC2 控制台的 Instances 或 Network Interfaces 页面或者使用命令行界面，将弹性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

如果您的实例的公有 IP 地址已释放，则在多个弹性网络接口与实例相连的情况下，该实例不会接收新地址。有关公有 IP 地址行为的更多信息，请参阅[公有 IP 地址和外部 DNS 主机名 \(p. 598\)](#)。

#### 使用实例页面将弹性网络接口连接至实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择 Actions、Networking、Attach Network Interface。
4. 在 Attach Network Interface 对话框中，选择弹性网络接口，然后选择 Attach。

#### 使用网络接口页面将弹性网络接口连接至实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择弹性网络接口，然后选择 Attach。
4. 在 Attach Network Interface 对话框中，选择实例，然后选择 Attach。

#### 使用命令行将弹性网络接口连接至实例

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)

## 从实例中分离弹性网络接口

您可随时通过 Amazon EC2 控制台的 Instances 或 Network Interfaces 页面或使用命令行界面来将辅助弹性网络接口断开。

#### 使用实例页面将弹性网络接口与实例断开

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择 Actions、Networking、Detach Network Interface。
4. 在 Detach Network Interface 对话框中，选择弹性网络接口，然后选择 Detach。

#### 使用网络接口页面将弹性网络接口与实例断开

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择弹性网络接口，然后选择 Detach。
4. 在 Detach Network Interface 对话框中，选择 Yes, Detach。如果弹性网络接口未能与实例断开，请选择 Force detachment，然后重试。

#### 使用命令行断开弹性网络接口

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

## 更改弹性网络接口的安全组

您可更改与弹性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 作为该接口的子网。

您可以使用 Amazon EC2 控制台或命令行更改您的弹性网络接口的安全组。



### Note

要更改其他服务（如 Elastic Load Balancing）所拥有的接口的安全组成员身份，请使用该服务的控制台或命令行界面。

#### 使用控制台更改弹性网络接口的安全组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 和 Change Security Groups。
4. 在 Change Security Groups 对话框中，选择要使用的安全组，然后选择 Save。

#### 使用命令行更改弹性网络接口的安全组

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

## 更改弹性网络接口的源/目标检查

源/目标检查属性用于控制源/目标检查是否已在实例上启用。禁用此属性后，实例会处理并未明确指定至该实例的网络通信。例如，运行网络地址转换、路由或防火墙等服务的实例应将此值设置为 disabled。默认值为 enabled。

您可以使用 Amazon EC2 控制台或命令行更改源/目标检查。

#### 使用控制台更改弹性网络接口的源/目标检查

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 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。

#### 使用命令行更改弹性网络接口的源/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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 将弹性 IP 地址与弹性网络接口相关联

如果您有弹性 IP 地址，则可将它与弹性网络接口的其中一个私有 IP 地址关联起来。您可以为每个私有 IP 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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 和 Associate Address。
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 IP 地址。
6. 选择 Allow reassociation 以允许弹性 IP 地址在已与另一个实例或网络接口相关联的情况下与指定网络接口关联，然后选择 Associate Address。

使用命令行关联弹性 IP 地址

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

- [associate-address \(AWS CLI\)](#)
- [Register-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 解除弹性 IP 地址与弹性网络接口的关联

如果弹性网络接口有一个与之关联的弹性 IP 地址，您可以取消此地址的关联，然后将其与另一个弹性网络接口关联，或将其释放回地址池中。请注意，要通过弹性网络接口将弹性 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，因为弹性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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 和 Disassociate Address。
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 \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 更改弹性网络接口的终止行为

您可设置连接至实例的弹性网络接口的终止行为，以便在您删除其所连接的实例时自动删除该接口。



### Note

默认情况下，使用控制台自动创建和连接至实例的弹性网络接口会设置为在实例终止时终止。但是使用命令行界面创建的网络接口不会被设置为在实例终止时终止。

您可以使用 Amazon EC2 控制台或命令行更改弹性网络接口的终止行为。

#### 使用控制台更改弹性网络接口的终止行为

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 和 Change Termination Behavior。
4. 如果您希望在终止实例时删除弹性网络接口，请在 Change Termination Behavior 对话框中选中 Delete on termination 复选框。

#### 使用命令行更改弹性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)

## 添加或编辑弹性网络接口的描述

您可以使用 Amazon EC2 控制台或命令行更改弹性网络接口的描述。

#### 使用控制台更改弹性网络接口的描述

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 依次选择弹性网络接口、Actions 和 Change Description。
4. 在 Change Description 对话框中，输入对弹性网络接口的描述，然后选择 Save。

#### 使用命令行更改弹性网络接口的描述

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)

## 添加或编辑弹性网络接口的标签

标签是您可以添加到弹性网络接口的元数据。标签是私有的，只有您的账户可见。每一个标签都包含一个密钥和一个可选值。有关标签的更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 737\)](#)。

您可以使用 Amazon EC2 控制台或命令行标记资源。

#### 使用控制台添加或编辑弹性网络接口的标签

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。

3. 选择弹性网络接口。
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弹性网络接口的标签

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

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (适用于 Windows PowerShell 的 AWS 工具)

## 置放群组

### Abstract

使用置放群组（具有单个可用区的实例的逻辑分组）进行紧密耦合的节点对节点通信。

置放群组是单个可用区中的实例的逻辑分组。使用置放群组使应用程序可以加入低延迟的 10 Gbps 网络。建议将置放群组用于可受益于低网络延迟、高网络吞吐量或两者的应用程序。要为置放群组提供最低延迟和最高每秒数据包数的网络性能，请选择支持增强联网的实例类型。有关更多信息，请参阅 [增强联网 \(p. 630\)](#)。

首先，您可创建置放群组，然后可将多个实例启动到该置放群组中。我们建议您在单个启动请求中启动置放群组中需要数量的实例，并对置放群组中的所有实例使用相同的实例类型。如果您以后尝试将更多实例添加到置放群组，或者如果您尝试在置放群组中启动多个实例类型，都会增大发生容量不足错误的可能性。

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重启该实例，尝试再次启动。

### 内容

- [置放群组的限制 \(p. 624\)](#)
- [将实例启动到置放群组中 \(p. 625\)](#)
- [删除置放群组 \(p. 626\)](#)

## 置放群组的限制

置放群组有以下限制：

- 置放群组不可跨越多个可用区。
- 您为置放群组指定的名称在您的 AWS 账户中必须是唯一的。
- 将实例启动到置放群组中时，仅可使用以下实例类型：
  - 通用型: m4.large | m4.xlarge | m4.2xlarge | m4.4xlarge | m4.10xlarge
  - 计算优化: c4.large | c4.xlarge | c4.2xlarge | c4.4xlarge | c4.8xlarge | c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge | cc2.8xlarge
  - 内存优化: cr1.8xlarge | r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge | x1.32xlarge

- 存储优化: d2.xlarge | d2.2xlarge | d2.4xlarge | d2.8xlarge | h1.4xlarge | hs1.8xlarge | i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge
- GPU: cg1.4xlarge | g2.2xlarge | g2.8xlarge
- 并非所有可以在置放群组中启动的实例类型都能够充分利用所提供的 10 Gbps 网络速度。[Amazon EC2 实例类型矩阵](#)列出了支持 10 Gb/s 网络速度的实例类型。
- 虽然可以将多个实例类型启动到一个置放群组中，但这会减小提供成功启动所需容量的可能性。我们建议对一个置放群组中的所有实例使用相同的实例类型。
- 不能合并置放群组。您必须在一个置放群组中终止相关实例，然后在另一个置放群组中重新启动这些实例。
- 置放群组可跨越多个对等 VPC，但是，您不会在对等 VPC 实例之间获取全部的等分带宽。了解更多有关 VPC 对等连接的信息，请参阅 [Amazon VPC 用户指南](#) 中的 [VPC 对等](#) 主题。
- 您不能将现有实例移动到置放群组中。您可以从现有实例创建 AMI，然后通过该 AMI 在置放群组中启动新实例。
- 预留实例可为可用区中的 EC2 实例提供容量预留。容量预留可供置放群组中分配到同一可用区的实例使用。但是，您无法为置放群组显式预留容量。
- 要确保可实现吞吐量保持为 10 Gb/s，置放群组的成员相互之间必须通过其私有 IP 地址寻址。使用成员之间相互使用公有 IP 地址来寻址，则吞吐量将降为 5 Gb/s。

## 将实例启动到置放群组中

我们建议您专门为要启动到置放群组中的实例创建一个 AMI。

### 使用控制台将实例启动到置放群组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 为您的实例创建一个 AMI。
  - a. 从 Amazon EC2 控制面板中，选择 Launch Instance。在完成向导后，选择 Launch。
  - b. 连接到您的实例。（有关更多信息，请参阅[使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。）
  - c. 在实例上安装软件和应用程序、复制数据或附加更多 Amazon EBS 卷。
  - d.（可选）如果您的实例类型支持增强联网，请通过执行[Windows 上的增强联网 \(p. 630\)](#)中的过程确保启用此功能。
  - e. 在导航窗格中，选择 Instances，选择您的实例，然后选择 Actions、Image、Create Image。提供 Create Image 对话框所请求的信息，然后选择 Create Image。
  - f.（可选）如果您无需进一步使用，则可终止该实例。
3. 创建置放群组。
  - a. 在导航窗格中，选择 Placement Groups。
  - b. 选择 Create Placement Group。
  - c. 在 Create Placement Group 对话框中，提供置放群组名称（该名称在您使用的 AWS 账户中是唯一的），然后选择 Create。
- 当置放群组的状态为available时，您可将实例启动到该置放群组中。
4. 将您的实例启动到置放群组。
  - a. 在导航窗格中，选择 Instances。
  - b. 选择 Launch Instance。按指示完成向导，注意执行以下操作：

- 在 Choose an Amazon Machine Image (AMI) 页面上，选择 My AMIs 选项卡，然后选择创建的 AMI。
- 在 Choose an Instance Type 页面上，选择可以启动到置放群组中的实例类型。
- 在 Configure Instance Details 页面上，输入您需要放在此置放群组中的实例总数，因为您以后可能无法将实例添加到置放群组。
- 在 Configure Instance Details 页面上，选择您从 Placement group 创建的置放群组。如果您在此页面上没有看到 Placement group 列表，请确保您选择了可启动到置放群组的实例类型，否则该选项会不可用。

## 使用命令行将实例启动到置放群组

### 1. 使用以下命令之一为实例创建 AMI：

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

### 2. 使用以下命令之一创建置放群组：

- [create-placement-group](#) (AWS CLI)
- [New-EC2PlacementGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

### 3. 使用以下选项之一将实例启动到置放群组：

- `--placement` 与 [run-instances](#) (AWS CLI)
- `-PlacementGroup` 与 [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

## 删除置放群组

如果您需要替换或不再需要置放群组，您可以删除置放群组。在删除置放群组前，您必须终止启动到该置放群组中的所有实例。

## 使用控制台删除置放群组

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 选择并终止置放群组中的所有实例。（在终止实例前，您可通过检查详细信息窗格中的 Placement Group (置放群组) 值来验证该实例是否位于相关置放群组中。）
4. 在导航窗格中，选择 Placement Groups。
5. 选择置放群组，然后选择 Delete Placement Group。
6. 当系统提示进行确认时，选择 Yes, Delete。

## 使用命令行删除置放群组

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

- [terminate-instances](#) 和 [delete-placement-group](#) (AWS CLI)

- [Stop-EC2Instance](#) 和 [Remove-EC2PlacementGroup](#); (适用于 Windows PowerShell 的 AWS 工具)

## EC2 实例的网络最大传输单位 (MTU)

### Abstract

EC2 实例支持的最大 MTU 取决于其实例类型。

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小 (以字节为单位)。连接的 MTU 越大，可在单个数据包中传递的数据越多。以太网数据包由帧 (或您发送的实际数据) 和围绕它的网络开销信息组成。

以太网帧有不同的格式，最常见的格式是标准以太网 v2 帧格式。它支持 1500 MTU，它是通过大部分 Internet 支持的最大以太网数据包大小。实例支持的最大 MTU 取决于其实例类型。所有 Amazon EC2 实例类型都支持 1500 MTU，并且当前很多实例大小都支持 9001 MTU 或极大帧。

### 内容

- [极大帧 \(9001 MTU\) \(p. 627\)](#)
- [路径 MTU 发现 \(p. 627\)](#)
- [查看两台主机之间的路径 MTU \(p. 628\)](#)
- [在您的 Amazon EC2 实例上检查并设置 MTU \(p. 628\)](#)
- [故障排除 \(p. 630\)](#)

## 极大帧 (9001 MTU)

极大帧通过增加每个数据包的负载大小，从而增加数据包中不属于数据包开销的百分比来支持 1500 个字节以上的数据。发送等量的可用数据所需要的数据包更少。但在给定 AWS 区域 (EC2-Classic) 或单一 VPC 的外部，您将遇到的最大路径为 1500 MTU。VPN 连接、VPC 对等连接和通过 Internet 网关发送的流量限制为 1500 MTU。如果数据包大于 1500 字节，则对数据包进行分片；如果在 IP 标头中设置了 Don't Fragment 标志，则丢弃数据包。

不应将极大帧用于 Internet 绑定的流量或离开 VPC 的任何流量。中间系统会对数据包进行分片，从而减缓此流量。要使用 VPC 中的极大帧而不减慢 VPC 外部的绑定流量的速度，您可按路由配置 MTU 大小，或者将弹性网络接口与不同 MTU 大小和不同路由结合使用。

对于在一个置放群组中并置的实例，极大帧可帮助达到可能的最大网络吞吐量，因此建议在这种情况下使用。有关更多信息，请参阅 [置放群组 \(p. 624\)](#)。

以下实例支持极大帧：

- 计算已优化：C3、C4、CC2
- 通用型：M3、M4、T2
- GPU：CG1、G2
- 内存已优化：CR1、R3
- 存储已优化：D2、HI1、HS1、I2

## 路径 MTU 发现

路径 MTU 发现用于确定两台设备之间的路径 MTU。路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机或设备将返回以下 ICMP 消息：Destination Unreachable: Fragmentation Needed

and Don't Fragment was Set (类型 3, 代码 4)。这指示原始主机调整 MTU，直到可以传输数据包。

默认情况下，安全组不允许任何入站 ICMP 流量。要确保您的实例可以收到此消息并且数据包不会丢失，您必须将具有无法访问目标协议的自定义 ICMP 规则添加到您实例的入站安全组规则。有关更多信息，请参阅 Amazon EC2 安全组主题中的[向安全组添加规则 \(p. 520\)](#)和[API 和命令概览 \(p. 521\)](#)部分。



#### Important

将您实例的安全组修改为允许路径 MTU 发现不能保证极大帧不会被某些路由器忽略。您 VPC 中的 Internet 网关仅将转发最多 1500 字节的数据包。建议对 Internet 流量使用 1500 MTU 数据包。

## 查看两台主机之间的路径 MTU

您可使用 mturoute.exe 命令查看两台主机之间的路径 MTU，。

### 使用 mturoute.exe 查看路径 MTU

1. 从 <http://www.elifulkerson.com/projects/mturoute.php> 下载 mturoute.exe。
2. 打开命令提示符窗口并更改为 mturoute.exe 的下载目录。
3. 使用以下命令查看您的 Amazon EC2 实例和另一台主机之间的路径 MTU。您可以使用 DNS 名称或 IP 地址作为目标；此示例将查看 EC2 实例和 www.elifulkerson.com 之间的路径 MTU。

```
PS C:\Users\Administrator\Downloads> .\mturoute.exe www.elifulkerson.com
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
+ ICMP payload of 1472 bytes succeeded.
- ICMP payload of 1473 bytes is too big.
Path MTU: 1500 bytes.
```

在此示例中，路径 MTU 为 1500。

## 在您的 Amazon EC2 实例上检查并设置 MTU

一些 AMI 配置为在实例上使用支持 AMI 的极大帧，另一些 AMI 配置为使用标准帧大小。您可能希望将极大帧用于您的 VPC 内的网络流量，或希望将标准帧用于 Internet 流量。无论您的使用案例如何，我们建议验证您的实例是否会按您的预期运行。您可以使用本部分中的过程查看您的网络接口的 MTU 设置并按需对其进行修改。

### 查看 Windows 实例上的 MTU 设置

- 如果您的实例使用的是 Windows 操作系统，则可使用 netsh 命令查看 MTU 值。运行以下命令以确定当前 MTU 值：

```
PS C:\Users\Administrator> netsh interface ipv4 show subinterface
 MTU MediaSenseState Bytes In Bytes Out Interface
----- ----- -----
 9001 1 317337 692805 Ethernet
```

在生成的输出中，查找标题为“Ethernet”、“Ethernet 2”或“Local Area Connection”的条目。

在以上示例中，MTU 列中的 **9001** 指示此实例使用极大帧。

## 在 Windows 实例上设置 MTU 值

- 如果您的实例使用的是 Windows 操作系统，则可使用 netsh 命令设置 MTU 值。运行以下命令以设置所需的 MTU 值。



### Note

这些步骤因您的 Windows 实例所使用的网络驱动程序而异，请确保针对您的驱动程序版本执行正确的命令。有关更多信息，请参阅 [半虚拟化驱动程序 \(p. 272\)](#)。

- 对于使用 AWS PV 驱动程序或 Intel 网络驱动程序以增强联网的 Windows 实例（例如，Windows Server 2012 R2），请执行以下命令将 MTU 设置为 1500。

```
PS C:\Users\Administrator> netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
Ok.
```

要将 MTU 设置为 9001，请执行以下命令。

```
PS C:\Users\Administrator> netsh interface ipv4 set subinterface "Ethernet" mtu=9001 store=persistent
Ok.
```

要完成将 MTU 设置为 9001 的操作，请执行以下命令。如果将 MTU 设置为 1500，则不必执行此命令。

```
PS C:\Users\Administrator> Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -RegistryValue 9014
```



### Note

如果您收到 Element not found 错误，请将 *Ethernet* 替换为来自与您的接口匹配的 [查看 Windows 实例上的 MTU 设置 \(p. 628\)](#) 过程的 Interface 列输出。

- 对于使用 Citrix PV 驱动程序的 Windows 实例，请先按照 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#) 中的过程操作以确保您的 PV 驱动程序处于最新状态。然后，执行以下命令将 MTU 设置为 1500。Citrix PV 驱动程序将 MTU 解释为平均最大帧大小，因此您必须从您的 mtu 设置中减去 18 才能设置正确值。例如，要设置 1500 MTU，请在以下命令中使用 1482，而要设置 9001 MTU，请改用 8983。

```
PS C:\Users\Administrator> netsh interface ipv4 set subinterface "Local Area Connection" mtu=1482 store=persistent
Ok.
```



### Note

如果您收到 Element not found 错误，请将 *Local Area Connection* 替换为来自与您的接口匹配的 [查看 Windows 实例上的 MTU 设置 \(p. 628\)](#) 过程的 Interface 列输出。

- ( 可选 ) 重启实例并验证 MTU 设置是否正确。

## 故障排除

如果在使用极大顿时您的 EC2 实例和 Amazon Redshift 群集之间出现连接问题 , 请参阅 *Amazon Redshift Cluster Management Guide* 中的 [查询挂起](#)

# Windows 上的增强联网

## Abstract

了解 VPC 中支持的 Windows 实例上的增强联网功能。

增强联网使用单个根 I/O 虚拟化 (SR-IOV) 在 [支持的实例类型 \(p. 630\)](#) 上提供高性能的联网功能。SR-IOV 是一种设备虚拟化方法 , 与传统虚拟化网络接口相比 , 它不仅能提高 I/O 性能 , 还能降低 CPU 利用率。增强联网可以提高带宽 , 提高每秒数据包数 (PPS) 性能 , 并不断降低实例间的延迟。使用增强联网不收取任何额外费用。

### 内容

- [增强联网类型 \(p. 630\)](#)
- [在实例上启用增强联网 \(p. 630\)](#)
- [在 VPC 中的 Windows 实例上启用 Intel 82599 VF 接口增强联网 \(p. 630\)](#)
- [在 VPC 中的 Windows 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 633\)](#)

## 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 :

### Intel 82599 虚拟功能 (VF) 接口

Intel 82599 虚拟功能接口支持高达 10 Gbps 的网络速度。

C3、C4、R3、I2、M4 和 D2 实例使用 Intel 82599 VF 接口实现增强联网。

### Elastic Network Adapter (ENA)

Elastic Network Adapter (ENA) 支持高达 20 Gbps 的网络速度。

X1 实例使用 Elastic Network Adapter 实现增强联网。

## 在实例上启用增强联网

如果您的实例类型支持使用 Intel 82599 VF 接口实现增强联网 , 请执行 [在 VPC 中的 Windows 实例上启用 Intel 82599 VF 接口增强联网 \(p. 630\)](#) 中的步骤。

如果您的实例类型支持使用 Elastic Network Adapter 实现增强联网 , 请执行 [在 VPC 中的 Windows 实例上启用 Elastic Network Adapter \(ENA\) 增强联网 \(p. 633\)](#) 中的步骤。

## 在 VPC 中的 Windows 实例上启用 Intel 82599 VF 接口增强联网

## Abstract

在 VPC 中的 Windows 实例上启用 Intel 82599 VF 接口增强联网。

Amazon EC2 通过使用 Intel ixgbevf 驱动程序的 Intel 82599 VF 接口向 C3、C4、R3、I2、M4 和 D2 实例提供增强联网功能。

要准备 Intel 82599 VF 接口增强联网 , 请按如下方式设置您的实例 :

- 从适用于 Windows Server 2012 或 Windows Server 2008 R2 的 64 位 HVM AMI 启动实例。( 您不能在 Windows Server 2008 和 Windows Server 2003 上启用增强联网 , Windows Server 2012 R2 上已启用增强联网。 ) 已针对 Windows Server 2012 R2 AMI 启用了 Windows Server 增强联网功能。但是 , Windows Server 2012 R2 包含 Intel 驱动程序 1.0.15.3 , 我们建议您使用 Pnputil.exe 实用工具将该驱动程序升级到最新版本。
- 在 VPC 中启动实例。( 如果实例在 EC2-Classic 中 , 则您不能启用增强联网功能。 )
- 在您选择的任意计算机 ( 最好是您的本地台式计算机或笔记本电脑 ) 上安装并配置 AWS CLI 。有关更多信息 , 请参阅访问 Amazon EC2 ( p. 3 ) 。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留 , 则应立即从您的实例创建 AMI , 来备份这些数据。更新内核和内核模块以及启用 sriovNetSupport 属性可能会导致实例不兼容或操作系统无法访问 ; 如果您有最新备份 , 则可在发生这种情况时保留数据。

#### 内容

- 测试是否启用了 Intel 82599 VF 接口增强联网 ( p. 631 )
- 在 Windows 上启用 Intel 82599 VF 接口增强联网 ( p. 632 )

## 测试是否启用了 Intel 82599 VF 接口增强联网

要测试是否已启用 Intel 82599 VF 接口增强联网 , 请确认实例上已安装驱动程序且设置了 sriovNetSupport 属性。

#### 驱动程序

要验证是否已安装驱动程序 , 请连接到您的实例并打开设备管理器。您应该可以看到 Network adapters ( 网络适配器 ) 下列出了 “Intel(R) 82599 Virtual Function” 。

#### 实例属性 (sriovNetSupport)

要检查实例是否设置了增强联网 sriovNetSupport 属性 , 请使用以下命令 :

- [describe-instance-attribute](#) (AWS CLI)

```
C:\> aws ec2 describe-instance-attribute --instance-id instance_id --attribute sriovNetSupport
```

如果此属性未设置 , 则 SriovNetSupport 为空 ; 否则 , 设置如下 :

```
"SriovNetSupport": {
 "Value": "simple"
},
```

#### 映像属性 (sriovNetSupport)

要检查 AMI 是否设置了增强联网 sriovNetSupport 属性 , 请使用以下命令 :

- [describe-image-attribute](#) (AWS CLI)

```
C:\> aws ec2 describe-image-attribute --image-id ami_id --attribute sriovNetSupport
```



#### Note

此命令仅适用于您拥有的映像。对于不属于您账户的映像，您会收到 AuthFailure 错误。

如果此属性未设置，则 SriovNetSupport 为空；否则，设置如下：

```
"SriovNetSupport": {
 "Value": "simple"
},
```

## 在 Windows 上启用 Intel 82599 VF 接口增强联网

如果您启动了您的实例且该实例未启用增强联网，则必须下载所需的网络适配器驱动程序并将其安装到您的实例上，然后设置 sriovNetSupport 实例属性以激活增强联网。您只能对支持的实例类型启用此属性。有关更多信息，请参阅 [增强联网类型 \(p. 630\)](#)。



#### Important

已针对 Windows Server 2012 R2 AMI 启用了 Windows Server 增强联网功能。但是，Windows Server 2012 R2 包含 Intel 驱动程序 1.0.15.3，我们建议您使用此处所述的 Pnputil.exe 实用工具将该驱动程序升级到最新版本。

### 启用增强联网

1. 连接到您的实例并以本地管理员身份登录。
2. 从实例安装驱动程序，如下所示：
  - a. 为操作系统下载 Intel 网络适配器驱动程序。
    - Microsoft Windows Server 2008 R2
    - Microsoft Windows Server 2012
    - Microsoft Windows Server 2012 R2
  - b. 在 Download 文件夹中找到 PROWinx64.exe 文件。将此文件重命名为 PROWinx64.zip。
  - c. 打开 PROWinx64.zip 的上下文（右键单击）菜单，并选择 Extract All。指定目标路径并选择 Extract。
  - d. 打开命令提示符窗口，转到包含提取的文件的文件夹，然后使用 pnputil 实用工具在驱动程序存储中添加和安装 INF 文件。

Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

Windows Server 2008 R2

```
C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
```

3. 从本地计算机中，使用 Amazon EC2 控制台或以下命令停止实例：[stop-instances](#) (AWS CLI)。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。
4. 从命令提示符窗口中，使用以下命令启用增强联网属性。



Warning

增强联网属性启用之后将无法禁用。

- [modify-instance-attribute](#) (AWS CLI)

```
C:\> aws ec2 modify-instance-attribute --instance-id instance_id --srivm-net-support simple
```

5. (可选) 从实例创建 AMI，如[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#) 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。
6. 从本地计算机中，使用 Amazon EC2 控制台或以下命令启动实例：[start-instances](#) (AWS CLI)。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 VPC 中的 Windows 实例上启用 Elastic Network Adapter (ENA) 增强联网

### Abstract

在 VPC 中支持的 Windows 实例上启用 Elastic Network Adapter (ENA) 增强联网功能。

要准备 ENA 网络适配器增强联网，请按如下方式设置您的实例：

- 在 VPC 中启动实例。（如果实例在 EC2-Classic 中，则您不能启用增强联网功能。）
- 在您选择的任意计算机（最好是您的本地台式计算机或笔记本电脑）上安装并配置 AWS CLI。有关更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留，则应立即从您的实例创建 AMI，来备份这些数据。更新内核和内核模块以及启用 enaSupport 属性可能会导致实例不兼容或操作系统无法访问；如果您有最新备份，则可在发生这种情况时保留数据。

### 内容

- [测试是否启用了 ENA 增强联网 \(p. 634\)](#)
- [在 Windows 上启用 ENA 增强联网 \(p. 634\)](#)

## 测试是否启用了 ENA 增强联网

要测试是否已启用 ENA 增强联网，请确认实例上已安装驱动程序且设置了 enaSupport 属性。

实例属性 (enaSupport)

要检查实例是否已设置了增强联网 enaSupport 属性，请使用以下命令：

- [describe-instances](#) (AWS CLI)

```
C:\> aws ec2 describe-instances --instance-id instance_id --query Reservations[].[Instances][].EnaSupport
```

如果 enaSupport 属性未设置，则返回的 JSON 为空；否则，设置如下：

```
[
 true
]
```

映像属性 (enaSupport)

要检查 AMI 是否已设置了增强联网 enaSupport 属性，请使用以下命令：

- [describe-image-attribute](#) (AWS CLI)

```
C:\> aws ec2 describe-image-attribute --image-id ami_id --attribute enaSupport
```



### Note

此命令仅适用于您拥有的映像。对于不属于您账户的映像，您会收到 AuthFailure 错误。

如果此属性未设置，则 EnaSupport 为空；否则，设置如下：

```
{
 "EnaSupport": {
 "Value": true
 },
 "ImageId": "ami_id"
}
```

## 在 Windows 上启用 ENA 增强联网

如果您启动了您的实例且该实例未启用增强联网，则必须下载所需的网络适配器驱动程序并将其安装到您的实例上，然后设置 enaSupport 实例属性以激活增强联网。您只能对支持的实例类型启用此属性。有关更多信息，请参阅 [增强联网类型 \(p. 630\)](#)。

### 使用 ENA 启用增强联网

- 右键单击网络图标，然后选择 Open Network and Sharing Center。
- 选择以太网适配器，例如 Ethernet 2。

- c. 选择 Details。Network Connection Details 窗口的 Description 字段应该具有值 Amazon Elastic Network Adapter。
1. 连接到您的实例并以本地管理员身份登录。
  2. 从实例安装驱动程序，如下所示：
    - a. 下载 Amazon ENA 适配器驱动[程序包](#)。
    - b. 提取 zip 档案。
    - c. 打开命令提示窗口并导航到包含适用于您 Windows 版本的驱动程序的文件夹，该版本必须是以下之一：
      - Microsoft Windows Server 2008 R2
      - Microsoft Windows Server 2012
      - Microsoft Windows Server 2012 R2
    - d. 在与您的操作系统版本对应的文件夹中，您应该会看到三个驱动程序文件：ena.cat、ena.inf 和 ena.sys。使用以下命令安装驱动程序：

```
C:\> pnputil -i -a ena.inf
```

如果安装成功，则应生成以下输出：

```
Microsoft PnP Utility

Processing inf : ena.inf
Successfully installed the driver on a device on the system.
Driver package added successfully.
Published name : oem9.inf

Total attempted: 1
Number successfully imported: 1
```

3. 从本地计算机中，使用 Amazon EC2 控制台或以下命令停止实例：[stop-instances](#) (AWS CLI)。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。
4. 在您的实例上启用 ENA 支持。



#### Note

除非您先前已按上面所述安装了 ENA 驱动程序，否则无法在实例上启用 ENA 支持。

- a. 在您的本地计算机上，通过运行以下命令来检查实例的 EC2 实例 ENA 支持属性。默认情况下 EnaSupport 设置为 false。

```
C:\> aws ec2 describe-instances --instance-id "instance-id" --query Reservations[].[Instances[]].EnaSupport
```

如果未启用属性，则输出将为“[]”。

- b. 要启用 ENA 支持 , 请运行以下命令 , 该命令不返回任何输出 :

```
C:\> aws ec2 modify-instance-attribute --instance-id "instance-id" --ena-support
```



Note

如果您在重新启动实例时遇到问题 , 也可以使用下面的命令来禁用 ENA 支持 :

```
C:\> aws ec2 modify-instance-attribute --instance-id "instance-id" --no-ena-support
```

- c. 通过按上面所示重新运行 describe-instances 命令 , 来验证该属性是否已设置为 true。您现在应看到 :

```
[
 true
]
```

5. 从本地计算机中 , 使用 Amazon EC2 控制台或以下命令启动实例 : [start-instances](#) (AWS CLI)。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。
6. 在实例上 , 验证 ENA 驱动程序是否已安装且正常工作。
7. ( 可选 ) 从实例创建 AMI。该 AMI 将从实例继承增强联网 enaSupport 属性。因此 , 您可以使用该 AMI 来启动默认情况下启用了 ENA 增强联网的另一个实例。

如果您的实例是 EBS 支持的实例 , 请按照[创建 Amazon EBS 支持的 Windows AMI](#) 中所述创建新的 AMI。

如果您的实例是实例存储支持的实例 , 请按照[创建实例存储支持的 Windows AMI](#) 中所述创建新的 AMI。要在从 AMI 创建的实例上默认启用增强联网 , 请确保在您注册实例时包含 --ena-support 标记。

# 存储

---

## Abstract

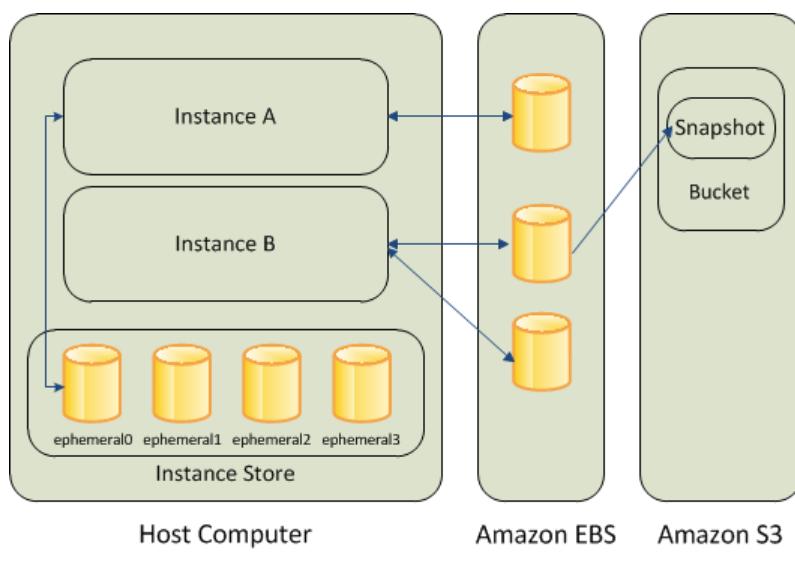
了解如何使用 Amazon EC2 支持的数据存储选项来满足您的存储要求。

Amazon EC2 为您的实例提供了灵活、经济且易于使用的数据存储选项。各选项都具有独特的性能和耐久性。这些存储选项既可以单独使用，也可以组合使用，以便满足您的需求。

阅读本部分后，您应该会对如何使用 Amazon EC2 支持的数据存储选项来满足特定要求有很好的了解。这些存储选项包含以下产品：

- [Amazon Elastic Block Store\(Amazon EBS\) \(p. 638\)](#)
- [Amazon EC2 实例存储 \(p. 701\)](#)
- [Amazon Simple Storage Service \(Amazon S3\) \(p. 707\)](#)

下图显示了这些不同存储类型之间的关系。



Amazon EBS 提供数据块级别的持久存储卷，您可将这些卷连接到正在运行的实例。您可以将 Amazon EBS 用作需要频繁和细粒度更新的数据的主存储设备。例如，如果在实例上运行数据库，则建议选用 Amazon EBS 作为存储设备。

EBS 卷就像原始未经格式化的外部数据块储存设备，可连接到单个实例。卷始终不受实例运行时间的影响。将 EBS 卷连接到实例后，您可以像使用其他物理硬盘一样使用它。如上图所示，可以将多个卷连接到一个实例。您也可以将 EBS 卷从实例中断开，并将其连接到另一个实例。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 \(p. 686\)](#)。

为保留您的数据的备份副本，您可以创建 EBS 卷的快照，该快照存储在 Amazon S3 中。您可以从快照创建 EBS 卷，并将其连接到另一个实例。有关更多信息，请参阅 [Amazon Elastic Block Store\(Amazon EBS\) \(p. 638\)](#)。

#### Amazon EC2 实例存储

很多实例可以访问物理连接到主机的磁盘中的存储。此磁盘存储称为 **实例存储**。实例存储可为实例提供临时性块级存储。实例存储卷上的数据仅在关联实例的生命周期内保留；如果您停止或终止实例，则实例存储卷上的任何数据都会丢失。有关更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。

#### Amazon S3

Amazon S3 是 Internet 数据的存储库。Amazon S3 提供了可靠、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。例如，您可以使用 Amazon S3 来存储数据和应用程序的备份副本。有关更多信息，请参阅 [Amazon Simple Storage Service \(Amazon S3\) \(p. 707\)](#)。

#### 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所有信息。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 \(p. 712\)](#)。

您还可以将 EBS 卷连接到运行中的实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。

## Amazon Elastic Block Store(Amazon EBS)

### Abstract

将 Amazon Elastic Block Store 用于数据块级存储卷以用于 Amazon EC2 实例。

Amazon Elastic Block Store (Amazon EBS) 提供数据块级存储卷以用于 EC2 实例。EBS 卷是高度可用和可靠的存储卷，可以挂载到同一可用区中任何正在运行的实例。挂载到 EC2 实例的 EBS 卷公开为独立于实例生命周期存在的存储卷。使用 Amazon EBS，您可以按实际用量付费。有关 Amazon EBS 定价的更多信息，请参阅 [Amazon Elastic Block Store 页](#) 的“预计费用”部分。

如果数据必须能够快速访问且需要长期保存，建议使用 Amazon EBS。EBS 卷特别适合用作文件系统和数据库的主存储，还适用于任何需要细粒度更新及访问原始的、未经格式化的数据块级存储的应用程序。Amazon EBS 非常适合依赖随机读写操作的数据库式应用程序以及执行长期持续读写操作的吞吐量密集型应用程序。

要使用简化的数据加密，可将 EBS 卷作为加密卷进行启动。Amazon EBS 加密 提供了用于 EBS 卷的简单加密解决方案，您无需构建、管理和保护自己的密钥管理基础设施。创建加密 EBS 卷并将它连接到支持的实例类型时，该卷上静态存储的数据、磁盘 I/O 和通过该卷创建的快照都会进行加密。加密在托管 EC2 实例的服务器上进行，从而为从 EC2 实例传输到 EBS 存储的数据提供加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 686\)](#)。

Amazon EBS 加密在创建加密卷以及通过加密卷创建任何快照时，使用 AWS Key Management Service (AWS KMS) 主密钥。首次在区域中创建加密的 EBS 卷时，将自动为您创建一个默认主密钥。此密钥将

用于 Amazon EBS 加密，除非您选择采用 AWS Key Management Service 单独创建的客户主密钥 (CMK)。创建您自己的 CMK 可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥的能力。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

您可以将多个卷连接到同一实例，但是不能超过 AWS 账户指定的限额。您的账户对您可以使用的 EBS 卷数量和总存储量有相应的限制。如要了解有关限制的更多信息，以及如何申请提高限额，请参阅[请求提高 Amazon EBS 卷限制](#)。

#### 内容

- [Amazon EBS 的功能 \(p. 639\)](#)
- [Amazon EBS 卷 \(p. 640\)](#)
- [Amazon EBS 快照 \(p. 676\)](#)
- [Amazon EBS 优化实例 \(p. 683\)](#)
- [Amazon EBS Encryption \(p. 686\)](#)
- [Amazon EBS 卷性能 \(Windows 实例上\) \(p. 689\)](#)

## Amazon EBS 的功能

- 您可以创建大小高达 16TiB 的 EBS 通用型 SSD (gp2)、Provisioned IOPS (io1)、吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷。您可以将这些卷作为设备装载在您的 Amazon EC2 实例上。您可以在同一实例上安装多个卷，但每个卷一次只能连接到一个实例。有关更多信息，请参阅 [创建 Amazon EBS 卷 \(p. 652\)](#)。
- 通过 通用型 SSD (gp2) 卷，基本性能可以达到 100 IOPS/GiB，并能突增至 3000 IOPS 并保持一段时间。gp2 卷适用于多种使用案例，例如引导卷、中小型数据库以及开发和测试环境。gp2 卷最高可支持 10000 的 IOPS 和 160MB/s 的吞吐量。有关更多信息，请参阅 [通用型 SSD \(gp2\) 卷 \(p. 643\)](#)。
- 通过 provisioned IOPS (io1) 卷，您可以预配置特定级别的 I/O 性能。io1 卷最高可支持 20000 IOPS 和 320 MB/s 吞吐量。因此，您可预见性地将每个 EC2 实例扩展到数万 IOPS。有关更多信息，请参阅 [provisioned IOPS \(io1\) 卷 \(p. 646\)](#)。
- 吞吐优化 HDD (st1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。这种卷的吞吐量高达 500MiB/s，非常适合大型顺序工作负载，例如 Amazon EMR、ETL、数据仓库和日志处理。有关更多信息，请参阅 [吞吐优化 HDD \(st1\) 卷 \(p. 646\)](#)。
- Cold HDD (sc1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。sc1 的吞吐量高达 250MiB/s，是大型顺序冷数据工作负载的理想选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的数据块存储。有关更多信息，请参阅 [Cold HDD \(sc1\) 卷 \(p. 648\)](#)。
- EBS 卷的行为类似于原始、未格式化的块储存设备。您可基于这些卷来创建文件系统，或以任何其他块储存设备（如硬盘）使用方式使用这些卷。有关创建文件系统和安装卷的更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 658\)](#)。
- 您可以使用加密 EBS 卷为监管/审核的数据和应用程序实现各种静态数据加密要求。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 686\)](#)。
- 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 \(p. 676\)](#)。
- EBS 卷在特定可用区中创建，随后可以挂载到同一可用区内的任何实例。若要在可用区外部提供某个卷，您可以创建快照并将该快照还原到该区域任何位置处的新卷。您可以将快照复制到其他区域，再将它们还原到那里的新卷，这样可更方便地利用多个 AWS 区域以实现地理扩展、数据中心迁移和灾难恢复。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 677\)](#)、[从快照还原 Amazon EBS 卷 \(p. 655\)](#) 和 [复制 Amazon EBS 快照 \(p. 679\)](#)。
- 可以将公用数据集快照的大型存储库还原到 EBS 卷，并无缝集成到基于 AWS 云的应用程序中。有关更多信息，请参阅 [使用公用数据集 \(p. 726\)](#)。
- 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 [Amazon EBS 卷性能 \(Windows 实例上\) \(p. 689\)](#)。

# Amazon EBS 卷

## Abstract

将 Amazon EBS 卷用作一个数据块级存储设备，您可以将该设备连接到单个 EC2 实例以充当经常更新的数据的主存储。

Amazon EBS 卷是一种耐用的数据块级存储设备，可以连接到单个 EC2 实例。您可以将 EBS 卷用作需要频繁更新的数据的主存储，例如实例的系统驱动器或数据库应用程序的存储，也可以用于执行持续硬盘扫描的吞吐量密集型应用程序。EBS 卷始终不受 EC2 实例运行时间的影响。将卷连接到实例后，您可以像使用其他物理硬盘一样使用它。Amazon EBS 提供以下卷类型：通用型 SSD (`gp2`)、provisioned IOPS (`io1`)、吞吐优化 HDD (`st1`)、Cold HDD (`sc1`) 和磁介质 (`standard`)。它们的性能特点和价格不同，您可根据应用程序要求定制您所需的存储性能和相应费用。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。

## 内容

- [使用 EBS 卷的优势 \(p. 640\)](#)
- [Amazon EBS 卷类型 \(p. 641\)](#)
- [创建 Amazon EBS 卷 \(p. 652\)](#)
- [从快照还原 Amazon EBS 卷 \(p. 655\)](#)
- [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)
- [使 Amazon EBS 卷可用 \(p. 658\)](#)
- [查看卷信息 \(p. 660\)](#)
- [监控您的卷状态 \(p. 660\)](#)
- [从实例断开 Amazon EBS 卷 \(p. 670\)](#)
- [删除 Amazon EBS 卷 \(p. 671\)](#)
- [在 Windows 上扩展 EBS 卷的存储空间 \(p. 671\)](#)

## 使用 EBS 卷的优势

EBS 卷可提供实例存储卷不支持的多种优势。

### • 数据可用性

当您在可用区域内创建 EBS 卷时，系统会在该区域内自动复制该卷，以防止因任何一个硬件组件故障而导致数据丢失。在您创建卷后，可将其连接到同一可用区域内的任何 EC2 实例。连接后，该卷显示为类似于硬盘或其他物理设备的本机块设备。这时，实例就像与本地硬盘交互一样与该卷相互；实例还可以使用文件系统（如 NTFS）将 EBS 卷格式化，然后安装应用程序。

一个 EBS 卷一次只能连接到同一可用区域中的一个实例。但是，可将多个卷连接到同一实例。如果您将多个卷连接到您指定的一个设备，则可以在卷内将数据条带化，以增强 I/O 性能和吞吐量。

您可以获取针对 EBS 卷的监控数据，而无需额外付费（其中包含 EBS 支持的实例根设备卷的数据）。有关更多信息，请参阅 [使用 CloudWatch 监控卷 \(p. 660\)](#)。

### • 数据持久性

EBS 卷是一种实例外存储，其数据的保存期限不受实例使用寿命的影响。只要数据存在，您就要继续支付卷的使用费用。

在默认情况下，当实例终止时，连接到该实例的 EBS 卷会自动断开连接，同时完整地保留数据。然后，可将卷重新连接到新的实例，从而快速恢复数据。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其连接的卷中保存的数据。在从停止到启动的整个周期中，该卷均为已连接状态。这使您能够无限期地在卷上处理和存储数据，并只在需要时使用处理和存储资源。数据将一直保留在该卷上，直至将其显式删除。已删除的 EBS 卷使用的物理数据块存储先由零覆盖，然后分配给其

他账户。如果要处理敏感数据，应考虑手动加密数据或将数据存储在由 Amazon EBS 加密 保护的卷上。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 686\)](#)。

在默认情况下，当实例终止时，在启动时创建并连接的 EBS 卷也会被删除。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `false`。修改值后，即使实例终止，也可将该卷保留下并连接到其他实例。

- 数据加密

为简化数据加密，您可以使用 Amazon EBS 加密功能创建加密 EBS 卷。所有 EBS 卷类型都支持加密。您可以使用加密 EBS 卷为监管/审核的数据和应用程序实现各种静态数据加密要求。Amazon EBS 加密使用 256 位高级加密标准算法 (AES-256) 和 Amazon 托管密钥基础设施。加密在托管 EC2 实例的服务器上进行，从而为从 EC2 实例传输到 Amazon EBS 存储的数据提供加密。有关更多信息，请参阅 [Amazon EBS Encryption \(p. 686\)](#)。

Amazon EBS 加密在创建加密卷以及通过加密卷创建任何快照时，使用 AWS Key Management Service (AWS KMS) 主密钥。首次在区域中创建加密的 EBS 卷时，将自动为您创建一个默认主密钥。此密钥用于 Amazon EBS 加密，除非您选择采用 AWS KMS 单独创建的客户主密钥 (CMK)。创建您自己的 CMK 可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥的能力。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

- 快照

Amazon EBS 提供为任何 EBS 卷创建快照（备份）并将卷中数据的副本写入 Amazon S3（其中数据以冗余方式存储在多个可用区中）的功能。不必将该卷连接到运行中的实例，也可以拍摄快照。因为您不断向卷写入数据，则可定期创建该卷的快照，以用作创建新卷的基线。也可利用这些快照创建多个新的 EBS 卷，增加卷的容量或在可用区域间移动卷的位置。加密 EBS 卷的快照会自动加密。

从快照创建新卷时，新卷是拍摄快照时的原始卷的精确副本。从加密快照还原的 EBS 卷会自动加密。需根据情况确定不同大小的卷或不同的可用区域，可以使用该功能来增加现有卷的大小或在新可用区域中创建副本卷。可与特定的 AWS 账户共享这些卷或使其公开可用。当您创建快照时，您需根据卷的总大小支付 Amazon S3 费用。对于连续的卷快照，您只需支付任何超过卷原始大小的附加数据的费用。

快照是增量备份，这意味着仅保存卷上在最新快照之后更改的数据块。如果您的卷中有 100 GiB 的数据，但自上次快照以来只更改了 5 GiB 的数据，则只有这 5 GiB 经过修改的数据会写入 Amazon S3。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

为了便于对卷和快照进行分类和管理，您可以使用选择的元数据对它们加以标记。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 737\)](#)。

## Amazon EBS 卷类型

### Abstract

使用 `gp2`、`io1`、`st1`、`sc1` 或 `standard` EBS 卷可对存储性能和成本进行定制，以满足应用程序的需求。

Amazon EBS 提供以下卷类型，各种类型性能特点和价格不同，因此您可根据应用程序要求定制您所需的存储性能和相应成本。卷类型归入两大类别：

- 支持 SSD 的卷针对涉及小型 I/O 的频繁读/写操作的事务性工作负载进行了优化，其中管理性能属性为 IOPS
- 支持 HDD 的卷针对吞吐量（以 MiB/s 为单位）是优于 IOPS 的性能指标的大型流式处理工作负载进行了优化

下表列出了每个卷类型的使用案例和性能特点：

|             | 固态硬盘 (SSD)                                                                                                                      |                                                                                                                                                                                                                                                                                              | 硬盘 (HDD)                                                                                                                            |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 卷类型         | 通用型 SSD (gp2)*                                                                                                                  | provisioned IOPS (io1)                                                                                                                                                                                                                                                                       | 吞吐优化 HDD (st1)                                                                                                                      | Cold HDD (sc1)                                                                                                |
| 描述          | 平衡价格和性能的通用 SSD 卷，可用多种事务性工作负载                                                                                                    | 为任务关键型应用程序设计的最高性能 SSD 卷                                                                                                                                                                                                                                                                      | 为频繁访问的吞吐量密集型工作负载设计的低成本 HDD 卷                                                                                                        | 为不常访问的工作负载设计的最低成本 HDD 卷                                                                                       |
| 使用案例        | <ul style="list-style-type: none"> <li>建议用于大多数工作负载</li> <li>系统启动卷</li> <li>虚拟桌面</li> <li>低延迟交互式应用程序</li> <li>开发和测试环境</li> </ul> | <ul style="list-style-type: none"> <li>需要持续 IOPS 性能或每卷高于 10000 IOPS 或 160 MiB/s 吞吐量的关键业务应用程序</li> <li>大型数据库工作负载，如： <ul style="list-style-type: none"> <li>MongoDB</li> <li>Cassandra</li> <li>Microsoft SQL Server</li> <li>MySQL</li> <li>PostgreSQL</li> <li>Oracle</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>以低成本流式处理需要一致、快速的吞吐量的工作负载</li> <li>大数据</li> <li>数据仓库</li> <li>日志处理</li> <li>不能是启动卷</li> </ul> | <ul style="list-style-type: none"> <li>适合大量不常访问的数据、面向吞吐量的存储</li> <li>最低存储成本至关重要的情形</li> <li>不能是启动卷</li> </ul> |
| API 名称      | gp2                                                                                                                             | io1                                                                                                                                                                                                                                                                                          | st1                                                                                                                                 | sc1                                                                                                           |
| 卷大小         | 1 GiB - 16 TiB                                                                                                                  | 4 GiB - 16 TiB                                                                                                                                                                                                                                                                               | 500 GiB - 16 TiB                                                                                                                    | 500 GiB - 16 TiB                                                                                              |
| 最大 IOPS**/卷 | 10000                                                                                                                           | 20000                                                                                                                                                                                                                                                                                        | 500                                                                                                                                 | 250                                                                                                           |
| 最大吞吐量/卷     | 160 MiB/s                                                                                                                       | 320 MiB/s                                                                                                                                                                                                                                                                                    | 500 MiB/s                                                                                                                           | 250 MiB/s                                                                                                     |
| 最大 IOPS/实例  | 48 000                                                                                                                          | 48 000                                                                                                                                                                                                                                                                                       | 48 000                                                                                                                              | 48 000                                                                                                        |
| 最大吞吐量/实例    | 800 MiB/s                                                                                                                       | 800 MiB/s                                                                                                                                                                                                                                                                                    | 800 MiB/s                                                                                                                           | 800 MiB/s                                                                                                     |
| 管理性能属性      | IOPS                                                                                                                            | IOPS                                                                                                                                                                                                                                                                                         | MiB/s                                                                                                                               | MiB/s                                                                                                         |

\*默认卷类型

\*\*gp2/io1 基于 16KiB I/O 大小，st1/sc1 基于 1 MiB I/O 大小

下表列出了上一代 EBS 卷类型。如果您需要比上一代卷更高的性能或性能一致性，建议您考虑使用通用型 SSD (gp2) 或其他最新卷类型。有关更多信息，请参阅[上一代卷](#)。

| 上一代卷   |             |
|--------|-------------|
| 卷类型    | EBS 磁介质     |
| 描述     | 上一代 HDD     |
| 使用案例   | 数据不常访问的工作负载 |
| API 名称 | standard    |

| 上一代卷       |               |
|------------|---------------|
| 卷大小        | 1 GiB - 1 TiB |
| 最大 IOPS/卷  | 40 – 200      |
| 最大吞吐量/卷    | 40-90 MiB/s   |
| 最大 IOPS/实例 | 48 000        |
| 最大吞吐量/实例   | 800 MiB/s     |
| 管理性能属性     | IOPS          |



#### Note

下面的 Amazon EBS 卷注意事项适用于 Windows 引导卷：

- 如果引导卷大小为 2 TiB (2048 GiB) 或更大，则 Windows 2003 实例不会启动。
- Windows 启动卷必须使用 MBR 分区表，无论卷大小如何，它都将可用空间限制为 2 TiB。
- 已转换为使用动态 MBR 分区表的 2 TiB (2048 GiB) 的 Windows 引导卷在用 Disk Manager 检查时会显示错误。

下面的 Amazon EBS 卷注意事项适用于 Windows 数据（非引导）卷：

- 2 TiB (2048 GiB) 或更大的 Windows 卷必须使用 GPT 分区表才能访问整个卷。
- 将自动使用 GPT 分区表对启动时附加到 Windows 实例的 2048 GiB 以上的 Amazon EBS 卷进行格式设置。
- 必须使用 GPT 分区表手动对启动后附加到 Windows 实例的 Amazon EBS 卷进行初始化。有关更多信息，请参阅[使 Amazon EBS 卷可用](#)。

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[Amazon EBS 卷性能（Windows 实例上）\(p. 689\)](#)。

有关这些卷类型的定价的更多信息，请参阅[Amazon EBS 定价](#)。

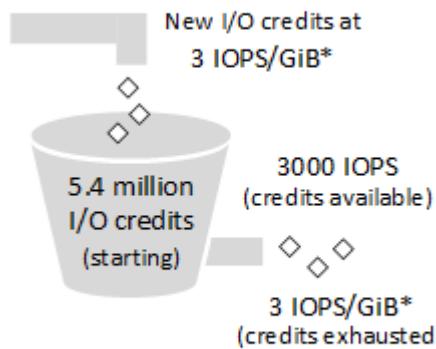
## 通用型 SSD (**gp2**) 卷

通用型 SSD (**gp2**) 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷可以提供几毫秒的延迟，能够突增至 3000 IOPS 并维持一段较长的时间。在最小 100 IOPS（以 33.33 GiB 及以下）和最大 10,000 IOPS（以 3334 GiB 及以上）之间，基准性能以每 GiB 卷大小 3 IOPS 的速度线性扩展。**gp2** 卷的大小范围为 1 GiB 到 16 TiB。

### I/O 点数和突增性能

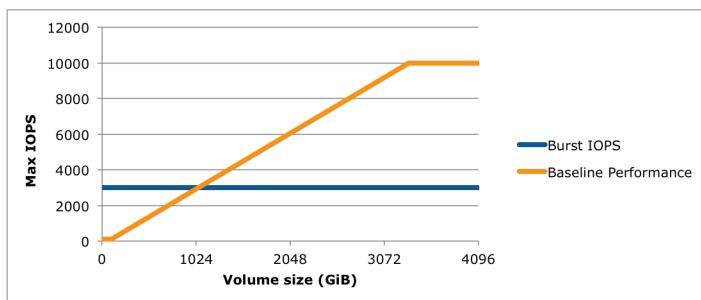
**gp2** 卷的性能与卷大小关联，卷大小确定卷的基准性能水平以及积累 I/O 点数的速度；卷越大，基准性能级别就越高，I/O 点数积累速度也越快。I/O 点数表示您的**gp2** 卷在需求超过基准性能时可用来突增大量 I/O 的可用带宽。您的卷拥有的 I/O 点数越多，它在需要更高性能时可以超过其基准性能水平的突增时间就越长，表现也越好。下图显示 **gp2** 的突增存储桶行为。

## GP2 burst bucket



\* Scaling linearly between minimum 100 IOPS and maximum 10,000 IOPS.

每个卷都有 540 万 I/O 点的初始 I/O 点数余额，这足以维持 3000 IOPS 的最大突增性能 30 分钟。设计初始点数余额的目的是为启动卷提供快速初始启动循环，并为其他应用程序提供良好的引导过程。卷以每 GiB 卷大小 3 IOPS 的基准性能率的速度获得 I/O 点数。例如，一个 100 GiB 的 gp2 卷具有 300 IOPS 的基准性能。



当卷的需求超出了基准性能 I/O 水平时，它会使用点数余额中的 I/O 点数突增到所需的性能水平，最大为 3000 IOPS。大于 1000 GiB 的卷的基准性能等于或大于最大突增性能，并且其 I/O 点数余额永远不会耗尽。如果卷在一秒内使用的 I/O 点数少于它所赚取的点数，未使用的 I/O 点数会加到 I/O 点数余额中。卷的最大 I/O 点数余额等于初始点数余额（540 万 I/O 点数）。

下表列出了几种卷大小以及卷的相关基准性能（也就是它积累 I/O 点数的速度）、在最大 3000 IOPS 时的突增持续时间（从完整点数余额开始时）以及卷重新填满空点数余额所需的秒数。

| 卷大小 (GiB)        | 基准性能 (IOPS) | 最大突增持续时间 @ 3000 IOPS (秒数) | 填满空点数余额的秒数 |
|------------------|-------------|---------------------------|------------|
| 1                | 100         | 1862                      | 54000      |
| 100              | 300         | 2000                      | 18000      |
| 214 (最大吞吐量的最小大小) | 642         | 2290                      | 8412       |
| 250              | 750         | 2400                      | 7200       |
| 500              | 1500        | 3600                      | 3600       |
| 750              | 2250        | 7200                      | 2400       |

| 卷大小 (GiB)                | 基准性能 (IOPS) | 最大突增持续时间 @ 3000 IOPS (秒数) | 填满空点数余额的秒数 |
|--------------------------|-------------|---------------------------|------------|
| 1000                     | 3000        | 不适用*                      | 不适用*       |
| 3334 ( 最大 IOPS 的最小大小 )   | 10000       | 不适用*                      | 不适用*       |
| 16384 ( 16 TiB , 最大卷大小 ) | 10000       | 不适用*                      | 不适用*       |

\* 突增和 I/O 点数仅与低于 1000 GiB 的卷有关，此时突增性能超出了基准性能。

卷的突增持续时间取决于卷的大小、所需的突增 IOPS 以及突增开始时的点数余额。如下面的等式所示：

$$\text{Burst duration} = \frac{\text{(Credit balance)}}{(\text{Burst IOPS}) - 3(\text{Volume size in GiB})}$$

如果我清空我的 I/O 点数余额，会发生什么情况？

如果 gp2 卷使用了其所有 I/O 点数余额，则卷的最大 IOPS 性能将保持在基准 IOPS 性能水平（即卷获得点数的速度），并且吞吐量限制会减少为基准 IOPS 乘以最大吞吐量并除以 3000，直到 I/O 需求降低至基准水平以下并且未使用的点数添加到 I/O 点数余额中。

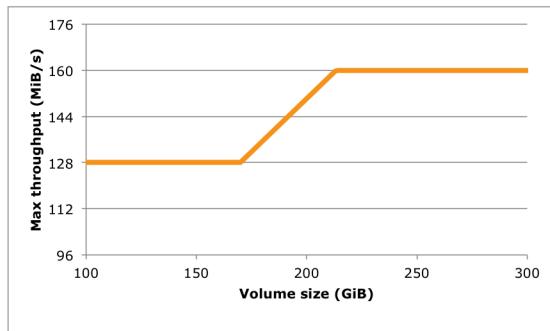
$$\text{Throughput limit with empty I/O credit balance} = \frac{(\text{Max throughput}) \times (\text{Baseline IOPS})}{3,000}$$

例如，一个点数余额已空的 100GiB gp2 卷的基准 IOPS 性能限制为 300 IOPS，吞吐量限制为 12.8MiB/s ( $(128\text{MiB/s}) * 300 / 3000$ )。卷越大，基准性能就越高，补充点数余额的速度也越快。有关如何测量 IOPS 的更多信息，请参阅 [I/O 特性 \(p. 694\)](#)。

如果您注意到卷性能常常受限于基准水平（由于空 I/O 点数余额），则应考虑使用较大的 gp2 卷（具有较高基准性能水平），或对需要大于 10000 IOPS 的持续 IOPS 性能的工作负载改用 io1 卷。

### 吞吐量性能

对于小于或等于 170 GiB 的卷，gp2 卷的吞吐量限制为 128 MiB/s；对于大于 170 GiB 的卷，此限制由每 GiB 速度 768 KiB/s 提高至最大 160 MiB/s ( 214 GiB 及更大情况下 )。

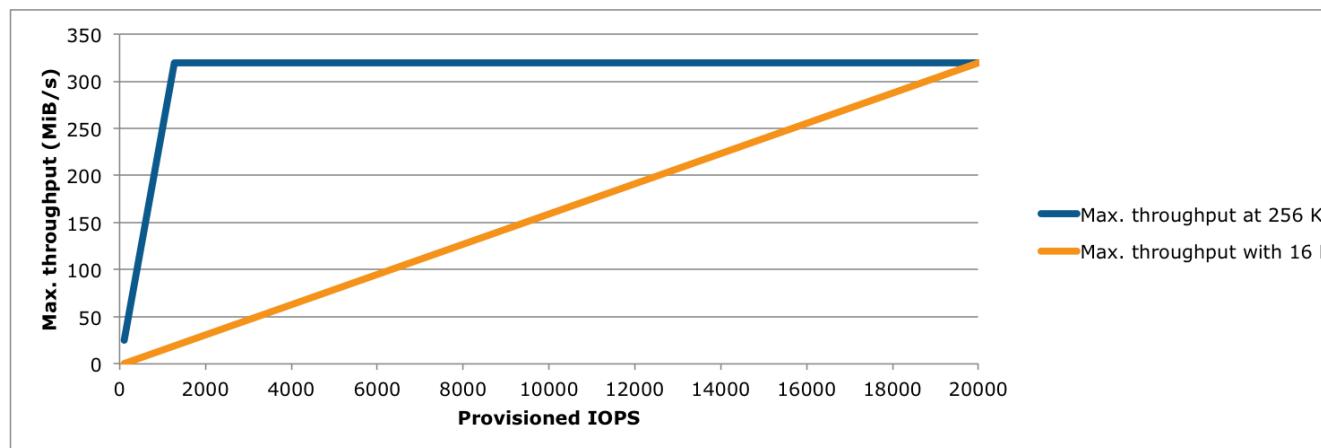


## provisioned IOPS (io1) 卷

provisioned IOPS (io1) 卷旨在满足 I/O 密集型工作负载（尤其是数据库工作负载）的需要，这些工作负载对存储性能和一致性非常敏感。io1 卷不使用存储桶和信用模型计算性能，它允许您在创建卷时指定一致的 IOPS 速率，Amazon EBS 在指定年份的超过 99.9% 的时间里可提供 10% 以内的预配置 IOPS 性能。

io1 卷的大小范围为 4 GiB 到 16 TiB，您可以预配置为每卷最大 20,000 IOPS。预配置 IOPS 与请求卷的大小之比最大为 30；例如，IOPS 为 3000 的卷至少必须为 100 GiB。可以在 RAID 配置中对多个卷一起进行条带化，以便实现更大大小和更高性能。

对于预配置的每个 IOPS，io1 卷的吞吐量限制为 256 KiB，最高可达 320 MiB/s（在 1280 IOPS 情况下）。



您的每个 I/O 延迟体验取决于预配置 IOPS 和您的工作负载模式。为获得最佳的 I/O 延迟体验，我们建议您将 IOPS 与 GB 之比预配置为大于 2:1（例如，在这种情况下，2000 IOPS 的卷将小于 1000 GiB）。



### Note

2012 年之前创建的某些 AWS 账户可能能够访问 us-east-1、us-west-1 或 ap-northeast-1 中的可用区，这些可用区不支持 provisioned IOPS (io1) 卷。如果您无法在其中一个区域中创建 io1 卷（或在其块储存设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

## 吞吐优化 HDD (st1) 卷

吞吐优化 HDD (st1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。此卷类型是大型顺序工作负载（如 Amazon EMR、ETL、数据仓库和日志处理）的理想之选。不支持可启动的 st1 卷。



### Note

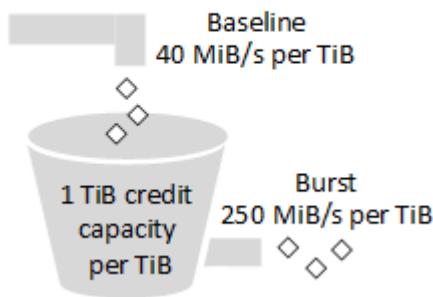
此卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅 [HDD 上的小型读/写效率低下问题 \(p. 652\)](#)。

## 吞吐量点数和突增性能

与 gp2 类似，st1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量点数的速度。卷大小还决定卷的突增吞吐量，即有点数可用时消耗点数的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的点数越多，它以突增水平驱动 I/O 的时间就越长。

下图显示 st1 的突增存储桶行为。

## ST1 burst bucket



st1 卷的可用吞吐量受吞吐量和吞吐量点数上限的约束，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Baseline Throughput}$$

对于 1 TiB st1 卷，突增吞吐量限制为 250 MiB/s，存储桶以 40 MiB/s 的速度填充，最多可容纳 1 TiB 点数。

较大卷以线性扩展这些限制，吞吐量上限为最大 500 MiB/s。存储桶耗尽后，吞吐量限制为每 TiB 40 MiB/s 的基准速率。

在从 0.5 到 16 TiB 的卷大小范围内，基准吞吐量从 20 到上限 500 MiB/s 变化，12.5 TiB 时达到上限，因为

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

突增吞吐量从 125 MiB/s 到上限 500 MiB/s 变化，2 TiB 时达到上限，因为

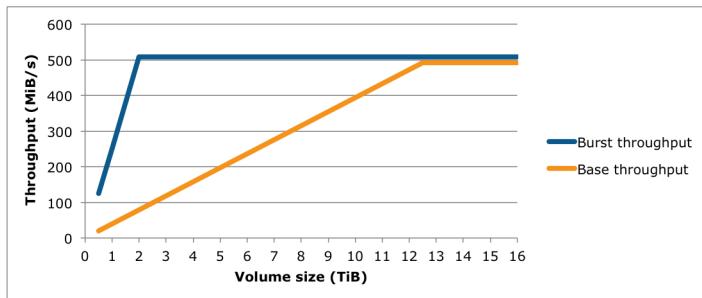
$$2 \text{ TiB} \times \frac{250 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

下表列出了 st1 基准和突增吞吐量值的完整范围：

| 卷大小 (TiB) | ST1 基准吞吐量 (MiB/s) | ST1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 0.5       | 20                | 125               |
| 1         | 40                | 250               |
| 2         | 80                | 500               |
| 3         | 120               | 500               |
| 4         | 160               | 500               |
| 5         | 200               | 500               |
| 6         | 240               | 500               |

| 卷大小 (TiB) | ST1 基准吞吐量 (MiB/s) | ST1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 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

创建快照后，st1 卷的吞吐量也以基准线为上限。

## Cold HDD (sc1) 卷

Cold HDD (sc1) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。sc1 的吞吐量限制比 st1 更低，是大型顺序冷数据工作负载的理想选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的数据块存储。不支持可启动的 sc1 卷。



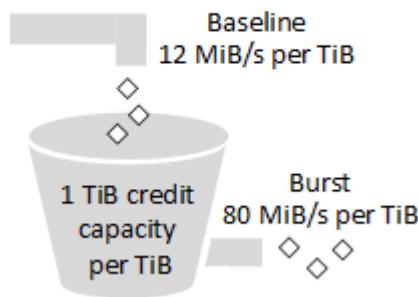
#### Note

此卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅 [HDD 上的小型读/写效率低下问题 \(p. 652\)](#)。

## 吞吐量点数和突增性能

与 gp2 类似，sc1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量点数的速度。卷大小还决定卷的突增吞吐量，即有点数可用时消耗点数的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的点数越多，它以突增水平驱动 I/O 的时间就越长。

## SC1 burst bucket



sc1 卷的可用吞吐量受吞吐量和吞吐量点数上限的约束，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Baseline Throughput}$$

对于 1 TiB sc1 卷，突增吞吐量限制为 80 MiB/s，存储桶以 12 MiB/s 的速度填充，最多可容纳 1 TiB 点数。

较大卷以线性扩展这些限制，吞吐量上限为最大 250 MiB/s。存储桶耗尽后，吞吐量限制为每 TiB 12 MiB/s 的基准速率。

在从 0.5 到 16 TiB 的卷大小范围内，基准吞吐量从 6 MiB/s 到最大 192 MiB/s 变化，16 TiB 时达到上限，因为

$$16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

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，因为

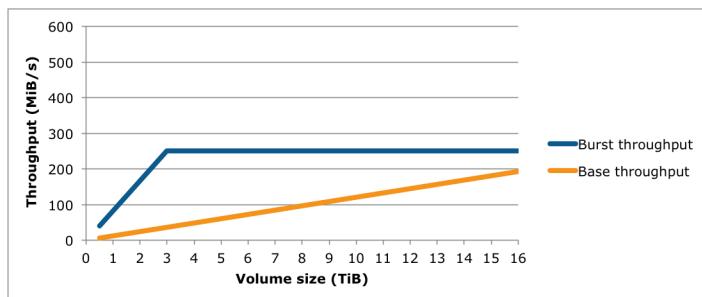
$$3.125 \text{ TiB} \times \frac{250 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

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               |

| 卷大小 (TiB) | SC1 基准吞吐量 (MiB/s) | SC1 突增吞吐量 (MiB/s) |
|-----------|-------------------|-------------------|
| 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：



## 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](#)。

## 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：

|                   |
|-------------------|
| Volume size       |
| ----- = Scan time |
| 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。

|                                                                |                  |  |
|----------------------------------------------------------------|------------------|--|
| 5 TiB                                                          | 5 TiB            |  |
| ----- = ----- = 10,486 s = 2.91 hours (optimal)                |                  |  |
| 500 MiB/s                                                      | 0.00047684 TiB/s |  |
|                                                                |                  |  |
| 2.91 hours                                                     |                  |  |
| 2.91 hours + ----- = 3.27 hours (minimum expected)             |                  |  |
| (0.90)(0.99) <-- From expected performance of 90% of burst 99% |                  |  |
| of the time                                                    |                  |  |

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。

|                                                    |  |  |
|----------------------------------------------------|--|--|
| 5 TiB                                              |  |  |
| ----- = 20972 s = 5.83 hours (optimal)             |  |  |
| 0.000238418 TiB/s                                  |  |  |
|                                                    |  |  |
| 5.83 hours                                         |  |  |
| 5.83 hours + ----- = 6.54 hours (minimum expected) |  |  |
| (0.90)(0.99)                                       |  |  |

| 卷大小 (TiB) | 带突增的 ST1 扫描时间 ( 小时 )<br>* | 带突增的 SC1 扫描时间 ( 小时 )<br>* |
|-----------|---------------------------|---------------------------|
| 1         | 1.17                      | 3.64                      |
| 2         | 1.17                      | 3.64                      |
| 3         | 1.75                      | 3.64                      |
| 4         | 2.33                      | 4.66                      |
| 5         | 2.91                      | 5.83                      |
| 6         | 3.50                      | 6.99                      |
| 7         | 4.08                      | 8.16                      |
| 8         | 4.66                      | 9.32                      |
| 9         | 5.24                      | 10.49                     |
| 10        | 5.83                      | 11.65                     |

| 卷大小 (TiB) | 带突增的 ST1 扫描时间 ( 小时 )<br>* | 带突增的 SC1 扫描时间 ( 小时 )<br>* |
|-----------|---------------------------|---------------------------|
| 11        | 6.41                      | 12.82                     |
| 12        | 6.99                      | 13.98                     |
| 13        | 7.57                      | 15.15                     |
| 14        | 8.16                      | 16.31                     |
| 15        | 8.74                      | 17.48                     |
| 16        | 9.32                      | 18.64                     |

\* 这些扫描时间在执行 1 MiB 顺序 I/O 时采取平均队列深度 ( 四舍五入到最近的整数 ) 四或更多。

因此，如果您有面向吞吐量的工作负载需要快速完成扫描（最快 500 MiB/s）或一天查询几个整卷，请使用 `st1`。如果您针对成本进行了优化，数据访问相对不频繁，而且不需要超过 250 MiB/s 的扫描性能，请使用 `sc1`。

### HDD 上的小型读/写效率低下问题

`st1` 和 `sc1` 卷的性能模型针对顺序 I/O 进行了优化，支持高吞吐量工作负载，对具有混合 IOPS 和吞吐量的工作负载提供可接受的性能，不建议使用具有小型随机 I/O 的工作负载。

例如，1 MiB 或更小的 I/O 请求计为 1 MiB I/O 点数。但是，如果是顺序 I/O，则会合并为 1 MiB I/O 数据块，并且只计为 1 MiB I/O 点数。

### 每实例吞吐量限制

`st1` 和 `sc1` 卷的吞吐量始终由以下限制中较小的决定：

- 卷的吞吐量限制
- 实例的吞吐量限制

对于所有 Amazon EBS 卷，我们建议选择适当的 EBS 优化的 EC2 实例来避免网络瓶颈。有关更多信息，请参阅 [Amazon EBS 优化实例](#)。

## 创建 Amazon EBS 卷

### Abstract

创建一个 EBS 卷，然后将它连接到同一可用区内的任何 EC2 实例。

您可以创建一个 Amazon EBS 卷，然后将它连接到同一可用区内的任何 EC2 实例。您可以选择创建加密 EBS 卷，但是加密卷只能连接到所选的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 687\)](#)。

如果通过指定块储存设备映射启动实例，也可以创建并连接 EBS 卷。有关更多信息，请参阅 [启动实例 \(p. 216\)](#) 和 [块储存设备映射 \(p. 712\)](#)。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 \(p. 655\)](#)。

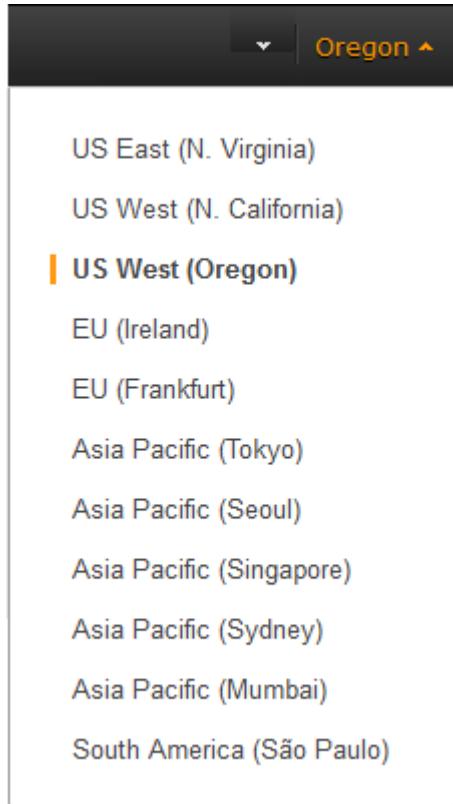
如果您要针对一种高性能存储情形来创建卷，应确保使用 provisioned IOPS (`io1`) 卷并将它连接到一个具有足够带宽支持您的应用程序的实例，如 EBS 优化实例或具有 10 GiB 网络连接的实例。对吞吐优化 HDD (`st1`) 和 Cold HDD (`sc1`) 卷也是同样的建议。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 691\)](#)。

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备

操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。访问数据完毕后，性能随之恢复。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 695\)](#)。

### 使用控制台创建 EBS 卷

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中，选择您想创建卷的区域。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅 [资源位置 \(p. 729\)](#)。



3. 在导航窗格中的 ELASTIC BLOCK STORE 下，选择 Volumes。
4. 在上方窗格上，选择 Create Volume。
5. 在 Create Volume 对话框中，对于 Volume Type 选择 通用型 SSD、Provisioned IOPS SSD 或 磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。



#### Note

2012 年之前创建的某些 AWS 账户可能能够访问 us-east-1、us-west-1 或 ap-northeast-1 中的可用区，这些可用区不支持 provisioned IOPS (io1) 卷。如果您无法在其中一个区域中创建 io1 卷（或在其块储存设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

6. 对于 Size，输入卷大小，以 GiB 为单位。



#### Note

下面的 Amazon EBS 卷注意事项适用于 Windows 引导卷：

- 如果引导卷大小为 2 TiB (2048 GiB) 或更大，则 Windows 2003 实例不会启动。

- Windows 启动卷必须使用 MBR 分区表，无论卷大小如何，它都将可用空间限制为 2 TiB。
- 已转换为使用动态 MBR 分区表的 2 TiB (2048 GiB) 的 Windows 引导卷在用 Disk Manager 检查时会显示错误。

下面的 Amazon EBS 卷注意事项适用于 Windows 数据 ( 非引导 ) 卷：

- 2 TiB (2048 GiB) 或更大的 Windows 卷必须使用 GPT 分区表才能访问整个卷。
- 将自动使用 GPT 分区表对启动时附加到 Windows 实例的 2048 GiB 以上的 Amazon EBS 卷进行格式设置。
- 必须使用 GPT 分区表手动对启动后附加到 Windows 实例的 Amazon EBS 卷进行初始化。有关更多信息，请参阅[使 Amazon EBS 卷可用](#)。

7. 对于 io1 卷，在 IOPS 字段中输入该卷应支持的每秒输入/输出操作 (IOPS) 的最大值。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。
9. ( 可选 ) 要创建加密卷，请选中 Encrypted (已加密) 框，然后选择您希望在加密卷时所使用的主密钥。您可以选择自己账户的默认主密钥，也可以选择此前使用 AWS Key Management Service 创建的任何客户主密钥 (CMK)。Master Key (主密钥) 下拉菜单中显示了可用的密钥，或者您可以粘贴您能访问的任何密钥的完整 ARN。有关更多信息，请参阅[AWS Key Management Service Developer Guide](#)。



#### Note

加密卷只能连接到所选的实例类型。有关更多信息，请参阅[支持的实例类型 \(p. 687\)](#)。

10. 选择 Yes, Create。



#### Important

如果您收到以下错误之一，则说明创建当前卷会导致超过您的账户的默认存储限制：

```
Maximum number of active volumes bytes, 20, exceeded.
Maximum number of active gp2 volumes bytes, 20, exceeded.
Maximum number of active io1 volumes bytes, 20, exceeded.
```

要查看 Amazon EBS 默认服务限制，请参阅 [Amazon Web Services General Reference](#) 中的 [Amazon Elastic Block Store \(Amazon EBS\) 限制](#)。要请求提高存储限额，请参阅[请求提高 Amazon EBS 卷限制](#)。

## 使用命令行创建 EBS 卷

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

- [create-volume \(AWS CLI\)](#)
- [New-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 从快照还原 Amazon EBS 卷

### Abstract

使用存储在 Amazon S3 中的快照的数据还原 Amazon EBS 卷。

您可以使用存储在 Amazon S3 中的快照的数据还原 Amazon EBS 卷。您需要知道您希望用来还原卷的快照的 ID，还需要拥有对该快照的访问权限。有关快照的更多信息，请参阅 [Amazon EBS 快照 \(p. 676\)](#)。

基于现有 EBS 快照创建的新卷在后台延时加载。也就是说，通过快照创建卷之后，无需等待所有数据从 Amazon S3 传输到 EBS 卷，连接的实例即可开始访问该卷及其所有数据。如果您的实例访问还没有加载的数据，卷会立即从 Amazon S3 下载请求的数据，并在后台继续加载剩余数据。

从加密快照还原的 EBS 卷会自动加密。加密卷只能连接到所选的实例类型。有关更多信息，请参阅 [支持的实例类型 \(p. 687\)](#)。

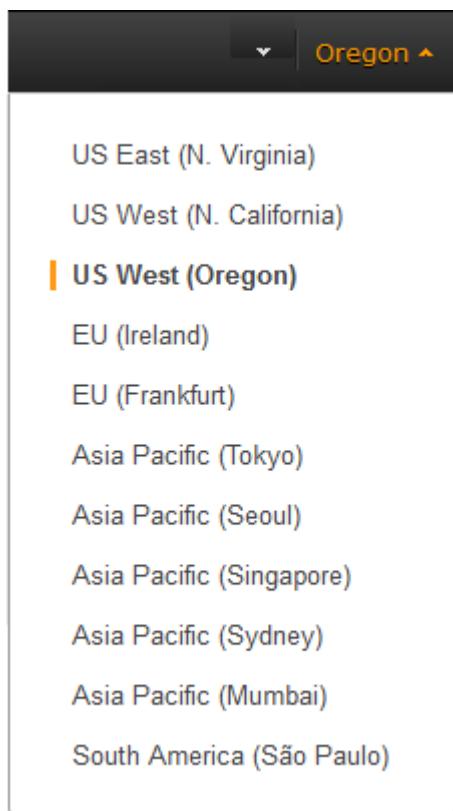
由于存在安全限制，您不可以从不属于您的共享加密快照直接还原 EBS 卷。您必须首先创建属于您的快照副本。之后，您便可以从该副本还原卷。有关更多信息，请参阅 [Amazon EBS 加密](#)。

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。访问数据完毕后，性能随之恢复。

对于大部分应用程序，可将此初始化成本分摊到卷的整个使用期限。如果您需要确保您的存储卷始终能在生产高峰期正常工作，可使用 dd 或 fio 对整个卷强制实施即时初始化。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 695\)](#)。

### 使用控制台从快照还原 EBS 卷

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航栏中，选择快照所处的区域。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅 [资源位置 \(p. 729\)](#)。如果您需要将快照还原到在不同区域的某个卷，则您可以将快照复制到该新区域，然后将它还原到该区域的一个卷。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 679\)](#)。



3. 在导航窗格中，选择 Volumes、Create Volume。
4. 在 Create Volume 对话框中，对于 Volume Type 选择 通用型 SSD、Provisioned IOPS SSD 或 磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。



#### Note

2012 年之前创建的某些 AWS 账户可能能够访问 us-east-1、us-west-1 或 ap-northeast-1 中的可用区，这些可用区不支持 provisioned IOPS (io1) 卷。如果您无法在其中一个区域中创建 io1 卷（或在其块储存设备映射中启动具有 io1 卷的实例），请尝试该区域中的其他可用区。您可以通过在某可用区创建 4 GiB io1 卷来验证该可用区是否支持 io1 卷。

5. 对于 Snapshot，开始键入您要用于还原卷的快照的 ID 或描述，并从所建议的选项列表中选择该快照。



#### Note

从加密快照还原的卷只能连接到支持 Amazon EBS 加密的实例。有关更多信息，请参阅 [支持的实例类型 \(p. 687\)](#)。

6. 对于 Size，输入卷的大小（以 GiB 为单位），或验证快照的默认大小是否足够。

如果您指定卷大小和快照 ID，其大小必须等于或大于快照的大小。当您选择一种卷类型和一个快照 ID 时，最小和最大卷大小将显示在 Size (大小) 列表旁边。任何来自快照的 AWS Marketplace 产品代码都会传送到该卷。



#### Note

下面的 Amazon EBS 卷注意事项适用于 Windows 引导卷：

- 如果引导卷大小为 2 TiB (2048 GiB) 或更大，则 Windows 2003 实例不会启动。
- Windows 启动卷必须使用 MBR 分区表，无论卷大小如何，它都将可用空间限制为 2 TiB。
- 已转换为使用动态 MBR 分区表的 2 TiB (2048 GiB) 的 Windows 引导卷在用 Disk Manager 检查时会显示错误。

下面的 Amazon EBS 卷注意事项适用于 Windows 数据（非引导）卷：

- 2 TiB (2048 GiB) 或更大的 Windows 卷必须使用 GPT 分区表才能访问整个卷。
- 将自动使用 GPT 分区表对启动时附加到 Windows 实例的 2048 GiB 以上的 Amazon EBS 卷进行格式设置。
- 必须使用 GPT 分区表手动对启动后附加到 Windows 实例的 Amazon EBS 卷进行初始化。有关更多信息，请参阅[使 Amazon EBS 卷可用](#)。

7. 对于 io1 卷，在 IOPS 字段中输入该卷可支持的每秒输入/输出操作 (IOPS) 的最大值。
8. 在 Availability Zone (可用区) 列表中，选择要在其中创建卷的可用区。EBS 卷只能挂载到同一可用区中的 EC2 实例。
9. 选择 Yes, Create。



#### Important

如果将一个快照还原到了超过该快照默认大小的一个较大的卷，则需要扩展卷上的文件系统以利用额外的空间。有关更多信息，请参阅[在 Windows 上扩展 EBS 卷的存储空间 \(p. 671\)](#)。

### 使用命令行还原 EBS 卷

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

- [create-volume](#) (AWS CLI)
- [New-EC2Volume](#) (适用于 Windows PowerShell 的 AWS 工具)

## 将 Amazon EBS 卷连接到实例

### Abstract

将您创建的 Amazon EBS 卷连接到 EC2 实例。

您可以将 EBS 卷连接到与该卷处于同一可用区中的实例之一。

### 先决条件

- 确定您将使用的设备名称。有关更多信息，请参阅[Windows 实例上的设备命名 \(p. 710\)](#)。
- 确定您可以将多少个卷连接到您的实例。有关更多信息，请参阅[实例卷限制 \(p. 709\)](#)。
- 如果卷是加密的，则只能将它连接到支持 Amazon EBS 加密的实例。有关更多信息，请参阅[支持的实例类型 \(p. 687\)](#)。
- 如果某个卷有 AWS Marketplace 产品代码：
  - 卷只能连接到已停止的实例。
  - 您必须订阅卷上的 AWS Marketplace 代码。
- 实例的配置（实例类型、操作系统）必须支持这一特定的 AWS Marketplace 代码。例如，您不能从 Windows 实例取用卷，然后将其连接到 Linux 实例。

- AWS Marketplace 产品代码从卷复制到实例。

### 使用控制台将 EBS 卷连接到实例

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择卷，并选择 Attach Volume。
4. 在 Attach Instance 对话框中，开始在 Instance 中键入要将卷挂载到的实例的名称或 ID，并从建议的选项（只显示与卷处于相同可用区中的实例）的列表中选择它。
5. 您可以保留推荐的设备名称，也可以输入其他受支持的设备名称。



#### Important

该实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的不同。

6. 选择 Attach。
7. 连接到您的实例并将卷置于可用状态。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 658\)](#)。

### 使用命令行将 EBS 卷连接到实例

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

- [attach-volume](#) (AWS CLI)
- [Add-EC2Volume](#) (适用于 Windows PowerShell 的 AWS 工具)

## 使 Amazon EBS 卷可用

### Abstract

使一个 Amazon EBS 卷可供使用，以便您可以像访问任何其他卷一样访问它。

将某个 Amazon EBS 卷连接到您的实例后，该卷将显示为块储存设备。您可以使用任何文件系统将卷格式化，然后进行安装。在使 EBS 卷可供使用后，您可以像访问其他所有卷一样访问该卷。任何写入此文件系统的数据均写入 EBS 卷，并且对使用该设备的应用程序是透明的。

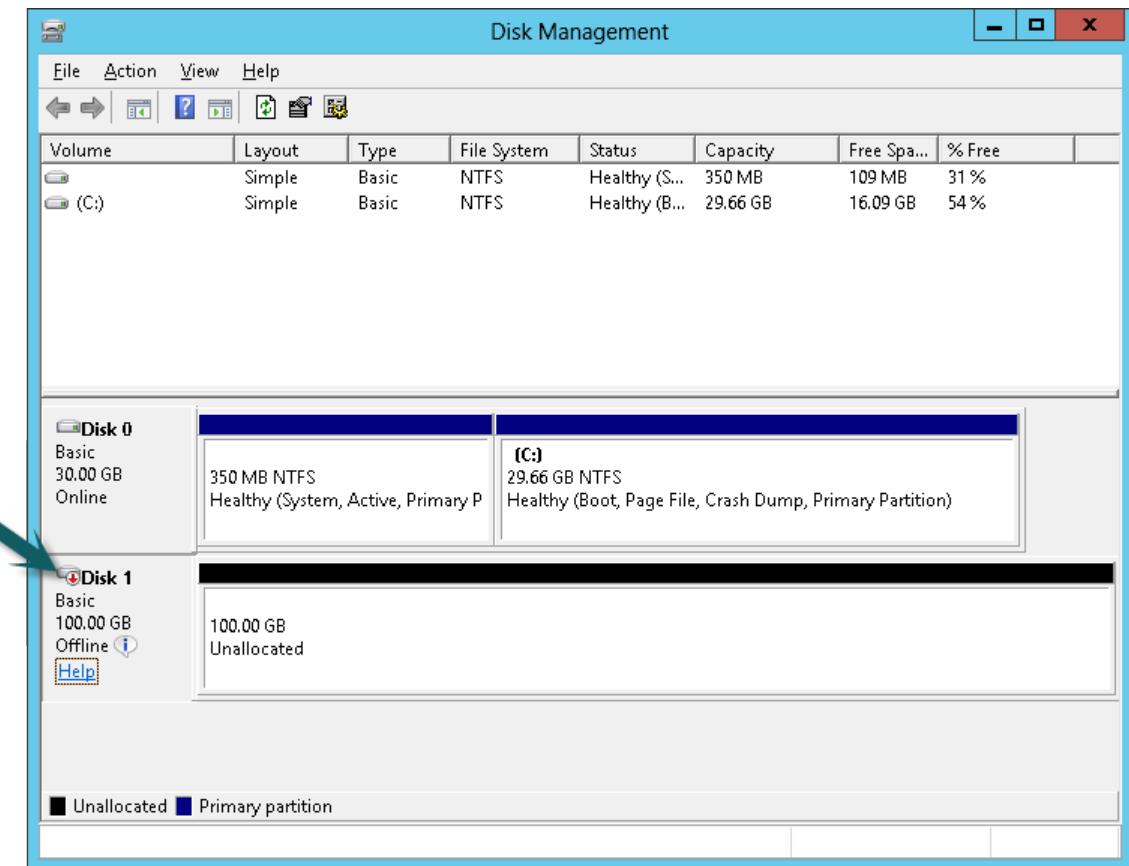
请注意，您可以拍摄 EBS 卷的快照以进行备份或在您创建其他卷时作为基线。有关更多信息，请参阅 [Amazon EBS 快照 \(p. 676\)](#)。

### 使卷可在 Windows 上使用

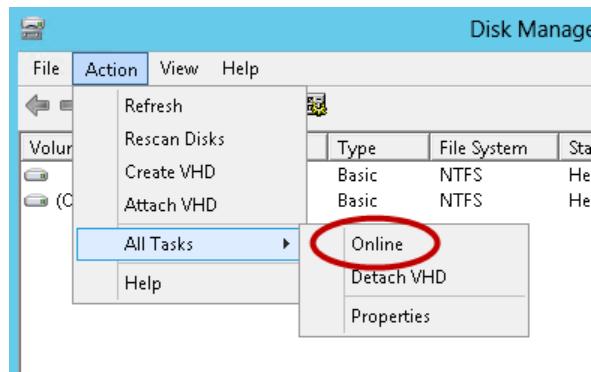
按照以下过程使卷可用。请注意，您可以从 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [使卷可在 Linux 上使用](#)，获得有关 Linux 实例上的卷的指示。

#### 使用 EBS 卷

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
2. 启动磁盘管理实用工具。在 Windows Server 2012 中，在任务栏上打开 Windows 徽标的上下文（右键单击）菜单，选择磁盘管理。在 Windows Server 2003/2008 中，选择开始、管理工具、计算机管理和磁盘管理。
3. 在下方窗格中，选择表示新 EBS 卷的磁盘。



- 在磁盘管理菜单上，选择操作、所有任务、联机。



- (有条件) 新磁盘在使用前需要进行初始化。



#### Caution

如果您装载的是已包含数据的卷（例如，公用数据集或您已从快照创建的卷），请务必确保您没有将卷重新格式化和删除现有数据。

初始化新磁盘：

- 在“磁盘管理”实用工具中，选择新的 EBS 卷磁盘。

- b. 在磁盘管理菜单中，选择操作、所有任务、初始化磁盘。
- c. 在初始化磁盘对话框中，选择要初始化的磁盘，选择所需分区形式，然后选择确定。

## 查看卷信息

### Abstract

列出有关 Amazon EBS 卷的信息，包括卷连接的特定 EC2 实例。

您可以在 AWS 管理控制台中同时查看所选区域中 Amazon EBS 卷的描述性信息。您还可以查看有关单个卷的详细信息，包括大小、卷类型、卷是否加密、加密卷所用的主密钥以及卷所连接的特定实例。

#### 使用控制台查看有关 EBS 卷的信息

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 要查看有关卷的更多信息，请选择该选项。

#### 使用命令行查看有关 EBS 卷的信息

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-volumes \(AWS CLI\)](#)
- [Get-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 监控您的卷状态

### Abstract

使用 CloudWatch 指标和卷状态检查监控 Amazon Elastic Block Store 卷。

Amazon Web Services (AWS) 自动提供数据，如 Amazon CloudWatch 指标和卷状态检查，您可以使用这些数据来监控您的 Amazon Elastic Block Store (Amazon EBS) 卷。

#### 内容

- [使用 CloudWatch 监控卷 \(p. 660\)](#)
- [使用状态检查来监控卷 \(p. 663\)](#)
- [监控卷事件 \(p. 664\)](#)
- [使用一个受损卷工作 \(p. 666\)](#)
- [使用 AutoEnableIO 卷属性 \(p. 668\)](#)

## 使用 CloudWatch 监控卷

CloudWatch 指标是统计数据，您可以使用这些指标来查看、分析和设置有关卷操作行为的警报。

下表描述适用于您的 Amazon EBS 卷的监控数据的类型。

| 类型 | 说明                                           |
|----|----------------------------------------------|
| 基本 | 数据在 5 分钟期间内自动可用，无需收费。该数据包括 EBS 支持的实例的根设备卷数据。 |

| 类型 | 说明                                              |
|----|-------------------------------------------------|
| 明细 | Provisioned IOPS (io1) 卷向 CloudWatch 自动发送一分钟指标。 |

当您从 CloudWatch 得到数据时，您可以列入一个 `Period` 请求参数来指定返回数据的粒度。这不同于我们收集数据时所用的时间（5分钟时间）。我们建议您在您的请求中指定的时间大于或等于收集时间，从而确保返回数据有效。

获取数据时，您可以使用 CloudWatch API 或 Amazon EC2 控制台。控制台从 CloudWatch API 中获取原始数据并根据数据显示一系列图表。根据您的需要，您既可以选择使用从 API 中获得的数据也可以选择使用控制台中的图表。

### Amazon EBS 指标

Amazon Elastic Block Store (Amazon EBS) 可将若干指标的数据点发送到 CloudWatch。Amazon EBS 通用型 SSD (gp2)、吞吐优化的 HDD (st1)、冷数据 HDD (sc1) 和磁盘（标准）卷自动将 5 分钟指标发送到 CloudWatch。预配置的 IOPS SSD (io1) 卷会自动向 CloudWatch 发送 1 分钟指标。有关如何监控 Amazon EBS 的更多信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [监控您的卷状态](#)。

| 指标                   | 说明                                                                                                                                                                                                                                     |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VolumeReadBytes      | 提供有关指定时段内的 I/O 操作的信息。Sum 统计数据将报告该时段内传输的总字节数。Average 统计数据将报告指定时段内每个 I/O 操作的平均大小。SampleCount 统计数据将报告指定时段内的 I/O 操作总数。Minimum 和 Maximum 统计数据与该指标无关，卷处于活动状态时，数据仅报告给 Amazon CloudWatch。如果卷处于空闲状态，则不会向 Amazon CloudWatch 报告任何数据。<br><br>单位：字节 |
| VolumeReadOps        | 在指定时间的 I/O 操作总数。                                                                                                                                                                                                                       |
| VolumeWriteOps       |  <b>Note</b><br><br>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。<br><br>单位：计数                                                                        |
| VolumeTotalReadTime  | 指定时间段中所有操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 5 分钟（300 秒）的时间段：如果该时间段内完成了 700 个操作，每个操作耗时 1 秒，值便是 700 秒。<br><br>单位：秒                                                                                                                 |
| VolumeTotalWriteTime | 未提交读取或写入操作的指定时间段中的总秒数。<br><br>单位：秒                                                                                                                                                                                                     |
| VolumeIdleTime       | 未提交读取或写入操作的指定时间段中的总秒数。<br><br>单位：秒                                                                                                                                                                                                     |
| VolumeQueueLength    | 指定时间段中等待完成的读取和写入操作请求的数量。<br><br>单位：计数                                                                                                                                                                                                  |

| 指标                          | 说明                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VolumeThroughput-Percentage | <p>仅用于 Provisioned IOPS 卷。每秒传输的 I/O 操作数 (IOPS) 在为 Amazon EBS 卷预配置的总 IOPS 中所占的百分比。Provisioned IOPS 卷在指定年份的超过 99.9% 的时间里可提供已调用 IOPS 的 10%。</p> <p> Note</p> <p>写入过程中，如果一分钟内没有其他待处理的 I/O 请求，指标值就会是 100%。另外，卷的 I/O 性能可能由于您已执行的操作而暂时降低（例如：在使用高峰期创建卷的快照、在非 EBS 优化的实例上运行卷，首次访问你卷上的数据）。</p> <p>单位：百分比</p> |
| VolumeConsumedRead-WriteOps | <p>仅用于 Provisioned IOPS 卷。指定时间段内使用的读取和写入操作的总量（规格化为 256K 容量单位）。</p> <p>每个小于 256K 的 I/O 操作算作使用了 1 IOPS。大于 256K 的 I/O 操作按 256K 容量单位计算。例如，1024K I/O 算作使用了 4 IOPS。</p> <p>单位：计数</p>                                                                                                                                                                                                     |
| BurstBalance                | <p>仅用于 吞吐优化 HDD (st1) 和 Cold HDD (sc1) 卷。提供有关突增存储桶中可用的余额。卷处于活动状态时，数据仅报告给 CloudWatch。如果未挂载卷，则不会报告任何数据。</p> <p>单位：百分比</p>                                                                                                                                                                                                                                                            |

### Amazon EC2 控制台中的图表

创建一个卷后，您可以在 Amazon EC2 控制台中查看该卷的监控图表。在控制台的 Volumes 页面上选择一个卷，然后选择 Monitoring。下表列出了显示的图表。右列说明如何使用从 CloudWatch API 中获得的原始数据指标来生成每一个图表。所有的图表周期都是 5 分钟。

| 图表              | 使用原始指标描述                         |
|-----------------|----------------------------------|
| 读取带宽 (KiB/s)    | 总和(VolumeReadBytes) / 周期 / 1024  |
| 写入带宽 (KiB/s)    | 总和(VolumeWriteBytes) / 周期 / 1024 |
| 读取吞吐量 (Ops/s)   | 总和(VolumeReadOps) / 周期           |
| 写入吞吐量 (Ops/s)   | 总和(VolumeWriteOps) / 周期          |
| 平均队列长度 (ops)    | 平均 (VolumeQueueLength)           |
| 空闲花费时间百分比       | 总和 (VolumeIdleTime) / 周期 * 100   |
| 平均读取大小 (KiB/op) | 平均 (VolumeReadBytes) / 1024      |
| 平均写入大小 (KiB/op) | 平均 (VolumeWriteBytes) / 1024     |
| 平均读取延迟 (ms/op)  | 平均 (VolumeTotalReadTime) * 1000  |
| 平均写入延迟 (ms/op)  | 平均 (VolumeTotalWriteTime) * 1000 |

对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

AWS 管理控制台包含用于 Amazon CloudWatch 的控制台。在 Amazon CloudWatch 控制台中可以搜索并浏览您所有的 AWS 资源指标，查看图表以排除问题并发现趋势，创建并编辑警报以获取问题通知，并且查看您的警报和 AWS 资源一目了然的概览。有关更多信息，请参阅 *Amazon CloudWatch 开发者指南* 中的 [AWS 管理控制台](#)。

## 使用状态检查来监控卷

通过卷状态检查，您可以更好地了解、追踪和管理 Amazon EBS 卷上数据的潜在不一致性。它们的作用是在您需要确定 Amazon EBS 卷是否损坏的时候为您提供信息，帮助您控制处理潜在不一致卷的方式。

卷状态检查为自动执行的测试，该测试每隔 5 分钟运行一次并返回通过或故障状态。如果所有的检查都通过，则卷的状态为 `ok`。如果一个检查返回故障，则卷的状态为 `impaired`。如果状态为 `insufficient-data`，那么该检查将在该卷上继续进行。您可以查看卷状态检查的结果来识别任意受损卷并进行所需操作。

当 Amazon EBS 判定一个卷中的数据具有潜在不一致性时，默认禁用从任何连接的 EC2 实例到该卷的 I/O，以此来防止数据损坏。禁用 I/O 后，下一个卷状态检查故障，并且卷状态为 `impaired`。此外，您还会看到一个通知您 I/O 被禁用的事件，并且您可以通过使能到该卷的 I/O 来解决卷的损坏状态。我们将一直等待，直至您启用 I/O 以便您能够决定是继续让实例使用该卷，还是使用命令（例如 `fsck` (Linux) 或 `chkdsk` (Windows)）来运行一致性检查。



### Note

卷状况以卷状况检查为依据，并不反映卷状态。因此，卷状况并不表示卷在 `error` 状态（例如卷不能接受 I/O 时）。

如果某一个卷的一致性对您无关重要，您可以立即使该卷可用，如果该卷受损，您可以配置该卷为自动使能 I/O 来覆盖默认行为，如果您使能了 `AutoEnableIO` 这一属性，那么该卷的状态检查将一直保持为通过。此外，您将会看到一个通知您该卷具有潜在不一致性的事件，但它的 I/O 不会自动使能。这使您能够检查卷的一致性或随后替换它。

I/O 性能状态检查将实际卷性能与卷的预期性能进行比较，并在卷性能低于预期时向您发出警示。此状态检查只适用于附加到实例的 `io1` 卷，对于通用型 SSD (`gp2`)、吞吐优化 HDD (`st1`)、Cold HDD (`sc1`) 或磁介质 (`standard`) 卷无效。I/O 性能状态检查每分钟执行一次，CloudWatch 每 5 分钟收集一次这些数据，因此在将 `io1` 卷附加到实例之后，最多可能要到 5 分钟后此检查才会报告 I/O 性能状态。



### Important

在初始化已从快照还原的 `io1` 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O Performance 状态检查中显示 `warning` 状态。这是预期行为，并且您可在初始化 `io1` 卷时忽略该卷上的 `warning` 状态。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 695\)](#)。

下表列出了 Amazon EBS 卷的状态。

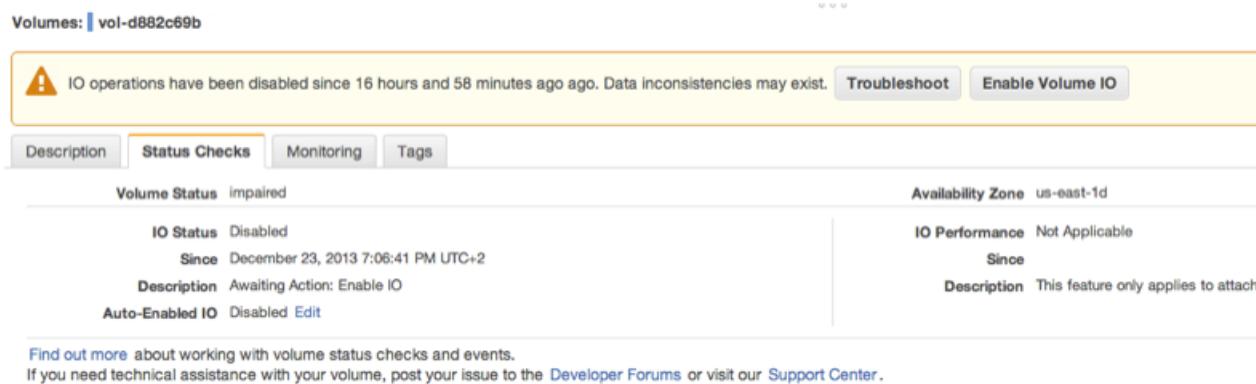
| 卷状态                  | I/O 使能状态             | I/O 性能状态（只适用于预配置 IOPS 卷）             |
|----------------------|----------------------|--------------------------------------|
| <code>ok</code>      | 使能（I/O 使能或 I/O 自动使能） | 正常（卷的期望性能）                           |
| <code>warning</code> | 使能（I/O 使能或 I/O 自动使能） | 降级（卷的性能低于期望性能）<br>严重降级（卷的性能大大低于期望性能） |

| 卷状态               | I/O 使能状态                                                 | I/O 性能状态 ( 只适用于预配置 IOPS 卷 )                            |
|-------------------|----------------------------------------------------------|--------------------------------------------------------|
| impaired          | 使能 ( I/O 使能或 I/O 自动使能 )<br>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 )<br>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 )<br>数据不足                          | 数据不足                                                   |

您可以使用 Amazon EC2 控制台、API 或命令行界面来查看和使用状态检查。

### 在控制台中查看状态检查

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中 , 选择 Volumes。
3. 在 EBS Volumes 页面上 , 使用 Volume Status 列列出每个卷的运行状态。
4. 要查看某个卷的状态 , 请选中该卷 , 然后选择 Status Checks。



5. 如果您的卷状态检查返回故障 ( 状态是 impaired ) , 请参阅[使用一个受损卷工作 \(p. 666\)](#)。

另外 , 您还可以使用“Events”窗格来查看一个单一窗格中的实例和卷所有的事件。有关更多信息 , 请参阅[监控卷事件 \(p. 664\)](#)。

### 使用命令行查看卷状态信息

您可以使用以下命令之一查看 Amazon EBS 卷的状态。有关这些命令行界面的更多信息 , 请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volume-status](#) (AWS CLI)
- [Get-EC2VolumeStatus](#) ( 适用于 Windows PowerShell 的 AWS 工具 )

## 监控卷事件

默认情况下 , 当 Amazon EBS 判定一个卷数据具有潜在不一致性时 , 它将会禁用从任何连接的 EC2 实例到该卷的 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 AutoEnableIO 卷属性的设置。更多关于改变这些属性的信息 , 请参阅[使用一个受损卷工作 \(p. 666\)](#)。

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 I/O**

卷数据具有潜在一致性。在您明确的使能它之前，将一直禁用 I/O。您明确使能 I/O 后，事件描述变为“IO Enabled”。

**I/O 使能**

明确地使能这些卷的 I/O 操作。

**I/O 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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Events。
3. 列出具有事件的所有实例和卷。可以按卷进行筛选以便仅查看卷状态。您也可以过滤指定的状态类型。
4. 选择一个卷以查看其特定事件。

Event: vol-3682c675

**!** IO operations have been disabled since 30 days, 15 hours and 22 minutes ago. Data inconsistencies may exist. [Enable Volume IO](#)

|                   |                                    |
|-------------------|------------------------------------|
| 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          |                                    |

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 \(p. 666\)](#)。如果您的卷 I/O 性能低于正常值，这可能是因为您之前的操作（例如，在使用高峰期间创建卷快照、在无法支持所需 I/O 带宽的实例上运行卷、第一次访问卷上的数据，等等）而造成的暂时状况。

### 使用命令行查看卷的事件

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volume-status \(AWS CLI\)](#)
- [Get-EC2VolumeStatus \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 使用一个受损卷工作

本节讨论了如果因为您的卷中数据具有潜在不一致性而导致一个卷受损时您可以进行的选择。

### 选项

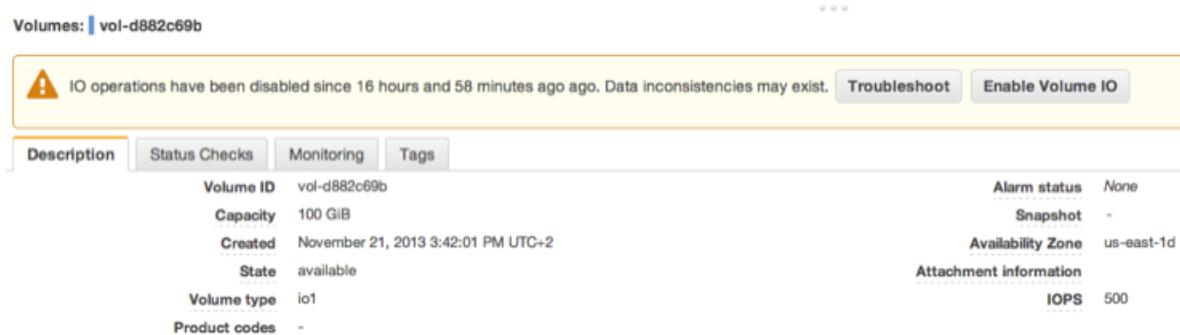
- [选择 1：在附加到它的实例上的卷上进行一次一致性检查。 \(p. 666\)](#)
- [选择 2：使用其他实例在该卷上进行一次一致性检查 \(p. 667\)](#)
- [选择 3：如果您不再需要它，请删除该卷 \(p. 668\)](#)

### 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.amazonaws.cn/ec2/>。
  - b. 在导航窗格中，选择 Volumes。
  - c. 选择要使能 I/O 操作的卷。
  - d. 在详细信息窗格中，选择 Enable Volume IO。



- e. 在 Enable Volume IO 中，选择 Yes, Enable。
3. 检查卷上数据。
  - a. 运行 fsck (Linux) 或 chkdsk (Windows) 命令。

- b. ( 可选 ) 查看所有适用的应用程序或系统日志以了解相关错误消息。
- c. 如果卷受损时间超过 20 分钟 , 您可以联系支持。选择 Troubleshoot , 然后在 Troubleshoot Status Checks 对话框上选择 Contact Support 提交一个支持案例。

## 使用命令行启用卷的 I/O

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息 , 请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [enable-volume-io \(AWS CLI\)](#)
- [Enable-EC2VolumeIO \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 选择 2 : 使用其他实例在该卷上进行一次一致性检查

按照以下程序在您的产品环境外检查该卷。

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。



### Important

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.amazonaws.cn/ec2/>。
  - b. 在导航窗格中 , 选择 Volumes。
  - c. 选择要分离的卷。
  - d. 选择 Actions、Force Detach Volume。系统会提示您进行确认。
3. 在该卷上使能 I/O。
  - a. 在导航窗格中 , 选择 Volumes。
  - b. 选择您在之前的步骤中分离的卷。
  - c. 在详细信息窗格中 , 选择 Enable Volume IO。

The screenshot shows the 'Volumes' page in the Amazon EC2 console. A yellow warning box at the top states: 'IO operations have been disabled since 16 hours and 58 minutes ago ago. Data inconsistencies may exist.' It includes 'Troubleshoot' and 'Enable Volume IO' buttons. Below the warning, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab is selected, showing details for a volume named 'vol-d882c69b'. The volume's state is listed as 'available'. Other visible details include 'Volume ID: vol-d882c69b', 'Capacity: 100 GiB', 'Created: November 21, 2013 3:42:01 PM UTC+2', 'State: available', 'Volume type: io1', and 'Product codes: -'. On the right side, there are columns for 'Alarm status: None', 'Snapshot: -', 'Availability Zone: us-east-1d', 'Attachment information', and 'IOPS: 500'.

- d. 在 Enable Volume IO 对话框中选择 Yes, Enable。

4. 将该卷附加到另一个实例。有关信息，请参阅 [启动实例 \(p. 216\)](#) 和 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。
5. 检查卷上数据。
  - a. 运行 fsck (Linux) 或 chkdsk (Windows) 命令。
  - b. (可选) 查看所有适用的应用程序或系统日志以了解相关错误消息。
  - c. 如果卷受损时间超过 20 分钟，您可以联系支持。选择 Troubleshoot，然后在故障排除对话框中选择 Contact Support 以提交支持案例。

## 使用命令行启用卷的 I/O

您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [enable-volume-io \(AWS CLI\)](#)
- [Enable-EC2VolumeIO \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 选择 3：如果您不再需要它，请删除该卷

如果您想将该卷从您的环境中去除，只需删除它即可。关于删除一个卷的信息，请查阅 [删除 Amazon EBS 卷 \(p. 671\)](#)。

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 \(p. 655\)](#)。

## 使用 AutoEnableIO 卷属性

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何连接的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来查明故障的原因。如果特定卷的一致性无关紧要，并且您希望在其为 impaired 的情况下该卷立即可用，可通过将该卷配置为自动启用 I/O 来覆盖默认行为。如果您启用 AutoEnableIO 卷属性，则会自动重新启用该卷与实例之间的 I/O，该卷的状态检查会通过。此外，您将会看到一个通知您该卷具有潜在不一致状态的事件，但它的 I/O 不会自动启用。如果发生此事件，您应该检查该卷的一致性，如有必要，可对其进行更换。有关更多信息，请参阅 [监控卷事件 \(p. 664\)](#)。

本部分介绍如何使用 Amazon EC2 控制台、命令行界面或 API 来查看和修改卷的 AutoEnableIO 属性。

### 在控制台中查看卷的 AutoEnableIO 属性

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 在下方窗格中，选择 Status Checks。
5. 在“Status Checks”标签中，“Auto-Enable IO”显示了您选中卷的当前设置，是 Enabled 或 Disabled。

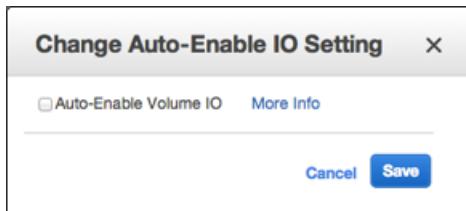
The screenshot shows the 'Status Checks' tab selected for a volume named 'vol-d882c69b'. A warning message indicates that IO operations have been disabled since 16 hours and 58 minutes ago, and data inconsistencies may exist. Buttons for 'Troubleshoot' and 'Enable Volume IO' are present. The volume status is listed as 'impaired' with 'IO Status' set to 'Disabled' since December 23, 2013. The 'Availability Zone' is 'us-east-1d'. A note at the bottom provides links for more information and developer forums.

想要修改一个卷的 AutoEnableIO 属性，需要进行以下操作在控制台中

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 在 Volumes 页面顶部，选择 Actions。
5. 选择 Change Auto-Enable IO Setting。



6. 在 Change Auto-Enable IO Setting (更改自动启用 IO 设置) 对话框中，选择 Auto-Enable Volume IO (自动启用卷 IO) 选项为受损卷自动启用 IO。想要禁用该功能，请清除该选项。



7. 选择 Save。

或者，不完成上一过程中的步骤 4-6，而是选择 Status Checks、Edit。

使用命令行查看或修改卷的 AutoEnableIO 属性

您可以使用以下命令之一查看 Amazon EBS 卷的 AutoEnableIO 属性。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-volume-attribute \(AWS CLI\)](#)
- [Get-EC2VolumeAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

要修改卷的 AutoEnableIO 属性，您可以使用以下命令之一。

- [modify-volume-attribute](#) (AWS CLI)
- [Edit-EC2VolumeAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

## 从实例断开 Amazon EBS 卷

### Abstract

明确地从实例断开 Amazon EBS 卷，或通过终止实例来断开连接。

您可以明确地从实例断开 Amazon EBS 卷，或终止实例。但是，如果实例正在运行，您必须首先从实例上卸载卷；否则，卷会在尝试分离时卡在繁忙状态。强行分离卡住的卷可能会导致以下问题：

- 对文件系统及其包含的数据造成损坏
- 无法使用相同的设备名称挂载新卷，除非您重启实例

如果 EBS 卷是实例的根设备，则在断开卷连接之前必须停止该实例。

如果具有 AWS Marketplace 产品代码的卷与实例断开，产品代码就不再与该实例关联。



### Important

断开卷之后，只要存储量超出了免费使用套餐的限额，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 \(p. 671\)](#)。

该示例卸载了卷，然后明确地将其从实例断开。当您要终止实例或将卷连接到其他实例时，这会非常有用。要验证该卷是否不再与该实例连接，可参阅 [查看卷信息 \(p. 660\)](#)。

注意，您可以重新连接断开的卷（无需卸载），但可能不能获得相同安装点，如果断开时正在写入卷，那么卷上的数据可能不同步。

### 使用控制台断开 EBS 卷

1. 首先，卸载该卷。打开 Disk Management (磁盘管理)，右键单击该卷，再选择 Change Drive Letter and Path (更改盘符和路径)。选择安装点，然后单击 Remove (删除)。
2. 打开 Amazon EC2 控制台。
3. 单击导航窗格中的 Volumes (卷)。
4. 选择一个卷并单击 Detach Volume (断开卷)。
5. 在确认对话框中，单击 Yes, Detach (是，断开)。

### 使用命令行将 EBS 卷从实例断开

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

- [detach-volume](#) (AWS CLI)
- [Dismount-EC2Volume](#) (适用于 Windows PowerShell 的 AWS 工具)

### 故障排除

如果您的卷处于正在断开状态，您可以通过单击 Force Detach (强制断开) 来强制执行断开操作。强制断开连接可能会导致数据丢失或文件系统损坏。请将此选项仅用作在不得已的情况下从故障实例断开卷的方式。

法，或是在要删除卷的情况下断开卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用此选项，则必须执行文件系统检查和修复流程。

如果在几分钟内多次尝试强制断开卷，并且该卷处于正在断开状态，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。

## 删除 Amazon EBS 卷

### Abstract

当您不再需要某个 Amazon EBS 卷时，删除该卷。

如果不再需要某个 Amazon EBS 卷，可以将其删除。删除后，卷上的数据都不复存在，并且再也不能连接到任何实例。然而，您可在删除之前，保存卷的快照，以便未来使用该快照重新创建该卷。

### 使用控制台删除 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 单击导航窗格中的 Volumes (卷)。
3. 选择一个卷并单击 Delete Volume (删除卷)。
4. 在确认对话框中，单击 Yes, Delete (是，删除)。

### 使用命令行删除 EBS 卷

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

- [delete-volume \(AWS CLI\)](#)
- [Remove-EC2Volume \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 在 Windows 上扩展 EBS 卷的存储空间

### Abstract

增大现有卷上的存储空间，而不丢失卷上的数据。

您可增加现有 EBS 卷的存储空间，同时不失去此卷上的数据。为此，您将您的数据迁移至更大的卷，然后扩展此卷上的文件系统以识别新近可用的空间。在确认新卷运行正常后，可以删除旧卷。

### 任务

- [将数据迁移到更大的卷 \(p. 672\)](#)
- [扩展 Windows 文件系统 \(p. 673\)](#)
- [删除旧卷 \(p. 676\)](#)

如果您需要扩展 Linux 实例上的卷的存储空间，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [扩展卷的存储空间](#)。

如果您创建更大的卷，则需要为额外的存储空间付费。有关更多信息，请参阅 [Amazon EC2 定价](#) 页面上的 [Amazon Elastic Block Store](#) 部分。



### Note

如果您的存储所需的 EBS 卷大小超出了 AWS 提供的卷大小，可以使用 RAID 0 跨多个物理卷“条带化”一个逻辑卷。有关更多信息，请参阅 [Windows 上的 RAID 配置](#)。

## 将数据迁移到更大的卷

您必须停止实例才能扩展存储空间。当您停止和启动实例时，需要注意以下事项：

- 将擦除任何实例存储卷上的任何数据。因此，如果实例存储卷上有任何您要保留的数据，请将其备份到持久性存储。
- 如果您的实例在 VPC 中运行并具有公有 IP 地址，则我们会释放该地址并向它提供新的公有 IP 地址。实例会保留其私有 IP 地址以及任何弹性 IP 地址。
- 如果实例在 EC2-Classic 中运行，则我们会为其提供新的公有和私有 IP 地址，并取消该实例与任何弹性 IP 地址的关联。您在重新启动实例后，必须重新关联任何弹性 IP 地址。
- 如果您的实例处于 Auto Scaling 组中，则 Auto Scaling 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。为预防这一问题，您可暂时挂起组的 Auto Scaling 进程。有关更多信息，请参阅 [Auto Scaling 用户指南](#) 中的 [挂起和恢复 Auto Scaling 进程](#)。

### 将数据迁移到更大的卷

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances，然后找到具有要扩展卷的实例。
3. 记录实例 ID 和可用区。当您在后续步骤中向实例挂载新卷时，您需要指定此信息。
4. 确保实例的 Shutdown Behavior 设置为 Stop 而不是 Terminate。
  - a. 选择实例。
  - b. 从上下文菜单（右键单击）中选择 Instance Settings，然后选择 Change Shutdown Behavior。
  - c. 如果 Shutdown behavior 设置为 Terminate，请选择 Stop，然后选择 Apply。

如果 Shutdown behavior 已经设置为 Stop，则选择 Cancel。
5. 停止实例。有关如何停止实例的更多信息，请参阅 [停止和启动您的实例 \(p. 229\)](#)。



### Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

6. 创建要扩展的卷的快照。
  - a. 在导航窗格中，选择 Volumes，然后找到要扩展的卷。
  - b. 从上下文菜单（右键单击）中，选择要扩展的卷，然后选择 Create Snapshot。
  - c. 在 Name 和 Description 字段中输入名称，然后选择 Yes, Create。
7. 从快照创建卷。
  - a. 在导航窗格中，选择 Snapshots。
  - b. 如果您刚创建的快照的状态设置为 completed，请选择快照，然后从上下文菜单（右键单击）中选择 Create Volume。
  - c. 在 Create Volume 对话框中，选择所需的卷类型并输入新卷大小。您还必须设置 Availability Zone 以匹配实例可用区。选择 Yes, Create。



### Important

如果不将 Availability Zone 设置为与实例匹配，则无法将新卷挂载到实例。

8. 断开旧卷。

- a. 在导航窗格中，选择 Volumes，然后从列表中选择旧卷。记录 Attachment Information 字段中的设备名称。当您在后续步骤中向实例挂载新卷时，您需要指定此信息。此信息的格式如下：

i-xxxxxxxxxxxxxxxxx (*instance\_name*):*device\_name*

- b. 从上下文菜单（右键单击）中选择旧卷，然后选择 Detach Volume。
- c. 在 Detach Volume 对话框中，选择 Yes, Detach。断开卷可能需要几分钟。

9. 连接新扩展的卷

- a. 在导航窗格中，选择 Volumes。
- b. 从上下文菜单（右键单击）中选择新卷，然后选择 Attach Volume。
- c. 开始在 Instance 字段中键入实例的名称或 ID，然后选择实例。
- d. 输入在[Step 8.a \(p. 673\)](#)中检索的相同设备名称，然后选择 Yes, Attach。请务必将新卷准确挂载到您之前记录的位置（例如 /dev/sda1）。

10. 重新启动实例。

- a. 在导航窗格中，选择 Instances，然后选择要重新启动的实例。
- b. 从上下文菜单（右键单击）中选择 Instance State，然后选择 Start。
- c. 在 Start Instances 对话框中，选择 Yes, Start。如果实例无法启动，并且扩展卷为根卷，请确认已使用与原始卷相同的设备名称连接了扩展卷，例如 /dev/sda1。

实例启动之后，可以检查文件系统大小，看实例是否识别这个更大的卷空间。

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[扩展 Windows 文件系统 \(p. 673\)](#)。

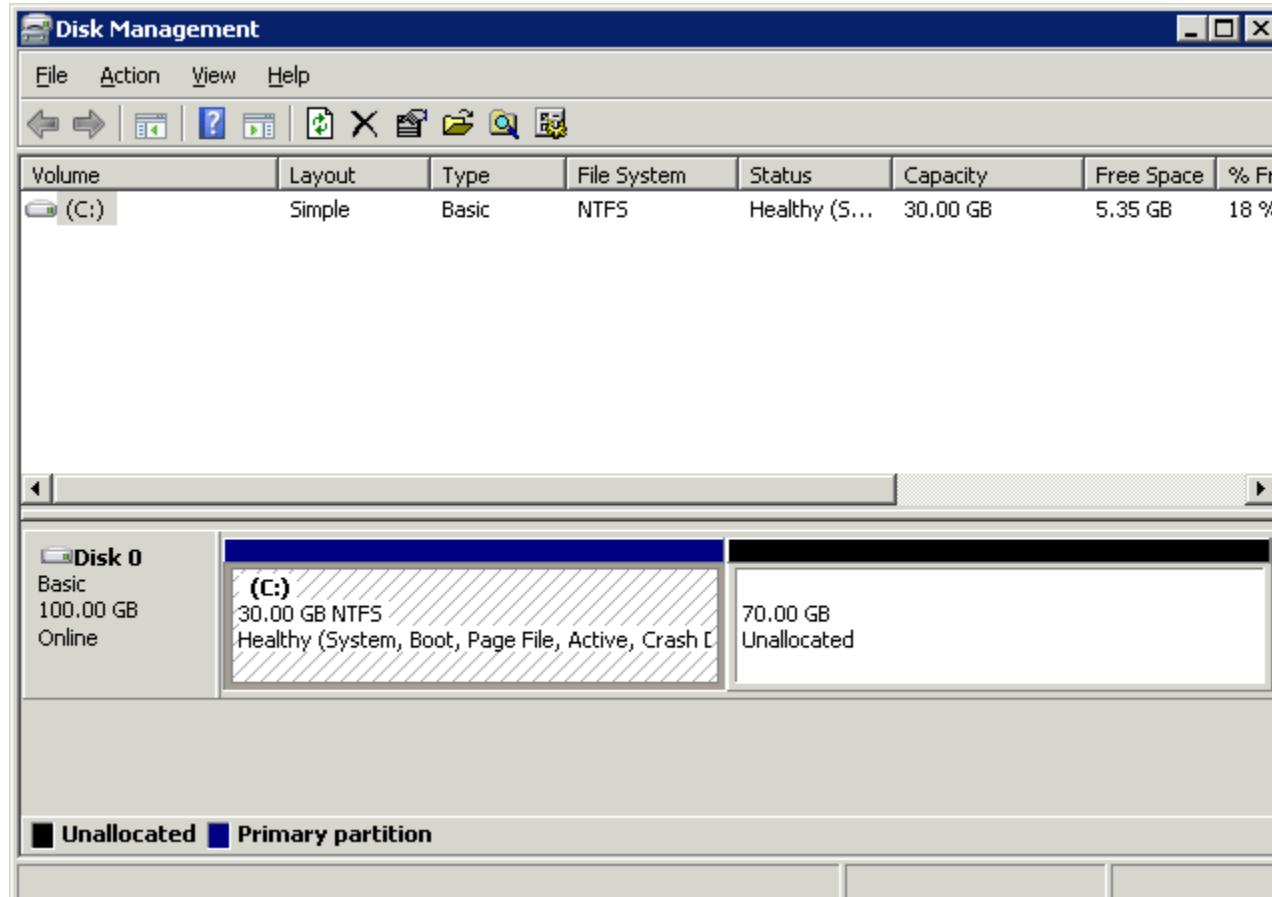
您可能需要将卷联机才能使用它。有关更多信息，请参阅[使 Amazon EBS 卷可用 \(p. 658\)](#)。您无需重新格式化卷。

## 扩展 Windows 文件系统

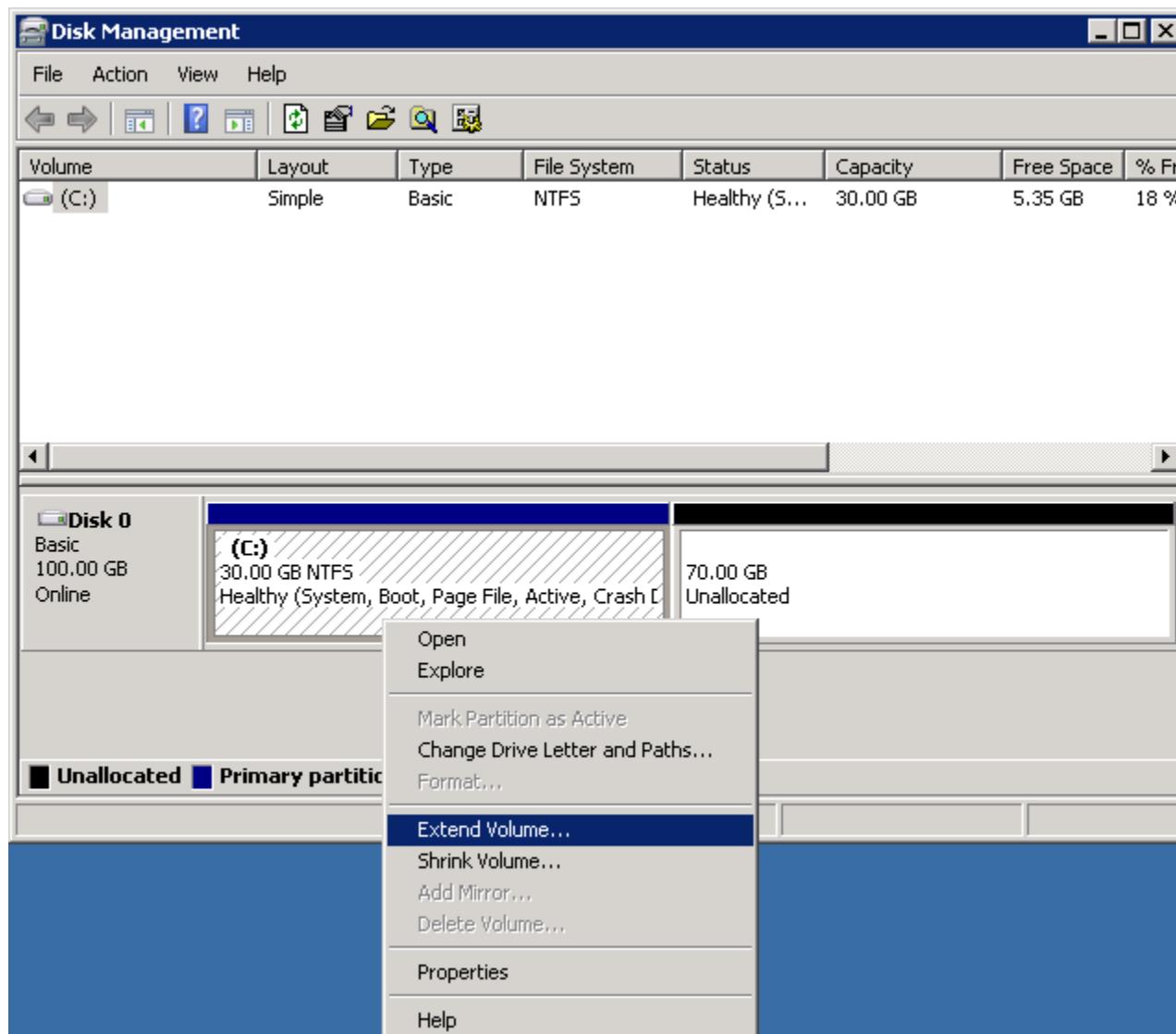
在 Windows 中，使用磁盘管理实用工具将磁盘大小扩展为新的卷大小。

### 扩展 Windows 文件系统

1. 使用远程桌面登录 Windows 实例。
2. 打开磁盘管理工具。
  - 在 Windows Server 2012 的“开始”屏幕上，在“搜索”窗格中键入 disk management 并选择创建并格式化硬盘分区。
  - 在 Windows Server 2008 上的运行对话框中键入 diskmgmt.msc，然后按 Enter。

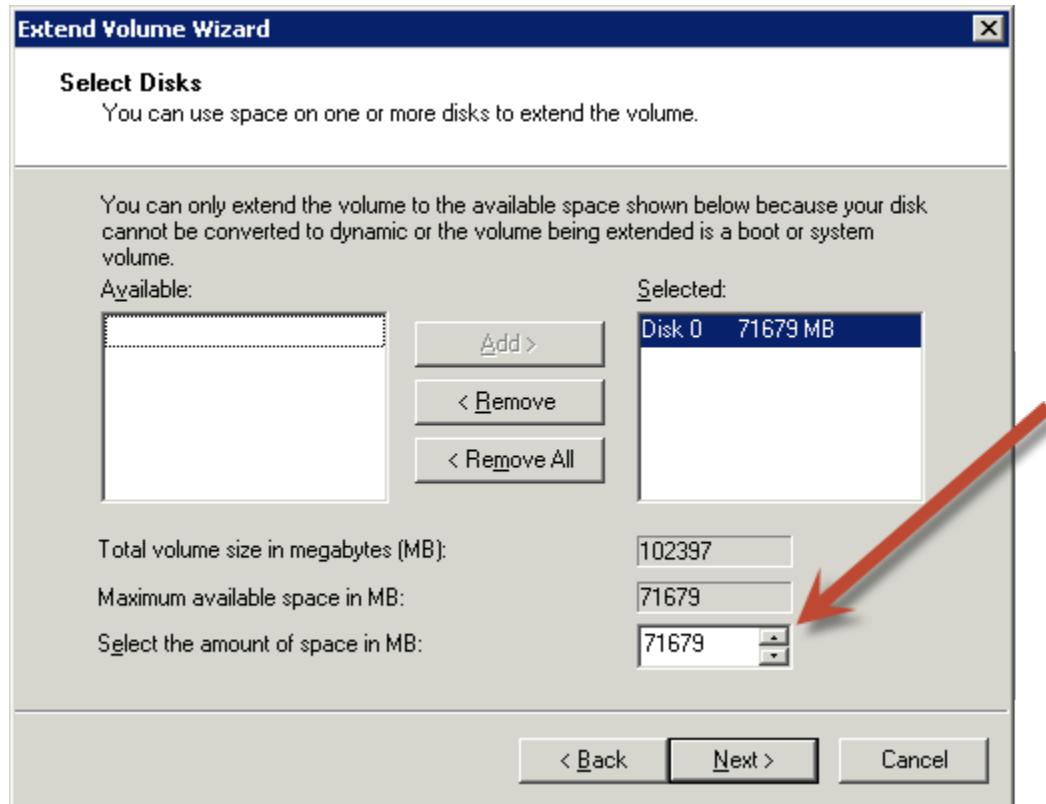


3. 右键单击扩展的硬盘并选择 Extend Volume (扩展卷)。



4. 在扩展卷向导中，选择 Next，然后将 Select the amount of space in MB 字段设置为要将卷扩展到的兆字节数。通常，您会将此设置为最大可用空间。请注意，Selected 下突出显示的文本是将添加的空间量，而不是卷最终将具有的大小。

完成向导。



## 删除旧卷

在实例中连接并扩展新卷后，如果不再需要旧卷，可以将其删除。

### 删除旧卷

1. 在 Amazon EC2 控制台中，在导航窗格中选择 Volumes，然后选择要删除的卷。
2. 从上下文菜单（右键单击）中选择 Delete Volume。
3. 在 Delete Volume 对话框中，选择 Yes, Delete。

## Amazon EBS 快照

### Abstract

将快照用作 Amazon EBS 卷的时间点备份副本。

您可以通过拍摄时间点快照将 EBS 卷上的数据备份到 Amazon S3。快照属于增量备份，这意味着仅保存设备上在最新快照之后更改的数据块。这将最大程度地缩短创建快照所需的时间，且可以节省存储成本。删除快照时，只有该快照特有的数据会被删除。活动快照包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。

### 内容

- [快照概述 \(p. 677\)](#)
- [创建 Amazon EBS 快照 \(p. 677\)](#)
- [删除 Amazon EBS 快照 \(p. 678\)](#)
- [复制 Amazon EBS 快照 \(p. 679\)](#)

- [查看 Amazon EBS 快照信息 \(p. 681\)](#)
- [共享 Amazon EBS 快照 \(p. 681\)](#)

## 快照概述

创建 EBS 卷时，可基于现有快照创建。新卷此时为用于创建快照的原始卷的精确副本。从现有快照创建卷时，其在后台延时加载，因此可以立即开始使用它们。如果您访问尚未加载的一部分数据，则卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的剩余数据。有关更多信息，请参阅 [创建 Amazon EBS 快照 \(p. 677\)](#)。

通过修改其访问权限，您可以在不同 AWS 账户之间共享快照。您可以复制您拥有的快照以及与您共享的快照。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 681\)](#)。

EBS 快照广泛支持 EBS 加密：

- 加密卷的快照会自动加密。
- 通过加密快照创建的卷会自动加密。
- 在复制您拥有的未加密快照时，您可以在复制过程中对其进行加密。
- 在复制您拥有的加密快照时，您可在复制过程中使用其他密钥重新加密。

有关更多信息，请参阅 [Amazon EBS 加密](#)。

快照受限于在其中创建它们的区域。在您创建 EBS 卷的快照之后，可以在同一区域使用它来创建新卷。有关更多信息，请参阅 [从快照还原 Amazon EBS 卷 \(p. 655\)](#)。您还可以跨区域复制快照，从而能够更轻松地将多个区域用于地理扩展、数据中心迁移和灾难恢复。您可以复制具有 completed 状态的任何可访问快照。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 679\)](#)。

## 创建 Amazon EBS 快照

### Abstract

创建 Amazon EBS 卷的快照以用作新卷的基准或用于数据备份。

将数据写入 EBS 卷之后，您可以定期创建卷快照，以用作新卷的基线或用于数据备份。如果您定期为卷拍摄快照，则快照为增量快照，因此新快照中仅保存设备上在保存上次快照之后更改的数据块。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

快照是异步拍摄的；时间点快照是立即创建的，但在快照完成（当所有已修改数据块都已转移到 Amazon S3 时）之前，其状态为 pending，很多大型初始快照或后续快照（其中的数据块已更改）可能需要几个小时才能完成。



### Important

尽管您可以在某个卷的前一个快照处于 pending 状态时拍摄该卷的快照，但一个卷有多个 pending 快照可能会导致该卷的性能降低，直至这些快照完成。

一个卷有 5 个 pending 快照的限制。如果您在尝试给同一个卷创建多个并发快照时收到 `ConcurrentSnapshotLimitExceeded` 错误，请等待一个或多个 pending 快照完成，然后再为该卷创建另一个快照。

从加密卷拍摄的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷及所有关联快照中的数据在静态或传输过程中均受到保护。有关更多信息，请参阅 [Amazon EBS 加密](#)。

默认情况下，只有您可以从您拥有的快照创建卷。但是，您可以将未加密的快照将共享给特定 AWS 账户，还可通过将其设为公开来与整个 AWS 社区共享。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 681\)](#)。

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 \(p. 681\)](#)。

在从具有 AWS Marketplace 产品代码的卷创建快照后，该卷的产品代码将会传送到该快照。

您可以拍摄正在使用的已连接卷的快照。但是，快照只能捕获发出快照命令时已经写入您的 Amazon EBS 卷的数据。其中可能不包括已由任何应用程序或操作系统缓存的任何数据。如果您可以将该卷的所有文件写入暂停足够长的时间以拍摄快照，则快照应该是完整的。但是，如果您无法暂停该卷的所有文件写入，则应该从实例中卸载该卷、发出快照命令，然后重新安装该卷，以确保获得一致且完整的快照。当快照状态为 pending 时，您可以重新安装并使用卷。

要为用作根设备的 Amazon EBS 卷创建快照，您应该在拍摄快照之前停止实例。

要在 Windows 中卸载卷，请打开“Disk Management (磁盘管理)”，然后右键单击要卸载的卷，再选择 Change Drive Letter and Path (更改盘符和路径)。选择要删除的安装点，然后单击 Remove (删除)。

### 使用控制台创建快照

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择 Create Snapshot。
4. 在 Create Snapshot 对话框中，选择要为其创建快照的卷，然后选择 Create。

### 使用命令行创建快照

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

- [create-snapshot \(AWS CLI\)](#)
- [New-EC2Snapshot\(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 删除 Amazon EBS 快照

### Abstract

使用 AWS 管理控制台、CLI 或 API 删除 Amazon EBS 卷的快照。

删除快照时，仅删除该快照专有的数据。删除卷之前的快照不会影响您使用该卷之后的快照还原卷的能力。

如果您定期为卷拍摄快照，则快照为增量快照，因此新快照上仅保存自上次快照后设备上新增加的块。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以作恢复卷之用。

请注意，您不能删除已注册 AMI 所用 EBS 卷的根设备的快照。您必须先取消注册 AMI，然后才能删除快照。有关更多信息，请参阅 [取消注册您的 AMI \(p. 89\)](#)。

### 如需使用控制台删除快照

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择快照，然后从 Actions 列表中选择 Delete。

4. 选择 Yes, Delete.

### 使用命令行删除快照

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

- [delete-snapshot \(AWS CLI\)](#)
- [Remove-EC2Snapshot \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 复制 Amazon EBS 快照

### Abstract

可以跨 地区复制这些快照，从而能够更轻松地将多个 AWS 地区用于地理扩展、数据中心迁移和灾难恢复。

利用 Amazon EBS，您可以创建卷的时间点快照，我们为您将其存储在 Amazon Simple Storage Service (Amazon S3) 中。在创建快照并且已完成到 Amazon S3 的复制（快照状态为 `completed` 时）后，您可将快照从一个 AWS 区域复制到另一个 AWS 区域或复制到相同区域内。Amazon S3 服务器端加密（256 位 AES）可在复制过程中保护传输中的快照数据。快照副本将获得与原始快照 ID 不同的快照 ID。



### Note

要复制 Amazon Relational Database Service (Amazon RDS) 快照，请参阅 Amazon Relational Database Service 用户指南 中的 [复制数据库快照](#)。

您可以通过以下方式使用快照副本：

- 地理扩展：在新的区域启动您的应用程序。
- 迁移：将应用程序迁移到新区域，以实现更好的可用性并最大限度地降低成本。
- 灾难恢复：在不同的地理位置定期备份您的数据和日志。为防止灾难发生，您可以使用辅助区域存储的时间点备份恢复您的应用程序。该操作能够让数据丢失和恢复时间降至最低。
- 加密：对之前未加密的快照进行加密、为加密快照或与您共享的加密快照更改密钥、为您拥有的快照创建副本以便从其中还原卷。
- 数据保留和审计要求：将您的加密 EBS 快照从一个 AWS 账户复制到其他 AWS 账户，以保留数据日志或其他文件，便于进行审计或数据保留。使用不同的账户有助于防止意外删除快照，并在您的主要 AWS 账户遭到泄露时为您提供保护。



### Note

由 CopySnapshot 操作创建的快照具有一个不应用于任何用途的任意卷 ID。

用户定义的标签不会从源快照复制到新快照。复制操作完成后，您可将用户定义的标签应用于新的快照。有关更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 737\)](#)。

每个账户最多可以同时进行到同一目的地的五个快照复制请求。您可以复制任何状态为 `completed` 的可访问快照，包括共享快照和您创建的快照。您也可以复制 AWS Marketplace、VM Import/Export 和 AWS Storage Gateway 快照，但必须确认目标区域支持该快照。

复制快照时，您只需支付用于跨地区快照数据复制及在目标地区内存储复制的快照的数据传输和存储的费用。如果快照复制失败，不收取费用。但是，如果您取消尚未完成的快照复制，或在复制期间删除源快照，则需要支付传输数据的带宽费用。

到另一个区域的第一个快照副本始终是完整副本。每个后续快照副本都是增量式的（可加快复制过程），这意味着只会传输在到同一目的地的最后一次快照复制以后发生更改的快照中的数据块。对增量快照的支

持是特定于某个区域对的，在该区域对中，源卷的上一个完整快照副本已在目标区域中可用，并且被限制为加密快照的默认 EBS CMK。例如，如果将未加密快照从 美国东部（弗吉尼亚北部）区域复制到 美国西部（俄勒冈）区域，则卷的第一个快照副本是完整副本，并且在相同区域间传输的相同卷的后续快照副本是增量副本。



#### Note

只要满足以下条件，单个区域内的快照副本就完全不会复制任何数据：

- 在复制操作过程中，快照副本的加密状态不会更改
- 对于加密快照，源快照和副本都使用默认 EBS CMK 进行加密

如果希望另一账户能够复制您的快照，您必须修改快照权限以允许访问该账户，或使快照公开可用，以便所有 AWS 账户均可复制它。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 681\)](#)。

#### 加密快照

复制快照时，您可选择加密副本（如果原始快照未加密），也可以指定一个与原始快照不同的 CMK，这样，生成的快照副本将使用新 CMK。但是，在复制操作过程中更改快照的加密状态或使用非默认 EBS CMK 总是会生成完整副本（非增量），这可能产生更多的数据传输和存储费用。

要通过其他账户复制加密快照，您必须拥有使用该快照以及用于加密原始快照的客户主密钥 (CMK) 的权限。有关更多信息，请参阅 [共享 Amazon EBS 快照 \(p. 681\)](#)。



#### Note

如果要复制一个与您共享的加密快照，那么您应考虑在复制过程中使用您控制的其他密钥重新加密快照。这样，即使原始密钥泄露或拥有者出于任何原因撤销了密钥，您也不会失去对您创建的卷的访问权限。

#### 使用 Amazon EC2 控制台复制快照

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 选择要复制的快照，然后从 Actions 列表中选择 Copy。
4. 在 Copy Snapshot (复制快照) 对话框中，根据需要进行以下更新：
  - Destination region (目标区域)：选择要在其中写入快照副本的区域。
  - Description (描述)：默认情况下，描述包括源快照的相关信息，以便您能区别副本和原始内容。必要时，您可以更改此描述。
  - 加密：如果源快照未加密，则可选择对副本进行加密。您无法解密已加密快照。
  - 主密钥：将用于对此快照进行加密的客户主密钥 (CMK)。您可以从您账户的主密钥中选择或从一个不同的账户中键入/粘贴密钥 ARN。您可在 IAM 控制台中创建新的加密主密钥。

5. 选择 Copy。
6. 在 Copy Snapshot 确认对话框中，选择 Snapshots 转至指定区域的 Snapshots 页面，或选择 Close。

要在稍后查看复制过程的进度，请切换到目标区域，然后刷新 Snapshots (快照) 页面。该页面的顶部将列出正在进行的复制。

#### 检查是否失败

如果您在未获得加密密钥使用权限的情况下试图复制加密快照，则操作将失败，且系统不会提示。您刷新页面后，控制台才会显示错误状态。您还可以通过命令行检查快照的状态。例如：

```
C:\> aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

如果复制因密钥权限不足而失败，您将看到以下消息：

```
"StateMessage": "Given key ID is not accessible"
```



#### Note

在复制加密的快照时，您必须对默认 CMK 具有描述权限。显式拒绝这些权限将导致复制失败。

### 使用命令行复制快照

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

- [copy-snapshot \(AWS CLI\)](#)
- [Copy-EC2Snapshot \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 查看 Amazon EBS 快照信息

### Abstract

描述您使用 AWS 管理控制台、CLI 或 API 创建的快照。

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.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Snapshots。
3. 要减少列表内容，请从 Filter 列表中选择一个选项。例如，要仅查看您的快照，请选择 Owned By Me。您可以使用高级搜索选项来进一步筛选您的快照。选择搜索栏可查看可用筛选条件。
4. 要查看有关某个快照的更多信息，请选择该快照。

### 使用命令行查看快照信息

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

- [describe-snapshots \(AWS CLI\)](#)
- [Get-EC2Snapshot \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## 共享 Amazon EBS 快照

### Abstract

与其他 AWS 用户共享您的快照。

您可以通过修改快照权限，与同事或 AWS 社区中的其他人共享未加密的快照。您授权的用户可以使用您的未加密共享快照为基础，快速创建其自己的 EBS 卷。如选择，您也可使您的未加密快照对所有 AWS 用户公开可用。

您可与特定 AWS 账户共享加密快照，但是您无法将其设为公开。要让其他账户使用快照，您还必须共享用于加密快照的自定义 CMK 密钥。跨账户权限可以在创建自定义密钥时应用于该密钥，也可以在创建之后应用于该密钥。获得访问权限的用户可以复制您的快照，并可基于您的快照创建自己的 EBS 卷，而您的原始快照不会受到影响。

与您共享 CMK 的用户如要访问您的加密快照，还必须获得 `DescribeKey` 和 `ReEncrypt` 权限。有关管理和共享 CMK 密钥的更多信息，请参阅[控制客户主密钥的访问权限](#)。



#### Important

AWS 会阻止您共享使用您的默认 CMK 加密的快照。您打算共享的快照必须使用自定义 CMK 加密。有关创建密钥的更多信息，请参阅[创建密钥](#)。

如果您拥有共享加密快照的访问权限，并且您希望从该快照还原卷，则必须自行创建该快照的一个副本，然后使用副本还原卷。



#### Note

我们建议您在复制过程中，使用您控制的其他密钥重新加密快照。这样，即使原始密钥遭到泄露或拥有者出于任何原因撤销了密钥，您也不会失去对卷的访问权限。

快照受限于在其中创建它们的区域。如果要与另一个区域共享快照，则需要将快照复制到该区域。有关复制快照的更多信息，请参阅[复制 Amazon EBS 快照 \(p. 679\)](#)。



#### Important

当您共享快照时（无论是将其与其他 AWS 账户共享，或使其公开可用），即表示您向他人授予了访问快照上所有数据的权限。仅与您要与其分享所有快照数据的人分享快照。

### 使用控制台修改快照权限

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 `Snapshots`。
3. 选择快照，然后从 Actions 列表中选择 `Modify Permissions`。
4. 选择是否公开快照或与特定 AWS 账户共享：
  - 要将快照设为公开，请选择 `Public`。



#### Note

加密快照或带有 AWS Marketplace 产品代码的快照不支持这一选项。

- 要仅向特定的 AWS 账户显示快照，请选择 `Private`，在 `AWS Account Number` 字段中输入 AWS 账户的 ID（无连字符），然后选择 `Add Permission`。重复以上操作，直至您添加完所有需要 AWS 账户。



#### Important

如果您的快照已加密，请确保满足以下条件：

- 快照使用自定义 CMK 加密，而不是默认 CMK。如果您尝试更改使用默认 CMK 进行加密的快照的权限，控制台将显示一条错误消息。
- 您与享有您的快照访问权限的账户共享了自定义 CMK。

5. 选择 Save。

#### 使用命令行查看和修改快照权限

要查看快照的 `createVolumePermission` 属性，您可以使用以下命令之一。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- [describe-snapshot-attribute \(AWS CLI\)](#)
- [Get-EC2SnapshotAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

要修改快照的 `createVolumePermission` 属性，您可以使用以下命令之一。

- [modify-snapshot-attribute \(AWS CLI\)](#)
- [Edit-EC2SnapshotAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## Amazon EBS 优化实例

### Abstract

通过使用 Amazon EBS 优化的实例为您的 Amazon EBS 卷提供最佳性能。

Amazon EBS 优化的实例使用优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过尽可能减少 Amazon EBS I/O 与来自实例的其他流量之间的争用提供最好的 EBS 卷性能。

EBS 优化实例为 Amazon EBS 提供了专用带宽，根据您使用的实例类型，此带宽可在 500 Mbps 到 4,000 Mbps 的范围中选择。当挂载到 EBS 优化实例时，通用型 SSD (`gp2`) 卷可在所指定一年 99% 的时间内提供其 10% 以内的基准性能和突增性能，而 provisioned IOPS (`iop1`) 卷可在所指定一年 99.9% 的时间内提供其 10% 以内的预置性能。吞吐优化 HDD (`st1`) 和 Cold HDD (`sc1`) 都可确保所指定一年 99% 的时间内 90% 的突增性能一致。不合规时间近似均匀分配，目标是达到 99% 的每小时预计总吞吐量。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。

当您对默认情况下不会进行 EBS 优化的实例启用 EBS 优化时，您需为专用容量支付一笔较小的按小时计算的额外费用。有关定价信息，请参阅 Amazon EC2 定价页中的 [EBS 优化实例](#)。

### 内容

- [支持 EBS 优化的实例类型 \(p. 683\)](#)
- [在启动时启用 EBS 优化 \(p. 685\)](#)
- [为正在运行的实例修改 EBS 优化 \(p. 685\)](#)

## 支持 EBS 优化的实例类型

下表显示了支持 EBS 优化实例类型、针对 Amazon EBS 的专用带宽、实例可以支持的最大 IOPS 量（如果您使用的是 16 KB I/O 大小）以及在具有流式处理读取工作负载和 128 KiB I/O 大小的连接上可实现的典型最大聚合吞吐量（以 MB/s 为单位）。请选择提供的专用 EBS 吞吐量大于应用程序所需的 EBS 优化实例；否则，Amazon EBS 与 Amazon EC2 的连接将成为性能障碍。

请注意，某些实例类型在默认情况下会进行 EBS 优化。对于默认情况下会进行 EBS 优化的实例，无需启用 EBS 优化，并且使用 CLI 或 API 禁用 EBS 优化也不会有影响。您可以在启动实例时对支持 EBS 优化的其他实例类型启用 EBS 优化，或在实例已在运行后启用 EBS 优化。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
EBS 优化

---

| 实例类型        | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS ( I/O 大小为 16KB ) ** |
|-------------|---------------|--------------|----------------|-----------------------------|
| c1.xlarge   |               | 1000         | 125            | 8000                        |
| c3.xlarge   |               | 500          | 62.5           | 4000                        |
| c3.2xlarge  |               | 1000         | 125            | 8000                        |
| c3.4xlarge  |               | 2000         | 250            | 16000                       |
| c4.large    | 是             | 500          | 62.5           | 4000                        |
| c4.xlarge   | 是             | 750          | 93.75          | 6000                        |
| c4.2xlarge  | 是             | 1000         | 125            | 8000                        |
| c4.4xlarge  | 是             | 2000         | 250            | 16000                       |
| c4.8xlarge  | 是             | 4000         | 500            | 32000                       |
| d2.xlarge   | 是             | 750          | 93.75          | 6000                        |
| d2.2xlarge  | 是             | 1000         | 125            | 8000                        |
| d2.4xlarge  | 是             | 2000         | 250            | 16000                       |
| d2.8xlarge  | 是             | 4000         | 500            | 32000                       |
| g2.2xlarge  |               | 1000         | 125            | 8000                        |
| i2.xlarge   |               | 500          | 62.5           | 4000                        |
| i2.2xlarge  |               | 1000         | 125            | 8000                        |
| i2.4xlarge  |               | 2000         | 250            | 16000                       |
| m1.large    |               | 500          | 62.5           | 4000                        |
| m1.xlarge   |               | 1000         | 125            | 8000                        |
| m2.2xlarge  |               | 500          | 62.5           | 4000                        |
| m2.4xlarge  |               | 1000         | 125            | 8000                        |
| m3.xlarge   |               | 500          | 62.5           | 4000                        |
| m3.2xlarge  |               | 1000         | 125            | 8000                        |
| m4.large    | 是             | 450          | 56.25          | 3600                        |
| m4.xlarge   | 是             | 750          | 93.75          | 6000                        |
| m4.2xlarge  | 是             | 1000         | 125            | 8000                        |
| m4.4xlarge  | 是             | 2000         | 250            | 16000                       |
| m4.10xlarge | 是             | 4000         | 500            | 32000                       |
| r3.xlarge   |               | 500          | 62.5           | 4000                        |
| r3.2xlarge  |               | 1000         | 125            | 8000                        |
| r3.4xlarge  |               | 2000         | 250            | 16000                       |

| 实例类型        | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS ( I/O 大小为 16KB ) ** |
|-------------|---------------|--------------|----------------|-----------------------------|
| x1.32xlarge | 是             | 10000        | 1250           | 65000                       |

\* 必须将这些实例类型作为 EBS 优化实例启动，才能始终实现此级别的性能。

\*\* 此值是基于 100% 只读工作负载的舍入近似值，作为基线配置帮助提供。EBS 优化连接是全双工连接，可以在同时使用两个通信通道的 50/50 读/写工作负载中驱动更多吞吐量和 IOPS。在某些情况下，网络、文件系统和 Amazon EBS 加密的开销可能会降低可用的最大吞吐量和 IOPS。

请注意，某些带 10 Gb 网络接口的实例（例如，i2.8xlarge 和 r3.8xlarge）不提供 EBS 优化，因此它们没有可用的专用 EBS 带宽且未在此处列出。在这些实例上，将在同一个 10 Gb 网络接口上共享网络流量和 Amazon EBS 流量。其他一些 10 Gb 网络实例（例如，c4.8xlarge 和 d2.8xlarge）提供专用 EBS 带宽以及专门用于网络流量的 10 Gb 接口。

## 在启动时启用 EBS 优化

您可以通过设置某个实例的 EBS 优化属性来对该实例启用 EBS 优化。

### 在启动实例时使用控制台启用 EBS 优化

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 单击 Launch Instance。在步骤 1：选择 Amazon 系统映像 (AMI) 中，选择 AMI。
3. 在 Step 2: Choose an Instance Type 中，选择作为支持性 EBS 优化列出的实例类型。
4. 在步骤 3：配置实例详细信息中，填写所需的字段并选择作为 EBS 优化实例启动。如果您在上一个步骤中选择的实例类型不支持 EBS 优化，此选项将不存在。如果您选择的实例类型在默认情况下会进行 EBS 优化，则会选择此选项，并且无法取消选择。
5. 按照说明来完成向导和启动实例。

### 在启动实例时使用命令行启用 EBS 优化

您可以将以下选项之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--ebs-optimized` 与 `run-instances` (AWS CLI)
- `-EbsOptimized` 与 `New-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

## 为正在运行的实例修改 EBS 优化

您可以修改正在运行的实例的 EBS 优化实例属性，以便为该实例启用或禁用 EBS 优化。

### 使用控制台为正在运行的实例启用 EBS 优化

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，单击 Instances，然后选择实例。
3. 单击 Actions (操作)，选择 Instance State (实例状态)，然后单击 Stop (停止)。



#### Warning

当您停止某个实例时，任何实例存储卷上的数据都将被擦除。因此，如果实例存储卷上有任何您要保留的数据，请确保将其备份到持久性存储。

4. 在确认对话框中，单击 Yes, Stop。停止实例可能需要几分钟时间。
5. 在实例仍处于选中状态的情况下，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为经过 EBS 优化的实例类型，则 EBS-optimized 已被选择，您无法取消选择。您可以单击 Cancel，因为该实例已启用 EBS 优化。
  - 如果您的实例的实例类型支持 EBS 优化，请选择 EBS-optimized，然后单击 Apply。
  - 如果您的实例的实例类型不支持 EBS 优化，则 EBS-optimized 已取消选择，您无法选择它。您可以从支持 EBS 优化的 Instance Type 中选择一个实例类型，选择 EBS-optimized，然后单击 Apply。
7. 单击 Actions (操作)，选择 Instance State (实例状态)，然后单击 Start (启动)。

#### 使用命令行为正在运行的实例启用 EBS 优化

您可以将以下选项之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--ebs-optimized` 与 [modify-instance-attribute \(AWS CLI\)](#)
- `-EbsOptimized` 与 [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

## Amazon EBS Encryption

### Abstract

Amazon EBS 加密提供了用于 EBS 卷的简单加密解决方案，您无需构建、维护和保护自己的密钥管理基础设施。

Amazon EBS 加密提供了用于 EBS 卷的简单加密解决方案，您无需构建、维护和保护自己的密钥管理基础设施。在创建加密的 EBS 卷并将其连接到支持的实例类型后，将对以下类型的数据进行加密：

- 卷中的静态数据
- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照

加密在托管 EC2 实例的服务器上进行，对从 EC2 实例传输到 EBS 存储的数据进行加密。

Amazon EBS 加密 在创建加密卷及其快照时，使用 AWS Key Management Service (AWS KMS) 客户主密钥(CMK)。首次在某个区域中创建加密卷时，将自动为您创建一个默认 CMK。除非您选择了使用 AWS KMS 单独创建的 CMK，否则此密钥将用于 Amazon EBS 加密。创建您自己的 CMK 可以实现更高的灵活性，让您可以创建、轮换、禁用密钥以定义访问控制，并审核用于保护数据的加密密钥。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。

所有 EBS 卷类型（通用型 SSD [gp2]、provisioned IOPS [io1]、吞吐优化 HDD [st1]、Cold HDD [sc1] 和磁介质 [standard]）都支持此功能，加密卷对延迟的影响极小，其 IOPS 性能与未加密卷一样。您可以通过与访问未加密卷相同的方式来访问加密卷；加密和解密以透明方式处理，您、您的 EC2 实例或您的应用程序都无需执行其他任何操作。

从加密卷拍摄的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷的快照无法公开，但是如果执行以下步骤，您可以与特定账户共享加密快照：

1. 使用自定义 CMK 而非默认 CMK 对您的卷进行加密。
2. 允许特定账户访问自定义 CMK。
3. 创建快照。

4. 允许特定账户访问该快照。

有关更多信息，请参阅[共享 Amazon EBS 快照](#)。

Amazon EBS 加密仅对特定实例类型可用。加密卷和未加密卷都可以连接到支持的实例类型。有关更多信息，请参阅[支持的实例类型 \(p. 687\)](#)。

内容

- [加密密钥管理 \(p. 687\)](#)
- [支持的实例类型 \(p. 687\)](#)
- [更改数据的加密状态 \(p. 688\)](#)

## 加密密钥管理

Amazon EBS 加密 为您处理密钥管理。每个新创建的卷都使用一个唯一的 256 位密钥加密；此卷的所有快照以及从这些快照创建的后续卷也共享该密钥。这些密钥受我们自己的密钥管理基础设施的保护，这将实施强逻辑和物理安全控制以防止未经授权的访问。您的数据和关联的密钥使用行业标准的 AES-256 算法进行加密。

您无法更改与现有快照或加密卷关联的 CMK。然而，您可在快照复制操作（包括加密未加密快照的副本）期间关联另一个 CMK，而生成的已复制快照将使用新的 CMK。

Amazon 的整体密钥管理基础设施使用联邦信息处理标准 (FIPS) 140-2 批准的加密算法，符合美国国家标准与技术研究院 (NIST) 800-57 建议。

每个 AWS 账户都具有一个唯一的主密钥，该密钥与数据完全分开，存储在一个受严格的物理和逻辑安全控制保护的系统上。每个加密卷（及其后续的快照）使用唯一卷加密密钥来加密，然后使用特定于区域的安全主密钥加密。卷加密密钥在托管您的 EC2 实例的服务器的内存中使用，永远不会以纯文本格式存储在磁盘上。

## 支持的实例类型

Amazon EBS 加密 适用于下表中所列的实例类型。这些实例类型利用 Intel AES 新指令 (AES-NI) 指令集提供更快且更简单的数据保护。您可以同时将加密卷和未加密卷连接到这些实例类型。

| 实例系列   | 支持 Amazon EBS 加密 的实例类型                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 通用型    | m3.medium m3.large m3.xlarge m3.2xlarge m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge t2.nano t2.micro t2.small t2.medium t2.large |
| 计算优化   | c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge                                   |
| 内存优化   | cr1.8xlarge r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge x1.32xlarge                                                               |
| 存储优化   | d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge                                                     |
| GPU 实例 | g2.2xlarge g2.8xlarge                                                                                                                     |

有关这些实例类型的更多信息，请参阅[实例类型详细信息](#)。

## 更改数据的加密状态

不能直接对现有的未加密卷加密或对加密卷删除加密。但是，您可以在加密卷与未加密卷之间迁移数据。您也可以在复制快照时应用新的加密状态：

- 在复制未加密卷的未加密快照时，您可以将副本加密。从该加密副本还原的卷也将被加密。
- 在复制加密卷的加密快照时，您可以使用不同的 CMK 将副本重新加密。从该加密副本还原的卷只能使用新应用的 CMK 进行访问。

### 在加密卷与未加密卷之间迁移数据

当您对加密卷和未加密卷都可以访问时，就可以在它们之间自由传输数据了。EC2 透明地执行加密和解密操作。

#### 在加密卷与未加密卷之间迁移数据

1. 按照 [创建 Amazon EBS 卷 \(p. 652\)](#) 中的程序创建您的目标卷（是否加密取决于您的需求）。
2. 将目标卷挂载到托管待迁移数据的实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。
3. 按照 [使 Amazon EBS 卷可用 \(p. 658\)](#) 中的过程使目标卷可用。对于 Linux 实例，您可以在 /mnt/destination 创建安装点，然后在此处安装目标卷。
4. 将数据从您的源目录复制到目标卷。使用批量复制实用工具执行此任务可能最为方便。

#### Linux

按如下所示使用 rsync 命令将数据从源复制到目标卷。在此示例中，源数据位于 /mnt/source 中，目标卷安装在 /mnt/destination。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

#### Windows

在命令提示符处，使用 robocopy 命令将数据从源复制到目标卷。在此示例中，源数据位于 D:\ 中，目标卷安装在 E:\。

```
PS C:\Users\Administrator> robocopy D:\ E:\ /e /copyall /eta
```

### 在复制快照时应用加密

因为可以在复制快照时对快照应用加密，所以复制数据的另一种途径步骤如下。

#### 通过快照复制对卷数据加密

1. 创建未加密 EBS 卷的快照。此快照也未加密。
2. 复制快照的同时应用加密参数。生成的目标快照是加密的。
3. 将加密快照还原到新卷，也还是加密的。

有关更多信息，请参阅 [复制 Amazon EBS 快照](#)。

## 使用新的 CMK 重新加密快照

由于能够在复制过程中加密快照，您可以重新加密您拥有的已加密过的快照。进行这一操作时，系统会使用您提供的新 CMK 对快照的纯文本进行加密。从生成的副本还原的卷只能使用新的 CMK 进行访问。

在相关的场景中，您可以选择对与您共享的快照进行重新加密。从共享的加密快照还原某个卷之前，您必须创建属于您自己的共享加密快照副本。默认情况下，系统会使用快照所有者共享的密钥对该副本进行加密。不过，我们建议您在复制过程中，使用您控制的其他密钥重新加密快照。这样，即使原始密钥遭到泄露或拥有者出于任何原因撤销了密钥，您也不会失去对卷的访问权限。

以下程序演示了如何重新加密您的快照。

### 使用控制台重新加密快照

1. 创建自定义 CMK。有关更多信息，请参阅 [AWS Key Management Service Developer Guide](#)。
2. 创建用您的默认 CMK（仅针对本示例）加密的 EBS 卷。
3. 创建加密 EBS 卷的快照。此快照也使用您的默认 CMK 进行加密。
4. 在 Snapshots 页面，选择 Actions，然后选择 Copy。
5. 在 Copy Snapshot 窗口中，在 Master Key 字段中输入您自定义的 CMK 的完整 ARN（以 arn:aws:kms:<i>us-east-1</i>：  
<i>012345678910</i>  
:key/  
<i>abcd1234-a123-456a-a12b-a123b4cd56ef</i>  
的形式），或从菜单中选择该 ARN。单击“Copy”。

生成的快照副本以及从其还原的所有卷都将使用您自定义的 CMK 进行加密。

以下程序演示了如何在复制过程中重新加密共享的加密快照。要进行这一操作，您需要拥有共享加密快照及用于对其进行加密的 CMK 的访问权限。

### 使用控制台复制并重新加密共享快照

1. 在 Snapshots 页面选择共享的加密快照，选择 Actions，然后选择 Copy。
2. 在 Copy Snapshot 窗口中，在 Master Key 字段中输入您拥有的 CMK 的完整 ARN（以 arn:aws:kms:<i>us-east-1</i>：  
<i>012345678910</i>  
:key/  
<i>abcd1234-a123-456a-a12b-a123b4cd56ef</i>  
的形式），或从菜单中选择该 ARN。单击“Copy”。

生成的快照副本以及从其还原的所有卷都将使用您提供的 CMK 进行加密。原始共享快照、其加密状态或共享 CMK 的更改不会对您的副本产生影响。

有关更多信息，请参阅 [复制 Amazon EBS 快照](#)。

## Amazon EBS 卷性能（Windows 实例上）

### Abstract

列出优化 Amazon EBS 卷性能的最佳实践。

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。

有关更多信息，请参阅 *Amazon EC2 用户指南（适用于 Microsoft Windows 实例）* 中的 [Windows 实例上的 Amazon EBS 卷性能](#)。

#### 内容

- [Amazon EBS 性能提示 \(p. 690\)](#)
- [Amazon EC2 实例配置 \(p. 691\)](#)
- [I/O 特性 \(p. 694\)](#)
- [初始化 Amazon EBS 卷 \(p. 695\)](#)
- [Windows 上的 RAID 配置 \(p. 697\)](#)

## Amazon EBS 性能提示

这些提示代表了在各种用户场景下能够获得最佳 EBS 卷性能的最佳实践。

### 使用 EBS 优化的实例

对于不支持 EBS 优化吞吐量的实例，网络流量可能会与实例和 EBS 卷之间的流量产生冲突；而在 EBS 优化实例中，这两种流量相互独立。部分 EBS 优化实例配置（如 C3、R3 和 M3）会产生额外成本，另一些实例（如 M4、C4 和 D2）始终可进行 EBS 优化而不会产生额外成本。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 691\)](#)。

### 了解如何计算性能

度量 EBS 卷的性能时，应了解所需采用的度量单位以及如何计算性能，这十分重要。有关更多信息，请参阅 [I/O 特性 \(p. 694\)](#)。

### 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。

### 请注意，在从快照初始化卷时，可能会有性能损失

当您首次访问从快照还原的新 EBS 卷上的每个数据块时，延迟会大大增加。您可以在将卷用于生产之前访问每个数据块，以避免这种性能影响。此过程称为 初始化（以前称为预热）。有关更多信息，请参阅 [初始化 Amazon EBS 卷 \(p. 695\)](#)。

### 可能降低 HDD 性能的因素

如果创建吞吐优化 HDD (st1) 或 Cold HDD (sc1) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。这种情况是这些卷类型特有的。其他可能会限制性能的因素包括迫使吞吐量超过实例的支持能力，在初始化从快照还原的卷时损失性能，以及卷上的小型随机 I/O 过多。有关计算 HDD 卷的吞吐量的更多信息，请参阅 [Amazon EBS 卷类型](#)。

如果您的应用程序没有发送足够的 I/O 请求，性能可能也会受影响。这可通过查看卷的队列长度和 I/O 大小来监控。队列长度是您的应用程序向卷发起的待处理 I/O 请求的数量。为实现最大程度的一致性，在执行 1 MiB 的顺序 I/O 时，HDD 卷必须保持 4 或更大的队列长度（四舍五入为最近的整数）。有关确保卷的性能一致的更多信息，请参阅 [I/O 特性 \(p. 694\)](#)

## 为 `st1` 和 `sc1` 上高吞吐量、读取操作量大的工作负载增大预读取值

一些工作负载读取操作量大，并会访问操作系统页缓存中的块储存设备（例如，从文件系统访问）。在这种情况下，为了实现最大的吞吐量，我们建议您将预读取设置配置为 1 MiB。每个块储存设备的设置不同，应该只应用于您的 HDD 卷。以下示例假设您在使用 Amazon Linux 实例。

要检查您的块储存设备的当前预读数值，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

块储存设备信息采用以下格式返回：

| RO | RA  | SSZ | BSZ  | StartSec | Size       | Device        |
|----|-----|-----|------|----------|------------|---------------|
| rw | 256 | 512 | 4096 | 4096     | 8587820544 | /dev/<device> |

以上显示的设备报告预读取值为 256 字节（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 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 [Windows 上的 RAID 配置 \(p. 697\)](#)。

## 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 \(p. 660\)](#)。

## Amazon EC2 实例配置

### Abstract

计划和配置 Amazon EBS 卷时对您的 EC2 实例进行配置。

为应用程序规划和配置 EBS 卷时，需考虑将卷连接到的实例的配置，这十分重要。为了获得最高的 EBS 卷性能，您应该将这些卷连接到具有足够带宽以支持您的卷的实例，如 EBS 优化实例或具有 10 Gb 网络连接的实例。在 RAID 配置中将多个卷条带化时，这尤其重要。

### 使用 EBS 优化的实例或 10 Gb 网络实例

对于需要最少变化以及专用 Amazon EC2 到 Amazon EBS 流量的任何性能敏感型工作负载（如生产数据库或业务应用程序），均应使用连接到 EBS 优化实例或具有 10 Gb 网络连接的实例的卷。不符合此条件的 EC2 实例不提供网络资源保证。确保 EC2 实例与 EBS 卷之间的持续可靠网络带宽的唯一方法是将 EC2 实例作为 EBS 优化实例启动，或选择具有 10 Gb 网络连接的实例类型。要了解哪些实例类型包括 10 Gb 网络连接，请参阅 [实例类型详细信息](#)。有关配置 EBS 优化实例的信息，请参阅 [Amazon EBS 优化的实例](#)。

### 选择具有足够带宽的 EC2 实例

启动进行了 EBS 优化的实例可为您提供 EC2 实例与 EBS 卷之间的专用连接。然而，仍可以为特定实例类型配置超过可用带宽的 EBS 卷，尤其是在 RAID 配置中将多个卷条带化时。下表显示了可以采用 EBS 优化形式启动的实例类型及其专用吞吐量、Amazon EBS 的专用带宽、实例可以支持的最大 IOPS 量（如果您使用的 I/O 大小为 16KB）以及该连接上可用的 I/O 带宽近似值（以 MB/s 为单位）。请务必选择提供的专用 EBS 吞吐量大于应用程序所需的 EBS 优化实例；否则，Amazon EBS 到 Amazon EC2 的连接将成为性能瓶颈。



#### Note

下表和以下示例仅出于说明目的使用 16 KB 作为 I/O 大小；您的应用程序 I/O 大小可能会有所不同（Amazon EBS 将每秒的每个 I/O 操作（即 256 KiB 或更小）作为一个 IOPS 进行度量）。有关 IOPS 以及 I/O 大小和卷吞吐量限制之间的关系的更多信息，请参阅 [I/O 特性 \(p. 694\)](#)。

| 实例类型       | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS (I/O 大小为 16KB) ** |
|------------|---------------|--------------|----------------|---------------------------|
| c1.xlarge  |               | 1000         | 125            | 8000                      |
| c3.xlarge  |               | 500          | 62.5           | 4000                      |
| c3.2xlarge |               | 1000         | 125            | 8000                      |
| c3.4xlarge |               | 2000         | 250            | 16000                     |
| c4.large   | 是             | 500          | 62.5           | 4000                      |
| c4.xlarge  | 是             | 750          | 93.75          | 6000                      |
| c4.2xlarge | 是             | 1000         | 125            | 8000                      |
| c4.4xlarge | 是             | 2000         | 250            | 16000                     |
| c4.8xlarge | 是             | 4000         | 500            | 32000                     |
| d2.xlarge  | 是             | 750          | 93.75          | 6000                      |
| d2.2xlarge | 是             | 1000         | 125            | 8000                      |
| d2.4xlarge | 是             | 2000         | 250            | 16000                     |
| d2.8xlarge | 是             | 4000         | 500            | 32000                     |
| g2.2xlarge |               | 1000         | 125            | 8000                      |
| i2.xlarge  |               | 500          | 62.5           | 4000                      |
| i2.2xlarge |               | 1000         | 125            | 8000                      |
| i2.4xlarge |               | 2000         | 250            | 16000                     |
| 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                      |

| 实例类型        | 默认情况下为 EBS 优化 | 最大带宽 (Mbps)* | 预期吞吐量 (MB/s)** | 最大 IOPS ( I/O 大小为 16KB ) ** |
|-------------|---------------|--------------|----------------|-----------------------------|
| m3.2xlarge  |               | 1000         | 125            | 8000                        |
| m4.large    | 是             | 450          | 56.25          | 3600                        |
| m4.xlarge   | 是             | 750          | 93.75          | 6000                        |
| m4.2xlarge  | 是             | 1000         | 125            | 8000                        |
| m4.4xlarge  | 是             | 2000         | 250            | 16000                       |
| m4.10xlarge | 是             | 4000         | 500            | 32000                       |
| r3.xlarge   |               | 500          | 62.5           | 4000                        |
| r3.2xlarge  |               | 1000         | 125            | 8000                        |
| r3.4xlarge  |               | 2000         | 250            | 16000                       |
| x1.32xlarge | 是             | 10000        | 1250           | 65000                       |

\* 必须将这些实例类型作为 EBS 优化实例启动，才能始终实现此级别的性能。

\*\* 此值是基于 100% 只读工作负载的舍入近似值，作为基线配置帮助提供。EBS 优化连接是全双工连接，可以在同时使用两个通信通道的 50/50 读/写工作负载中驱动更多吞吐量和 IOPS。在某些情况下，网络、文件系统和 Amazon EBS 加密的开销可能会降低可用的最大吞吐量和 IOPS。

请注意，某些带 10 Gb 网络接口的实例（如 i2.8xlarge、c3.8xlarge 和 r3.8xlarge）不提供 EBS 优化，因此它们没有可用的专用 EBS 带宽且未在此处列出。不过，如果您的应用程序不推送与 Amazon EBS 竞争的其他网络流量，则可以使用 Amazon EBS 流量的所有带宽。其他一些 10 GB 网络实例（例如，c4.8xlarge 和 d2.8xlarge）提供专用 Amazon EBS 带宽以及专门用于网络流量的 10 GB 接口。

m1.large 实例最大的 16 KB IOPS 值为 4 000，但是，除非此实例类型作为 EBS 优化实例启动，否则该值只是理想情况下的值，且无法得到保证；要切实确保 16 KB IOPS 的值为 4 000，您必须将此实例作为 EBS 优化实例启动。但是，如果 IOPS 为 4000 的 io1 卷挂载到 EBS 优化的 m1.large 实例，Amazon EC2 与 Amazon EBS 之间的连接带宽限制将使此卷无法提供它本可以实现的 320 MB/s 最大聚合吞吐量。在这种情况下，我们必须使用支持至少 320 MB/s 吞吐量的 EBS 优化 EC2 实例，如 c4.8xlarge 实例类型。

通用型 SSD (gp2) 类型的卷的吞吐量限制为 128 MB/s 到 160 MB/s 之间（具体取决于卷大小），这与 1000 Mbps 的 EBS 优化连接很相称。向 Amazon EBS 提供的吞吐量大于 1000 Mbps 的实例类型可以使用多个 gp2 卷来利用可用吞吐量。对于预配置的每个 IOPS，provisioned IOPS (io1) 类型的卷的吞吐量限制为 256 KiB，最高可达 320 MiB/s（1280 IOPS 情况下）。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。

具有 10 Gb 网络连接性的实例类型对于未加密的 Amazon EBS 卷支持最多 800 MB/s 吞吐量和 48 000 16K IOPS，对于已加密的 Amazon EBS 卷，最多支持 25 000 16K IOPS。由于 EBS 卷的最大 io1 值为 20,000（对于 io1 卷）和 10,000（对于 gp2 卷），您可以同时使用多个 EBS 卷来达到这些实例类型可实现的 I/O 性能水平。有关哪些实例类型具有 10 Gb 网络连接能力的更多信息，请参阅 [实例类型详细信息](#)。

您应该使用 EBS 优化实例（如可用）以发挥 Amazon EBS gp2 和 io1 卷的全部性能优势。有关更多信息，请参阅 [Amazon EBS 优化实例 \(p. 683\)](#)。

## I/O 特性

### Abstract

在卷配置中设置 I/O 特性以提高后端的性能。

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 provisioned IOPS (`io1`)）能够提供一致的性能，无论 I/O 操作是随机的还是顺序的。HDD 卷（即吞吐优化 HDD (`st1`) 和 Cold HDD (`sc1`)）仅当 I/O 操作是大型顺序操作时才能提供最佳性能。要了解 SSD 和 HDD 卷在您的应用程序中性能如何，务必要知道卷上的需求之间的联系、卷能支持的 IOPS 数量、完成 I/O 操作所需的时间，以及卷的吞吐量限制。

### IOPS

IOPS 是表示每秒输入/输出操作数的度量单位。操作数以 KiB 来度量，底层驱动技术确定卷类型计算为单次 I/O 的最大数据量。SSD 卷的最大 I/O 大小为 256 KiB，HDD 卷的最大 I/O 大小为 1024 KiB，因为 SSD 卷比 HDD 卷处理小型或随机 I/O 的效率高很多。

当小型 I/O 操作在物理上连续进行时，Amazon EBS 会尝试将这些操作合并为单个 I/O，直至最大大小。例如，对于 SSD 卷，一个 1024 KiB 的 I/O 操作会计为 4 个操作，而 64 个 4 KiB 的 I/O 操作会计为 256 个操作。但是，256 个随机 4 KiB I/O 操作将被计为 256 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 操作会计为 8 个操作。

这样，当您创建支持 3000 IOPS（通过将 `io1` 配置为 3000 IOPS 或将 `gp2` 卷大小确定为 1000 GiB）的 SSD 卷时，您就可以将它连接到一个 EBS 优化实例，该实例可以提供足够的带宽，您可以每秒传输最高 3000 次数据 I/O，其吞吐量由 I/O 大小决定。

### 卷队列长度和延迟

卷队列长度是指等待设备处理的 I/O 请求的数量。延迟为 I/O 操作的实际端到端客户端时间，也就是说，从将 I/O 发送到 EBS 到接收来自 EBS 的确认以表示 I/O 读取或写入完成所经过的时间。队列长度必须进行适当调整，以便与 I/O 大小和延迟匹配，避免在来宾操作系统上或在到 EBS 的网络链路上产生瓶颈。

每个工作负载的最佳队列长度不同，具体取决于您的特定应用程序对于 IOPS 和延迟的敏感程度。如果您的工作负载未提供足够的 I/O 请求来充分利用 EBS 卷的可用性能，则卷可能无法提供您预置的 IOPS 或吞吐量。

事务密集型应用程序对 I/O 延迟增加很敏感，很适合使用 SSD 支持的 `io1` 和 `gp2` 卷。您可以通过使卷保持较小的队列长度和较高的 IOPS 数量，来维持高 IOPS 和低延迟。持续迫使一个卷的 IOPS 高于它能够支持的 IOPS 可能增加 I/O 延迟。

吞吐量密集型应用程序对 I/O 延迟增加较不敏感，很适合使用 HDD 支持的 `st1` 和 `sc1` 卷。您可以在执行大型顺序 I/O 时维持大队列长度，从而对 HDD 卷保持高吞吐量。

### I/O 大小和卷吞吐量限制

对于 SSD 卷，如果 I/O 大小非常大，由于达到卷的吞吐量限制，您的 IOPS 数可能会少于预配置数量。例如，对于具有可用突增额度的 1000 GiB 以下的 `gp2` 卷，IOPS 限制为 3000，卷吞吐量限制为 160 MiB/s。如果您正在使用 256 KiB 的 I/O 大小，则您的卷在 IOPS 为 640 时将达到其吞吐量限制 ( $640 \times 256 \text{ KiB} = 160 \text{ MiB}$ )。当 I/O 大小较小（如 16 KiB）时，这个卷可以支持 3000 IOPS，这是因为吞吐量远低于 160 MiB/s（这些例子都假设卷的 I/O 不会达到实例的吞吐量限制。）有关每种 EBS 卷类型吞吐量限制的更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。

对于较小的 I/O 操作，从实例内部进行度量时，您可能会看到 IOPS 值高于预配置值。当实例操作系统在将小型 I/O 操作传递到 Amazon EBS 之前将其合并为一个较大的操作时，会发生这种情况。

对于 HDD 支持的 `st1` 和 `sc1` 卷，如果您的工作负载使用顺序 I/O，则从实例内部进行度量时，您的 IOPS 值可能会高于预期数量。当实例操作系统将顺序 I/O 进行合并，并以 1024 KiB 大小为单位来对其进行计

数时，会发生这种情况。如果您的工作负载使用小型随机 I/O，则吞吐量可能会低于您的预期。这是因为我们会将每个随机的非顺序 I/O 计入总的 IOPS 计数，这可能导致您比预期更快达到卷的 IOPS 限制。

无论您采用何种 EBS 卷类型，如果您的 IOPS 或吞吐量与您在配置中的预期不同，请确保 EC2 实例带宽并不是导致这种结果的限制因素。您应始终使用最新一代的 EBS 优化实例（或包含 10 Gb/s 网络连接的实例）以实现最佳性能。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 691\)](#)。未达到预期 IOPS 的另一个可能原因是未对 EBS 卷执行足够多的 I/O 操作。

#### 使用 CloudWatch 监控 I/O 特性

您可以通过每个卷的 [CloudWatch 指标](#) 监控这些 I/O 特性。要考虑的重要指标包括：

- `BurstBalance`
- `VolumeReadBytes`
- `VolumeWriteBytes`
- `VolumeReadOps`
- `VolumeWriteOps`
- `VolumeQueueLength`

`BurstBalance` 以百分比形式显示 HDD 卷的突增存储桶平衡值。当您的突增存储桶耗尽时，卷吞吐量会限制为基准值。检查 `BurstBalance` 值以确定卷是否因为此原因而受限制。

HDD 支持的 `st1` 和 `sc1` 卷最适用于最大 I/O 为 1024KiB 的工作负载。要确定卷的平均 I/O 大小，请将 `VolumeWriteBytes` 除以 `VolumeWriteOps`。同样的计算也适用于读取操作。如果平均 I/O 大小低于 64 KiB，则提高发送到 `st1` 或 `sc1` 卷的 I/O 操作的大小应该能够提高性能。



#### Note

如果平均 I/O 大小达到或接近 44 KiB，说明您可能是在不支持间接描述符的情况下使用实例或内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，任何当代实例也具有此支持。

如果您的 I/O 延迟高于您的所需，请检查 `VolumeQueueLength`，以确保应用程序尝试驱动的 IOPS 不会超过您的配置。如果您的应用程序需要的 IOPS 数量超出您的卷所能提供的数量，则应考虑使用基本性能水平较高的较大 `gp2` 卷，或使用预配置 IOPS 更高的 `io1` 卷，以实现更短的延迟。

有关 Amazon EBS I/O 特征的更多信息，请参阅本主题上的 [Amazon EBS：为性能而设计](#) re:Invent 演示文稿。

## 初始化 Amazon EBS 卷

### Abstract

借助称为初始化的过程，可避免提高从快照还原的 EBS 卷上的首次接触延迟。

新 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照还原的卷上的存储数据块必须先进行初始化（从 Amazon S3 取下并写入到卷），然后您才能访问该数据块。此预备操作需要花费时间，并可能会造成首次访问每个数据块时的 I/O 操作的延迟大大提高。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。访问数据完毕后，性能随之恢复。

您可以通过在使用之前对卷上的所有数据块进行读取，在生产环境中避免这种性能冲击；此过程称为初始化。对于从快照创建的新卷，您应该在使用该卷前读取所有包含数据的块。



### Important

在初始化已从快照还原的 io1 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O Performance 状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 io1 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅 [使用状态检查来监控卷 \(p. 663\)](#)。

## 在 Windows 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，请使用适用于 Windows 的 dd 命令来对卷上的所有数据块进行读取。卷上的所有现有数据都会保留。

### 安装适用于 Windows 的 dd

适用于 Windows 的 dd 程序的使用类似于 Linux 和 Unix 系统中常用的 dd 程序，允许您初始化已从快照还原的 Amazon EBS 卷。撰写本文时，最新 Beta 版本包含初始化从快照还原的卷所需的 /dev/null 虚拟设备。程序的完整文档可在 <http://www.chrysocome.net/dd> 上获得。

1. 可从 <http://www.chrysocome.net/dd> 下载适用于 Windows 的最新二进制版本的 dd。必须使用版本 0.6 Beta 3 或更新版本初始化还原的卷。
- 2.（可选）为命令行实用工具创建易于查找和记住的文件夹，如 C:\bin。如果您已拥有用于命令行实用工具的指定文件夹，则可以在以下步骤中改用该文件夹。
3. 解压缩二进制程序包并将 dd.exe 文件复制到命令行实用工具文件夹（如 C:\bin）。
4. 将命令行实用工具文件夹添加到 Path 环境变量，以便您可以从任何位置执行该文件夹中的程序。



### Important

以下步骤不会在您当前的“命令提示符”窗口中更新环境变量。您在完成这些步骤后打开的“命令提示符”窗口将包含更新。这就是为什么需要打开一个新“命令提示符”窗口来确认环境已正确设置。

- a. 选择开始，打开计算机的上下文（右键单击）菜单，然后选择属性。
- b. 依次选择高级系统设置和环境变量。
- c. 对于系统变量，选择变量 Path，然后选择编辑。
- d. 在变量值中，将一个分号和命令行实用工具文件夹的位置（;C:\bin\）附加到现有值末尾。
- e. 选择确定关闭编辑系统变量窗口。

## 使用适用于 Windows 的 dd 来初始化卷

1. 使用 wmic 命令列出系统上的可用磁盘。

```
C:\>wmic diskdrive get size,deviceid
DeviceID Size
\\.\PHYSICALDRIVE2 80517265920
\\.\PHYSICALDRIVE1 80517265920
\\.\PHYSICALDRIVE0 128849011200
\\.\PHYSICALDRIVE3 107372805120
```

标识要在后面的步骤中初始化的磁盘。C：驱动器位于 \\.\PHYSICALDRIVE0。如果您不确定要使用的驱动器号，则可以使用 diskmgmt.msc 实用工具将驱动器盘符与磁盘驱动器号进行比较。

2. 执行以下命令可读取指定设备上的所有数据块（并将输出发送到 /dev/null 虚拟设备）。此命令可安全初始化现有数据。

```
C:\>dd if=\\.\\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```



#### Note

如果 dd 尝试读取卷末尾以外的空间，您可能会看到一个错误，但可以安全地忽略此错误。

- 操作完成时，您即准备就绪，可使用新卷。有关更多信息，请参阅 [使 Amazon EBS 卷可用 \(p. 658\)](#)。

## Windows 上的 RAID 配置

### Abstract

使用可与具有 Amazon EBS 卷的传统裸机服务器结合使用的任何标准 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](#)。

如果您需要在 Linux 实例上创建一个 RAID 阵列，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Linux 上的 RAID 配置](#)。

### 内容

- [RAID 配置选项 \(p. 697\)](#)
- [在 Windows 上创建 RAID 阵列 \(p. 698\)](#)

## RAID 配置选项

下表比较常见的 RAID 0 和 RAID 1 选项。

| 配置     | 使用                                            | 优点                              | 缺点                                                                 |
|--------|-----------------------------------------------|---------------------------------|--------------------------------------------------------------------|
| RAID 0 | 当 I/O 性能比容错能力更重要时；例如在频繁使用的数据库中（其中，已单独设置数据复制）。 | I/O 在卷内以条带状分布。如果您添加卷，则会直接增加吞吐量。 | 条带的性能受限于该集合中的最差的执行卷。丢失单个卷会导致完全丢失阵列的数据。                             |
| RAID 1 | 当容错能力比 I/O 性能更重要时；例如在关键应用程序中。                 | 在数据持久性方面更具安全性。                  | 不提供写入性能改进；需要比非 RAID 配置更大的 Amazon EC2 到 Amazon EBS 带宽，因为数据将同时写入多个卷。 |



### Important

不建议对 Amazon EBS 使用 RAID 5 和 RAID 6，因为这些 RAID 模式的奇偶校验写入操作会使用您的卷的一些可用 IOPS。根据您的 RAID 阵列配置，这些 RAID 模式提供的可用 IOPS 比 RAID 0 配置少 20-30%。成本增加也是与这些 RAID 模式有关的一个因素；在使用相同的卷大小和速度时，一个 2 卷 RAID 0 阵列明显胜过两倍成本的 4 卷 RAID 6 阵列。

相比在单个 Amazon EBS 卷上配置，通过创建 RAID 0 阵列，文件系统可以获得更高性能。为获得额外冗余性，RAID 1 阵列提供了数据的一个“镜像”。在执行此步骤之前，您需要确定 RAID 阵列的大小以及需要配置多少 IOPS。

RAID 0 阵列的最终大小是阵列中各个卷的大小之和，带宽是阵列中各个卷的可用带宽之和。RAID 1 阵列的最终大小和带宽等于阵列中各个卷的大小和带宽。例如，预配置 IOPS 为 4000 的两个 500 GiB Amazon EBS 卷将创建可用带宽为 8000 IOPS、吞吐量为 640 MB/s 的 1000 GiB RAID 0 阵列，或创建可用带宽为 4000 IOPS、吞吐量为 320 MB/s 的 500 GiB RAID 1 阵列。

本文档提供基本的 RAID 设置示例。有关 RAID 配置、性能和恢复的更多信息，请参阅 Linux RAID Wiki，网址为 [https://raid.wiki.kernel.org/index.php/Linux\\_Raid](https://raid.wiki.kernel.org/index.php/Linux_Raid)。

## 在 Windows 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 Linux 实例）* 中的 [在 Linux 上创建 RAID 阵列](#) 获得有关 Linux 实例的说明。

### 在 Windows 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 \(p. 652\)](#)。



#### Important

为阵列创建具有相等大小和 IOPS 性能值的卷。确保不创建超过 EC2 实例的可用带宽的阵列。有关更多信息，请参阅 [Amazon EC2 实例配置 \(p. 691\)](#)。

2. 将 Amazon EBS 卷连接到要承载该阵列的实例。有关更多信息，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。
3. 连接到您的 Windows 实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
4. 打开命令提示符并键入 diskpart 命令。

```
PS C:\Users\Administrator> diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. 在 DISKPART 提示符处，使用以下命令列出可用磁盘。

```
DISKPART> list disk

Disk ### Status Size Free Dyn Gpt
----- -----
Disk 0 Online 30 GB 0 B
Disk 1 Online 8 GB 0 B
Disk 2 Online 8 GB 0 B
Disk 3 Online 8 GB 0 B
Disk 4 Online 8 GB 0 B
Disk 5 Online 419 GB 0 B
Disk 6 Online 419 GB 0 B
```

标识您要在阵列中使用的磁盘并记下其磁盘编号。

6. 您要在阵列中使用的每个磁盘都必须是不包含任何现有卷的联机动态磁盘。使用以下步骤可将基本磁盘转换为动态磁盘并删除任何现有卷。

- a. 使用以下命令选择您要在阵列中使用的磁盘（将 *n* 替换为磁盘编号）。

```
DISKPART> select disk n
Disk n is now the selected disk.
```

- b. 如果所选磁盘列为 offline 状态，则通过运行 online disk 使它联机。  
c. 如果所选磁盘在前面的 Dynlist disk 命令输出的 列中没有星号，则需要将它转换为动态磁盘。

```
DISKPART> convert dynamic
```



Note

如果显示磁盘写保护错误，可以使用 ATTRIBUTE DISK CLEAR READONLY 命令清除只读标记，然后重试动态磁盘转换。

- d. 使用 detail disk 命令检查所选磁盘是否存在现有卷。

```
DISKPART> detail disk

XENSRV PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type : SCSI
Status : Online
Path : 0
Target : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only : No
Boot Disk : No
Pagefile Disk : No
Hibernation File Disk : No
Crashdump Disk : No
Clustered Disk : No

Volume ### Ltr Label Fs Type Size Status
Info
----- --- -----
Volume 2 D NEW VOLUME FAT32 Simple 8189 MB Healthy
```

记下磁盘上的任何卷编号。在此示例中，卷编号是 2。如果没有卷，则您可以跳过下一步。

- e. (仅当上一步中标识了卷时才需要) 选择并删除磁盘上在上一步中标识的所有现有卷。



Warning

这会销毁卷上的所有现有数据。

- i. 选择卷（将 *n* 替换为卷编号）。

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. 删除卷。

```
DISKPART> delete volume
DiskPart successfully deleted the volume.
```

iii. 对所选磁盘上需要删除的每个卷重复这些子步骤。

f. 对您要在阵列中使用的每个磁盘重复[Step 6 \(p. 698\)](#)。

7. 验证您要使用的磁盘现在是否为动态。

```
DISKPART> list disk
Disk ### Status Size Free Dyn Gpt
----- -----
Disk 0 Online 30 GB 0 B
Disk 1 Online 8 GB 0 B *
Disk 2 Online 8 GB 0 B *
Disk 3 Online 8 GB 0 B *
* Disk 4 Online 8 GB 0 B *
Disk 5 Online 419 GB 0 B
Disk 6 Online 419 GB 0 B
```

8. 创建 RAID 阵列。在 Windows 上，RAID 0 卷称为条带卷，RAID 1 卷称为镜像卷。

(仅条带卷) 要在磁盘 1 和 2 上创建条带卷阵列，请使用以下命令 (注意用于将阵列条带化的 stripe 选项)：

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

(仅镜像卷) 要在磁盘 3 和 4 上创建镜像卷阵列，请使用以下命令 (注意用于将阵列镜像化的 mirror 选项)：

```
DISKPART> create volume mirror disk=3,4
DiskPart successfully created the volume.
```

9. 验证您的新卷。

```
DISKPART> list volume
Volume ### Ltr Label Fs Type Size Status Info
----- -- -
Volume 0 C NTFS Partition 29 GB Healthy System
* Volume 1 RAW Mirror 8190 MB Healthy
Volume 2 RAW Stripe 15 GB Healthy
```

|          |   |             |      |           |        |         |
|----------|---|-------------|------|-----------|--------|---------|
| Volume 5 | Z | Temporary S | NTFS | Partition | 419 GB | Healthy |
| Volume 6 | Y | Temporary S | NTFS | Partition | 419 GB | Healthy |

请注意，对于此示例，Type 列列出一个 Mirror 卷和一个 Stripe 卷。

10. 选择并格式化您的卷，以便可以开始使用它。

- a. 选择您要格式化的卷（将 *n* 替换为卷编号）。

```
DISKPART> select volume n
Volume n is the selected volume.
```

- b. 格式化卷。



Note

要执行完整格式化，请省略 quick 选项。

```
DISKPART> format quick recommended label="My new volume"
100 percent completed
DiskPart successfully formatted the volume.
```

- c. 向卷分配可用驱动器号。

```
DISKPART> assign letter f
DiskPart successfully assigned the drive letter or mount point.
```

新卷现在已准备就绪，可供使用。

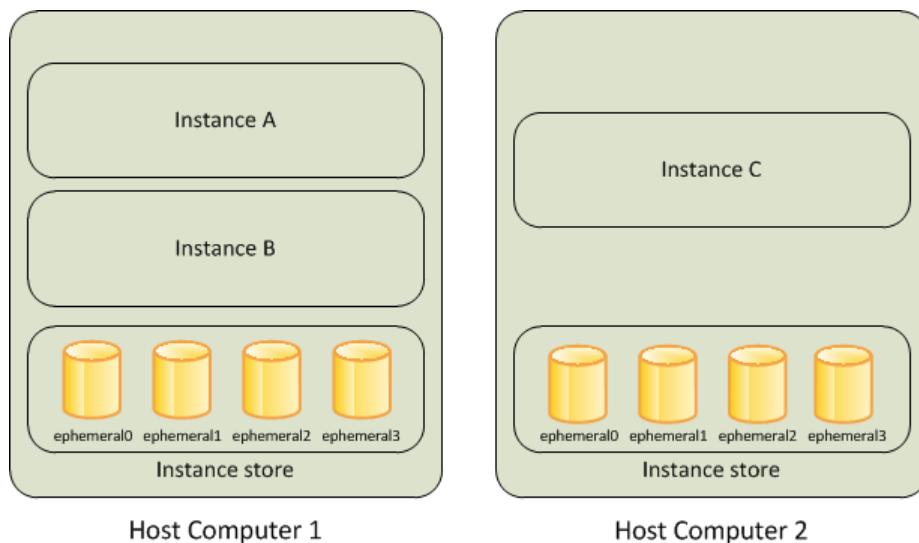
## Amazon EC2 实例存储

### Abstract

使用实际连接到实例的主机计算机的磁盘存储。

实例存储为您的实例提供临时性块级存储。此存储位于已物理连接到主机的磁盘上。实例存储是一种理想的临时存储解决方案，非常适合存储需要经常更新的信息，如缓存、缓冲、临时数据和其他临时内容，或者存储从一组实例上复制的数据，如 Web 服务器的负载均衡池。

实例存储由一个或多个显示为块储存设备的实例存储卷组成。实例存储的大小因实例类型而异。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。尽管实例存储专用于特定实例，但是磁盘子系统是在主机上的实例间共享的。



## 内容

- [实例存储生命周期 \(p. 702\)](#)
- [实例存储卷 \(p. 702\)](#)
- [将实例存储卷添加到您的 EC2 实例 \(p. 704\)](#)
- [SSD 实例存储卷 \(p. 707\)](#)

## 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。实例存储内的数据仅在与关联的实例的生命周期内保留。如果实例重启（无论是故意还是意外），实例存储内的数据都会保留下。然而，在以下情况下，实例存储中的数据会丢失：

- 底层磁盘驱动器发生故障
- 实例停止
- 实例终止

因此，切勿依赖实例存储来存储珍贵且需要长期保存的数据。相反，您可构建某种程度的冗余（例如，RAID 1/5/6）或使用支持冗余和容错的文件系统（例如，HDFS 和 MapR-FS）。您还可以定期将数据备份到更持久的数据存储解决方案（如 Amazon S3 或 Amazon EBS）。

您无法将实例存储卷与一个实例分离并将该卷挂载到另一个实例。如果您从实例创建 AMI，则从此 AMI 中启动实例时，实例存储卷上的数据不能保存且不会出现在实例存储卷上。

## 实例存储卷

实例类型决定了可用的实例存储的大小以及用于实例存储卷的硬件类型。实例存储卷包含在实例小时成本中。您必须先指定在启动实例时要使用的实例存储卷，然后在使用实例存储卷之前格式化并挂载这些卷。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 \(p. 704\)](#)。

某些实例类型使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。如果您需要延迟非常低的存储，且实例终止时不需要保留数据或可以使用容错架构，则可以选择这种实例。有关更多信息，请参阅 [SSD 实例存储卷 \(p. 707\)](#)。

下表列出了每种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。

| 实例类型        | 实例存储卷                 | 类型  | 需要初始化 * | TRIM Support** |
|-------------|-----------------------|-----|---------|----------------|
| c1.medium   | 1 x 350 GB            | HDD | ✓       |                |
| c1.xlarge   | 4 x 420 GB (1680 GB)  | HDD | ✓       |                |
| c3.large    | 2 x 16 GB (32 GB)     | SSD | ✓       |                |
| c3.xlarge   | 2 x 40 GB (80 GB)     | SSD | ✓       |                |
| c3.2xlarge  | 2 x 80 GB (160 GB)    | SSD | ✓       |                |
| c3.4xlarge  | 2 x 160 GB (320 GB)   | SSD | ✓       |                |
| c3.8xlarge  | 2 x 320 GB (640 GB)   | SSD | ✓       |                |
| cc2.8xlarge | 4 x 840 GB (3360 GB)  | HDD | ✓       |                |
| cgl.4xlarge | 2 x 840 GB (1680 GB)  | HDD | ✓       |                |
| cr1.8xlarge | 2 x 120 GB (240 GB)   | SSD | ✓       |                |
| d2.xlarge   | 3 x 2000 GB (6 TB)    | HDD |         |                |
| d2.2xlarge  | 6 x 2000 GB (12 TB)   | HDD |         |                |
| d2.4xlarge  | 12 x 2000 GB (24 TB)  | HDD |         |                |
| d2.8xlarge  | 24 x 2000 GB (48 TB)  | HDD |         |                |
| g2.2xlarge  | 1 x 60 GB             | SSD | ✓       |                |
| g2.8xlarge  | 2 x 120 GB (240 GB)   | SSD | ✓       |                |
| hi1.4xlarge | 2 x 1024 GB (2048 GB) | SSD |         |                |
| hs1.8xlarge | 24 x 2000 GB (48 TB)  | HDD | ✓       |                |
| i2.xlarge   | 1 x 800 GB            | SSD |         | ✓              |
| i2.2xlarge  | 2 x 800 GB (1600 GB)  | SSD |         | ✓              |
| i2.4xlarge  | 4 x 800 GB (3200 GB)  | SSD |         | ✓              |

| 实例类型        | 实例存储卷                 | 类型  | 需要初始化 * | TRIM Support** |
|-------------|-----------------------|-----|---------|----------------|
| i2.8xlarge  | 8 x 800 GB (6400 GB)  | SSD |         | ✓              |
| m1.small    | 1 x 160 GB            | HDD | ✓       |                |
| m1.medium   | 1 x 410 GB            | HDD | ✓       |                |
| m1.large    | 2 x 420 GB (840 GB)   | HDD | ✓       |                |
| m1.xlarge   | 4 x 420 GB (1680 GB)  | HDD | ✓       |                |
| m2.xlarge   | 1 x 420 GB            | HDD | ✓       |                |
| m2.2xlarge  | 1 x 850 GB            | HDD | ✓       |                |
| m2.4xlarge  | 2 x 840 GB (1680 GB)  | HDD | ✓       |                |
| m3.medium   | 1 x 4 GB              | SSD | ✓       |                |
| m3.large    | 1 x 32 GB             | SSD | ✓       |                |
| m3.xlarge   | 2 x 40 GB (80 GB)     | SSD | ✓       |                |
| m3.2xlarge  | 2 x 80 GB (160 GB)    | SSD | ✓       |                |
| r3.large    | 1 x 32 GB             | SSD |         | ✓              |
| r3.xlarge   | 1 x 80 GB             | SSD |         | ✓              |
| r3.2xlarge  | 1 x 160 GB            | SSD |         | ✓              |
| r3.4xlarge  | 1 x 320 GB            | SSD |         | ✓              |
| r3.8xlarge  | 2 x 320 GB (640 GB)   | SSD |         | ✓              |
| x1.32xlarge | 2 x 1920 GB (3840 GB) | SSD |         |                |

\* 如果挂载到特定实例上的卷没有初始化，则会遭受初始写入惩罚。有关初始化实例存储卷的更多信息，请参阅[优化实例存储卷的磁盘性能](#)。

## 将实例存储卷添加到您的 EC2 实例

### Abstract

启动时将实例存储卷添加到 EC2 实例，然后准备好卷以供使用。

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。有关更多信息，请参阅[块储存设备映射 \(p. 712\)](#)。

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 \(p. 63\)](#)。将自动安装根卷。对于根卷的具有实例存储卷的实例，此卷的大小因 AMI 而异，但最大大小为 10 GB。

您可在启动实例时使用块储存设备映射来指定额外的 EBS 卷，或者可在实例运行后挂载额外的 EBS 卷。有关更多信息，请参阅 [Amazon EBS 卷 \(p. 640\)](#)。

您只能在启动实例时为您的实例指定实例存储卷。无法在启动实例后将实例存储卷挂载到该实例。

对您的实例可用的实例存储卷的数量和大小因实例类型而异。一些实例类型不支持实例存储卷。有关每种实例类型支持的实例存储卷的更多信息，请参阅 [实例存储卷 \(p. 702\)](#)。如果为您的实例选择的实例类型支持实例存储卷，则您必须在启动实例时将这些卷添加到实例的块储存设备映射。在启动实例后，您必须先确保已格式化和安装实例的实例存储卷，然后才能使用这些存储卷。请注意，将自动安装实例存储所支持的实例的根卷。

#### 内容

- [将实例存储卷添加到 AMI \(p. 705\)](#)
- [将实例存储卷添加到实例 \(p. 706\)](#)
- [使实例存储卷在您的实例上可用 \(p. 707\)](#)

## 将实例存储卷添加到 AMI

您可创建带包括实例存储卷的块储存设备映射的 AMI。将实例存储卷添加到 AMI 后，您从该 AMI 启动的所有实例都会包含这些实例存储卷。请注意，在启动实例时，可忽略 AMI 块储存设备映射中指定的卷，并添加新卷。



#### Important

对于 M3 实例，请在实例而不是 AMI 的块储存设备映射中指定实例存储卷。Amazon EC2 可能会忽略仅在 AMI 的块储存设备映射中指定的实例存储卷。

#### 使用控制台向 Amazon EBS 支持的 AMI 添加实例存储卷

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
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，为您的映像添加一个有意义的名称和描述。
5. 对于要添加的每个实例存储卷，请选择 Add New Volume，从 Type 中选择实例存储卷，然后从 Device 中选择设备名称。(有关更多信息，请参阅 [Windows 实例上的设备命名 \(p. 710\)](#).) 可用的实例存储卷数量取决于实例类型。



6. 单击 Create Image (创建映像)。

## 使用命令行向 AMI 添加实例存储卷

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

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

## 将实例存储卷添加到实例

启动实例时，指定的 AMI 将提供默认块储存设备映射。如果需要额外的实例存储卷，您必须在启动实例时将这些卷添加到实例。请注意，您还可忽略 AMI 块储存设备映射中指定的设备。



### Important

对于 M3 实例，即使您未在实例的块储存设备映射中指定实例存储卷，您也可能收到这些卷。

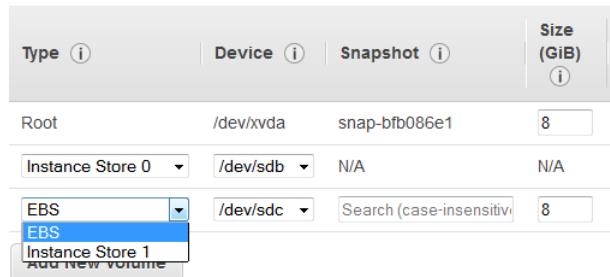


### Important

对于 HS1 实例，无论您在 AMI 的块储存设备映射中指定了多少个实例存储卷，从 AMI 中启动的实例的块储存设备映射都会自动包括最大数目的支持的实例存储卷。您必须先从块储存设备映射中显式删除不需要的实例存储卷，然后再启动该映射。

## 使用控制台更新实例的块储存设备映射

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择 Launch Instance。
3. 在 Step 1: Choose an Amazon Machine Image (AMI) 中，选择要使用的 AMI，然后选择 Select。
4. 按照向导说明操作以完成 Step 1: Choose an Amazon Machine Image (AMI)、Step 2: Choose an Instance Type 和 Step 3: Configure Instance Details。
5. 在 Step 4: Add Storage 中，根据需要修改现有条目。对于要添加的每个实例存储卷，请单击 Add New Volume，从 Type 中选择实例存储卷，然后从 Device 中选择设备名称。可用的实例存储卷数量取决于实例类型。



6. 完成向导以启动实例。

## 使用命令行更新实例的块储存设备映射

您可将下列选项命令之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 [访问 Amazon EC2 \(p. 3\)](#)。

- `--block-device-mappings` 与 [run-instances](#) (AWS CLI)
- `-BlockDeviceMapping` 与 [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

## 使实例存储卷在您的实例上可用

启动实例后，该实例可使用实例存储卷，但是必须先安装该卷，然后再使用。对于 Linux 实例，实例类型决定应为您挂载哪种实例存储卷，以及哪些存储卷可由您自行挂载。对于 Windows 实例，EC2Config 服务可为实例挂载实例存储卷。该实例的块储存设备驱动程序会在安装卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的名称不同。

许多实例存储卷都预先经过 ext3 文件系统的格式化处理。支持 TRIM 指令的基于 SSD 的实例存储卷不会预先经过任何文件系统的格式化处理。然而，您可以在启动实例后，使用您选择的文件系统将卷格式化。有关更多信息，请参阅 [实例存储卷 TRIM 支持 \(p. 707\)](#)。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 \(p. 719\)](#)。

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[列出使用 Windows 磁盘管理的磁盘 \(p. 720\)](#)。

## SSD 实例存储卷

### Abstract

某些 EC2 实例支持固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。

以下实例支持使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能的实例存储卷：C3、G2、H1、I2、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 \(p. 702\)](#)。

像其他实例存储卷一样，您必须在启动实例时映射实例的 SSD 实例存储卷，而且 SSD 实例卷上的数据仅可在其关联的实例的生命周期内保留。有关更多信息，请参阅[将实例存储卷添加到您的 EC2 实例 \(p. 704\)](#)。

## 实例存储卷 TRIM 支持

以下实例支持带 TRIM 的 SSD 卷：I2、R3。



### Important

从 AWS 半虚拟化驱动程序版本 7.3.0 起，运行 Windows Server 2012 R2 的实例支持 TRIM。运行更早版本的 Windows Server 的实例不支持 TRIM。

利用支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关使用 TRIM 命令的更多信息，请参阅您的实例的操作系统文档。

支持 TRIM 的实例存储卷先经全面删减，然后再分配到您的实例。这些卷在实例启动时未经过文件系统的格式化处理，因此，您必须先进行格式化，而后才能装载和使用。为快速访问这些卷，在格式化卷时您应当指定特定于文件系统的选项以跳过 TRIM 操作。在 Linux 上，您还应当在支持 TRIM 的设备的装载命令或 /etc/fstab 文件条目中添加 discard 选项，以便设备有效使用此功能。在 Windows 上，使用以下命令：fsutil behavior set DisableDeleteNotify 1。

## Amazon Simple Storage Service (Amazon S3)

### Abstract

使用 Amazon S3 作为 Internet 数据的存储库，以便可以访问可靠、快速和廉价的数据存储基础设施。

Amazon S3 是 Internet 数据的存储库。Amazon S3 提供了可靠、快速和廉价的数据存储基础设施。它的目的是通过支持您随时从 Amazon EC2 内部或从网络上的任何地方存储和检索任何数量的数据来简化整个网络计算。Amazon S3 以冗余方式跨多个设施在多个设备上存储数据元，允许多个不同的客户端或应用程序线程同时对这些数据元进行读或写操作。您可以使用存储在 Amazon S3 中的冗余数据快速、可靠地恢复实例或应用程序故障。

Amazon EC2 使用 Amazon S3 来存储 Amazon Machine Images (AMIs)。您可以使用 AMI 启动 EC2 实例。万一实例发生故障，您可以使用已存储的 AMI 立即启动其他实例，从而实现快速故障恢复和确保业务的连续性。

Amazon EC2 还使用 Amazon S3 来存储数据卷的快照（备份副本）。在应用程序或系统发生故障的情况下，您可以使用快照来快速、可靠地恢复数据。您也可以将快照用作基线来创建多个数据卷，扩展现有数据卷的大小，或者跨多个可用区域移动数据，因此使您的数据使用具有高度的可扩展性。有关使用数据卷和快照的更多信息，请参阅 [Amazon Elastic Block Store \(p. 638\)](#)。

数据元是 Amazon S3 中存储的基本实体。Amazon S3 中存储的每个数据元都包含在存储段中。存储段在最高级别上组织管理 Amazon S3 命名空间，并指定负责该存储的账户。Amazon S3 存储段类似于 Internet 域名。存储在存储段中的数据元具有唯一的密钥值，可以使用 HTTP URL 地址进行检索。例如，如果密钥值为 /photos/mygarden.jpg 的对象存储在 myawsbucket 存储桶中，则可以使用 <http://myawsbucket.s3.amazonaws.com/photos/mygarden.jpg>。

有关 Amazon S3 功能的更多信息，请参阅 [Amazon S3 产品页](#)。

## Amazon S3 和 Amazon EC2

凭借 Amazon S3 的存储优势，您可以选择使用此服务存储文件和数据集以用于 EC2 实例。有几种方法可在 Amazon S3 和您的实例间移动数据。除下面所讨论的示例外，您还可以使用其他人编写的各种工具从您的计算机或实例访问您在 Amazon S3 中的数据。AWS 论坛中对其中一些常见工具进行了讨论。

如果您有权限，就可以使用以下某种方法在 Amazon S3 和您的实例之间复制文件。

GET 或 wget

wget 实用工具是 HTTP 和 FTP 客户端，可用于从 Amazon S3 下载公有对象。该实用工具在 Amazon Linux 和大多数其他分发版中均为默认安装，可在 Windows 上下载安装。要下载 Amazon S3 对象，请使用以下命令（替换要下载的对象的 URL）。

```
wget http://s3.amazonaws.com/my_bucket/my_folder/my_file.ext
```

此方法要求您请求的数据元是公用数据元；如果数据元不是公用的，您会收到一条 ERROR 403: Forbidden 消息。如果您收到此错误，请打开 Amazon S3 控制台并将该对象的权限更改为公用。有关更多信息，请参阅 [Amazon Simple Storage Service 开发人员指南](#)。

AWS 命令行界面

AWS 命令行界面 (AWS CLI) 是用于管理 AWS 服务的统一工具。只通过一个工具进行下载和配置，您就可以使用命令行控制多个 AWS 服务并利用脚本来自动执行这些服务。AWS CLI 允许用户对自己进行身份验证，从 Amazon S3 下载受限制的项目和上传项目。有关更多信息，例如如何安装和配置这些工具，请参阅 [AWS 命令行界面详细信息页](#)。

aws s3 cp 命令类似于 Unix cp 命令（语法是：aws s3 cp *source destination*）。您可以将文件从 Amazon S3 复制到您的实例，从您的实例复制到 Amazon S3，甚至可以将文件从一个 Amazon S3 位置复制到另一个位置。

使用以下命令可将一个对象从 Amazon S3 复制到您的实例。

```
C:\> 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。

```
C:\> aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

使用以下命令可将一个对象从一个 Amazon S3 位置复制到另一个位置。

```
C:\> aws s3 cp s3://my_bucket/my_folder/my_file.ext s3://my_bucket/my_folder/my_file2.ext
```

aws s3 sync 命令可以将整个 Amazon S3 存储桶同步到本地目录位置。这可以用于下载数据集并使本地副本随远程集保持更新。命令语法是：aws s3 sync *source destination*。如果您对 Amazon S3 存储桶拥有合适权限，则当您最后在命令中将源与目标位置反转时，可以将本地目录备份推送到云。

使用以下命令可将整个 Amazon S3 存储桶下载到实例上的本地目录。

```
C:\> aws s3 sync s3://remote_S3_bucket local_directory
```

适用于 Windows PowerShell 的 AWS 工具

Windows 实例有图形浏览器优势，您可以用图形浏览器直接访问 Amazon S3 控制台；不过，出于脚本编写目的，Windows 用户也可以使用[适用于 Windows PowerShell 的 AWS 工具](#)在实例与 Amazon S3 之间移动对象。

使用以下命令可将一个 Amazon S3 对象复制到您的 Windows 实例。

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key my_folder/my_file.ext -LocalFile my_copied_file.ext
```

Amazon S3 API

如果您是一名开发人员，则可以使用 API 访问 Amazon S3 中的数据。有关更多信息，请参阅[Amazon Simple Storage Service 开发人员指南](#)。您可以使用此 API 及其示例帮助开发应用程序并将其与其他 API 和 SDK（例如 boto Python 接口）集成。

## 实例卷限制

### Abstract

了解您的 EC2 实例的卷限制。

您的实例可以连接的卷的最大数量取决于操作系统。考虑应将多少个卷添加到实例时，应考虑是否需要增加 I/O 带宽或存储容量。

#### 内容

- [特定于 Linux 的卷限制 \(p. 710\)](#)
- [特定于 Windows 的卷限制 \(p. 710\)](#)
- [带宽与容量 \(p. 710\)](#)

## 特定于 Linux 的卷限制

连接的卷数超出 40 会导致启动失败。请注意，此数字包括根卷以及所有连接的实例存储卷和 EBS 卷。如果连接了大量卷的实例出现启动问题，请停止该实例，断开所有在启动过程中不必要的卷，然后在实例运行之后重新连接这些卷。



### Important

如果将 40 个以上的卷连接到 Linux 实例，系统只会尽力支持，不对此进行保证。

## 特定于 Windows 的卷限制

下表基于所使用的驱动程序显示 Windows 实例的卷限制。请注意，这些数字包括根卷以及所有连接的实例存储卷和 EBS 卷。



### Important

如果连接到 Windows 实例的卷的数量超过下面的数字，系统只会尽力支持，不对此提供保证。

| 驱动程序            | 卷限制 |
|-----------------|-----|
| AWS 半虚拟化驱动程序    | 26  |
| Citrix 半虚拟化驱动程序 | 26  |
| Red Hat 半虚拟化    | 17  |

建议 Windows 实例连接的使用 AWS 半虚拟化或 Citrix 半虚拟化驱动程序的卷不要超过 26 个，否则可能导致性能问题。

要确定您的实例所使用的半虚拟化驱动程序，或是要将 Windows 实例从 Red Hat 升级到 Citrix 半虚拟化驱动程序，请参阅在 [Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。

有关设备名称与卷如何相关的更多信息，请参阅 [将磁盘映射到 Windows EC2 实例上的卷 \(p. 720\)](#)。

## 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 Provisioned IOPS 卷。按照 [Amazon EC2 实例配置 \(p. 691\)](#) 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。

## Windows 实例上的设备命名

### Abstract

了解您可以对 EC2 实例的卷使用的设备名称。

当您将卷连接到实例时，需要为卷提供设备名称。该设备名称由 Amazon EC2 使用。实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 使用的名称不同。

### 内容

- 可用设备名称 (p. 711)
- 设备名称注意事项 (p. 711)

有关在 Linux 实例上的设备名称的信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [Linux 实例上的设备命名](#)。

## 可用设备名称

下表列出了 Windows 实例的可用设备名称。您可以连接到实例的卷的数量取决于操作系统。有关更多信息，请参阅 [实例卷限制 \(p. 709\)](#)。

| Xen 驱动程序类型           | 可用                                                                               | 根预留                    | 用于实例存储卷                                | 建议用于 EBS 卷                                                                                                                                             |
|----------------------|----------------------------------------------------------------------------------|------------------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS 半虚拟化，Citrix 半虚拟化 | xvd[b-z]<br>xvd[b-c][a-z]<br><code>/dev/sda1</code><br><code>/dev/sd[b-e]</code> | <code>/dev/sda1</code> | xvd[a-e]<br>xvdc[a-x]<br>(hs1.8xlarge) | xvd[f-z]<br><br> Warning<br>如果您映射名称为 xvda 的 EBS 卷，则 Windows 无法识别该卷。 |
| Red Hat 半虚拟化         | xvd[a-z]<br>xvd[b-c][a-z]<br><code>/dev/sda1</code><br><code>/dev/sd[b-e]</code> | <code>/dev/sda1</code> | xvd[a-e]<br>xvdc[a-x]<br>(hs1.8xlarge) | xvd[f-p]                                                                                                                                               |

请注意，您可以使用以下 AWS CLI 命令确定您的特定 AMI 的根设备名称：

```
aws ec2 describe-images --image-ids image_id --query Images[].RootDeviceName
```

有关实例存储卷的更多信息，请参阅 [Amazon EC2 实例存储 \(p. 701\)](#)。有关根设备存储的信息，请参阅 [根设备卷 \(p. 8\)](#)。

## 设备名称注意事项

在选择设备名称时请记住以下原则：

- 尽管您可以使用用于连接实例存储卷的设备名连接 EBS 卷，我们还是强烈建议您不要这样做，因为这种操作具有不可预测性。
- Amazon EC2 Windows AMI 安装有一个附加服务，即 Ec2Config 服务。首次启动时，Ec2Config 服务会作为本地系统运行并执行各种功能以准备实例。使用驱动器映射设备后，Ec2Config 服务会初始化驱动器并进行安装。根硬盘经过初始化后安装为 `c:\`。连接到实例的实例存储卷已初始化并安装为 `z:\`、`y:\` 等。在默认情况下，当 EBS 卷连接到 Windows 实例时，它在实例上可能会显示为任何盘符。您可以更改 Ec2Config Service 的设置来设置各个 EBS 卷的盘符。有关更多信息，请参阅 [使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#) 和 [将磁盘映射到 Windows EC2 实例上的卷 \(p. 720\)](#)。

# 块储存设备映射

## Abstract

使用块储存设备映射可在实例启动时为实例指定其他 EBS 卷或实例存储卷。

您启动的每个实例都有一个关联根设备卷，它是 Amazon EBS 卷或实例存储卷。您可以使用块储存设备映射来指定实例启动时要连接的其他 EBS 卷或实例存储卷。您还可以将其他 EBS 卷连接到运行中的实例，请参阅 [将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。然而，将实例存储卷连接到实例的唯一办法是，在实例启动时，使用块储存设备映射来进行连接。

有关根设备卷的更多信息，请参阅 [根设备卷 \(p. 8\)](#)。

### 内容

- [块储存设备映射的概念 \(p. 712\)](#)
- [AMI 块储存设备映射 \(p. 714\)](#)
- [实例块储存设备映射 \(p. 716\)](#)

## 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和广泛使用缓存 I/O。例如，包括硬盘、CD-ROM 盘和闪存盘。块储存设备可以实际连接到计算机，或者就像实际连接到计算机一样对进行远程访问。Amazon EC2 支持两种类型的块储存设备：

- 实例存储卷（虚拟设备，其底层硬件实际连接到该实例的主机）
- EBS 卷（远程存储设备）

块储存设备映射定义了挂载到某个实例的块储存设备（实例存储卷和 EBS 卷）。您可以指定块储存设备映射作为创建 AMI 的一部分，以便使从该 AMI 启动的所有实例均可使用该映射。或者，您还可以在启动实例时指定块储存设备映射，这样该映射会覆盖您在启动实例的 AMI 中指定的块储存设备映射。

### 内容

- [块储存设备映射条目 \(p. 712\)](#)
- [块储存设备映射实例存储注意事项 \(p. 713\)](#)
- [块储存设备映射示例 \(p. 713\)](#)
- [如何使设备在操作系统可用 \(p. 714\)](#)

## 块储存设备映射条目

当您创建块储存设备映射时，可以为需要挂载到该实例的每个块储存设备指定以下信息：

- 在 Amazon EC2 内使用的设备名称。有关更多信息，请参阅 [Windows 实例上的设备命名 \(p. 710\)](#)。



### Important

该实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的不同。

- [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。
- [EBS 卷] 用于创建块储存设备的快照的 ID (snap-xxxxxxxx)。只要您指定卷大小，此值为可选。

- [EBS 卷] 卷的大小，以 GiB 计算。所指定的大小必须大于或等于指定快照的大小。
- [EBS 卷] 是否在实例终止时删除卷 ( true 或 false )。根设备卷的默认值为 true，挂载的卷的默认值为 false。当您创建 AMI 时，其块储存设备映射会从该实例继承此设置。当您启动某个实例时，该实例会从 AMI 继承此设置。
- [EBS 卷] 卷类型。对于通用型 SSD 卷是 gp2，对于 provisioned IOPS 卷是 io1，对于吞吐优化 HDD 卷是 st1，对于 Cold HDD 卷是 sc1，对于磁介质卷是 standard。在 Amazon EC2 控制台中，默认值为 gp2；在 AWS 开发工具包和 AWS CLI 中，默认值为 standard。
- [EBS 卷] 该卷支持的每秒输入/输出操作(IOPS) 次数。（不适用于 gp2、st1、sc1 或 standard 卷。）

## 块储存设备映射实例存储注意事项

使用在其块储存设备映射中具有实例存储卷的 AMI 启动实例时，要考虑一些注意事项。

- 有些实例类型包含的实例存储卷多于其他类型，而有些实例类型根本不包含实例存储卷。如果实例类型支持一个实例存储卷，而且 AMI 具有用于两个实例存储卷的映射，则实例会在启动时带有一个实例存储卷。
- 实例存储卷只能在启动时进行映射。不能停止没有实例存储卷的实例（如 t2.micro），将实例更改为支持实例存储卷的类型，然后重新启动带有实例存储卷的实例。但是，您可以从实例创建 AMI 并以支持实例存储卷的实例类型启动它，然后将这些实例存储卷映射到实例。
- 如果您启动映射了实例存储卷的实例，然后停止实例，将它更改为具有较少实例存储卷的实例类型并重新启动它，则来自初始启动的实例存储卷映射会出现在实例元数据中。但是，实例使用的实例存储卷不能超出该实例类型支持的最大数量。



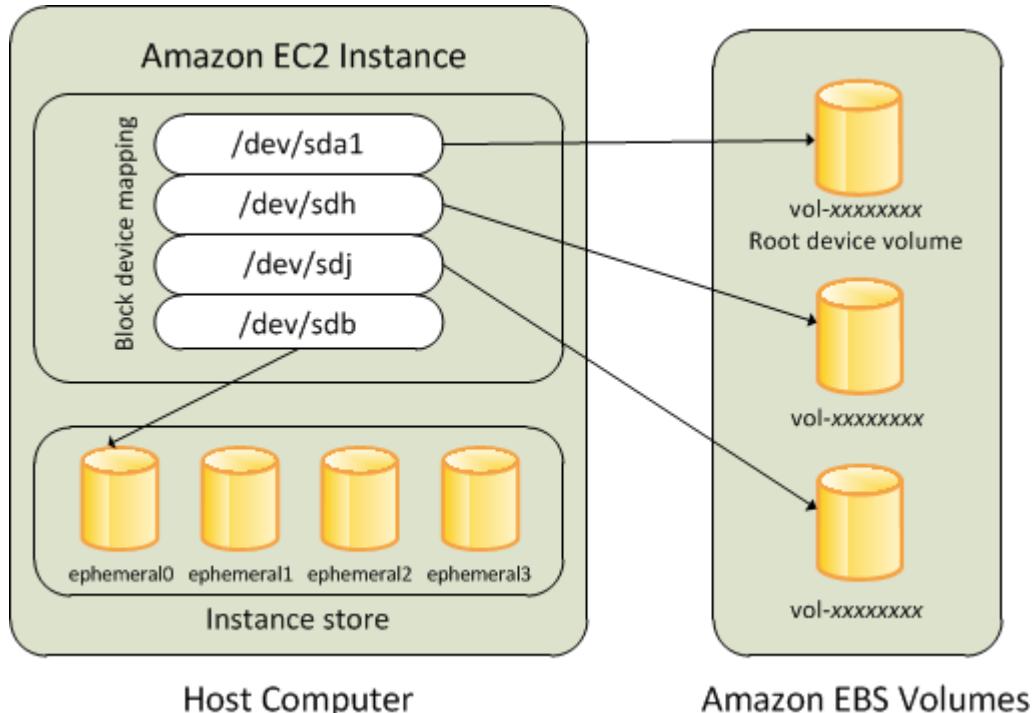
### Note

实例停止时，实例存储卷上的所有数据都会丢失。

- 根据启动时的实例存储容量，M3 实例可能会在启动时忽略 AMI 实例存储块储存设备映射（除非在启动时指定它们）。您应在启动时指定实例存储块储存设备映射（即使启动的 AMI 在 AMI 中映射了实例存储卷），以确保实例存储卷在实例启动时可用。

## 块储存设备映射示例

此图显示了 EBS 支持的实例的块储存设备映射示例。它将 /dev/sdb 映射到 ephemeral0，并将两个 EBS 卷一个映射到 /dev/sdh，另一个映射到 /dev/sdj。图中还显示了作为根设备卷的 EBS 卷 /dev/sda1。



请注意，此块储存设备映射示例是在本主题中的示命令和 API 中例使用的。您可以在[为 AMI 指定块储存设备映射 \(p. 714\)](#)和[在启动实例时更新快设备映射 \(p. 717\)](#)中找到创建块储存设备映射的示例命令和 API。

## 如何使设备在操作系统可用

Amazon EC2 使用 /dev/sdh 和 xvdh 等设备名称来描述块储存设备。Amazon EC2 使用块储存设备映射来指定要连接到 EC2 实例的块储存设备。当块储存设备连接到实例后，您必须先将其安装到操作系统，然后才可以访问此存储设备。当块储存设备从实例断开后，就被操作系统卸载下来，而您也不能再访问该存储设备。

通过 Windows 实例，可在第一次启动实例时，将在块储存设备映射中指定的设备名称映射到相应的块储存设备，然后 Ec2Config 服务会初始化并安装这些硬盘。根设备卷安装为 C:\。实例存储卷挂载为 Z:\、Y:\等。安装 EBS 卷时，可使用任何可用盘符进行安装。然而，您可以配置 Ec 如何给 EBS 卷分配盘符；要了解更多信息，请参阅[使用 EC2Config 服务配置 Windows 实例 \(p. 250\)](#)。

## AMI 块储存设备映射

各个 AMI 都拥有块储存设备映射，指定实例启动时要连接的块储存设备。Amazon 提供的 AMI 仅包含根设备。要向 AMI 添加更多块储存设备，必须创建自己的 AMI。

### 内容

- [为 AMI 指定块储存设备映射 \(p. 714\)](#)
- [查看 AMI 块储存设备映射中的 EBS 卷 \(p. 716\)](#)

## 为 AMI 指定块储存设备映射

创建 AMI 时，您可以使用两种方法来指定除根卷以外的卷。如果您在从该实例创建 AMI 前已将卷连接到运行中的实例，则 AMI 的块储存设备映射将包括这些相同的卷。对于 EBS 卷，这些现存的数据会保存在一个新的快照中，而且是块储存设备映射指定的新快照。而实例存储卷的数据无法保存。

对于 EBS 支持的 AMI，您可以使用块储存设备映射来添加 EBS 卷和实例存储卷。对于实例存储支持的 AMI，您只能添加实例存储卷，方法是在注册镜像时修改镜像清单文件中的块储存设备映射条目。



### Note

对于 M3 实例，您必须在启动实例时，在块储存设备映射中指定适用于实例的实例存储卷。当您启动 M3 实例时，如果在块储存设备映射中为 AMI 指定的实例存储卷未指定为块储存设备映射的一部分，则该卷可能会被忽略。

## 使用控制台向 AMI 添加卷

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。

使用以下参数指定块储存设备映射：

```
--block-device-mappings [mapping, ...]
```

要添加实例存储卷，请使用以下映射：

```
{
 "DeviceName": "xvdb",
 "VirtualName": "ephemeral0"
}
```

要添加空的 100 GiB 磁介质卷，请使用以下映射：

```
{
 "DeviceName": "xvdg",
 "Ebs": {
 "VolumeSize": 100
 }
}
```

要添加基于快照的 EBS 卷，请使用以下映射：

```
{
 "DeviceName": "xvdh",
 "Ebs": {
 "SnapshotId": "snap-xxxxxxxx"
 }
}
```

要对设备省略映射，请使用以下映射：

```
{
 "DeviceName": "xvdj",
 "NoDevice": ""
}
```

或者，您可以使用 `-BlockDeviceMapping` 参数和以下命令（适用于 Windows PowerShell 的 AWS 工具）：

- [New-EC2Image](#)
- [Register-EC2Image](#)

## 查看 AMI 块储存设备映射中的 EBS 卷

您可以轻松列举块储存设备映射中适用于 AMI 的 EBS 卷。

### 使用控制台查看 AMI 的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从 Filter 列表中选择 EBS images 以获取 EBS 支持的 AMI 的列表。
4. 选择所需的 AMI，然后查看 Details (详细信息) 选项卡。至少，以下信息适用于根设备：
  - Root Device Type (根设备类型) (ebs)
  - Root Device Name (根设备名称) ( 如，/dev/sda1 )
  - Block Devices (数据块储存设备) ( 例如，/dev/sda1=snap-1234567890abcdef0:8:true )

如果使用块储存设备映射创建的 AMI 带有额外卷，则 Block Devices (块储存设备) 字段会显示针对这些额外 EBS 卷的映射。（请注意，此屏幕不显示实例存储卷。）

### 使用命令行查看 AMI 的 EBS 卷

使用 [describe-images](#) (AWS CLI) 命令或 [Get-EC2Image](#) (适用于 Windows PowerShell 的 AWS 工具) 命令来枚举 AMI 块储存设备映射中的 EBS 卷。

## 实例块储存设备映射

在默认情况下，您启动的实例包含所有在 AMI 的块储存设备映射中指定的储存设备（您是从该 AMI 启动实例的）。您可以在启动实例时，为实例指定要对块储存设备映射执行的更改，而这些更新会覆盖 AMI 的块储存设备映射或与其合并。但是，

### 限制

- 对于根卷，您只能修改下列内容：卷大小、卷类型和 Delete on Termination 标志。
- 修改 EBS 卷时，无法减小其大小。因此，您必须指定大小等于或大于 AMI 的块储存设备映射中指定的快照大小的快照。

### 内容

- [在启动实例时更新快设备映射 \(p. 717\)](#)
- [更新正在运行的实例的块储存设备映射 \(p. 718\)](#)

- [查看实例块储存设备映射中的 EBS 卷 \(p. 718\)](#)
- [查看实例存储卷的实例块储存设备映射 \(p. 719\)](#)

## 在启动实例时更新快设备映射

您可以在启动实例时向其添加 EBS 卷和实例存储卷。请注意，针对实例更新块储存设备映射不会对启动实例的 AMI 的块储存设备映射造成永久性更改。

### 使用控制台向实例添加卷

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面中，您可以按以下方法修改根卷、EBS 卷和实例存储卷：
  - 若要更改根卷的大小，请查找 Type (类型) 列下的 Root (根) 卷，然后更改其 Size (大小) 字段。
  - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的 EBS 卷，请找到该卷并单击其对应的 Delete (删除) 图标。
  - 要添加 EBS 卷，请选择 Add New Volume，从 Type 列表中选择 EBS，并填写 (Device、Snapshot 等) 字段。
  - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的实例存储卷，请找到该卷并选择其对应的 Delete 图标。
  - 要添加实例存储卷，请选择 Add New Volume，从 Type 列表中选择 Instance Store，然后从 Device 中选择设备名称。
6. 完成其余向导页面，然后选择 Launch。

### 使用命令行向实例添加卷

使用 `run-instances` AWS CLI 命令可为实例指定块储存设备映射。

使用以下参数指定块储存设备映射：

```
--block-device-mappings [mapping, ...]
```

例如，假定 EBS 支持的 AMI 指定了以下块储存设备映射：

- `xvdb=ephemeral0`
- `xvdh=snap-1234567890abcdef0`
- `xvdj=:100`

要防止 `xvdj` 连接到从该 AMI 启动的实例，请使用以下映射：

```
{
 "DeviceName": "xvdj",
 "NoDevice": ""
}
```

要将 xvdh 的大小增加到 300 GiB，请指定以下映射。请注意，您不必为 xvdh 指定快照 ID，因为指定设备名称就足以识别卷。

```
{
 "DeviceName": "xvdh",
 "Ebs": {
 "VolumeSize": 300
 }
}
```

要额外附加一个实例存储卷 xvdc，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": "xvdc",
 "VirtualName": "ephemeral1"
}
```

或者，您可以使用 `-BlockDeviceMapping` 参数和 [New-EC2Instance](#) 命令（适用于 Windows PowerShell 的 AWS 工具）。

## 更新正在运行的实例的块储存设备映射

您可以使用 [modify-instance-attribute](#) AWS CLI 命令更新正在运行的实例的块储存设备映射。请注意，在更改此属性之前，您不需要停止该实例。

```
C:\> aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings file://mapping.json
```

例如，要在实例终止时保留根卷，请在 `mapping.json` 中指定以下内容：

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

或者，您可以使用 `-BlockDeviceMapping` 参数和 [Edit-EC2InstanceAttribute](#) 命令（适用于 Windows PowerShell 的 AWS 工具）。

## 查看实例块储存设备映射中的 EBS 卷

您可以轻松枚举映射到实例的 EBS 卷。



### Note

对于在 2009-10-31 API 发行之前启动的实例，AWS 不会显示块储存设备映射。您必须先断开并重新连接该卷，AWS 才能显示块相应的设备映射。

### 使用控制台查看实例的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances。
3. 在搜索栏中，键入 Root Device Type，然后选择 EBS。此操作会显示 EBS 支持的实例列表。
4. 选择所需的实例，然后查看 Description 选项卡中显示的详细信息。至少，以下信息适用于根设备：
  - 根设备类型 (ebs)
  - Root device (根设备) ( 例如，/dev/sda1 )
  - Block devices (块储存设备) ( 例如 /dev/sda1、xvhd 和 xvdf )

如果使用块储存设备映射启动的实例有附加 EBS 卷，则 Block devices 字段会将这些附加卷也显示为根设备。（请记住，此对话框不显示实例存储卷。）

|                         |           |
|-------------------------|-----------|
| <b>Root device type</b> | ebs       |
| <b>Root device</b>      | /dev/sda1 |
| <b>Block devices</b>    | /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)
  - 根设备类型 (ebs)
  - 连接时间 (yyyy-mmThh:mm:ss.ssTZD)
  - 块储存设备状态 (attaching, attached, detaching, detached)
  - 终止时删除 (Yes, No)

### 使用命令行查看实例的 EBS 卷

使用 [describe-instances](#) (AWS CLI) 命令或 [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具) 命令来枚举实例的块储存设备映射中的 EBS 卷。

## 查看实例存储卷的实例块储存设备映射

当您查看实例的块储存设备映射时，可以只查看 EBS 卷，但是不能查看实例存储卷。您可以使用实例元数据来查询完整的块储存设备映射。所有针对实例元数据的请求的基本 URI 均为 <http://169.254.169.254/latest/>。

首先，连接到运行中的实例。对于 Windows 实例，在实例上安装 wget ( 如果尚未安装 )。

对正在运行的实例使用此查询以了解其块储存设备映射的相关信息。

```
C:\> wget http://169.254.169.254/latest/meta-data/block-device-mapping/
```

该响应包含实例的块储存设备名称。举例来说，由实例存储支持的 m1.small 实例的输出如下所示。

```
ami
ephemeral0
```

```
root
swap
```

ami 设备显然是实例的根设备。实例存储卷命名为 ephemeral[0-23]。交换设备用于存储页面文件。如果您还映射了多个 EBS 卷，它们会依次显示为 ebs1、ebs2 等。

要了解块储存设备映射中的单个块储存设备的详细信息，可将其名称添加到上述查询，如下所示。

```
C:\> wget http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

有关更多信息，请参阅 [实例元数据和用户数据 \(p. 239\)](#)。

## 将磁盘映射到 Windows EC2 实例上的卷

您的 Windows EC2 实例附带一个作为根卷的 EBS 卷。如果您的 Windows 实例使用 AWS 半虚拟化或 Citrix 半虚拟化驱动程序，您可以选择最多添加 25 个卷，最终一共连接 26 个卷。有关更多信息，请参阅 [实例卷限制 \(p. 709\)](#)。

根据您的实例的实例类型，您将有 0 到 24 个可能的实例存储卷可用于实例。要使用可用于您的实例的任何实例存储卷，您必须在创建 AMI 或启动实例时指定这些卷。您还可以在创建 AMI 或启动实例时添加 EBS 卷，或在您的实例正在运行时连接这些卷。

将卷添加到实例时，您可以指定 Amazon EC2 使用的设备名称。有关更多信息，请参阅 [Windows 实例上的设备命名 \(p. 710\)](#)。AWS Windows Amazon 系统映像 (AMI) 包含 Amazon EC2 所使用的一系列驱动程序，用于将实例存储和 EBS 卷映射到 Windows 磁盘和驱动器盘符。如果从使用 Citrix 半虚拟化 (PV) 或 AWS 半虚拟化驱动程序的 Windows AMI 启动实例，则可以使用本页介绍的关系，将 Windows 磁盘映射到实例存储和 EBS 卷。如果您的 Windows AMI 使用 Red Hat PV 驱动程序，那么您可以更新您的实例以使用 Citrix 驱动程序。有关更多信息，请参阅 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。

### 内容

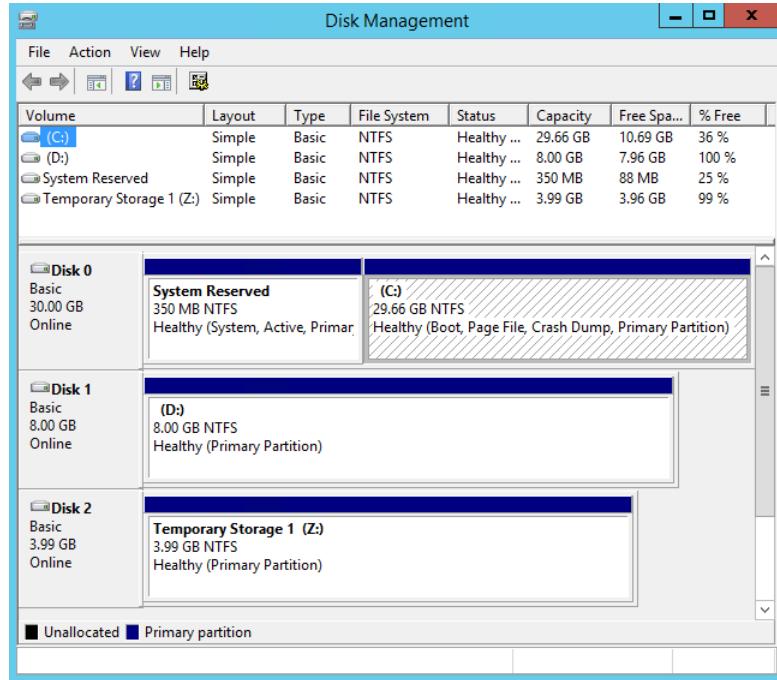
- [列出使用 Windows 磁盘管理的磁盘 \(p. 720\)](#)
- [使用 Windows PowerShell 列出磁盘 \(p. 722\)](#)
- [磁盘设备到设备名称的映射 \(p. 724\)](#)

## 列出使用 Windows 磁盘管理的磁盘

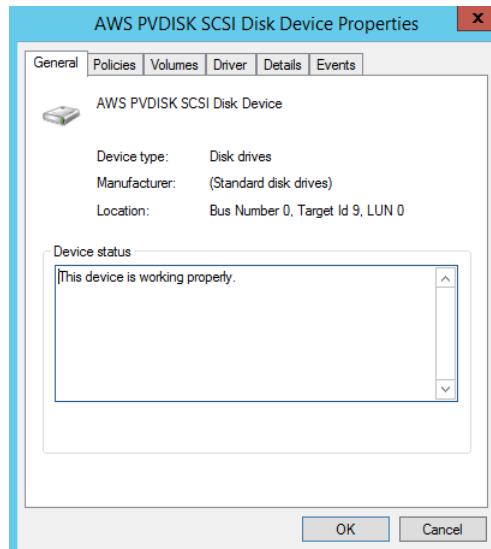
您可以使用 Windows 磁盘管理工具，在您的 Windows 实例上查找磁盘。

### 查找 Windows 实例上的磁盘

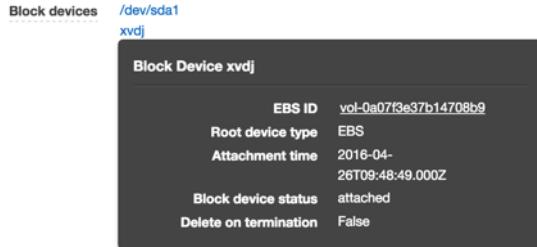
1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅 [使用 RDP 连接到 Windows 实例 \(p. 225\)](#)。
2. 启动磁盘管理实用工具。在 Windows Server 2012 的任务栏上，右键单击 Windows 徽标，然后选择 Disk Management(磁盘管理)。在 Windows Server 2008 上，单击 Start(开始)，指向 Administrative Tools(管理工具)，依次选择 Computer Management(计算机管理) 和 Disk Management(磁盘管理)。
3. 检查磁盘。磁盘 0 为根卷，即装载为 C:\ 的 EBS 卷。如果未显示其他任何磁盘，表示您的实例并未附带实例存储卷，并且您在创建 AMI 或启动实例时未指定任何 EBS 卷。否则，您将看到其他磁盘。例如，如果您使用另外的空 EBS 卷启动 m3.medium 实例，则以下磁盘可用。磁盘 1 为 EBS 卷，磁盘 2 为实例存储卷。



- 右键单击标记为“Disk 1(磁盘 1)”的灰色窗格，然后选择 Properties(属性)。记下 Location(位置)值，并在[磁盘设备到设备名称的映射\(p. 724\)](#)中的表中查找该值。例如，以下磁盘的位置值为 Bus Number 0, Target Id 9, LUN 0。根据 EBS 卷的表，此位置的设备名称为 xvdj。



- 要将 EBS 卷的设备名称映射到其卷 ID，请在计算机上打开 Amazon EC2 控制台。在“Navigation(导航)”窗格中，单击 Instances，然后选择您的实例。在 Block devices(块储存设备) 下，单击设备名称，然后查找 EBS ID。在本例中，卷 ID 为 vol-0a07f3e37b14708b9。



请注意，Amazon EC2 控制台只显示 EBS 卷。

## 使用 Windows PowerShell 列出磁盘

以下 PowerShell 脚本列出每个磁盘以及相应的设备名称和卷。

```
List the Windows disks

Create a hash table that maps each device to a SCSI target
$Map = @{"0" = '/dev/sda1'}
for($x = 1; $x -le 25; $x++) {$Map.add($x.ToString(),
[String]::Format("xvd{0}", [char](97 + $x)))}
for($x = 26; $x -le 51; $x++) {$Map.add($x.ToString(),
[String]::Format("xvda{0}", [char](71 + $x)))}
for($x = 52; $x -le 77; $x++) {$Map.add($x.ToString(),
[String]::Format("xvdb{0}", [char](45 + $x)))}
for($x = 78; $x -le 103; $x++) {$Map.add($x.ToString(),
[String]::Format("xvdc{0}", [char](19 + $x)))}
for($x = 104; $x -le 129; $x++) {$Map.add($x.ToString(),
[String]::Format("xvdd{0}", [char]($x - 7))))}

Try {
 # Use the metadata service to discover which instance the script is running
 # on
 $InstanceId = (Invoke-WebRequest '169.254.169.254/latest/meta-data/instance-
id').Content
 $AZ = (Invoke-WebRequest '169.254.169.254/latest/meta-data/placement/avail-
ability-zone').Content
 $Region = $AZ.Substring(0, $AZ.Length -1)

 #Get the volumes attached to this instance
 $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance $In-
stanceId).Instances.BlockDeviceMappings
}
Catch
{
 Write-Host "Could not access the AWS API, therefore, VolumeId is not
available.
Verify that you provided your access keys." -ForegroundColor Yellow
}

Get-WmiObject -Class Win32_DiskDrive | % {
 $Drive = $_
 # Find the partitions for this drive
 Get-WmiObject -Class Win32_DiskDriveToDiskPartition | Where-Object
 {$_.Antecedent -eq $Drive.Path.Path} | %{


```

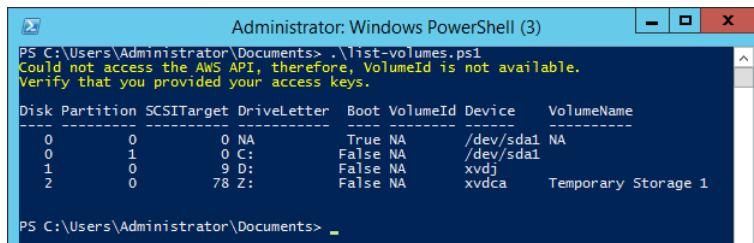
```
$D2P = $_
Get details about each partition
$Partition = Get-WmiObject -Class Win32_DiskPartition | Where-Object
{$_.Path.Path -eq $D2P.Dependent}
 # Find the drive that this partition is linked to
 $Disk = Get-WmiObject -Class Win32_LogicalDiskToPartition | Where-Object
{$_.Antecedent -in $D2P.Dependent} | %{
 $L2P = $_
 #Get the drive letter for this partition, if there is one
 Get-WmiObject -Class Win32_LogicalDisk | Where-Object {$_.Path.Path
-in $L2P.Dependent}
 }
 $BlockDeviceMapping = $BlockDeviceMappings | Where-Object {$_.DeviceName
-eq $Map[$Drive.SCSITargetId.ToString()]}

 # Display the information in a table
New-Object PSObject -Property @{
 Device = $Map[$Drive.SCSITargetId.ToString()];
 Disk = [Int]::Parse($Partition.Name.Split(",")[0].Replace("Disk
#", ""));
 Boot = $Partition.BootPartition;
 Partition = [Int]::Parse($Partition.Name.Split(",")[1].Replace("Partition
#", ""));
 SCSITarget = $Drive.SCSITargetId;
 DriveLetter = If($Disk -eq $NULL) {"NA"} else {$Disk.DeviceID};
 VolumeName = If($Disk -eq $NULL) {"NA"} else {$Disk.VolumeName};
 VolumeId = If($BlockDeviceMapping -eq $NULL) {"NA"} else {$Block
DeviceMapping.Ebs.VolumeId}
}
}
} | Sort-Object Disk, Partition | Format-Table -AutoSize -Property Disk, Partition,
SCSITarget, DriveLetter, Boot,
VolumeId, Device, VolumeName
```

在您运行此脚本前，请确保运行以下命令以支持 PowerShell 脚本的执行。

```
Set-ExecutionPolicy RemoteSigned
```

复制脚本并将其以 .ps1 文件存储在 Windows 实例上。如果您运行脚本而不设置访问密钥，您将看到类似如下的输出。



| Disk | Partition | SCSITarget | DriveLetter | Boot  | VolumeId | Device    | VolumeName          |
|------|-----------|------------|-------------|-------|----------|-----------|---------------------|
| 0    | 0         | 0          | NA          | True  | NA       | /dev/sdal | NA                  |
| 0    | 1         | 0          | C:          | False | NA       | /dev/sdal |                     |
| 1    | 0         | 9          | D:          | False | NA       | xvdj      |                     |
| 2    | 0         | 78         | Z:          | False | NA       | xvdca     | Temporary Storage 1 |

如果您指定 IAM 角色时使用的是允许启动实例时访问 Amazon EC2 的策略，或者如果您按照适用于 Windows PowerShell 的 AWS 工具 用户指南 中的 使用 AWS 证书 所述，在 Windows 实例上设置您的证书，那么您将在 VolumeId 列而不是 NA 中获得 EBS 卷的卷 ID (vol-xxxxxxx)。

## 磁盘设备到设备名称的映射

下表描述了 Citrix PV 和 AWS PV 驱动程序是如何将实例存储卷映射到 Windows 卷的。可用的实例存储卷数量由实例类型决定。有关更多信息，请参阅 [实例存储卷 \(p. 702\)](#)。

| 地点                        | 设备名称  |
|---------------------------|-------|
| 总线编号 0 , 目标 ID 78 , LUN 0 | xvdca |
| 总线编号 0 , 目标 ID 79 , LUN 0 | xvdcb |
| 总线编号 0 , 目标 ID 80 , LUN 0 | xvdcc |
| 总线编号 0 , 目标 ID 81 , LUN 0 | xvdcd |
| 总线编号 0 , 目标 ID 82 , LUN 0 | xvdce |
| 总线编号 0 , 目标 ID 83 , LUN 0 | xvdcf |
| 总线编号 0 , 目标 ID 84 , LUN 0 | xvdcg |
| 总线编号 0 , 目标 ID 85 , LUN 0 | xvdch |
| 总线编号 0 , 目标 ID 86 , LUN 0 | xvdci |
| 总线编号 0 , 目标 ID 87 , LUN 0 | xvdcj |
| 总线编号 0 , 目标 ID 88 , LUN 0 | xvdck |
| 总线编号 0 , 目标 ID 89 , LUN 0 | xvdcl |

下表描述了 Citrix 半虚拟化和 AWS 半虚拟化驱动程序是如何将 EBS 卷映射到 Windows 卷的。有关更多信息，请参阅 [Windows 实例上的设备命名 \(p. 710\)](#)。

| 地点                        | 设备名称      |
|---------------------------|-----------|
| 总线编号 0 , 目标 ID 0 , LUN 0  | /dev/sda1 |
| 总线编号 0 , 目标 ID 1 , LUN 0  | xvdb      |
| 总线编号 0 , 目标 ID 2 , LUN 0  | xvdc      |
| 总线编号 0 , 目标 ID 3 , LUN 0  | xvdd      |
| 总线编号 0 , 目标 ID 4 , LUN 0  | xvde      |
| 总线编号 0 , 目标 ID 5 , LUN 0  | xvdf      |
| 总线编号 0 , 目标 ID 6 , LUN 0  | xvdg      |
| 总线编号 0 , 目标 ID 7 , LUN 0  | xvdh      |
| 总线编号 0 , 目标 ID 8 , LUN 0  | xvdi      |
| 总线编号 0 , 目标 ID 9 , LUN 0  | xvdj      |
| 总线编号 0 , 目标 ID 10 , LUN 0 | xvdk      |
| 总线编号 0 , 目标 ID 11 , LUN 0 | xvdl      |
| 总线编号 0 , 目标 ID 12 , LUN 0 | xvdm      |

| 地点                        | 设备名称 |
|---------------------------|------|
| 总线编号 0 , 目标 ID 13 , LUN 0 | xvdn |
| 总线编号 0 , 目标 ID 14 , LUN 0 | xvdo |
| 总线编号 0 , 目标 ID 15 , LUN 0 | xvdp |
| 总线编号 0 , 目标 ID 16 , LUN 0 | xvdq |
| 总线编号 0 , 目标 ID 17 , LUN 0 | xvdr |
| 总线编号 0 , 目标 ID 18 , LUN 0 | xvds |
| 总线编号 0 , 目标 ID 19 , LUN 0 | xvdt |
| 总线编号 0 , 目标 ID 20 , LUN 0 | xvdu |
| 总线编号 0 , 目标 ID 21 , LUN 0 | xvdv |
| 总线编号 0 , 目标 ID 22 , LUN 0 | xvdw |
| 总线编号 0 , 目标 ID 23 , LUN 0 | xvdx |
| 总线编号 0 , 目标 ID 24 , LUN 0 | xvdy |
| 总线编号 0 , 目标 ID 25 , LUN 0 | xvdz |

# 使用公用数据集

## Abstract

将公用数据集无缝集成到基于 AWS 云的应用程序中。

Amazon Web Services 提供可无缝集成到基于 AWS 云的应用程序中的公用数据集存储库。Amazon 将数据集免费存储到社区中，与所有 AWS 服务一样，您只需要为自己的应用程序所用的计算和存储付费。

### 内容

- [公用数据集概念 \(p. 726\)](#)
- [查找公用数据集 \(p. 726\)](#)
- [从快照创建公用数据集卷 \(p. 727\)](#)
- [连接和装载公用数据集卷 \(p. 728\)](#)

## 公用数据集概念

以前，查找、下载、自定义以及分析大数据集，如人类基因组的映射和美国人口普查局的数据，需要几小时甚至几天才能完成。现在，任何人都可以通过 EC2 实例访问这些数据集并在数分钟内开始这些数据的计算工作。您还可以利用整个 AWS 生态系统，轻松与其他 AWS 用户协作工作。例如，您可以通过工具和应用程序生产或使用预先构建的系统镜像来分析数据集。通过利用经济实惠的服务，如 Amazon EC2，托管这些重要数据，AWS 希望为各个学科和行业的研究人员提供实用的工具，促进更多、更快的创新。

有关更多信息，请参阅 [AWS 上的公用数据集页面](#)。

## 可用的公用数据集

目前，以下类别中的公用数据集可用：

- 生物学 - 包括人类基因组计划、基因库和其他内容。
- 化学 - 包括多个版本的 PubChem 和其他内容。
- 经济学 - 包括人口普查数据、劳动统计数据、交通统计数据和其他内容。
- 百科知识 - 包括多种来源的维基百科数据和其他内容。

## 查找公用数据集

在能够使用公用数据集之前，必须查找该数据集，然后确定托管该数据集所采用的格式。这些数据集采用两种可能的格式：Amazon EBS 快照或 Amazon S3 存储桶。

### 查找公用数据集并确定其格式

1. 转到[公用数据集页面](#)以查看所有可用公用数据集的列表。您还可以在此页面上输入搜索短语以查询可用公用数据集列表。
2. 单击数据集的名称以查看其详细信息页面。
3. 在数据集详细信息页面上，查找快照 ID 列表以标识 Amazon EBS 格式化数据集或 Amazon S3 URL。

采用快照格式的数据集用于创建连接到 EC2 实例的新 EBS 卷。有关更多信息，请参阅 [从快照创建公用数据集卷 \(p. 727\)](#)。

对于采用 Amazon S3 格式的数据集，可以使用 AWS 开发工具包或 HTTP 查询 API 访问信息，也可以使用 AWS CLI 将数据复制或同步到实例或是从实例复制或同步数据。有关更多信息，请参阅 [Amazon S3 和 Amazon EC2 \(p. 708\)](#)。

还可以使用 Amazon EMR 分析和使用公用数据集。有关更多信息，请参阅 [Amazon EMR 是什么？](#)。

## 从快照创建公用数据集卷

要使用采用快照格式的公用数据集，请创建新卷，指定公用数据集的快照 ID。可以使用 AWS 管理控制台创建新卷，如下所示。如果您愿意，也可以使用 [create-volume](#) AWS CLI 命令。

### 从快照创建公用数据集卷

1. 打开 Amazon EC2 控制台。
2. 在导航栏中，选择您的数据集快照所处的区域。



#### Important

快照 ID 限制在单个区域，您无法从处于另一个区域的快照创建卷。此外，您只能将 EBS 卷连接到同一个可用区中的实例。有关更多信息，请参阅 [资源位置 \(p. 729\)](#)。

如果您需要在不同区域中创建此卷，则可以将快照复制到所需区域，然后将其恢复到该区域中的卷。有关更多信息，请参阅 [复制 Amazon EBS 快照 \(p. 679\)](#)。

3. 在导航窗格中，单击 Volumes (卷)。
4. 在上方窗格上，单击 Create Volume (创建卷)。
5. 在 Create Volume (创建卷) 对话框中的 Type (类型) 列表中，选择 General Purpose SSD、Provisioned IOPS SSD 或 磁介质。有关更多信息，请参阅 [Amazon EBS 卷类型 \(p. 641\)](#)。
6. 在 Snapshot (快照) 字段中，开始为数据集键入快照的 ID 或描述。从建议选项列表中选择快照。



#### Note

如果您预期看到的快照 ID 未出现，则您可能在 Amazon EC2 控制台中选择了不同区域。如果在 [查找公用数据集 \(p. 726\)](#) 中标识的数据集未在其详细信息页面上指定区域，则它可能包含在 us-east-1 ( 弗吉尼亚北部 ) 区域中。

7. 在 Size (大小) 字段中，输入卷的大小（以 GiB 或 TiB 为单位），或验证快照的默认大小是否足够。



#### Note

如果您指定卷大小和快照 ID，其大小必须等于或大于快照的大小。当您选择一种卷类型和一个快照 ID 时，最小和最大卷大小将显示在 Size (大小) 列表旁边。

8. 对于 Provisioned IOPS 卷，在 IOPS 字段中输入该卷可支持的每秒输入/输出操作 (IOPS) 的最大值。
9. 在 Availability Zone (可用区) 列表中，选择要在其中启动实例的可用区。



#### Important

EBS 卷只能连接到位于相同可用区中的实例。

10. 单击 Yes, Create (是，创建)。



### Important

如果您创建的卷大于该快照的默认大小（通过在[Step 7 \(p. 727\)](#)中指定大小），您需要扩展卷上的文件系统以利用额外空间。有关更多信息，请参阅[在 Windows 上扩展 EBS 卷的存储空间 \(p. 671\)](#)。

## 连接和装载公用数据集卷

创建新数据集卷之后，您需要将其连接到 EC2 实例才能访问数据（此实例还必须处于与新卷相同的可用区中）。有关更多信息，请参阅[将 Amazon EBS 卷连接到实例 \(p. 657\)](#)。

将卷连接到实例之后，您需要在实例上装载该卷。有关更多信息，请参阅[使 Amazon EBS 卷可用 \(p. 658\)](#)。

# 资源和标签

---

## Abstract

管理 Amazon EC2 资源，如 AMI、实例、卷和快照。

Amazon EC2 提供您可创建和使用的不同资源。这些资源中的一部分资源包括映像、实例、卷和快照。在您创建某个资源时，我们会为该资源分配一个唯一资源 ID。

可以用您定义的值标记某些资源，来帮助您组织和识别它们。

以下主题介绍了资源和标签，以及如何使用它们。

### 主题

- [资源位置 \(p. 729\)](#)
- [资源 ID \(p. 730\)](#)
- [列出并筛选您的资源 \(p. 734\)](#)
- [标记 Amazon EC2 资源 \(p. 737\)](#)
- [Amazon EC2 服务限制 \(p. 746\)](#)
- [Amazon EC2 使用率报告 \(p. 747\)](#)

## 资源位置

## Abstract

为每种类型的 Amazon EC2 资源列出资源位置（无论是全球性、区域性还是基于可用区）。

下表描述了何种 Amazon EC2 资源是全球性的、何种是区域性的，或何种是基于可用区域的。

| 资源     | 类型   | 说明                    |
|--------|------|-----------------------|
| AWS 账户 | 服务全球 | 您可以在所有区域使用同一个 AWS 账户。 |

| 资源               | 类型      | 说明                                                                                                                              |
|------------------|---------|---------------------------------------------------------------------------------------------------------------------------------|
| 密钥对              | 全球性或区域性 | 您可以只在使用 Amazon EC2 创建密钥对的区域使用密钥对。您可以创建和上传所有区域均可使用的 RSA 密钥对。<br>有关更多信息，请参阅 <a href="#">Amazon EC2 密钥对和 Windows 实例 (p. 510)</a> 。 |
| 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 <a href="#">复制 AMI (p. 84)</a> 。                                   |
| 弹性 IP 地址         | 区域性的    | 弹性 IP 地址与区域相关联，并且只能与同一区域的实例相关联。                                                                                                 |
| 安全组              | 区域性的    | 安全组与区域相关联，并且只能分配给同一区域的实例。您不能使用安全组规则让一个实例与其所在区域外的实例通信。另一个区域实例的流量被视为 WAN 带宽。                                                      |
| EBS 快照           | 区域性的    | EBS 快照与其区域相关联，并且只能用于在同一区域创建卷。您可以将快照从一个区域复制到另一个区域。有关更多信息，请参阅 <a href="#">复制 Amazon EBS 快照 (p. 679)</a> 。                         |
| EBS 卷            | 可用区域    | Amazon EBS 卷与其可用区相关联，只能与同一可用区内的实例相连接。                                                                                           |
| 实例               | 可用区域    | 实例与您在其中启动实例的可用区相关联。但请注意，它的实例 ID 与区域相关联。                                                                                         |

## 资源 ID

### Abstract

查看和管理支持的资源类型的较长 ID 设置。

创建资源时，我们会为每个资源分配一个唯一资源 ID。您可以使用资源 ID 在 Amazon EC2 控制台中查找您的资源。如果您正在通过命令行工具或 Amazon EC2 API 使用 Amazon EC2，则某些命令需要资源 ID。例如，如果您正在使用 `stop-instances` AWS CLI 命令来停止实例，则必须在该命令中指定实例 ID。

#### 资源 ID 长度

资源 ID 采用以下格式：资源标识符（例如，快照的 `snap`）后接连字符以及字母与数字的唯一组合。自 2016 年 1 月起，我们将逐步引入适合部分 Amazon EC2 和 Amazon EBS 资源类型的较长 ID。字母数字字符组合的长度采用 8 个字符的格式；新 ID 采用 17 个字符的格式，例如实例 ID 的 `i-1234567890abcdef0`。

支持的资源类型将有一个选择周期，在此周期内，您可以启用较长的 ID 格式。在为某个资源类型启用较长 ID 后，您创建的任何新资源在创建后将拥有较长的 ID，除非您明确禁用较长的 ID 格式。资源 ID 在创建后不可更改；因此，不会影响具有较短 ID 的现有资源。同样，如果您为某个资源类型禁用较长 ID，您创建的具有较长 ID 的任何资源不受影响。

所有支持的资源类型将拥有一个截止日期，在此日期后，此类型的所有新资源将默认为较长的 ID 格式，并且您不能再禁用较长的 ID 格式。您可以按 IAM 用户和 IAM 角色启用或禁用较长 ID。默认情况下，IAM 用户或角色的默认设置与根用户相同。

根据您创建账户的时间，支持的资源类型可能默认为使用较长的 ID。但是，在该资源类型的截止日期前，您可以选择不再使用较长 ID。有关更多信息，请参阅 [Amazon EC2 常见问题](#) 中的较长的 EC2 和 EBS 资源 ID。

无论个人设置如何，所有 IAM 用户和 IAM 角色均可查看创建的具有较长 ID 的资源，前提是他们拥有查看相关资源类型的权限。

#### 主题

- [使用较长的 ID \(p. 731\)](#)
- [控制对较长 ID 设置的访问 \(p. 733\)](#)

## 使用较长的 ID

您可以为自己或账户中的其他 IAM 用户、IAM 角色和根用户查看和修改较长的 ID 设置。

#### 主题

- [查看和修改较长的 ID 设置 \(p. 731\)](#)
- [查看和修改特定用户或角色的较长 ID 设置 \(p. 733\)](#)

## 查看和修改较长的 ID 设置

您可以使用 Amazon EC2 控制台或 AWS CLI 查看支持长 ID 的资源类型，并为自己启用或禁用较长的 ID 格式。本节中的程序适用于已登录控制台或提出请求的 IAM 用户或 IAM 角色，但不适用于整个 AWS 账户。

### 使用控制台查看和修改较长的 ID 设置

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在屏幕顶部的导航栏中，会显示当前区域。选择要查看或更改其较长 ID 设置的区域。设置不在区域之间共享。
3. 在控制面板中的 Account Attributes 下，选择 Resource ID length management。将列出支持较长 ID 的资源类型。您将自动切换为对每个资源类型使用较长 ID 的日期将在 Deadline 列中显示。
4. 要为支持的资源类型启用较长 ID 格式，请选中 Use Longer IDs 列的复选框。要禁用较长 ID 格式，请清除此复选框。



#### Important

如果您作为根用户登录，这些设置将适用于整个账户，除非 IAM 用户或角色登录并明确为其覆盖这些设置。无论个人设置如何，创建的具有较长 ID 的资源对所有 IAM 用户可见，只要他们有权查看相关资源类型。

### 使用 AWS CLI 查看和修改较长的 ID 设置

要查看所有受支持资源的较长 ID 设置，请使用 [describe-id-format](#) AWS CLI 命令：

```
aws ec2 describe-id-format

{
 "Statuses": [
 {
 "Deadline": "2016-11-01T13:00:00.000Z",
 "UseLongIds": false,
 "Resource": "instance"
 },
 {
 "Deadline": "2016-11-01T13:00:00.000Z",
 "UseLongIds": true,
 "Resource": "reservation"
 },
 {
 "Deadline": "2016-11-01T13:00:00.000Z",
 "UseLongIds": false,
 "Resource": "volume"
 },
 {
 "Deadline": "2016-11-01T13:00:00.000Z",
 "UseLongIds": false,
 "Resource": "snapshot"
 }
]
}
```

结果适用于提出请求的 IAM 用户、IAM 角色或根用户，但不适用于整个 AWS 账户。上述结果表明，`instance`、`reservation`、`volume` 和 `snapshot` 资源类型可启用或禁用较长 ID；`reservation` 资源已启用。`Deadline` 字段指明您将自动切换为对该资源使用较长 ID 的日期（采用 UTC 表示）。如果截止日期尚不可用，则不会返回此值。

要为指定的资源启用较长 ID，请使用 [modify-id-format](#) AWS CLI 命令：

```
aws ec2 modify-id-format --resource resource-type --use-long-ids
```

要为指定的资源禁用较长 ID，请使用 [modify-id-format](#) AWS CLI 命令：

```
aws ec2 modify-id-format --resource resource-type --no-use-long-ids
```

如果您以根用户的身份使用这些操作，则这些设置将适用于整个账户，除非 IAM 用户或角色明确为其覆盖这些设置。这些命令仅应用于单个区域。要修改其他区域的设置，请在命令中使用 `--region` 参数。



#### Note

在 2015-10-01 版本的 Amazon EC2 API 中，如果您使用 IAM 角色凭证调用 `describe-id-format` 或 `modify-id-format`，结果将适用于整个 AWS 账户，而不是特定的 IAM 角色。在当前版本的 Amazon EC2 API 中，结果仅适用于 IAM 角色。

或者，您可以使用以下命令：

#### 描述 ID 格式

- [DescribeIdFormat](#) (Amazon EC2 API)
- [Get-EC2IdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

#### 修改 ID 格式

- [ModifyIdFormat](#) (Amazon EC2 API)
- [Edit-EC2IdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

## 查看和修改特定用户或角色的较长 ID 设置

使用 `describe-identity-id-format` 和 `modify-identity-id-format` AWS CLI 命令，您可以查看受支持的资源类型，并为您账户中的特定 IAM 用户、IAM 角色或根用户启用较长 ID 设置。要使用这些命令，您必须在请求中指定 IAM 用户、IAM 角色或根账户用户的 ARN。例如，在账户 123456789012 中，角色“EC2Role”的 ARN 为 `arn:aws:iam::123456789012:role/EC2Role`。有关更多信息，请参阅 [IAM 用户指南](#) 中的 [委托人](#)。

要查看特定 IAM 用户或 IAM 角色的所有受支持资源的较长 ID 设置，请使用以下 AWS CLI 命令：

```
aws ec2 describe-identity-id-format --principal-arn arn-of-iam-principal
```

要为特定 IAM 用户或 IAM 角色的特定资源启用较长 ID 设置，请使用以下 AWS CLI 命令：

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --resource resource-type --use-long-ids
```

这些命令适用于请求中指定的 ARN，但不适用于提出请求的 IAM 用户、IAM 角色或根用户。

或者，您可以使用以下命令：

#### 描述 ID 格式

- [DescribeIdentityIdFormat](#) (Amazon EC2 API)
- [Get-EC2IdentityIdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

#### 修改 ID 格式

- [ModifyIdentityIdFormat](#) (Amazon EC2 API)
- [Edit-EC2IdentityIdFormat](#) (适用于 Windows PowerShell 的 AWS 工具)

## 控制对较长 ID 设置的访问

默认情况下，IAM 用户和角色没有使用 `ec2:DescribeIdFormat`、`ec2:DescribeIdentityIdFormat`、`ec2:ModifyIdFormat` 和 `ec2:ModifyIdentityIdFormat` 操作的权限，除非他们通过关联的 IAM 策略明确获得了相应权限。例如，通过在策略语句中添加 `Action": "ec2:*` 元素可授予 IAM 角色使用所有 Amazon EC2 操作的权限。

为防止 IAM 用户和角色查看或修改其自身或您账户中的其他用户和角色的较长资源 ID 设置，请确保 IAM 策略包含以下语句：

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "ec2:ModifyIdFormat",
 "ec2:DescribeIdFormat",
 "ec2:ModifyIdentityIdFormat",
 "ec2:DescribeIdentityIdFormat"
],
 "Resource": "*"
 }
]
}
```

对于 `ec2:DescribeIdFormat`、`ec2:DescribeIdentityIdFormat`、`ec2:ModifyIdFormat` 和 `ec2:ModifyIdentityIdFormat` 操作，我们不支持资源级权限。

## 列出并筛选您的资源

### Abstract

列出并筛选您的其他可用 AWS 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。如果您拥有很多资源，可以筛选结果以仅包含符合特定标准的资源。

#### 主题

- [高级搜索 \(p. 734\)](#)
- [使用控制台列出资源 \(p. 735\)](#)
- [使用控制台筛选资源 \(p. 736\)](#)
- [使用 CLI 和 API 列出并筛选 \(p. 737\)](#)

## 高级搜索

高级搜索使您可以通过组合筛选条件执行搜索，从而获得精确的结果。您可以按关键字、用户定义的标签键和预定义资源属性进行筛选。

可用的特定搜索类型有：

- [按关键字搜索](#)

要按关键字进行搜索，请在搜索框中键入或粘贴要查找的内容，然后选择 Enter。例如，要搜索特定实例，可以键入实例 ID。

- [按字段搜索](#)

也可以按与资源关联的字段、标签和属性进行搜索。例如，若要查找处于停止状态的所有实例：

1. 在搜索框中，开始键入 `Instance State`。随着您的键入，将显示建议字段的列表。
2. 从列表中选择 `Instance State` (实例状态)。
3. 从建议值列表中选择 `Stopped` (已停止)。
4. 要进一步优化您的列表，请选择搜索框以获得更多搜索选项。

- 高级搜索

可以通过添加多个筛选器创建高级查询。例如，可以按标签进行搜索，并查看生产堆栈中运行的 Flying Mountain 项目的实例，然后按属性搜索以查看所有 t2.micro 实例，或查看 us-west-2a 中的所有实例，或者查看同时符合这两个条件的实例。

- 逆向搜索

您可以搜索与特定值不匹配的资源。例如，要列出未终止的所有实例，可按 Instance State(实例状态) 字段进行搜索，并为已终止值添加惊叹号前缀 (!)。

- 部分搜索

按字段进行搜索时，还可以输入部分字符串以查找字段中包含该字符串的所有资源。例如，先按 Instance Type (实例类型) 搜索，然后键入 t2 以查找所有 t2.micro、t2.small 或 t2.medium 实例。

- 正则表达式

当需要匹配字段中具有特定模式的值时，可以使用正则表达式。例如，先按名称标签搜索，然后键入 ^s.\* 以查看其名称标签以“s”开头的所有实例。正则表达式搜索不区分大小写。

获得搜索的精确结果之后，您可以为 URL 添加书签以便于参考。在具有数千实例的情况下，筛选条件和书签可以为您节省大量时间；您不必重复运行搜索。

#### 结合搜索筛选条件

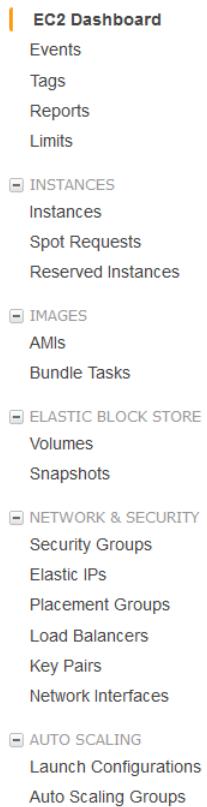
通常，具有相同键字段（例如，tag:Name、search、Instance State）的多个筛选条件会自动以 OR 运算符联接。这是特意设计的，因为绝大部分筛选条件如果以 AND 运算符联接将不合逻辑。例如，如果以“Instance State=running AND Instance State=stopped”为条件进行搜索，将返回零个结果。在许多情况下，您可以对不同键字段使用补充性搜索词来细化搜索结果，此时将自动改用 AND 规则。如果您搜索“tag: Name:=All values AND tag:Instance State=running”，您将获得包含这两个条件的搜索结果。要优化结果，您只需删除字符串中的一个筛选条件，直到结果符合您的要求。

## 使用控制台列出资源

您可以使用控制台查看最常用的 Amazon EC2 资源类型。要查看其他资源，请使用命令行界面或 API 操作。

#### 要使用控制台列出 EC2 资源

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/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 `cn-north-1b` 可用区域中状态为 `available` 的卷

1. 在导航窗格中，选择 Volumes。
2. 单击搜索框，从菜单中选择 Attachment Status (连接状态)，然后选择 Detached (已断开)。（分离的卷可附加到同一个可用区域中的某个实例上。）
3. 再次单击搜索框，选择 State (状态)，然后选择 Available (可用)。
4. 再次单击搜索框中，选择 Availability Zone (可用区)，然后选择 `cn-north-1b`。
5. 会显示所有符合此标准的卷。

列出由 Amazon EBS 支持的 64 位公有 Windows AMI

1. 在导航窗格中，选择 AMIs。

2. 在 Filter (筛选条件) 窗格中，从 Filter (筛选条件) 列表中依次选择 Public images (公有映像)、EBS images (EBS 映像) 和您的 Windows。
3. 在搜索字段中输入 x86\_64。
4. 会显示所有符合此标准的卷。

## 使用 CLI 和 API 列出并筛选

每个资源类型都有相应的 CLI 命令或 API 请求，您可用来列出该类型的资源。例如，使用 `ec2-describe-images` 或 `DescribeImages` 可以列出 Amazon 系统映像 (AMI)。响应中包含您所有资源的信息。

资源的结果列表可能很长，建议您筛选结果以使结果中只留下符合一定标准的资源。您可以指定多个筛选值，也可以指定多个筛选条件。例如，您可以列出类型为 `m1.small` 或 `m1.large` 的所有实例，以及附加了一个被设置为在实例终止时删除的 EBS 卷的所有实例。该实例必须与结果中所包含的您的所有筛选条件相匹配。



### Note

如果使用标签筛选条件，响应将包含您的资源的标签；否则，响应中将省略标签。

您还可以将通配符与筛选值一同使用。星号 (\*) 匹配的是零或更多字符，问号 (?) 恰好匹配一个字符。例如，您可以将 `*database*` 用作筛选值以获取描述中包含 `database` 的所有 EBS 快照。如果您要将 `database` 指定为筛选值，则只能返回描述为 `database` 的快照。筛选值区分大小写。我们只支持字符串精确匹配或子字符串匹配（带通配符）。如果得到的资源列表很长，使用精确的字符串筛选条件可能会更快返回响应。



### Tip

您的搜索中可包含通配符的字面值；您只需要在字符前用反斜线隔开字符。例如，用 `\*amazon\?\\\值` 搜索文字字符串 `*amazon?*`。

有关每个 Amazon EC2 资源支持的筛选器列表，请参阅相关文档：

- 对于 AWS CLI，请参阅 [AWS Command Line Interface Reference](#) 中的相关命令。
- 对于 Windows PowerShell，请参阅 [适用于 Windows PowerShell 的 AWS 工具 Reference](#) 中的相关 `Get` 命令。
- 对于查询 API，请参阅 [Amazon EC2 API Reference](#) 中的相关 API 操作。

## 标记 Amazon EC2 资源

### Abstract

为每个 Amazon EC2 资源分配您自己的元数据标签，以管理您的实例、映像以及其他资源。

为了方便管理您的实例、映像以及其他 Amazon EC2 资源，您可以选择通过标签的形式为每个资源分配您自己的元数据。本主题介绍标签并说明如何创建标签。

### 内容

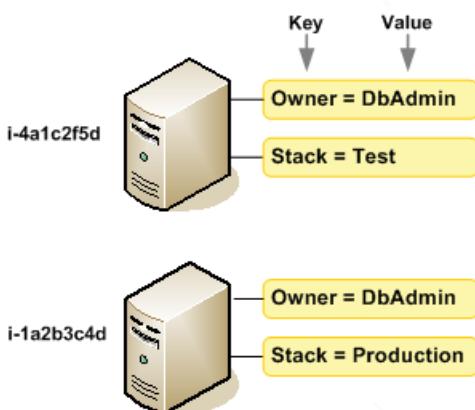
- [有关标签的基本知识 \(p. 738\)](#)
- [标签限制 \(p. 738\)](#)
- [标记资源以便于计费 \(p. 740\)](#)

- 通过控制台使用标签 (p. 740)
- 通过 CLI 或 API 使用标签 (p. 745)

## 有关标签的基本知识

标签可让您按各种标准（例如用途、所有者或环境）对 AWS 资源进行分类。这在您具有相同类型的许多资源时会很有用 — 您可以根据分配给资源的标签快速识别特定资源。每个标签都包含您定义的一个键和一个可选值。例如，您可以为账户中的 Amazon EC2 实例定义一组标签，以跟踪每个实例的所有者和堆栈级别。我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签密钥，管理资源时会更加轻松。您可以根据添加的标签搜索和筛选资源。

下图说明了标签的工作方式。在此示例中，您为每个实例分配了两个标签，一个是 Owner，另一个是 Stack。各个标签都拥有相关的值。



标签对 Amazon EC2 没有任何语义意义，应严格按字符串进行解析。同时，标签不会自动分配至您的资源。

您可以通过 AWS 管理控制台、Amazon EC2 命令行界面 (CLI)、AWS CLI 和 Amazon EC2 API 来使用标签。

您只能向已经存在的资源分配标签。在创建资源时无法分配标签；例如，当您使用 `run-instances` AWS CLI 命令时。当您使用 Amazon EC2 控制台时，您能够利用一些资源创建屏幕指定在创建资源之后立即应用的标签。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。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 IAM 的更多信息，请参阅 [控制对 Amazon EC2 资源的访问 \(p. 522\)](#)。

## 标签限制

下面是适用于标签的基本限制：

- 每个资源的标签数上限 - 10
- 最大密钥长度 - 127 个 Unicode 字符（采用 UTF-8 格式）
- 最大值长度 - 255 个 Unicode 字符（采用 UTF-8 格式）
- 标签密钥和值要区分大小写。

- 请勿在标签名称或值中使用 aws: 前缀，因为它专为 AWS 使用预留。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。
- 如果您的标记方案将在多个服务和资源中使用，请记得其他服务可能对允许使用的字符有限制。通常允许使用的字符包括：可用 UTF-8 格式表示的字母、空格和数字以及特殊字符 + - = . : / @。

您不能仅依据标签终止或删除资源，而必须指定资源的标识符。例如，要删除您使用名为 DeleteMe 的标签密钥标记的快照，您必须将 DeleteSnapshots 操作与快照的资源标识符（如 snap-1234567890abcdef0）结合使用。要按资源的标签标识资源，您可以使用 DescribeTags 操作列出您的所有标签及其相关资源。您也可以按资源类型或标签密钥和值进行筛选。您不能通过指定标签的筛选器调用 DeleteSnapshots。要了解有关使用筛选器列出资源的更多信息，请参阅 [列出并筛选您的资源 \(p. 734\)](#)。

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。

您不能标记所有资源，且部分资源只能通过 API 操作或命令行进行标记。下表列出了所有 Amazon EC2 资源和适用于这些资源的标记限制（如果有）。无标记限制的资源可通过 API 操作、CLI 和控制台来进行标记。

| 资源                | 标记支持 | 标记限制 |
|-------------------|------|------|
| AMI               | 是    | 无    |
| 捆绑任务              | 否    |      |
| 客户网关              | 是    | 无    |
| 专用主机              | 否    |      |
| DHCP 选项           | 是    | 无    |
| EBS 卷             | 是    | 无    |
| 实例存储卷             | 否    |      |
| 弹性 IP             | 否    |      |
| 实例                | 是    | 无    |
| Internet 网关       | 是    | 无    |
| 密钥对               | 否    |      |
| NAT 网关            | 否    |      |
| 网络 ACL            | 是    | 无    |
| 网络接口              | 是    | 无    |
| 置放群组              | 否    |      |
| Reserved Instance | 是    | 无    |
| 预留实例示例            | 否    |      |
| 路由表               | 是    | 无    |
| 竞价型实例请求           | 是    | 无    |
| 安全组 - EC2-Classic | 是    | 无    |
| 安全组 – VPC         | 是    | 无    |

| 资源           | 标记支持 | 标记限制 |
|--------------|------|------|
| 快照           | 是    | 无    |
| 子网           | 是    | 无    |
| 虚拟专用网关       | 是    | 无    |
| VPC          | 是    | 无    |
| VPC endpoint | 否    |      |
| VPC 流日志      | 否    |      |
| VPC 对等连接     | 是    | 无    |
| VPN 连接       | 是    | 无    |

有关如何使用 AWS 管理控制台进行标记的更多信息，请参阅[通过控制台使用标签 \(p. 740\)](#)。有关如何使用 API 或命令行进行标记的更多信息，请参阅[通过 CLI 或 API 使用标签 \(p. 745\)](#)。

## 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。有关设置包含标签的成本分配报告的更多信息，请参阅 *AWS Account Billing* 简介中的[设置月度成本分配报告](#)。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。要了解更多信息，请参阅 *About AWS Account Billing* 部分的 [Cost Allocation and Tagging](#)。



### Note

如果您刚刚启用了报告，则可以在大约 24 小时内查看当月的数据。

## 通过控制台使用标签

通过 Amazon EC2 控制台，您可以查看同一区域中哪些标签是所有 Amazon EC2 资源都使用的。您可以按资源和资源类型来查看资源，也可以查看与指定标签相关的每种资源类型的项目数量。您还可以通过 Amazon EC2 控制台同时在一个或多个资源中应用或删除标签。

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 [AWS 管理控制台入门](#) 中的[使用标签编辑器](#)。

### 内容

- [显示标签 \(p. 740\)](#)
- [为单个资源添加和删除标签 \(p. 741\)](#)
- [为一组资源添加和删除标签 \(p. 742\)](#)
- [在启动实例时添加标签 \(p. 744\)](#)
- [按标签筛选资源列表 \(p. 744\)](#)

## 显示标签

您可以在 Amazon EC2 控制台中以两种不同的方式显示标签。您可以显示单个资源或所有资源的标签。

### 显示单个资源的标签

当您在 Amazon EC2 控制台中选择特定资源页面时，它会显示这些资源列表。例如，如果您在导航窗格中选择 Instances，则控制台会显示 Amazon EC2 实例列表。当您从其中一个列表中选择一种资源时（例如，实例），如果该资源支持标签，则您可以查看和管理标签。在大多数资源页面上，您可以在详细信息窗格的 Tags (标签) 选项卡中查看标签。

您可以在资源列表中添加列，以显示密钥相同的标签的所有值。通过该列，您可以按照标签对资源列表进行分类和筛选。资源列表中添加新列以显示标签的方法有两种。

- 在 Tags 选项卡上，选择 Show Column。新列将添加到控制台中。
- 选择 Show/Hide Columns 齿轮状图标，然后在 Show/Hide Columns 对话框中的 Your Tag Keys 下选择标签密钥。

### 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。

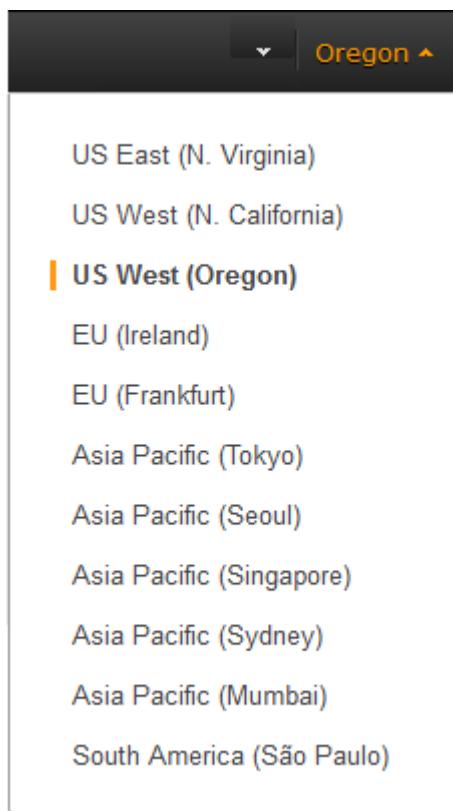
| Tag Key    | Tag Value | Total              | Instances | AMIs | Volumes |
|------------|-----------|--------------------|-----------|------|---------|
| Manage Tag | Name      | DNS Server         | 1         | 1    | 0       |
| Manage Tag | Owner     | TeamB              | 2         | 0    | 2       |
| Manage Tag | Owner     | TeamA              | 2         | 0    | 2       |
| Manage Tag | Purpose   | Project2           | 1         | 0    | 1       |
| Manage Tag | Purpose   | Logs               | 1         | 0    | 1       |
| Manage Tag | Purpose   | Network Management | 1         | 1    | 0       |
| Manage Tag | Purpose   | Project1           | 2         | 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.amazonaws.cn/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 729\)](#)。



3. 在导航窗格中，选择资源类型（例如，Instances）。
4. 从资源列表中选择资源。
5. 在详细信息窗格中，选择 Tags (标签) 选项卡。
6. 选择 Add/Edit Tags 按钮。
7. 在 Add/Edit Tags 对话框中，为每个标签指定密钥和值，然后选择 Save。

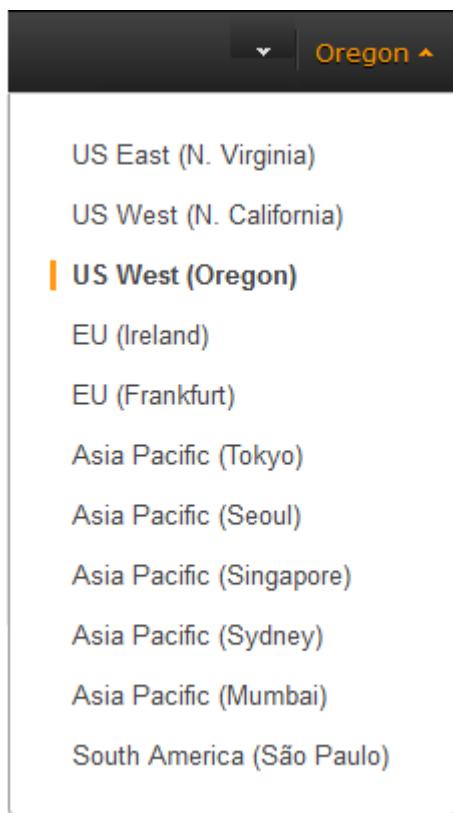
#### 删除单个资源的标签

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 729\)](#)。
3. 在导航窗格中，选择资源类型（例如，Instances）。
4. 从资源列表中选择资源。
5. 在详细信息窗格中，选择 Tags (标签) 选项卡。
6. 依次选择 Add/Edit Tags、与标签对应的 Delete 图标和 Save。

## 为一组资源添加和删除标签

#### 为一组资源添加标签

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 729\)](#)。



3. 在导航窗格中，选择 Tags。
4. 在内容窗格的顶部，选择 Manage Tags。
5. 在 Filter (筛选条件) 下拉列表中，选择您要添加标签的资源类型（例如，实例）。
6. 在资源列表中，选中您要添加标签的资源旁边的复选框。
7. 在 Add Tag 下的 Key 和 Value 框中，键入所需的标签密钥和值，然后选择 Add Tag。



#### Note

如果您添加的新标签的标签密钥与现有标签的相同，则新标签将覆盖现有标签。

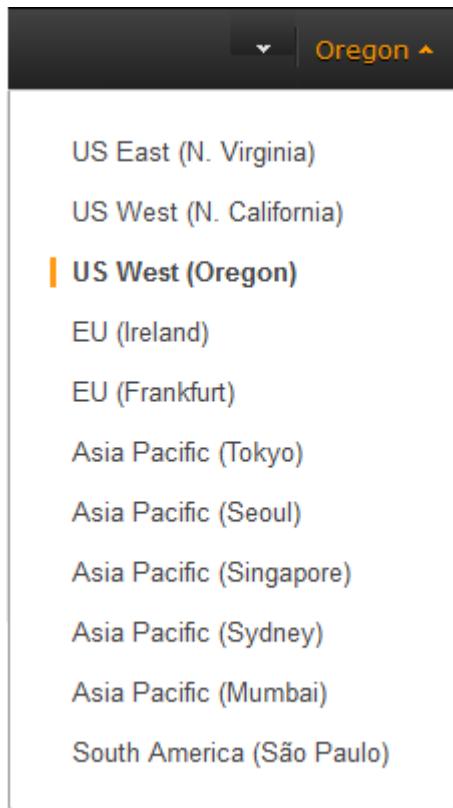
### 删除一组资源的标签

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏，选择符合需要的地区。这一选择很重要，这是因为有些 Amazon EC2 资源可以在区域之间共享，另一些却不能。有关更多信息，请参阅[资源位置 \(p. 729\)](#)。
3. 在导航窗格中，选择 Tags。
4. 在内容窗格的顶部，选择 Manage Tags。
5. 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，选择您要查看的标签密钥，然后选择 Close。
6. 在 Filter (筛选条件) 下拉列表中，选择您要删除标签的资源类型（例如，实例）。
7. 在资源列表中，选中您要删除标签的资源旁边的复选框。
8. 在 Remove Tag 下的 Key 框中键入标签的名称，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

- 从导航栏中选择实例地区。该选择很重要，这是因为有些 Amazon EC2 资源可以在区域间共享，另一些却不能。请选择能满足您的需求的区域。有关更多信息，请参阅 [资源位置 \(p. 729\)](#)。



- 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。选择您要使用的 AMI，然后选择 Select。有关选择 AMI 的更多信息，请参阅 [查找 Windows AMI \(p. 65\)](#)。
- 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。完成时选择 Next: Tag Instance。
- 在 Tag Instance (标签实例) 页面上，通过提供密钥和值组合为实例指定标签。选择 Create 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密钥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：

- a. 选择一种资源。
  - b. 在详细信息窗格中，选择 Tags (标签) 选项卡。
  - c. 在列表中查找标签，然后选择 Show Column。
2. 选择标签列右上角的筛选图标，以显示筛选列表。
3. 选择标签值，然后选择 Apply Filter 以筛选结果列表。



#### Note

有关筛选条件的更多信息，请参阅[列出并筛选您的资源 \(p. 734\)](#)。

## 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 Power-Shell 的 AWS 工具 | API 操作                       |
|---------------|-------------------------------|----------------------------------|------------------------------|
| 添加或覆盖一个或多个标签。 | <a href="#">create-tags</a>   | <a href="#">New-EC2Tag</a>       | <a href="#">CreateTags</a>   |
| 删除一个或多个标签。    | <a href="#">delete-tags</a>   | <a href="#">Remove-EC2Tag</a>    | <a href="#">DeleteTags</a>   |
| 描述一个或多个标签。    | <a href="#">describe-tags</a> | <a href="#">Get-EC2Tag</a>       | <a href="#">DescribeTags</a> |

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。

**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
```



#### Important

如果您在描述资源时未使用标签筛选条件，则结果可能不会为您的资源返回标签。为确保在结果中返回标签，建议您描述标签（并在必要时使用资源筛选条件）或描述您的资源并使用一个或多个标签筛选条件。

# Amazon EC2 服务限制

## Abstract

查看您的 Amazon EC2 的当前限制；并根据需要请求提高这些限制。

Amazon EC2 提供您可使用的不同资源。这些资源包括映像、实例、卷和快照。在创建 AWS 账户时，我们根据区域设置对这些资源的默认限制。举例来说，对您可在某一区域中启动的实例数存在限制。因此，在美国西部（俄勒冈）区域启动实例时，请求一定不能导致您的用量超出您在该区域的当前实例限制。

Amazon EC2 控制台提供了对 Amazon EC2 和 Amazon VPC 控制台管理的资源的限制信息。您可以请求提高这些限制的值。使用我们提供的限制信息可管理您的 AWS 基础设施。需要时请提前计划请求提高限制。

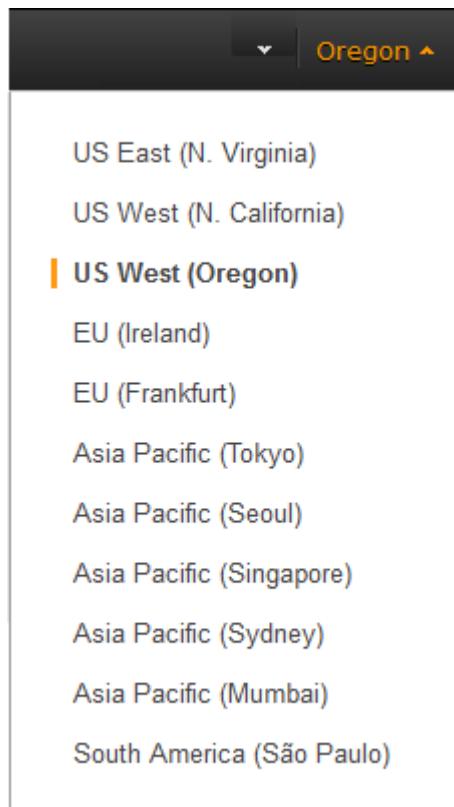
有关其他服务的限制的更多信息，请参阅 *Amazon Web Services General Reference* 中的 [AWS 服务限制](#)。

## 查看当前限制

使用 Amazon EC2 控制台中的 EC2 Service Limits (EC2 服务限制) 页面可按区域查看 Amazon EC2 和 Amazon VPC 提供的资源的当前限制。

### 查看当前限制

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中选择区域。



3. 从导航窗格中，选择 Limits。
4. 在列表中找到资源。Current Limit (当前限制) 列显示您的账户对该资源的当前最大限制。

## 申请提高限制

使用 Amazon EC2 控制台中的 Limits (限制) 页面可按区域申请提高 Amazon EC2 或 Amazon VPC 提供的资源的限制。

### 申请提高限制

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 Limits。
4. 在列表中找到资源。选择 Request limit increase。
5. 填写提高限制表格中的必填字段。我们将通过您指定的联系方式进行响应。

## Amazon EC2 使用率报告

### Abstract

使用 Amazon EC2 使用率报告可分析您的实例使用率。

通过 Amazon EC2 提供的使用率报告，您可以深入分析您实例的使用率。使用率报告中的数据每天会多次更新。您可以按 AWS 账户、区域、可用区、操作系统、实例类型、购买选项、租期和标签筛选报告。

要获取账户的使用率和成本数据，您必须具有其账户证书并为账户启用包含资源和标签的详细账单报告。如果您使用整合账单并登录到付款人账户，可以查看付款人账户及其所有关联账户的数据。如果您使用整合账单并登录到关联账户之一，只能查看该关联账户的数据。有关整合账单的信息，请参阅[使用整合账单为多个账户支付账单](#)。

### 主题

- [可用报告 \(p. 747\)](#)
- [开始设置使用率报告 \(p. 747\)](#)
- [向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限 \(p. 749\)](#)
- [实例使用率报告。 \(p. 750\)](#)
- [预留实例使用率报告 \(p. 753\)](#)

## 可用报告

您可以生成以下报告：

- [实例使用率报告 \(p. 750\)](#)。此报告包括按需实例、竞价型实例和预留实例的使用率。
- [预留实例使用率报告 \(p. 753\)](#)。此报告包括容量预留的使用率。

要查看报告，请打开 AWS 管理控制台。在导航窗格中，选择 Reports，然后选择您希望查看的报告。

## 开始设置使用率报告

在开始之前，请按以下过程所示，启用包含资源和标签的详细账单报告。完成此过程之后，我们将开始为实例收集使用率数据。如果您已启用了详细账单报告，则可以访问我们自您启用它们以来收集的使用率数据。



### Important

要完成这些过程，必须使用 AWS 账户证书登录。如果使用 IAM 用户证书登录，则无法完成这些过程。

#### 启用详细账单报告

1. 选择现有 Amazon S3 存储桶以接收使用率数据。请务必管理对此存储桶的访问，因为它包含账单数据。（我们不要求您保留这些文件；事实上，如果不需它们，您可以立即将它们删除。）如果您没有存储桶，请按如下所示创建一个：
  - a. 打开 Amazon S3 控制台。
  - b. 选择 Create Bucket。
  - c. 在 Create a Bucket 对话框中，为您的存储桶输入一个名称（例如 `用户名-ec2-usage-data`），选择一个区域，然后选择 Create。有关存储桶名称要求的更多信息，请参阅 *Amazon Simple Storage Service 控制台用户指南* 中的 [创建存储桶](#)。
2. 打开账单和成本管理控制台 <https://console.amazonaws.cn/billing/home?#>。
3. 在导航窗格中选择 Preferences。
4. 选择 Receive Billing Reports (接收账单报告)。
5. 在 Save to S3 Bucket 中指定您的 Amazon S3 存储桶的名称，然后选择 Verify。
6. 授予 AWS 权限以将使用率数据发布到 Amazon S3 存储桶。
  - a. 在 Receive Billing Reports 下，选择 sample policy。复制示例策略。请注意，示例策略使用您指定的存储桶名称。
  - b. 在另一个浏览器选项卡打开 Amazon S3 控制台。选择您的存储桶，选择 Properties，然后展开 Permissions。在 Permissions 部分，选择 Add bucket policy。将示例策略粘贴到文本区域中，然后选择 Save。在 Permissions 部分，选择 Save。
  - c. 返回包含示例策略的浏览器选项卡并选择 Done。
7. 在 Report (报告) 下，选择 Detailed billing report with resources and tags (包含资源和标签的详细账单报告)。
8. 选择 Save preferences。



### Note

最多需要一天，您就可以查看报告中的数据。

可以使用标签对实例分类。标记实例之后，您必须启用有关这些标签的报告。

#### 启用按标签进行的使用率报告

1. 标记您的实例。为了获得最佳结果，请确保您将计划用于报告的每个标签添加到每个实例。有关如何标记实例的更多信息，请参阅 [标记 Amazon EC2 资源 \(p. 737\)](#)。
2. 打开账单和成本管理控制台 <https://console.amazonaws.cn/billing/home?#>。
3. 在导航窗格中，选择 Preferences。
4. 在 Report 下，选择 Manage report tags。
5. 页面显示您已创建的标签列表。选择要用于对实例使用率数据进行筛选或分组的标签，然后单击 Save (保存)。我们自动从实例使用率报告中排除您未选择的所有标签。



#### Note

我们仅将这些更改应用于当前月的数据。这些更改最多一天就会生效。

## 向 IAM 用户授予对 Amazon EC2 使用率报告的访问权限

默认情况下，IAM 用户无法访问 Amazon EC2 使用率报告。必须创建向 IAM 用户授予访问这些报告的权限的 IAM 策略。

以下策略允许用户查看两个 Amazon EC2 使用率报告。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2-reports:*",
 "Resource": "*"
 }
]
}
```

以下策略允许用户查看实例使用率报告。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2-reports:ViewInstanceUsageReport",
 "Resource": "*"
 }
]
}
```

以下策略允许用户查看预留实例使用率报告。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2-reports:ViewReservedInstanceUtilizationReport",
 "Resource": "*"
 }
]
}
```

有关更多信息，请参阅 [IAM 用户指南 中的权限与策略](#)。

## 实例使用率报告。

### Abstract

以报告形式查看您的实例使用率。

您可以使用实例使用率报告查看实例使用率和成本趋势。可以按实例小时数或成本查看使用率数据。可以选择查看使用率数据的每小时、每日和每月汇总。可以按区域、可用区、实例类型、AWS 账户、平台、租期、购买选项或标签对报告进行筛选或分组。配置报告之后，您可以对其添加标签，以方便以后返回。

下面是一些您可以通过创建实例使用率报告回答的问题的示例：

- 我在每种实例类型的实例上分别花费了多少？
- 特定部门使用的实例小时数是多少？
- 我的实例使用率在可用区间是如何分配的？
- 我的实例使用率在 AWS 账户间是如何分配的？

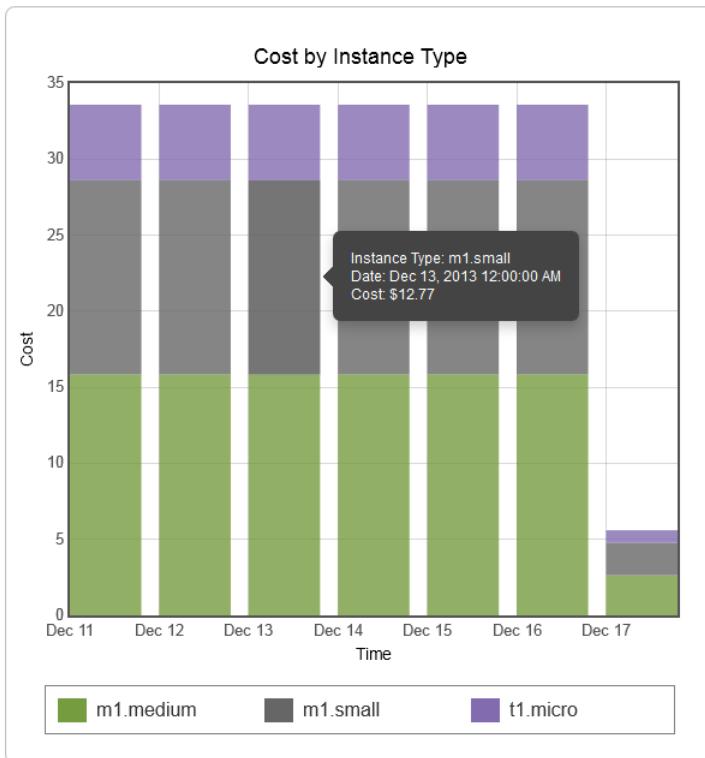
#### 主题

- [报告格式 \(p. 750\)](#)
- [查看实例使用率 \(p. 751\)](#)
- [为自定义报告添加书签 \(p. 753\)](#)
- [导出使用率数据 \(p. 753\)](#)

## 报告格式

我们同时以图和表的形式显示您请求的使用率数据。

例如，下图按实例类型显示成本。图的色例指示哪种颜色表示哪个实例类型。要获取有关条形图的分段的详细信息，请将鼠标悬停在它上方。



对应表为每种实例类型显示一列。请注意，我们在列标题中包含一个色带，其颜色与图中的实例类型相同。

| Time (UTC) | m1.medium | m1.small | t1.micro |
|------------|-----------|----------|----------|
| 12/11/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/12/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/13/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/14/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/15/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/16/13   | \$15.84   | \$12.77  | \$4.97   |
| 12/17/13   | \$2.64    | \$2.13   | \$0.83   |
| Total      | \$97.68   | \$78.75  | \$30.65  |

## 查看实例使用率

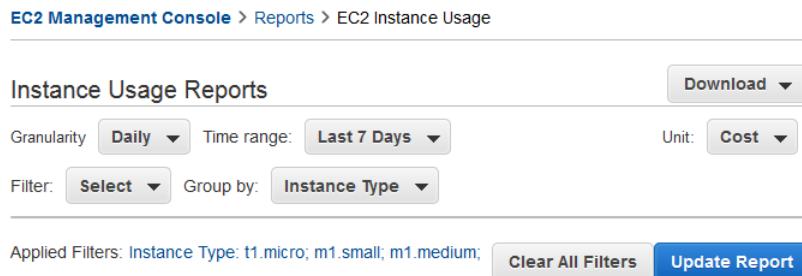
以下过程演示如何使用我们提供的一些功能生成使用率报告。

开始之前，您必须进行设置。有关更多信息，请参阅 [开始设置使用率报告 \(p. 747\)](#)。

按实例类型对实例使用率进行筛选和分组

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Reports，然后选择 EC2 Instance Usage Report。

3. 为 Unit (单位) 选择选项。要查看实例已运行的时间 (以小时为单位)，请选择 Instance Hours。要查看实例使用率的成本，请选择 Cost。
4. 为 Granularity (粒度) 和 Time range (时间范围) 选择选项。
  - 要查看针对时间范围内每小时汇总的数据，请选择 Hourly 粒度。查看每小时数据时，可以选择多达 2 天的时间范围。
  - 要查看针对时间范围内每天汇总的数据，请选择 Daily 粒度。查看每天数据时，可以选择多达 2 个月的时间范围。
  - 要查看针对时间范围内每个月汇总的数据，请选择 Monthly 粒度。
5. 在 Filter (筛选条件) 列表中，选择 Instance Type。在 Group by (分组依据) 列表中，选择 Instance Type。
6. 在筛选条件区域中，选择一个或多个实例类型，然后选择 Update Report。您指定的筛选条件会出现在 Applied Filters (应用的筛选条件) 下。



请注意，您可以通过选择页面顶部的 Reports 或 EC2 Management Console 返回 Amazon EC2 控制台。

#### 基于标签对实例使用率分组

1. 打开实例使用率报告页面。
2. 为 Unit (单位) 选择选项。要查看实例已运行的时间 (以小时为单位)，请选择 Instance Hours。要查看实例使用率的成本，请选择 Cost。
3. 为 Granularity (粒度) 和 Time range (时间范围) 选择选项。
  - 要查看针对时间范围内每小时汇总的数据，请选择 Hourly 粒度。查看每小时数据时，可以选择多达 2 天的时间范围。
  - 要查看针对时间范围内每天汇总的数据，请选择 Daily 粒度。查看每天数据时，可以选择多达 2 个月的时间范围。
  - 要查看针对时间范围内每个月汇总的数据，请选择 Monthly 粒度。
4. 在 Group by (分组依据) 列表中，选择 Tag (标签)。
5. 选择 Key Name 框，从列表中选择一个名称，然后选择 Update Report。如果此列表中没有项目，则您必须启用按标签分组的使用率报告。有关更多信息，请参阅 [启用按标签进行的使用率报告 \(p. 748\)](#)。

The screenshot shows the 'Instance Usage Reports' interface. At the top, there are dropdown menus for 'Granularity' (set to 'Daily'), 'Time range' (set to 'Last 14 Days'), and 'Unit' (set to 'Instance Hours'). Below these are 'Filter' and 'Group by' dropdowns, both set to 'Select'. A search bar 'Key Name: Project' is also present. At the bottom, there are buttons for 'Applied Filters: None', 'Clear All Filters', and 'Update Report'.

## 为自定义报告添加书签

您可能希望再次生成自定义报告。通过为报告添加书签可实现此目的。

### 向自定义报告添加书签

1. 为报告选择选项和筛选条件。您进行的每个选择都会向控制台 URL 添加一个参数。例如，`granularity=Hourly` 和 `Filters=filter_list`。
2. 使用浏览器将控制台 URL 添加为书签。
3. 将来若要生成相同的报告，请使用您创建的书签。

## 导出使用率数据

您可能希望在其他报告中包含您的报告图或表。通过导出数据可实现此目的。

### 导出使用率数据

1. 为报告选择选项和筛选条件。
2. 若要以 .csv 文件的形式从表中导出使用率数据，请单击 Download (下载) 并选择 CSV Only (仅 CSV)。
3. 若要以 .png 文件的形式导出图表使用率数据，请单击 Download (下载) 并选择 Graph Only (仅图表)。

## 预留实例使用率报告

### Abstract

使用预留实例使用率报告可查看您所购买的 Amazon EC2 预留实例的使用情况。

预留实例使用率报告描述您拥有的每组（或存储桶）Amazon EC2 预留实例在一段时间内的使用情况。每个存储桶都有区域、可用区、实例类型、租期、产品类型和平台的唯一组合。您可以指定报告涵盖的时间范围，从自定义范围到数周、数月、一年或三年。可用数据取决于您为账户启用详细账单报告的时间（请参阅[开始设置使用率报告 \(p. 747\)](#)）。预留实例使用率报告会将您为存储桶中所使用实例支付的预留实例价格与按需价格进行对比，并显示您在报告涵盖的时间范围内节省的成本。

要获取账户的使用率和成本数据，您必须具有其账户证书并为账户启用包含资源和标签的详细账单报告。如果您使用整合账单并登录到付款人账户，可以查看付款人账户及其所有关联账户的数据。如果您使用整合账单并登录到关联账户之一，只能查看该关联账户的数据。有关整合账单的信息，请参阅[使用整合账单为多个账户支付账单](#)。



### Note

预留实例存储桶使用与账单计算同样的方式跨 EC2-VPC 和 EC2-Classic 网络平台类型汇集预留实例。另外，存储桶中的预留实例可以会有不同的预付费用和小时价格。

下面是一些您可以使用预留实例使用率报告回答的问题的示例：

- 我使用预留实例的情况如何？
- 预留实例是否在帮助我节省开支？

开始之前，您必须进行设置。有关更多信息，请参阅 [开始设置使用率报告 \(p. 747\)](#)。

#### 主题

- [了解报告 \(p. 754\)](#)
- [查看预留实例使用率 \(p. 755\)](#)
- [为自定义报告添加书签 \(p. 756\)](#)
- [导出使用率数据 \(p. 756\)](#)
- [选项参考 \(p. 756\)](#)

## 了解报告

预留实例使用率报告显示以图和表格式显示您请求的使用率数据。

要查看报告，请打开 AWS 管理控制台。在导航窗格中，选择 Reports，然后选择 EC2 Reserved Instance Usage Report。

报告按存储桶汇集了特定时间内的预留实例使用率数据。在报告中，表格中的每一行代表一个存储桶，提供以下指标：

- Count (数量) - 报告周期内同一时间拥有的最高预留实例数。
- Usage Cost (使用率成本) - 预留实例存储桶的实例使用率所产生的总预留实例使用费。
- Total Cost (总成本) – 与预留实例存储桶关联的使用成本加上使用期的摊销预付费用。



#### Note

如果存储桶中包含您在预留实例市场上售出的预留实例，而该实例在报告期间内的某一时间点处于活动状态，则存储桶总成本可能会被夸大，而您的成本节省量可能会被低估。

- Savings (节省成本) – 相应时间段内采用按需价格时的预留实例使用成本与实际成本（总成本）之间的差异。
- Average Utilization (平均使用率) – 相应时间段内预留实例存储桶的平均每小时使用率。
- Maximum Utilization (最大使用率) - 报告期内任一小时的最高使用率。

对于表中的每行（即预留实例存储桶），在所选报告 Time range (时间范围) 内，图中基于所选 Show (显示) 指标表示数据。图中每个点代表一个时间点的指标。有关报告选项的信息，请参阅 [选项参考 \(p. 756\)](#)。

表中每个所选行边缘处的色带对应于图中的报告行。您可以通过选中行开头的复选框，在图中显示行。

默认情况下，预留实例使用率报告为所有预留实例存储桶返回最近 14 天内的数据。图中显示表中前五个存储桶的平均使用率。您可以自定义报告图以显示某个时间段（从 7 天到数周、数月或数年）内的不同使用率（平均使用率、最大使用率）或成本（总成本、使用率成本）数据。

## 自定义报告

您可以使用 Time range (时间范围) 和 Filter (筛选条件) 选项自定义预留实例使用率报告。

Time range 提供常用相对时间范围的列表，从 Last 7 Days 到 Last 3 Years。选择最适合您需要的时间范围，然后单击 Update Report (更新报告) 以应用更改。要应用不在该列表中的时间范围，请选择 Custom (自定义)，然后输入要运行报告的开始日期和结束日期。

通过 Filter 可以按以下一个或多个预留实例特性来限定预留实例使用率报告的范围：区域、实例类型、账户、平台、租期和产品类型。例如，您可以按区域、区域中的特定可用区或两者来进行筛选。要按区域进行筛选，请选择 Regions，然后选择您要在报告中包含的区域和可用区，并选择 Update Report。

如果不应用任何筛选条件，则报告将返回所有结果。

有关报告选项的信息，请参阅[选项参考 \(p. 756\)](#)。

## 查看预留实例使用率

在本部分中，我们将重点介绍图和表捕获的预留实例使用率的各个方面。为进行此讨论，我们将使用以下报告（该报告基于测试数据）。



此预留实例使用率报告显示最近两个月内的预留实例平均使用率。此报告显示有关账户的预留实例以及如何使用这些实例的以下信息。

- Average Utilization (平均使用率)

表中大多数预留实例的使用情况不错。最突出的是两个 m1.medium 中型使用率预留实例（第 2 行）（它们始终以 100% 平均使用率使用）以及 m1.xlarge（第 3 行）和 m1.small（第 4 行）大型使用率预留实例（它们也始终在使用）。相比之下，高计数大型使用率预留实例（第 5 行）的平均使用率较低。

同样值得注意的是，12 个 m1.large 中型利用率预留实例（第 1 行）平均仅在 27% 的时间内使用。

- Maximum Utilization (最大使用率)

在两个月时间段中的某个时间，所有预留实例都使用了 100%。

- Savings (节省成本)

从整体上来看，该报告显示对于此测试账户，使用预留实例而不是按需实例可为账户拥有者节省成本。

- 问题

该账户的 m1.large 中型使用率预留实例（第 1 行）是否太多？

## 为自定义报告添加书签

您可能希望再次生成自定义报告。通过为报告添加书签可实现此目的。

### 向自定义报告添加书签

1. 为报告选择选项和筛选条件。您进行的每个选择都会向控制台 URL 添加一个参数。例如，`granularity=Hourly` 和 `Filters=filter_list`。
2. 使用浏览器将控制台 URL 添加为书签。
3. 将来若要生成相同的报告，请使用您创建的书签。

## 导出使用率数据

您可能希望在其他报告中包含您的报告图或表。通过导出数据可实现此目的。

### 导出使用率数据

1. 为报告选择选项和筛选条件。
2. 若要以 .csv 文件的形式从表中导出使用率数据，请单击 Download (下载) 并选择 CSV Only (仅 CSV)。
3. 若要以 .png 文件的形式导出图表使用率数据，请单击 Download (下载) 并选择 Graph Only (仅图表)。

## 选项参考

使用 Show (显示) 选项可指定报告图要显示的指标。

- Average Utilization (平均使用率)

显示所选时间范围内每小时的平均使用率，其中存储桶一小时的使用率是用于该小时的实例小时数除以该小时内拥有的预留实例总数。

- Maximum Utilization (最大使用率)

显示所选时间范围内任何小时的最高使用率，其中存储桶一小时的使用率是用于该小时的实例小时数除以该小时内拥有的预留实例总数。

- 总费用

显示在生成报告的时间段内，存储桶中预留实例的使用率成本加上预付成本的摊销部分。

- Usage Cost (使用率成本)

基于每小时费用显示预留实例的所选存储桶的总成本。

使用 Time range (时间范围) 可指定报告所基于的时间段。



Note

所有时间都以 UTC 时间指定。

- 最近 7 天

显示在当前和前六个日历日中的使用率数据。可以与每天或每月粒度一起使用。

- 最近 14 天

显示在当前和前 13 个日历日中的使用率数据。可以与每天或每月粒度一起使用。

- 本月

显示在当前日历月中的使用率数据。可以与每天或每月粒度一起使用。

- 最近 3 个月

显示当前和前 2 个日历月中的使用率数据。可以与每天或每月粒度一起使用。

- 最近 6 个月

显示当前和前 5 个日历月中的使用率数据。可以与每月粒度一起使用。

- 最近 12 个月

显示当前和前 11 个日历月中的使用率数据。可以与每月粒度一起使用。

- 今年

显示在当前历年中的使用率数据。可以与每月粒度一起使用。

- 最近 3 年

显示当前和前两个历年中的使用率数据。可以与每月粒度一起使用。

- 自定义

显示输入的 Start (开始) 和 End (结束) 日期 (按 mm/dd/yyyy 格式指定) 之间的时间范围的数据。可以与每小时、每天或每月粒度一起使用，但是对于每小时数据只能指定最多两天的时间范围，对于每天数据只能指定最多两个月的时间范围，而对于每月数据只能指定最多三年的时间范围。

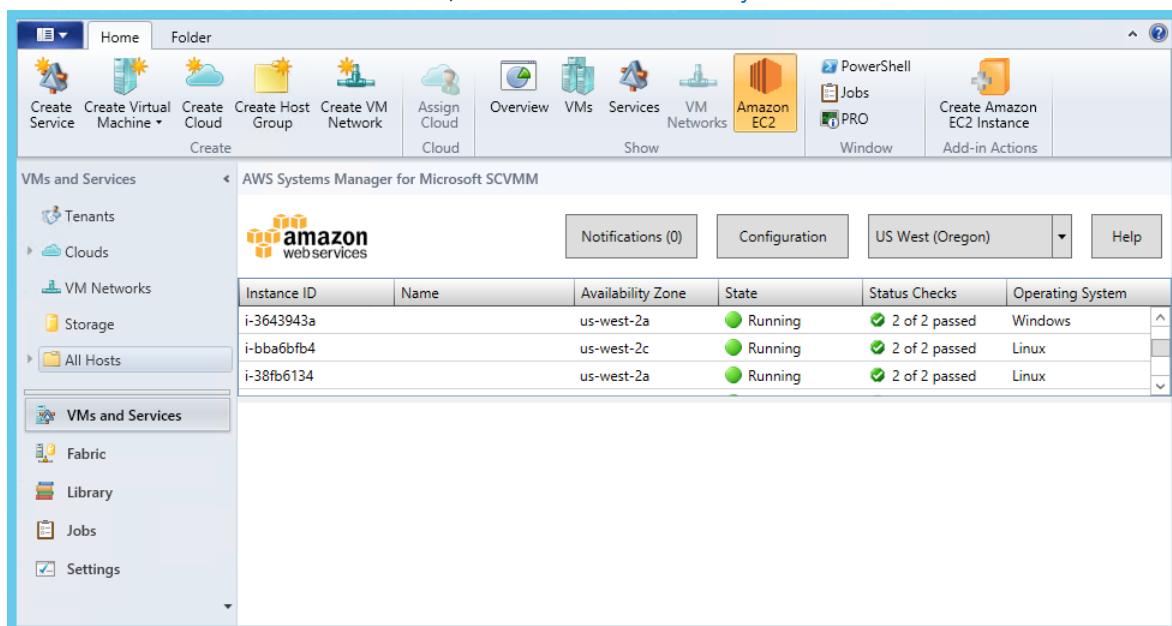
使用 Filter (筛选条件) 可限定报告中显示的数据的范围。

- 区域
- 实例类型
- 账户
- 平台
- 租期
- 产品类型

# AWS Systems Manager for Microsoft System Center VMM

---

Amazon Web Services (AWS) Systems Manager for Microsoft System Center Virtual Machine Manager (SCVMM) 为从 Microsoft SCVMM 管理 AWS 资源（如 EC2 实例）提供了简单易用的界面。该程序作为 VMM 控制台的插件实施。有关更多信息，请参阅[适用于 Microsoft System Center 的 AWS 插件](#)。



## 特色

- 管理员可以授权用户从 SCVMM 管理 EC2 实例。
- 如果用户具有所需权限，则可以启动、查看、重启、停止、开始和终止实例。
- 用户可以获得其 Windows 实例的密码并使用 RDP 连接到实例。
- 用户可以获取其 Linux 实例的公有 DNS 名称并使用 SSH 连接到这些实例。
- 用户可以将其 Hyper-V Windows 虚拟机从 SCVMM 导入到 Amazon EC2。

## 限制

- 用户必须具备能用于登录 SCVMM 的账户。
- 您不能将 EC2 实例启动到 EC2-Classic 中；您必须将这种实例启动到 VPC 中。
- 您不能将 Linux 虚拟机从 SCVMM 导入到 Amazon EC2。
- 它不是用于创建和管理 AWS 资源的全面工具。SCVMM 用户可借助插件，快速开始其 EC2 实例的基本管理任务。未来版本可能支持管理其他 AWS 资源。

## 要求

- AWS 账户
- 具最新 Update Roll-up 的 Microsoft System Center VMM 2012 R2 或 System Center VMM 2012 SP1

## 入门

要开始入门，请参阅以下文档：

- [设置 \(p. 759\)](#)
- [管理 EC2 实例 \(p. 763\)](#)
- [故障排除 \(p. 769\)](#)

## 设置 AWS Systems Manager for Microsoft SCVMM

当您设置 AWS Systems Manager 时，贵组织中的用户可以访问您的 AWS 资源。过程涉及创建账户、部署插件并提供您的证书。

### 任务

- [注册 AWS \(p. 759\)](#)
- [设置用户的访问 \(p. 760\)](#)
- [部署插件 \(p. 761\)](#)
- [提供您的 AWS 证书 \(p. 762\)](#)

## 注册 AWS

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

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。

### 如需注册 AWS 账户

1. 打开 <http://www.amazonaws.cn/>，然后选择 Create an AWS Account。
2. 按照屏幕上的说明进行操作。

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

## 设置用户的访问

您第一次使用 AWS Systems Manager 时，必须提供 AWS 证书。为使多个用户可使用唯一证书和权限访问同一 AWS 账户，可为每个用户创建一个 IAM 用户。您可以使用授权执行有限任务的策略创建一个或多个组。然后，创建一个或多个 IAM 用户，并将每个用户添加到适当的组。

## 创建管理员组

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
  2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
  3. 在 Group Name 框中，指定 Administrators，然后选择 Next Step。
  4. 在 Attach Policy 页面上，选择 AdministratorAccess AWS 托管策略。
  5. 选择 Next Step，然后选择 Create Group。

## 创建对 Amazon EC2 具有限访问权限的组

1. 打开 <https://console.amazonaws.cn/iam/> 上的 Identity and Access Management (IAM) 控制台。
  2. 在导航窗格中，选择 Groups，然后选择 Create New Group。
  3. 在 Group Name 框中，为组指定一个有意义的名称，然后选择 Next Step。
  4. 在 Attach Policy 页面上，请勿选择 AWS 托管策略 — 选择 Next Step，然后选择 Create Group。
  5. 选择您刚创建的组的名称。在 Permissions 选项卡上，选择 Inline Policies，然后选择 click here。
  6. 选择 Custom Policy 单选按钮，然后选择 Select。
  7. 为授予对 Amazon EC2 的有限访问权的策略和策略文档输入名称，然后选择 Apply Policy。例如，您可以指定以下自定义策略之一。

授予此组中的用户仅查看 EC2 实例相关信息的权限

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:Describe*",
 "iam>ListInstanceProfiles"
],
 "Resource": "*"
 }
]
}
```

授予此组中的用户对插件所支持的 EC2 实例执行全部操作的权限

```
 "ec2:RebootInstances", "ec2:StartInstances",
 "ec2:StopInstances", "ec2:TerminateInstances"
],
 "Resource": "*"
}
]
```

授予此组用户将 VM 导入 Amazon EC2 的权限

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "s3>ListAllMyBuckets", "s3>CreateBucket",
 "s3>DeleteBucket", "s3>DeleteObject",
 "s3>GetBucketLocation", "s3>GetObject",
 "s3>ListBucket", "s3>PutObject",
 "ec2>DescribeTags", "ec2>CancelConversionTask",
 "ec2>DescribeConversionTasks", "ec2>DescribeInstanceAttribute",
 "ec2>CreateImage", "ec2>AttachVolume",
 "ec2>ImportInstance", "ec2>ImportVolume",
 "dynamodb>DescribeTable", "dynamodb>CreateTable",
 "dynamodb>Scan", "dynamodb>PutItem", "dynamodb>UpdateItem"
],
 "Resource": "*"
 }
]
}
```

要创建 IAM 用户，请获取用户的 AWS 证书，并且授予用户权限

1. 在导航窗格中选择 Users，然后选择 Create New Users。
2. 在框 1 中，指定一个用户名，然后选择 Create。
3. 选择 Download Credentials，并将此 IAM 用户的 AWS 凭证保存在安全的位置。您需要这些证书才能访问 AWS Systems Manager。下载凭证之后选择 Close。
4. 选择您刚创建的用户。
5. 在 Groups 选项卡上，选择 Add User to Groups。
6. 选择适当的组，然后选择 Add to Groups。
7. ( 可选 ) 如果此用户还必须访问 AWS 管理控制台，则您必须创建密码。在 Security Credentials 选项卡上的 Sign-In Credentials 下，选择 Manage Password。按照指示为此 IAM 用户创建密码。

## 部署插件

适用于 System Center VMM 的插件以 .zip 文件的形式分发。要部署插件，请按照下列过程操作。

### 部署插件

1. 从您的实例，转到 [AWS Systems Manager for Microsoft System Center Virtual Machine Manager](#)，然后单击 SCVMM。将 aws-systems-manager-1.5.zip 文件保存到您的实例。

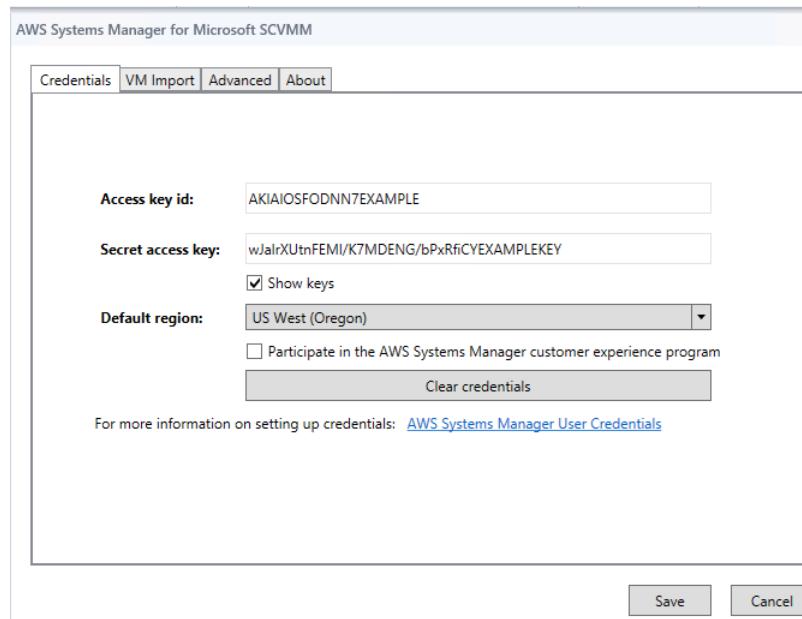
2. 打开 VMM 控制台。
3. 在“Navigation (导航)”窗格中，依次单击 Settings (设置) 和 Console Add-Ins (控制台插件)。
4. 在功能区中，单击 Import Console Add-in (导入控制台插件)。
5. 在 Select an Add-in 页面上，单击 Browse 并为已下载的插件选择 aws-systems-manager-1.5.zip 文件。
6. 忽略插件中存在未经可信颁发机构签署的程序集的任何警告。选择 Continue installing this add-in anyway (无论如何继续安装此插件)，然后单击 Next (下一步)。
7. 在 Summary (摘要) 页面上，单击 Finish (完成)。
8. 在导入插件时，作业状态为 Completed。您可以关闭 Jobs (作业) 窗口。

## 提供您的 AWS 证书

您第一次使用 AWS Systems Manager 时，必须提供 AWS 证书。AWS 通过您的访问密钥识别您。有两个类型的访问密钥：访问密钥 ID（例如，AKIAIOSFODNN7EXAMPLE）和秘密访问密钥（例如，wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY）。在您收到访问密钥后，应该将它们存储在安全位置。

### 提供您的 AWS 证书

1. 打开 VMM 控制台。
2. 在“Navigation (导航)”窗格中，单击 VMs and Services (虚拟机和服务)。
3. 在功能区上，单击 Amazon EC2。
4. 在 Credentials (证书) 选项卡上，指定您的 AWS 证书，选择默认区域，然后单击 Save (保存)。



任何时候若要更改这些证书，请单击 Configuration。

# 使用 AWS Systems Manager for Microsoft SCVMM 管理 EC2 实例

您使用 AWS 证书登录 AWS Systems Manager 后，便可以管理您的 EC2 实例。

## 任务

- [创建 EC2 实例 \(p. 763\)](#)
- [查看实例 \(p. 764\)](#)
- [连接到您的实例 \(p. 765\)](#)
- [重启您的实例 \(p. 765\)](#)
- [停止实例 \(p. 766\)](#)
- [启动实例 \(p. 766\)](#)
- [终止实例 \(p. 766\)](#)

## 创建 EC2 实例

由管理员授予您的权限决定您是否可以创建实例。

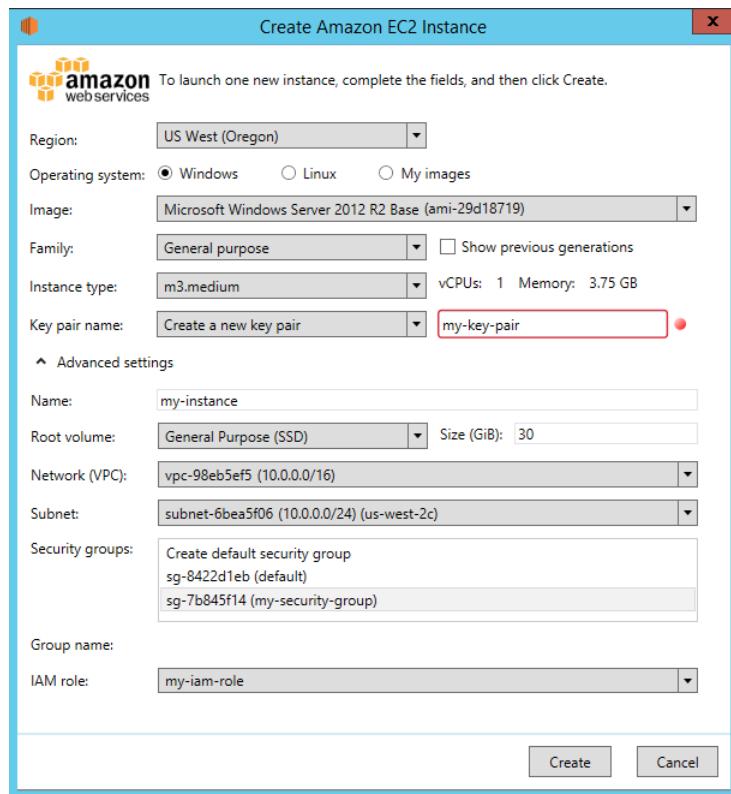
### 先决条件

- 启动实例的可用区中带子网的 Virtual Private Cloud (VPC)。有关如何创建 VPC 的更多信息，请参阅 [Amazon VPC 入门指南](#)。

### 创建 EC2 实例

1. 打开 SCVMM。
2. 在功能区上，单击 Create Amazon EC2 Instance。
3. 完成 Create Amazon EC2 Instance 对话框，如下所示：
  - a. 为您的实例选择区域。默认情况下，我们选择您已配置为默认区域的区域。
  - b. 为您的实例选择模板（称为 AMI）。要使用 Amazon 提供的 AMI，请选择 Windows 或 Linux，然后从 Image 选择 AMI。要使用您创建的 AMI，请选择 My images，然后从 Image 选择相应 AMI。
  - c. 选择实例的实例类型。首先，从 Family 中选择一个最新实例系列，然后从 Instance type 中选择实例类型。要在列表中包含上一代实例系列，请选择 Show previous generations。有关更多信息，请参阅 [Amazon EC2 实例](#) 和 [上一代实例](#)。
  - d. 创建或选择密钥对。要创建密钥对，请从 Key pair name 中选择 Create a new key pair，然后在突出显示的字段中输入密钥对名称（例如，my-key-pair）。
  - e. (可选) 在 Advanced Settings 下，指定实例的显示名称。
  - f. (可选) 在 Advanced Settings 下，从 Network (VPC) 中选择 VPC。请注意，此列表包含区域的所有 VPC，包括使用 Amazon VPC 控制台创建的 VPC 和默认 VPC（如果存在）。如果该区域有默认 VPC，则会默认选择该 VPC。如果系统提示“*There is no VPC available for launch or import operations in this region*”，则必须使用 Amazon VPC 控制台在此区域中创建 VPC。
  - g. (可选) 在 Advanced Settings 下，从 Subnet 中选择子网。请注意，此列表包含所选 VPC 的所有子网，包括所有默认子网。如果此列表为空，则必须使用 Amazon VPC 控制台向该 VPC 添加子网，或者选择其他 VPC。否则，我们为您选择一个子网。
  - h. (可选) 在 Advanced Settings 下创建安全组，或者选择一个或多个安全组。如果您选择 Create default security group，那么我们将创建向所有人授予 RDP 和 SSH 访问权限的安全组，您可以使用 Amazon EC2 或 Amazon VPC 控制台修改该安全组。您可以在 Group name 框中输入该安全组的名称。

- i. (可选) 在 Advanced Settings 下, 选择 IAM 角色。如果此列表为空, 则可以使用 IAM 控制台创建角色。



4. 单击 Create(创建)。在创建密钥对时, 系统将提示您保存 .pem 文件。请将此文件保存在安全位置; 您将需要使用该文件来登录实例。您将收到实例已启动的确认。单击 Close(关闭)。

创建实例后, 该实例将显示在您启动实例的区域的实例列表中。该实例最初的状态是 pending。在状态变为 running 后, 您的实例即准备就绪, 可以使用。

您可以根据本页中的说明, 使用 AWS Systems Manager 管理实例的生命周期。要执行其他任务(如以下任务), 必须使用 AWS 管理控制台:

- 将 Amazon EBS 卷挂载到您的实例 (p. 657)
- 将弹性 IP 地址与您的实例相关联 (p. 609)
- 启用终止保护 (p. 234)

## 查看实例

您能否查看实例并获取有关实例的详细信息, 由管理员授予您的权限决定。

### 查看您的实例并获取详细信息

1. 打开 AWS Systems Manager。
2. 从区域列表中, 选择一个区域。
3. 在实例列表中, 选择一个或多个实例。
4. 在下方窗格中, 单击每个实例旁边的向下箭头, 可查看有关实例的详细信息。

| Virtual machine information |                                             | Networking          |                                          |
|-----------------------------|---------------------------------------------|---------------------|------------------------------------------|
| Instance ID:                | i-343e9f3a                                  | Public DNS name:    |                                          |
| Name:                       | my-instance                                 | Public IP address:  |                                          |
| State:                      | Running                                     | Private DNS name:   | ip-10-0-0-147.us-west-2.compute.internal |
| Launch time:                | 1/20/2015 12:26:48 PM -08:00 (1 minute ago) | Private IP address: | 10.0.0.147                               |
| Instance type:              | m3.medium                                   | Vpc ID:             | vpc-f1663d98                             |
| Tenancy:                    | default                                     | Subnet ID:          | subnet-c9663da0                          |
| Image ID:                   | ami-29d18719                                | Network interfaces: | eni-89b0bed0                             |
| Operating system:           | Windows                                     |                     |                                          |

## 连接到您的实例

如果您具有在启动实例时指定的密钥对的私有密钥（.pem文件），那么您可以登录EC2实例。您将用于连接到实例的工具取决于实例是Windows实例还是Linux实例。

### 连接到Windows EC2实例

1. 打开AWS Systems Manager。
2. 从实例列表中选择实例，右键单击该实例，然后单击Retrieve Windows Password（检索Windows密码）。
3. 在Retrieve Default Windows Administrator Password（检索默认Windows管理员密码）对话框中，单击Browse（浏览）。选择密钥对的私有密钥，然后单击Open（打开）。
4. 单击“Decrypt Password”。保存密码或将其复制到剪贴板。
5. 选择实例，右键单击该实例，然后单击Connect via RDP（通过RDP连接）。当系统提示您提供证书时，使用您在上一步中保存的管理员账户名称和密码。
6. 由于证书为自签名，您可能会收到安全证书并非来自可信证书颁发机构的警告。单击Yes（是）以继续。

如果连接失败，请参阅*Amazon EC2 用户指南（适用于 Microsoft Windows 实例）*中的[Windows 实例故障排除](#)。

### 连接到Linux EC2实例

1. 打开AWS Systems Manager。
2. 从实例列表中选择实例。
3. 在下方窗格中，单击实例ID旁边的向下箭头，可查看有关实例的详细信息。
4. 查找公有DNS名称。您需要此信息连接到您的实例。
5. 使用PuTTY连接到实例。有关分步指导，请参阅*Amazon EC2 用户指南（适用于 Linux 实例）*中的[使用 PuTTY 从 Windows 连接到 Linux 实例](#)。

## 重启您的实例

您能否重启实例，由管理员授予您的权限决定。

### 重启您的实例

1. 打开AWS Systems Manager。
2. 从实例列表中选择实例。
3. 右键单击实例，然后单击Reset (Reboot)（重置（重启））。
4. 当系统提示进行确认时，单击Yes（是）。

## 停止实例

您能否停止实例，由管理员授予您的权限决定。

### 停止您的实例

1. 打开 AWS Systems Manager。
2. 从实例列表中选择实例。
3. 右键单击实例，然后单击 Shut Down (Stop) (关闭 (停止))。
4. 当系统提示进行确认时，单击 Yes (是)。

## 启动实例

您能否启动实例，由管理员授予您的权限决定。

### 启动您的实例

1. 打开 AWS Systems Manager。
2. 从实例列表中选择实例。
3. 右键单击实例，然后单击 Power On (Start) (打开 (启动))。
4. 当系统提示进行确认时，单击 Yes (是)。

如果您在尝试启动实例时看到配额错误，表示您已达到并行运行的实例限制。您的 AWS 账户的默认限制为 20。如果您需要运行更多的实例，请在此处填写申请表：[请求提高 Amazon EC2 实例限制](#)。

## 终止实例

您能否终止实例，由管理员授予您的权限决定。

### 终止您的实例

1. 打开 AWS Systems Manager。
2. 从实例列表中选择实例。
3. 右键单击实例，然后单击 Delete (Terminate) (删除 (终止))。
4. 当系统提示进行确认时，单击 Yes (是)。

## 使用 AWS Systems Manager for Microsoft SCVMM 导入虚拟机

您可以通过从 SCVMM 导入到 Amazon EC2 的虚拟机来启动 EC2 实例。



### Important

您不能将 Linux 虚拟机从 SCVMM 导入到 Amazon EC2。

### 内容

- [先决条件 \(p. 767\)](#)
- [导入您的虚拟机 \(p. 767\)](#)

- 检查导入任务状态 (p. 768)
- 备份已导入的实例 (p. 768)

## 先决条件

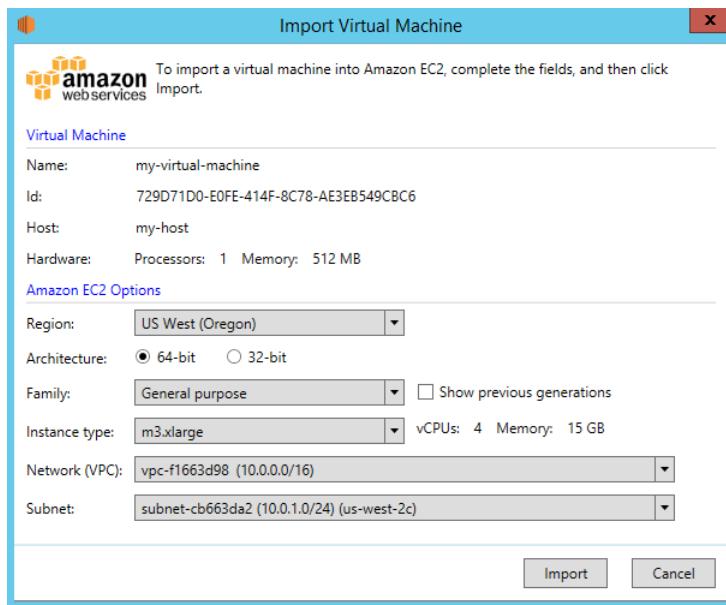
- 确保您的 VM 已就绪。有关更多信息，请参阅[准备您的 VM \(p. 423\)](#)。
- 在 AWS Systems Manager 中，单击 Configuration，选择 VM Import 选项卡，检查以下设置：
  - S3 bucket prefix：导入之前，我们为要上传的磁盘映像创建存储桶。存储桶的名称以这里列出的前缀开头，包含区域（例如，us-west-2）。要在导入磁盘映像后删除这些磁盘映像，请选择 Clean up S3 bucket after import。
  - VM image export path：从 VM 中导出的磁盘映像的位置。要在导入磁盘映像后删除这些磁盘映像，请选择 Clean up export path after import。
  - Alternate Hyper-V PowerShell module path：Hyper-V PowerShell 模块的位置，如果该模块未安装在标准位置。有关更多信息，请参阅 Microsoft TechNet 库中的[安装 Hyper-V 管理工具](#)。

## 导入您的虚拟机

管理员授予您的权限决定了您是否可以将 HyperV Windows 虚拟机从 SCVMM 导入到 AWS。

### 导入您的虚拟机

1. 打开 SCVMM。
2. 在功能区上，单击 VM。从列表中选择虚拟机。
3. 在功能区上，单击 Import VM to Amazon EC2。
4. 完成 Import Virtual Machine 对话框，如下所示：
  - a. 为实例选择区域。默认情况下，我们选择您已配置为默认区域的区域。
  - b. 选择实例的实例类型。首先，从 Family 中选择一个最新实例系列，然后从 Instance type 中选择实例类型。要在列表中包含上一代实例系列，请选择 Show previous generations。有关更多信息，请参阅[Amazon EC2 实例和上一代实例](#)。
  - c. 从 Network (VPC) 中选择 VPC。请注意，此列表包含区域的所有 VPC，包括使用 Amazon VPC 控制台创建的 VPC 和默认 VPC（如果存在）。如果该区域有默认 VPC，则会默认选择该 VPC。如果系统提示“*There is no VPC available for launch or import operations in this region*”，则必须使用 Amazon VPC 控制台在此区域中创建 VPC。
  - d. 从 Subnet 中选择子网。请注意，此列表包含所选 VPC 的所有子网，包括所有默认子网。如果此列表为空，则必须使用 Amazon VPC 控制台向该 VPC 添加子网，或者选择其他 VPC。否则，我们为您选择一个子网。



- 单击 Import (导入)。如果您没有在 VM Import 选项卡中指定所需信息，那么您将收到错误消息，要求您提供所需信息。否则，您将收到导入任务已经开始的确认。单击 Close (关闭)。

## 检查导入任务状态

导入任务可能需要几个小时才能完成。要查看当前状态，请打开 AWS System Manager 并单击 Notifications。

随着导入任务的进行，您将收到以下通知：

- Import VM: Created Import VM Task
- Import VM: Export VM Disk Image Done
- Import VM: Upload to S3
- Import VM: Image Conversion Starting
- Import VM: Image Conversion Done
- Import VM: Import Complete

请注意，对于每个转换的磁盘映像，您都将收到 Import VM: Upload to S3、Import VM: Image Conversion Starting 和 Import VM: Image Conversion Done 通知。

如果导入任务失败，您将收到通知 Import VM: Import Failed。有关导入任务的故障排除问题的更多信息，请参阅[导入 VM 时的错误 \(p. 770\)](#)。

## 备份已导入的实例

导入操作完成后，实例将继续运行，直至终止。实例终止后，您无法连接或恢复该实例。要确保可以根据需要使用与导入的实例相同的软件启动新实例，请从导入的实例创建 Amazon 系统映像 (AMI)。有关更多信息，请参阅[创建 Amazon EBS 支持的 Windows AMI \(p. 76\)](#)。

# AWS Systems Manager for Microsoft SCVMM 故障排除

以下是常见的错误和故障排除步骤。

## 内容

- [错误：无法安装插件 \(p. 769\)](#)
- [安装错误 \(p. 769\)](#)
- [检查日志文件 \(p. 770\)](#)
- [导入 VM 时的错误 \(p. 770\)](#)
- [卸载插件 \(p. 770\)](#)

## 错误：无法安装插件

如果收到以下错误，请尝试在运行 VMM 控制台的计算机上安装 [KB2918659](#)。有关更多信息，请参阅 [System Center 2012 SP1 更新汇总 5 的说明](#)。请注意，要解决此问题，您无需安装本文列出的所有更新，只需安装 KB2918659。

```
Add-in cannot be installed
The assembly "Amazon.Scvmm.Addin" referenced to by add-in component "AWS Systems
Manager for
Microsoft SCVMM" could not be found in the add-in package. This could be due
to the following
reasons:
1. The assembly was not included with the add-in package.
2. The AssemblyName attribute for the add-in does not match the name of the
add-in assembly.
3. The assembly file is corrupt and cannot be loaded.
```

## 安装错误

如果您在安装过程中收到以下错误之一，很可能是由于 SCVMM 存在问题：

```
Could not update managed code add-in pipeline due to the following error:
Access to the path 'C:\Program Files\Microsoft System Center 2012\Virtual Machine
Manager
\Bin\AddInPipeline\PipelineSegments.store' is denied.
```

```
Could not update managed code add-in pipeline due to the following error:
The required folder 'C:\Program Files\Microsoft System Center 2012\Virtual Ma
chine Manager
\Bin\AddInPipeline\HostSideAdapters' does not exist.
```

```
Add-in cannot be installed
The assembly "Microsoft.SystemCenter.VirtualMachineManager.UIAddIns.dll" refer
enced by the
add-in assembly "Amazon.Scvmm.AddIn" could not be found in the add-in package.
Make sure
that this assembly was included with the add-in package.
```

尝试执行以下步骤之一以解决此问题：

- 授予经身份验证的用户读取和执行 C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Bin\AddInPipeline 文件夹的权限。在 Windows 资源管理器中，右键单击该文件夹，选择 Properties (属性)，然后选择 Security (安全) 选项卡。
- 关闭 SCVMM 控制台，并以管理员身份再次启动该控制台。从 Start (开始) 菜单中，找到 SCVMM 并右键单击，然后选择 Run as administrator (以管理员身份运行)。

## 检查日志文件

如果您使用插件时遇到问题，可检查生成的日志文件 %APPDATA%\Amazon\SCVMM\ec2addin.log，以获取有用的信息。

## 导入 VM 时的错误

日志文件 %APPDATA%\Amazon\SCVMM\ec2addin.log 包含有关导入任务状态的详细信息。将 VM 从 SCVMM 导入到 Amazon EC2 时，可能会在日志文件中看到以下常见错误。

错误：无法提取 Hyper-V VirtualMachine 对象

解决方案：配置 Hyper-V PowerShell 模块的路径。

错误：您没有执行操作的权限

解决方案：联系您的管理员。

## 卸载插件

如果您需要卸载插件，请按照以下过程操作。

### 卸载插件

- 打开 VMM 控制台。
- 选择 Settings (设置) 工作区，然后单击 Console Add-Ins (控制台插件)。
- 选择 AWS Systems Manager for Microsoft SCVMM。
- 在功能区中，单击 Remove (删除)。
- 当系统提示进行确认时，单击 Yes (是)。

如果您在卸载插件后重新安装并收到以下错误，可删除错误消息中建议的路径。

```
Error (27301)
There was an error while installing the add-in. Please ensure that the following
path does not
exist and then try the installation again.

C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Bin\AddIn
Pipeline\
AddIns\EC2WINDOWS...
```

# AWS Management Pack for Microsoft System Center

---

## Abstract

使用 Microsoft System Center Operations Manager 监控您的 AWS 资源。

Amazon Web Services (AWS) 提供了一整套基础设施和应用程序服务，用于在云中运行几乎所有应用程及项目 — 从企业应用程序和大数据项目，到社交游戏和移动应用程序。AWS Management Pack for Microsoft System Center 针对 AWS 中运行的应用程序提供可用性和性能监控功能。

AWS Management Pack 允许 Microsoft System Center Operations Manager 访问您的 AWS 资源（如实例和卷），因此它可以收集性能数据并监控您的 AWS 资源。AWS Management Pack 是 System Center Operations Manager 的一种扩展程序。AWS Management Pack 有两个版本：一个版本用于 System Center 2012 — Operations Manager，另一个版本用于 System Center Operations Manager 2007 R2。

AWS Management Pack 使用 Amazon CloudWatch 指标和警报监控您的 AWS 资源。Amazon CloudWatch 指标在 Microsoft System Center 中以性能计数器的形式显示，而 Amazon CloudWatch 警报则以警报形式显示。

您可以监控以下 资源：

- EC2 实例
- EBS 卷
- ELB 负载均衡器
- Auto Scaling 组和可用区
- Elastic Beanstalk 应用程序
- CloudFormation 堆栈
- CloudWatch 警报
- CloudWatch 自定义指标

## 内容

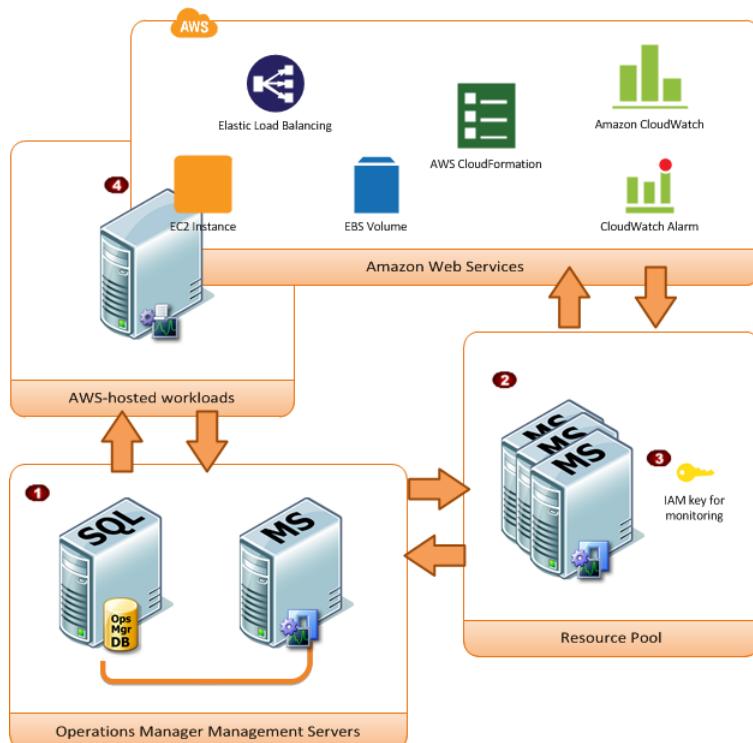
- [适用于 System Center 2012 的 AWS Management Pack 概述 \(p. 772\)](#)
- [适用于 System Center 2007 R2 的 AWS Management Pack 概述 \(p. 773\)](#)

- 下载 AWS Management Pack (p. 774)
- 部署 AWS Management Pack (p. 775)
- 使用 AWS Management Pack (p. 785)
- 升级 AWS Management Pack (p. 803)
- 卸载 AWS Management Pack (p. 805)
- 排查 AWS Management Pack方面的问题 (p. 805)

## 适用于 System Center 2012 的 AWS Management Pack概述

适用于 System Center 2012—Operations Manager 的 AWS Management Pack 使用一个资源池，其中包含一个或多个管理服务器来发现和监控您的 AWS 资源。在您增加所用的 AWS 资源数量时可以向池中添加管理服务器。

下图显示了 AWS Management Pack 的主要组件。



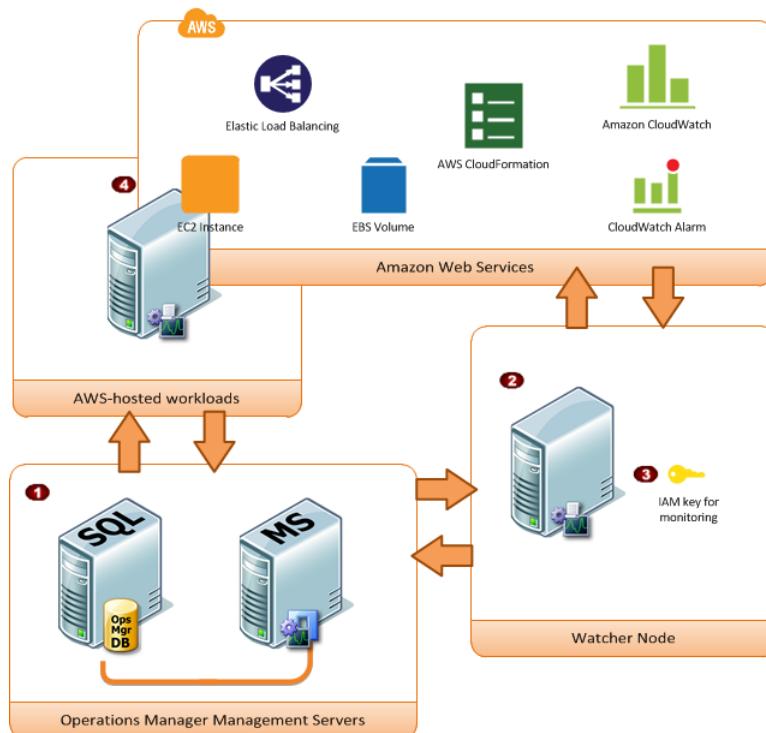
| Item | 组建                      | 说明                                                                                                    |
|------|-------------------------|-------------------------------------------------------------------------------------------------------|
| ①    | Operations Manager 基础设施 | 一个或多个管理服务器及其依赖项，例如 Microsoft SQL Server 和 Microsoft Active Directory 域。这些服务器可以在本地或 AWS 云内部署；两种情况均受支持。 |
| ②    | 资源池                     | 用于通过适用于 .NET 的 AWS 软件开发工具包与 AWS 通信的一个或多个管理服务器。这些服务器必须具有 Internet 连接。                                  |

| Item | 组建     | 说明                                                                                                                                                                               |
|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ③    | AWS 凭证 | 管理服务器用以进行 AWS API 调用的访问密钥 ID 和秘密访问密钥。当您配置 AWS Management Pack 时必须指定这些证书。我们建议您创建一个具有只读特权的 IAM 用户并使用这些凭证。有关创建 IAM 用户的更多信息，请参阅 <i>IAM 用户指南</i> 中的 <a href="#">向您的 AWS 账户添加新用户</a> 。 |
| ④    | EC2 实例 | AWS 云内运行的虚拟计算机。部分实例可能已安装 Operations Manager 代理，而其他实例可能没有。安装 Operations Manager 代理时，除实例运行状况之外，您还可以看到操作系统和应用程序运行状况。                                                                |

## 适用于 System Center 2007 R2 的 AWS Management Pack 概述

适用于 System Center Operations Manager 2007 R2 的 AWS Management Pack 使用连接到您的 System Center 环境且能够访问 Internet 的指定计算机（称为观察程序节点）调用 AWS API，以远程发现并收集有关您的 AWS 资源的信息。

下图显示了 AWS Management Pack 的主要组件。



| Item | 组建                      | 说明                                                                                                    |
|------|-------------------------|-------------------------------------------------------------------------------------------------------|
| ①    | Operations Manager 基础设施 | 一个或多个管理服务器及其依赖项，例如 Microsoft SQL Server 和 Microsoft Active Directory 域。这些服务器可以在本地或 AWS 云内部署；两种情况均受支持。 |

| Item | 组建     | 说明                                                                                                                                                                                                                               |
|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ②    | 观察程序节点 | 指定的代理托管计算机，用于通过适用于 .NET 的 AWS 开发工具包与 AWS 进行通信。它可以在本地或 AWS 云内部署，但其必须是代理托管计算机并具有 Internet 连接功能。您可以使用一个观察程序节点来监控一个 AWS 账户。不过，一个观察程序节点可以监控多个 AWS 账户。有关设置观察程序节点的更多信息，请参阅 Microsoft System Center 文档中的 <a href="#">部署 Windows 代理</a> 。 |
| ③    | AWS 凭证 | 观察程序节点用以调用 AWS API 的访问密钥 ID 和秘密访问密钥。当您配置 AWS 管理包时必须指定这些证书。我们建议您创建一个具有只读特权的 IAM 用户并使用这些凭证。有关创建 IAM 用户的更多信息，请参阅 IAM 用户指南中的 <a href="#">向您的 AWS 账户添加新用户</a> 。                                                                       |
| ④    | EC2 实例 | AWS 云内运行的虚拟计算机。部分实例可能已安装 Operations Manager 代理，而其他实例可能没有。安装 Operations Manager 代理时，除实例运行状况之外，您还可以看到操作系统和应用程序运行状况。                                                                                                                |

## 下载 AWS Management Pack

### Abstract

下载 AWS Management Pack。

首先，请下载 AWS Management Pack。AWS Management Pack 是免费的。根据您的监控配置或所监控的 AWS 资源的数量，可能会产生有关 Amazon CloudWatch 的费用。

## System Center 2012

在下载 AWS Management Pack 前，请确保系统满足以下系统要求和先决条件。

### 系统要求

- System Center Operations Manager 2012 R2 或 System Center Operations Manager 2012 SP1
- 累积更新 1 或更高版本。必须对监控 AWS 资源的管理服务器以及运行监视器节点的代理和要使用 AWS Management Pack 监控的代理部署更新。我们建议您对监控 AWS 资源的所有计算机部署最新的可用 Operations Manager 更新。
- Microsoft.Unix.Library MP 版本 7.3.2026.0 或更高版本

### 先决条件

- 数据中心必须有至少一个管理服务器配置了 Internet 连接。管理服务器必须安装有 Microsoft .NET Framework 版本 4.5 或更高版本和 PowerShell 2.0 或更高版本。
- 管理服务器的操作账户必须在管理服务器上具有本地管理员特权。

### 下载 AWS Management Pack

1. 在 [AWS Add-Ins for Microsoft System Center](#) 网站上，单击 SCOM 2012。
2. 将 AWS-SCOM-MP-2.5.zip 保存到您的计算机并解压缩。

[继续部署 AWS Management Pack \(p. 775\)。](#)

## System Center 2007 R2

在下载 AWS Management Pack 前，请确保系统满足以下系统要求和先决条件。

### 系统要求

- System Center Operations Manager 2007 R2
- Microsoft.Unix.Library MP 版本 6.1.7000.256 或更高版本

### 先决条件

- 数据中心必须有一台指定为观察程序节点、具有 Internet 连接的代理托管计算机。观察程序节点必须启用了以下代理程序选项：Allow this agent to act as a proxy and discover managed objects on other computers (允许此代理充当代理并发现其他计算机上的托管对象)。观察程序节点必须安装有 Microsoft .NET Framework 版本 3.5.1 或更高版本和 PowerShell 2.0 或更高版本。
- 观察程序节点的操作账户必须在观察程序节点上具有本地管理员特权。
- 您必须确保观察程序节点已经安装了代理、可以访问 Internet，并且能够与您数据中心内的管理服务器通信。有关更多信息，请参阅 Microsoft System Center 文档中的[部署 Windows 代理](#)。

### 下载 AWS Management Pack

1. 在 [AWS Add-Ins for Microsoft System Center](#) 网站上，单击 SCOM 2007。
2. 将 AWS-MP-Setup-2.5.msi 保存到您的计算机。

[继续部署 AWS Management Pack \(p. 775\)。](#)

## 部署 AWS Management Pack

### Abstract

查看 AWS Management Pack 组件如何协同工作，然后部署 AWS Management Pack。

在部署 AWS Management Pack 之前必须先下载它。有关更多信息，请参阅 [下载 AWS Management Pack \(p. 774\)](#)。

### 任务

- [步骤 1：安装 AWS Management Pack \(p. 775\)](#)
- [步骤 2：配置观察程序节点 \(p. 777\)](#)
- [步骤 3：创建 AWS 运行方式账户 \(p. 778\)](#)
- [步骤 4：运行添加监视向导 \(p. 780\)](#)
- [步骤 5：配置端口和终端节点 \(p. 784\)](#)

## 步骤 1：安装 AWS Management Pack

### Abstract

安装 AWS Management Pack for Microsoft System Center。

下载 AWS Management Pack 后，您必须将其配置为监控一个或多个 AWS 账户。

## System Center 2012

### 安装 AWS Management Pack

1. 在操作控制台的 Go 菜单上，依次单击 Administration 和 Management Packs。
2. 在 Actions 窗格中，单击 Import Management Packs。
3. 在 Select Management Packs 页面中，依次单击 Add 和 Add from disk。
4. 在 Select Management Packs to import 对话框中，从下载 Amazon.AmazonWebServices.mpb 文件的位置选择该文件，然后单击 Open。
5. 在 Select Management Packs 页面的 Import list 下，选择 Amazon Web Services 管理包，然后单击 Install。



#### Note

System Center Operations Manager 不会导入 Import (导入) 列表中显示 Error (错误) 图标的任何管理包。

6. Import Management Packs (导入管理包) 页面会显示导入过程的进度。如果出现问题，请在列表中选择管理包以查看状态详细信息。单击 Close (关闭)。

## System Center 2007 R2

### 安装 AWS Management Pack

该管理包以 Microsoft System 安装程序文件（即 AWS-MP-Setup.msi）的形式分发。它包含适用于观察程序节点、根管理服务器和操作控制台的必需 DLL 以及 Amazon.AmazonWebServices.mp 文件。

1. 运行 AWS-MP-Setup.msi。



#### Note

如果根管理服务器、操作控制台和观察程序节点位于不同的计算机上，则您必须在每台计算机上运行安装程序。

2. 在 Welcome to the Amazon Web Services Management Pack Setup Wizard (欢迎使用 Amazon Web Services 管理包设置向导) 屏幕上，单击 Next (下一步)。
3. 在 End-User License Agreement (最终用户许可协议) 屏幕上，阅读许可协议，如果同意条款，则选中 I accept the terms in the License Agreement (我接受许可协议中的条款) 复选框，然后单击 Next (下一步)。
4. 在 Custom Setup (自定义设置) 屏幕上，选择您想安装的功能，然后再单击 Next (下一步)。

#### 操作控制台

安装 Amazon.AmazonWebServices.UI.Pages.dll 并在全局程序集缓存 (GAC) 中注册，然后安装 Amazon.AmazonWebServices.mp。

#### 根管理服务器

安装 Amazon.AmazonWebServices.Modules.dll、  
Amazon.AmazonWebServices.SCOM.SDK.dll 和适用于 .NET 的 AWS 开发工具包  
(AWSSDK.dll)，然后在 GAC 中进行注册。

#### AWS 观察程序节点

安装 Amazon.AmazonWebServices.Modules.dll 和 Amazon.AmazonWebServices.SCOM.SDK.dll，然后安装适用于 .NET 的 AWS 开发工具包 (AWSSDK.dll)，并在 GAC 中注册该工具包。

5. 在 Ready to install Amazon Web Services Management Pack 屏幕上，单击 Install。
6. 在 Completed the Amazon Web Services Management Pack Setup Wizard 屏幕上，单击 Finish。



#### Note

系统会复制必需的 DLL 并在 GAC 中注册，同时将管理包文件 (\*.mp) 复制到运行操作控制台的计算机上的 Program Files (x86)/Amazon Web Services Management Pack 文件夹中。接下来，您必须将管理包导入 System Center。

7. 在操作控制台的 Go 菜单上，依次单击 Administration 和 Management Packs。
8. 在 Actions 窗格中，单击 Import Management Packs。
9. 在 Select Management Packs 页面中，依次单击 Add 和 Add from disk。
10. 在 Select Management Packs to import 对话框中，将目录更改为 C:\Program Files (x86)\Amazon Web Services Management Pack，选择 Amazon.AmazonWebServices.mp 文件，然后单击 Open。
11. 在 Select Management Packs 页面的 Import list 下，选择 Amazon Web Services 管理包，然后单击 Install。



#### Note

System Center Operations Manager 不会导入 Import (导入) 列表中显示 Error (错误) 图标的任何管理包。

12. Import Management Packs (导入管理包) 页面会显示导入过程的进度。如果出现问题，请在列表中选择管理包以查看状态详细信息。单击 Close (关闭)。

## 步骤 2：配置观察程序节点

### Abstract

配置观察程序节点以启用代理程序，从而允许发现其他计算机上的对象。

在 System Center Operations Manager 2007 R2 上，观察程序节点会在观察程序节点计算机范围之外运行发现，因此您必须在观察程序节点上启用代理程序选项。代理程序允许这些发现访问其他计算机上的对象。



#### Note

如果您的系统配置有大量资源，那么建议您将一个管理服务器配置为观察程序节点。拥有单独的观察程序节点管理服务器可以提高性能。

如果您使用 System Center 2012 — Operations Manager，可以跳过此步骤。

在 System Center Operations Manager 2007 上启用代理程序 R2

1. 在操作控制台的 Go 菜单上，单击 Administration。

2. 在 Administration (管理) 工作区的 Device Management (设备管理) 下，单击 Agent Managed (代理管理)。
3. 在 Agent Managed (代理管理) 列表中，右键单击观察程序节点，然后再单击 Properties (属性)。
4. 在 Agent Properties (代理属性) 对话框中，单击 Security (安全) 选项卡并选中 Allow this agent to act as proxy and discover managed objects on other computers (允许此代理充当代理并发现其他计算机上的托管对象)，然后单击 OK (确定)。

## 步骤 3：创建 AWS 运行方式账户

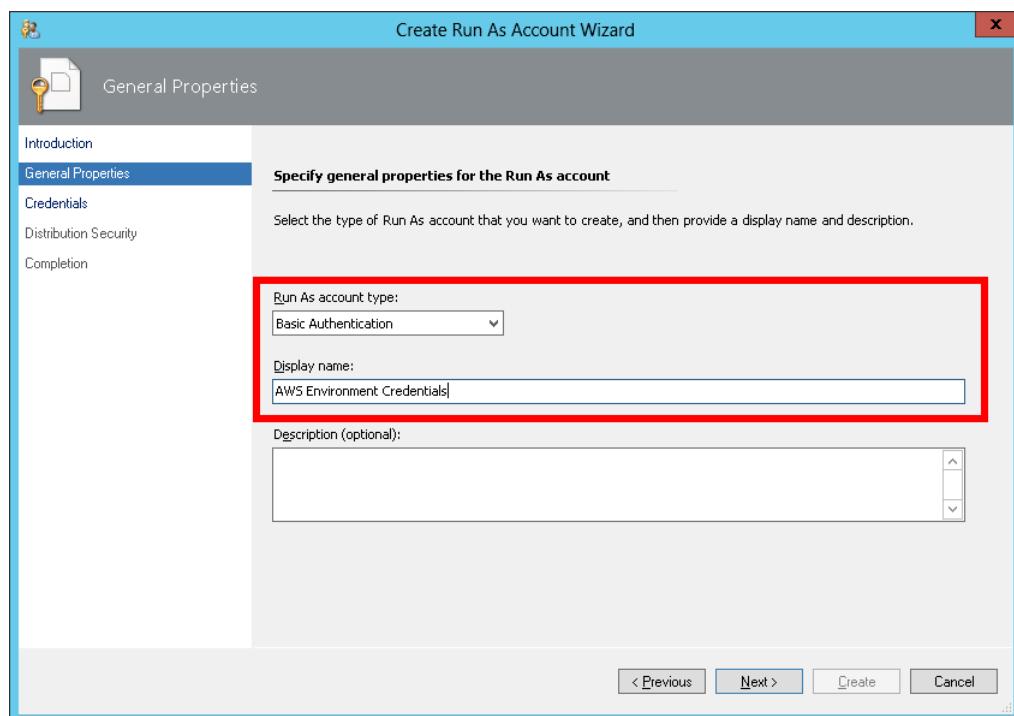
### Abstract

创建 AWS Run As 账户以允许访问资源。

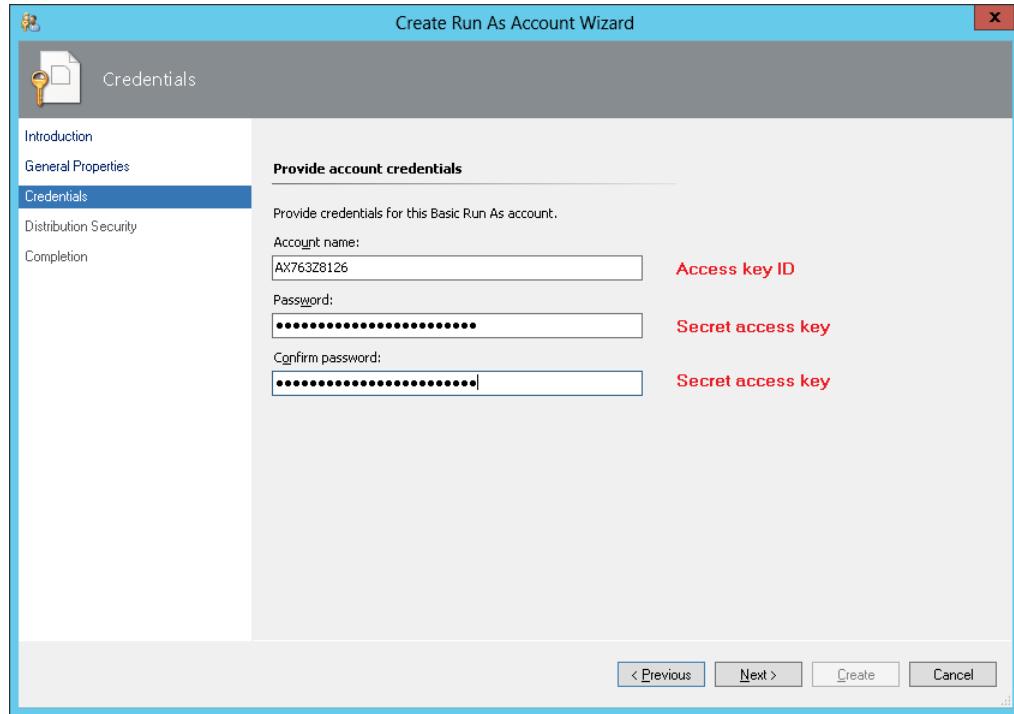
您必须设置授权 AWS Management Pack 访问您的 AWS 资源的证书。

### 如何创建 AWS 运行方式账户

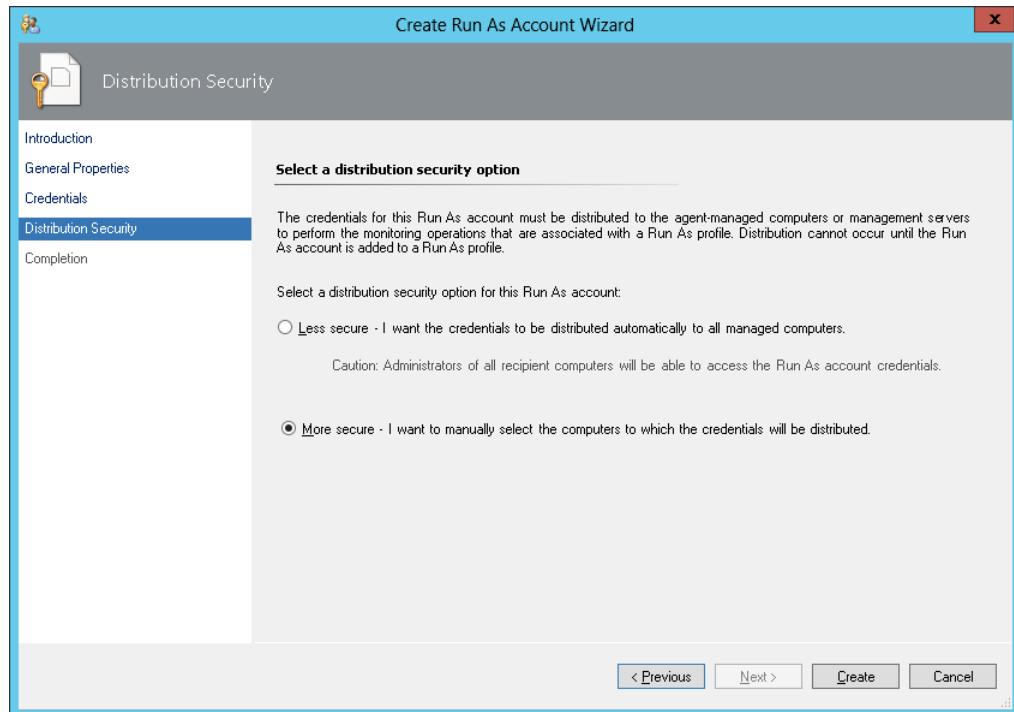
1. 建议您创建具有最低所需访问权限（例如，大多数情况下，可以使用 ReadOnlyAccess AWS 托管策略）的 IAM 用户。此用户要完成此过程还需要访问密钥（访问密钥 ID 和秘密访问密钥）。有关更多信息，请参阅 [IAM 用户指南中的管理 IAM 用户的访问密钥](#)。
2. 在操作控制台的 Go 菜单上，单击 Administration。
3. 在管理工作区中，展开运行方式配置节点，然后选择账户。
4. 右键单击账户窗格，然后单击创建运行方式账户。
5. 在 Create Run As Account Wizard (创建运行方式账户向导) 中的 General Properties (常规属性) 页面上，在 Run As account type (运行方式账户类型) 列表中选择 Basic Authentication (基本身份验证)。
6. 输入显示名称（例如“我的 IAM 账户”）和描述，然后单击 Next (下一步)。



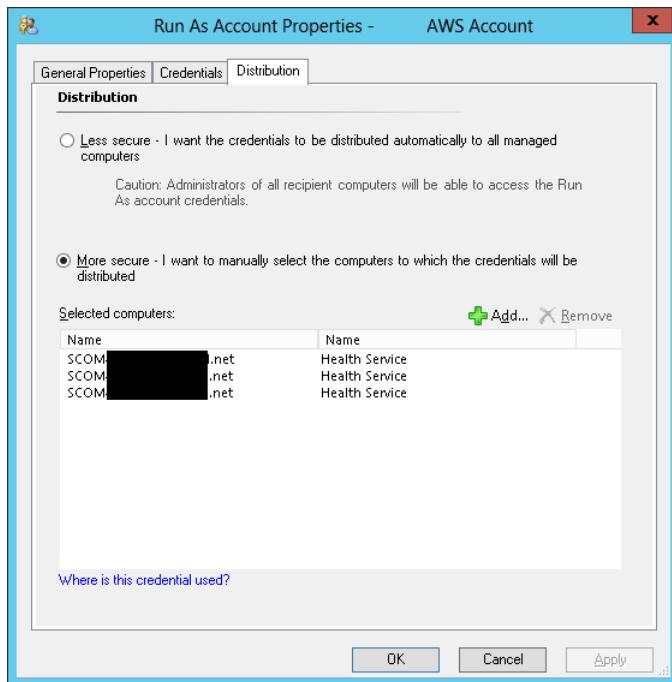
7. 在 Credentials (证书) 页上的 Account name (账户名称) 框中输入访问密钥 ID，在 Password (密码) 框中输入秘密访问密钥，然后单击 Next (下一步)。



8. 在 Distribution Security (分配安全性) 页面上，选择 More secure - I want to manually select the computers to which the credentials will be distributed (安全级别较高 - 我想手动选择证书分发到的计算机)，然后单击 Create (创建)。



9. 单击 Close (关闭)。
10. 在账户列表中，选择刚刚创建的账户。
11. 在 Actions (操作) 窗格中，单击 Properties (属性)。
12. 在 Properties (属性) 对话框中，确认选择了 More Secure(安全级别较高) 选项，并且所有要用于监控您的 AWS 资源的管理服务器都已列出。



## 步骤 4：运行添加监视向导

### Abstract

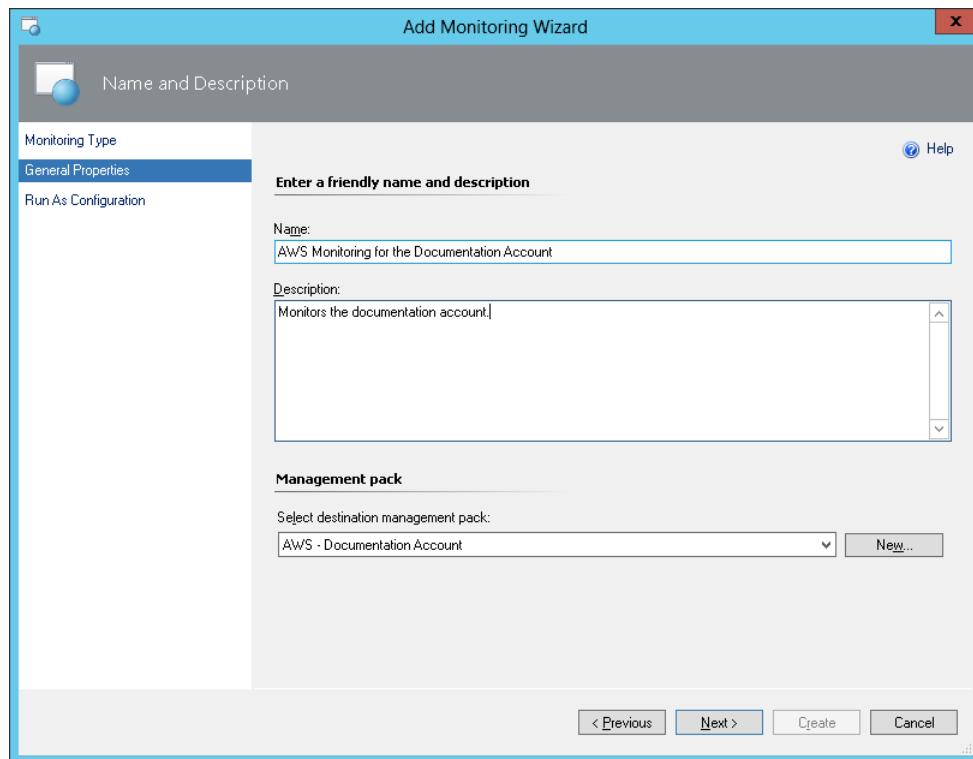
运行添加监视向导，该向导创建包含要监控的 AWS 账户的设置的新管理包。

您可以使用“Add Monitoring Wizard”（可在操作控制台的 Authoring 工作区中找到）配置 AWS Management Pack 以监控特定 AWS 账户。此向导会创建一个管理包，其中包含要监控的 AWS 账户的设置。您必须运行该向导以监控每个 AWS 账户。例如，如果您要监控两个 AWS 账户，则必须运行该向导两次。

## System Center 2012

### 在 System Center 2012 — Operations Manager 上运行添加监视向导

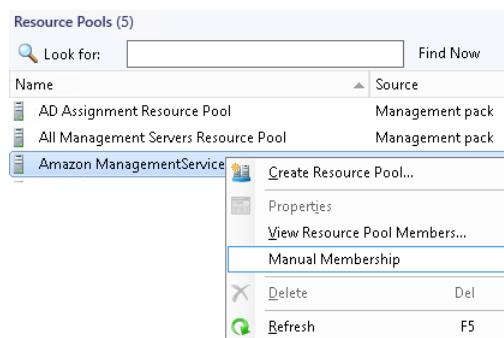
1. 在操作控制台的 Go 菜单上，单击 Authoring。
2. 在 Authoring 工作区中，展开 Management Pack Templates 节点并右键单击 Amazon Web Services，然后再单击 Add Monitoring Wizard。
3. 在 Add Monitoring Wizard 的 Select the monitoring type (选择监视类型) 列表中，选择 Amazon Web Services，然后再单击 Next (下一步)。
4. 在 General Properties (常规属性) 页面上的 Name (名称) 框中，输入名称（例如，“我的 AWS 资源”）。在 Description (描述) 框中输入描述。
5. 在 Select destination management pack (选择目标管理包) 列表中，选择要用于保存设置的现有管理包（或单击 New (新建) 以新建一个）。单击 Next (下一步)。



### Note

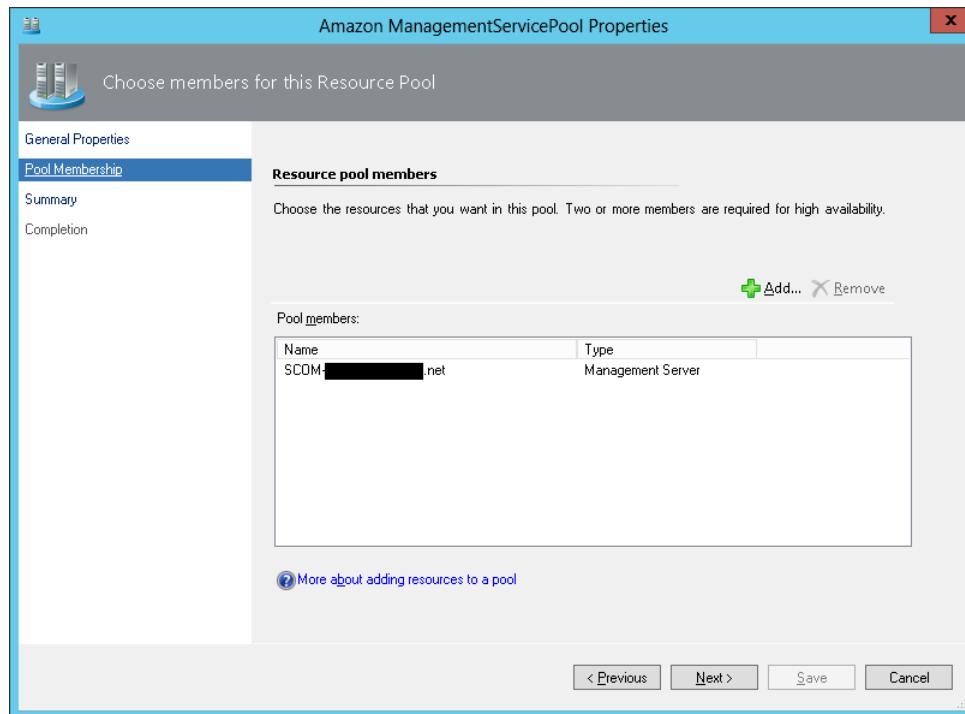
默认情况下，当您创建管理包对象、禁用规则或监控或者创建覆盖时，Operations Manager 会将此设置保存到默认管理包中。作为最佳做法，您应该为您想自定义的每个密封管理包创建一个独立管理包，而不是将您的自定义设置保存到默认管理包中。

6. AWS Management Pack 会自动创建一个资源池并将管理服务器添加到其中。要控制服务器成员资格，请执行以下更改：
  - a. 在 Go (转到) 菜单上单击 Administration (管理)。
  - b. 单击 Resource Pools (资源池) 节点。
  - c. 右键单击 Resource Pools (资源池) 窗格中的 AWS Resource Pool (AWS 资源池)，选择 Manual Membership (手动成员资格)。

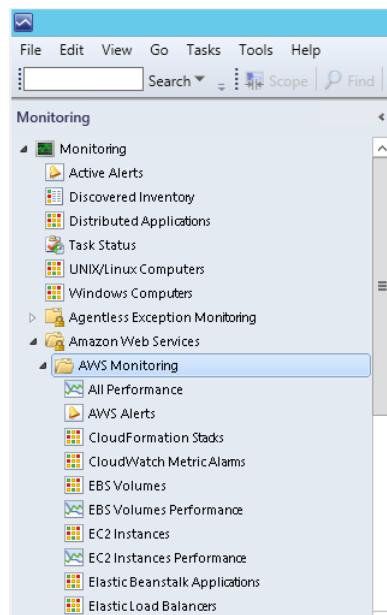


- d. 右键单击 Resource Pools (资源池) 窗格中的 AWS Resource Pool (AWS 资源池)，选择 Properties (属性)。

- e. 在 Pool Membership (池成员资格) 页面上，删除不应监控 AWS 资源的管理服务器。



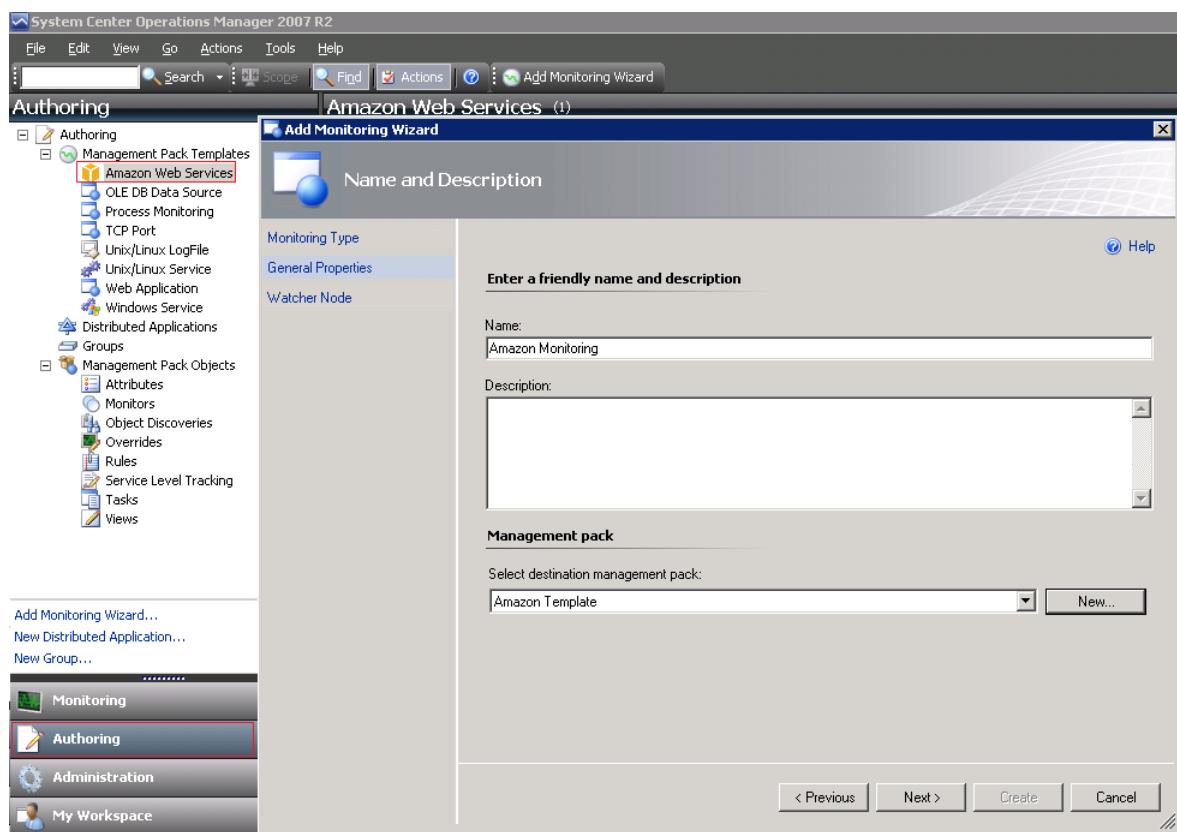
7. 配置 AWS Management Pack 之后，它将在操作控制台的 Monitoring 工作区中显示为 Amazon Web Services 文件夹的子文件夹。



## System Center 2007 R2

在 System Center Operations Manager 2007 上运行添加监视向导

1. 在操作控制台的 Go 菜单上，单击 Authoring。
2. 在创作工作区中，展开管理包模板节点并右键单击 Amazon Web Services，然后再单击添加监视向导。
3. 在添加监视向导的选择监视类型列表中，选择 Amazon Web Services，然后再单击下一步。
4. 在 General Properties (常规属性) 页面上的 Name (名称) 框中，输入名称（例如，“我的 AWS 资源”）。在 Description (描述) 框中输入描述。
5. 在 Select destination management pack (选择目标管理包) 下拉列表中，选择要用于保存设置的现有管理包（或单击 New (新建) 以新建一个）。单击 Next (下一步)。



### Note

默认情况下，当您创建管理包对象、禁用规则或监控或者创建覆盖时，Operations Manager 将设置保存到默认管理包中。作为最佳做法，您应该为您想自定义的每个密封管理包创建一个独立管理包，而不是将您的自定义设置保存到默认管理包中。

6. 在 Watcher Node Configuration (观察程序节点配置) 页面上的 Watcher Node (观察程序节点) 列表中，选择充当观察程序节点的代理托管计算机。
7. 在 Select AWS Run As account (选择 AWS 运行方式账户) 下拉列表中，选择您之前创建的 Run As 账户，然后单击 Create (创建)。
8. 配置 AWS Management Pack 之后，它会首先发现观察程序节点。要验证系统是否已成功发现观察程序节点，请在操作控制台中导航至 Monitoring 工作区。您应该会看到一个新的 Amazon Web

Services 文件夹，其下还有一个 Amazon Watcher Nodes 子文件夹。该子文件夹会显示观察程序节点。AWS Management Pack 自动检查并监控观察程序节点与 AWS 的连接。观察程序节点被发现之后，会显示在该列表中。观察程序节点准备就绪之后，其状态会变为 Healthy。



#### Note

要与 AWS 建立连接，AWS Management Pack 需要您向观察程序节点部署适用于 .NET 的 AWS 软件开发工具包、模块和脚本。这可能需要大约 10 分钟。如果观察程序节点没有显示或者您发现状态为 Not Monitored，请仔细检查您的 Internet 连接和 IAM 权限。有关更多信息，请参阅 [排查 AWS Management Pack 方面的问题 \(p. 805\)](#)。

The screenshot shows the Microsoft System Center Operations Manager interface. On the left, there is a navigation tree under the 'Monitoring' category. Under 'AWS Monitoring', there is a folder named 'AWS Watcher Nodes'. On the right, there is a table titled 'AWS Watcher Nodes (1)'. The table has columns for 'Look For:', 'State', 'Maintenance...', 'Name', 'Path', and 'Display Name'. There is one row in the table with the state set to 'Healthy', name 'MTabc on WIN...', path 'WIN-EWGY9OO...', and display name 'MTabc on WIN-...'. The 'State' column contains a green checkmark icon.

9. 系统发现观察程序节点之后，会触发从属发现，可以看到 AWS 资源添加到操作控制台的 Monitoring 工作区中。



#### Note

发现 AWS 资源的过程应该会在 20 分钟内完成，但也可能需要更长时间，具体取决于您的 Operations Manager 环境、AWS 环境、管理服务器负载和观察程序节点负载。有关更多信息，请参阅 [排查 AWS Management Pack 方面的问题 \(p. 805\)](#)。

## 步骤 5：配置端口和终端节点

### Abstract

启用适用于 Microsoft System Center 的 AWS 管理包来通过配置端口和终端节点监控 AWS 服务。

适用于 Microsoft System Center 的 AWS 管理包必须能与 AWS 服务通信，以便监控这些服务的执行并在 System Center 中提供警报。为了成功监控，必须将管理包服务器的防火墙配置为允许以下服务通过端口 80 和 443 对 AWS 终端节点进行出站 HTTP 调用。

这将允许对以下 AWS 服务进行监控：

- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing
- Auto Scaling
- AWS Elastic Beanstalk
- Amazon CloudWatch

- AWS CloudFormation

AWS 管理包使用适用于 .NET 的 AWS 开发工具包中的公用 API 通过端口 80 和 443 检索来自这些服务的信息。登录每台服务器并对端口 80 和 443 启用出站防火墙规则。

如果防火墙应用程序支持更详细的设置，您可以为每个服务配置特定终端节点。终端节点是作为 Web 服务入口点的 URL。例如，[ec2.us-west-2.amazonaws.com](http://ec2.us-west-2.amazonaws.com) 是 Amazon EC2 服务的入口点。要配置防火墙终端节点，请为要运行的 AWS 服务[找到特定终端节点 URL](#)，并在防火墙应用程序中指定这些终端节点。

## 使用 AWS Management Pack

### Abstract

监控 AWS 资源的运行状态、查看您的指标并执行上下文感知任务。

您可以使用 AWS Management Pack 监控 AWS 资源的运行状态。

#### 内容

- [视图 \(p. 785\)](#)
- [发现 \(p. 799\)](#)
- [监视器 \(p. 800\)](#)
- [规则 \(p. 800\)](#)
- [事件 \(p. 801\)](#)
- [运行状况模型 \(p. 801\)](#)
- [自定义 AWS Management Pack \(p. 803\)](#)

## 视图

AWS Management Pack 提供以下视图，这些视图显示在操作控制台的 Monitoring 工作区中。

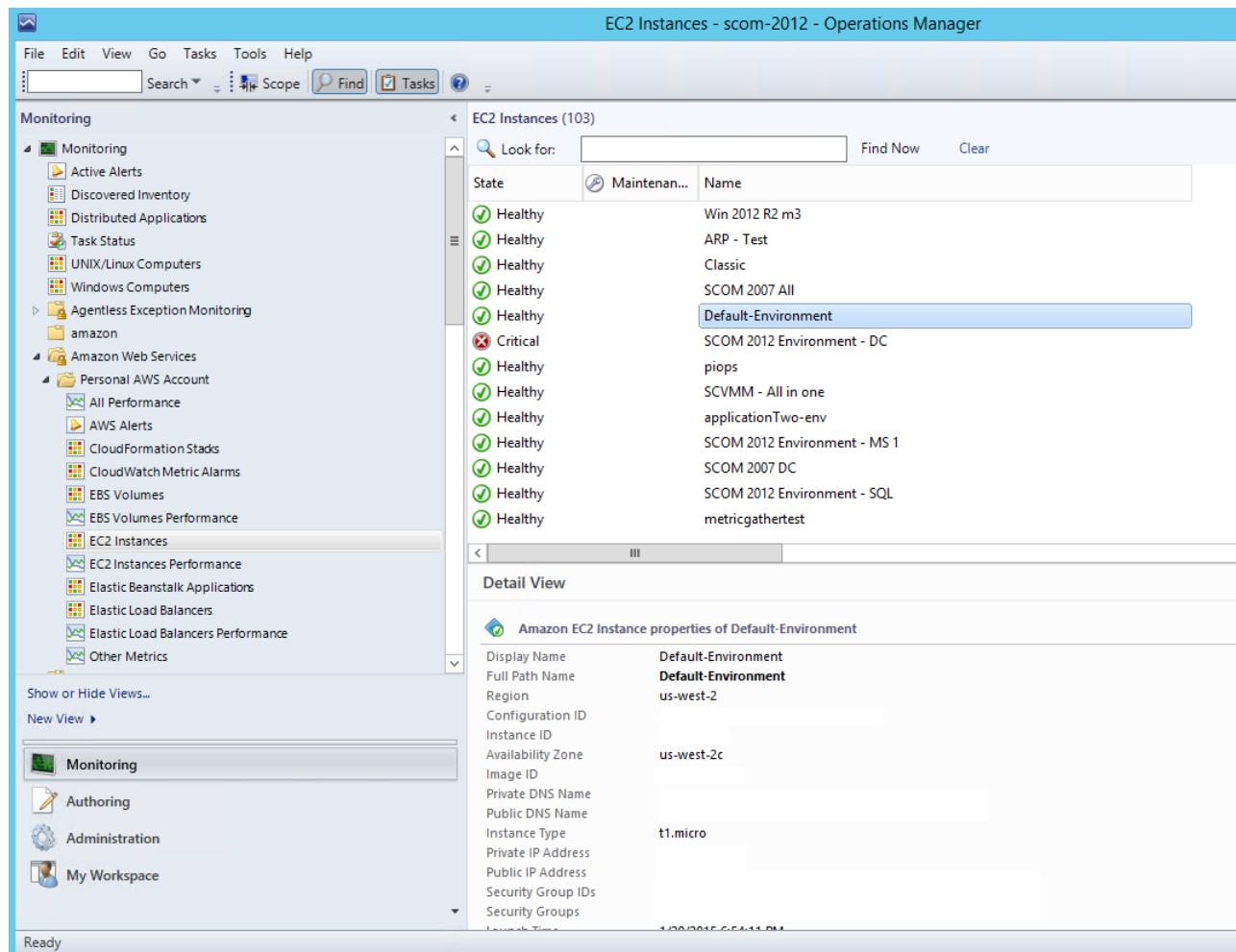
#### 视图

- [EC2 实例 \(p. 785\)](#)
- [Amazon EBS 卷 \(p. 787\)](#)
- [弹性负载均衡器 \(p. 789\)](#)
- [AWS Elastic Beanstalk 应用程序 \(p. 791\)](#)
- [AWS CloudFormation 堆栈 \(p. 793\)](#)
- [Amazon 性能视图 \(p. 795\)](#)
- [Amazon CloudWatch 指标警报 \(p. 796\)](#)
- [AWS 警报 \(p. 797\)](#)
- [观察程序节点 \(System Center Operations Manager 2007 R2\) \(p. 798\)](#)

## EC2 实例

查看所有可用区和区域中属于某特定 AWS 账户的 EC2 实例的运行状态。该视图还包括 Virtual Private Cloud (VPC) 中运行的 EC2 实例。AWS Management Pack 会检索标签，以便您可以使用这些标签来搜索和筛选该列表。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图

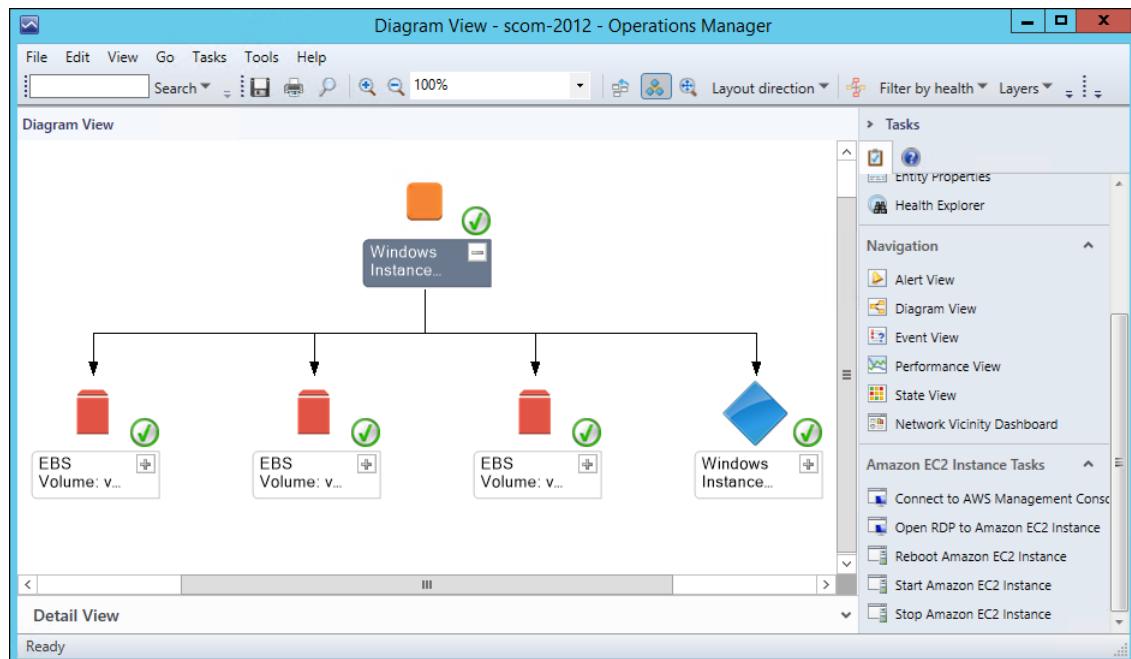


选择 EC2 实例时，您可以执行实例运行状况任务：

- Open Amazon Console：在 Web 浏览器中启动 AWS 管理控制台。
- Open RDP to Amazon EC2 Instance：打开指向所选 Windows 实例的 RDP 连接。
- Reboot Amazon EC2 Instance：重启所选 EC2 实例。
- Start Amazon EC2 Instance：启动所选 EC2 实例。
- Stop Amazon EC2 Instance：停止所选 EC2 实例。

#### EC2 实例关系图视图

显示实例与其他组件之间的关系。



## Amazon EBS 卷

显示所有可用区和区域中属于某特定 AWS 账户的所有 Amazon EBS 卷的运行状态。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图

The screenshot shows the Microsoft System Center Operations Manager interface titled "EBS Volumes - scom-2012 - Operations Manager". The left pane displays a navigation tree under the "Monitoring" category, including "Active Alerts", "Discovered Inventory", "Distributed Applications", "Task Status", "UNIX/Linux Computers", "Windows Computers", "Agentless Exception Monitoring", "amazon", "Amazon Web Services", "Personal AWS Account", "All Performance", "AWS Alerts", "CloudFormation Stacks", "CloudWatch Metric Alarms", "EBS Volumes", "EBS Volumes Performance", "EC2 Instances", "EC2 Instances Performance", "Elastic Beanstalk Applications", "Elastic Load Balancers", "Elastic Load Balancers Performance", and "Other Metrics". A "Show or Hide Views..." button and a "New View" link are also present. The right pane is titled "EBS Volumes (214)" and contains a table with the following data:

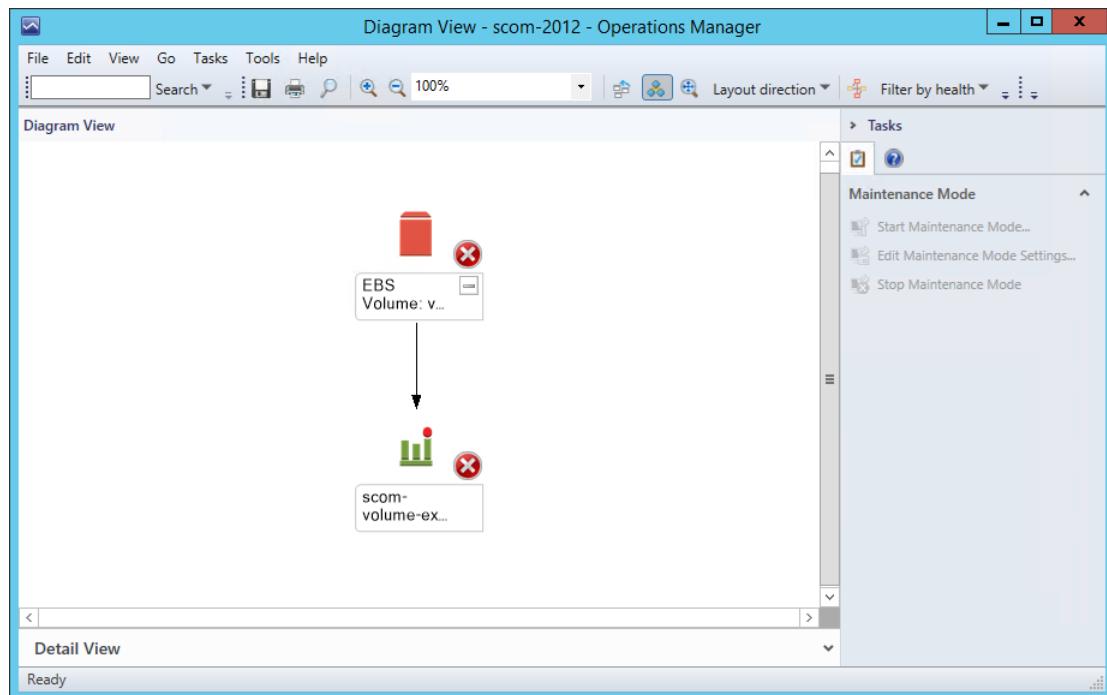
| State    | Maintain... | Display Name       | Volume ID | Availability Zone | Size | Create Time           |
|----------|-------------|--------------------|-----------|-------------------|------|-----------------------|
| Critical |             | EBS Volume: vo...  |           | us-west-2b        | 200  | 1/19/2015 6:35:58 PM  |
| Healthy  |             | regedit volume     |           | us-east-1c        | 30   | 8/22/2014 7:16:44 PM  |
| Healthy  |             | EBS Volume: vo...  |           | us-east-1c        | 100  | 8/22/2014 5:16:44 PM  |
| Healthy  |             | EBS Volume: vo...  |           | eu-west-1a        | 30   | 8/29/2014 9:08:44 PM  |
| Healthy  |             | EBS Volume: vo...  |           | ap-southeast-2a   | 150  | 8/22/2014 6:06:44 PM  |
| Healthy  |             | EBS Volume: vo...  |           | us-west-2a        | 250  | 3/2/2015 8:07:55 PM   |
| Healthy  |             | EBS Volume: vo...  |           | ap-southeast-2b   | 10   | 1/11/2015 12:55:55 PM |
| Healthy  |             | EBS Volume: vo...  |           | eu-west-1c        | 10   | 1/19/2015 11:25:55 PM |
| Healthy  |             | reboot loop vol... |           | eu-west-1a        | 80   | 8/28/2014 10:05:55 PM |
| Healthy  |             | EBS Volume: vo...  |           | us-west-2c        | 75   | 8/23/2014 11:15:55 PM |
| Healthy  |             | EBS Volume: vo...  |           | ap-southeast-2a   | 30   | 8/29/2014 12:25:55 PM |
| Healthy  |             | EBS Volume: vo...  |           | us-east-1c        | 30   | 8/28/2014 11:18:55 PM |
| Healthy  |             | EBS Volume: vo...  |           | us-east-1b        | 100  | 8/23/2014 3:29:55 PM  |
| Healthy  |             | EBS Volume: vo...  |           | eu-west-1a        | 100  | 8/29/2014 9:07:55 PM  |

The "Detail View" section shows properties for a selected EBS volume, including:

- Display Name: **us-west-2**
- Region: **us-west-2**
- Volume ID: **gp2**
- Account Guid: **1/19/2015 6:35:58 PM**
- Availability Zone: **us-west-2b**
- Size: **200**
- IOPS: **600**
- Attachments: **Snapshot ID**
- Volume Type: **gp2**
- Create Time: **1/19/2015 6:35:58 PM**
- Tags: **None**

### Amazon EBS 卷关系图视图

显示一个 Amazon EBS 卷和所有相关警报。下图显示了一个示例：

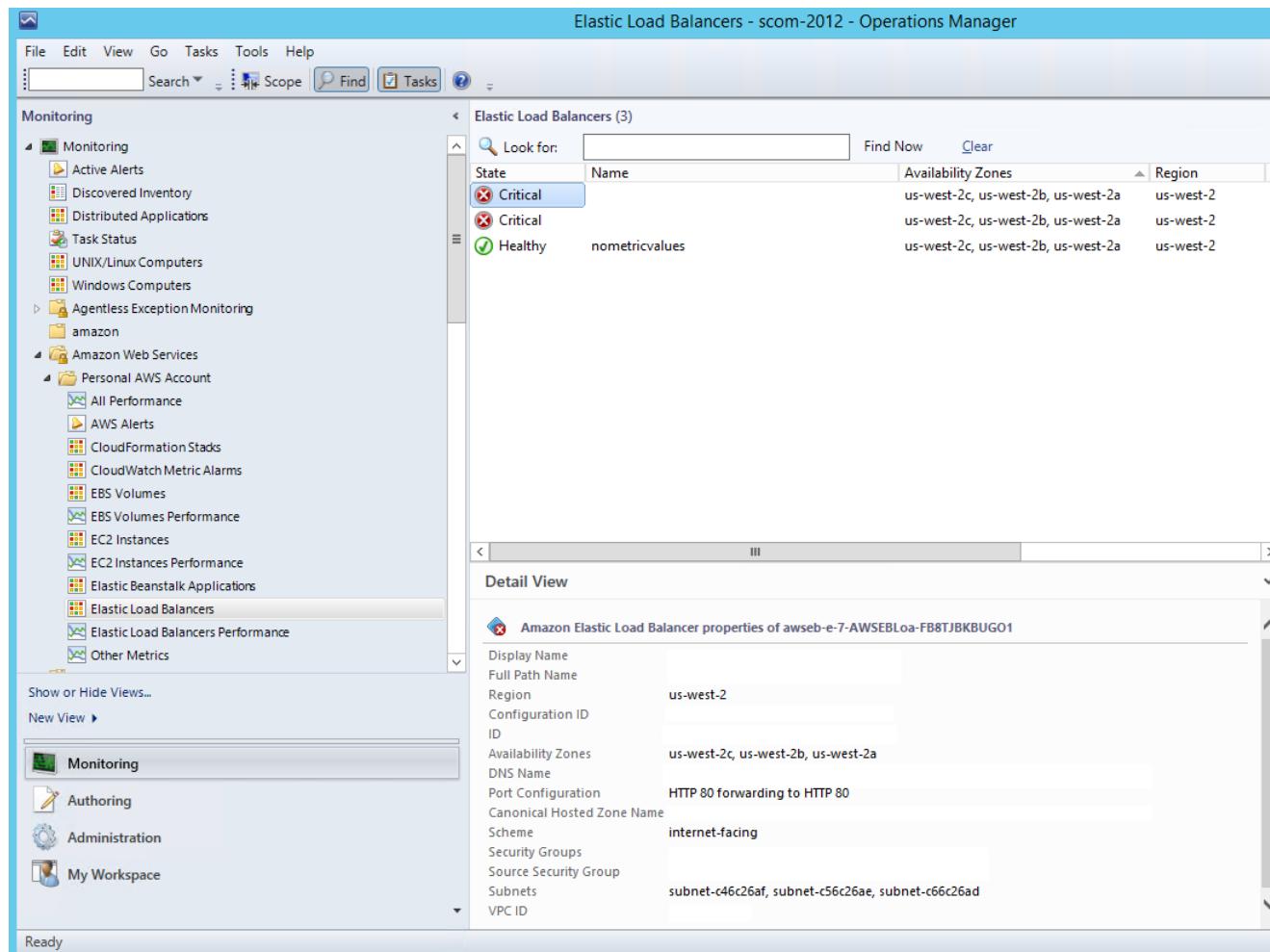


## 弹性负载均衡器

显示所有区域中属于某特定 AWS 账户的所有负载均衡器的运行状态。

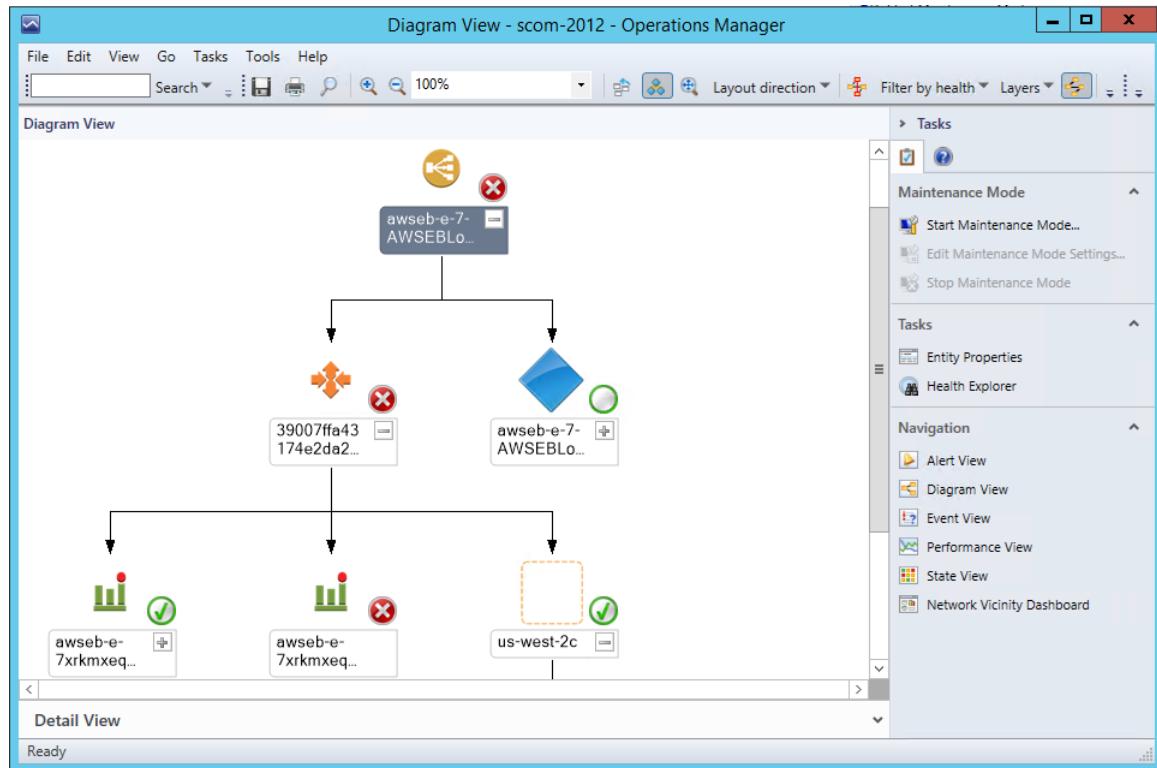
Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图

---



### Elastic Load Balancing 关系图视图

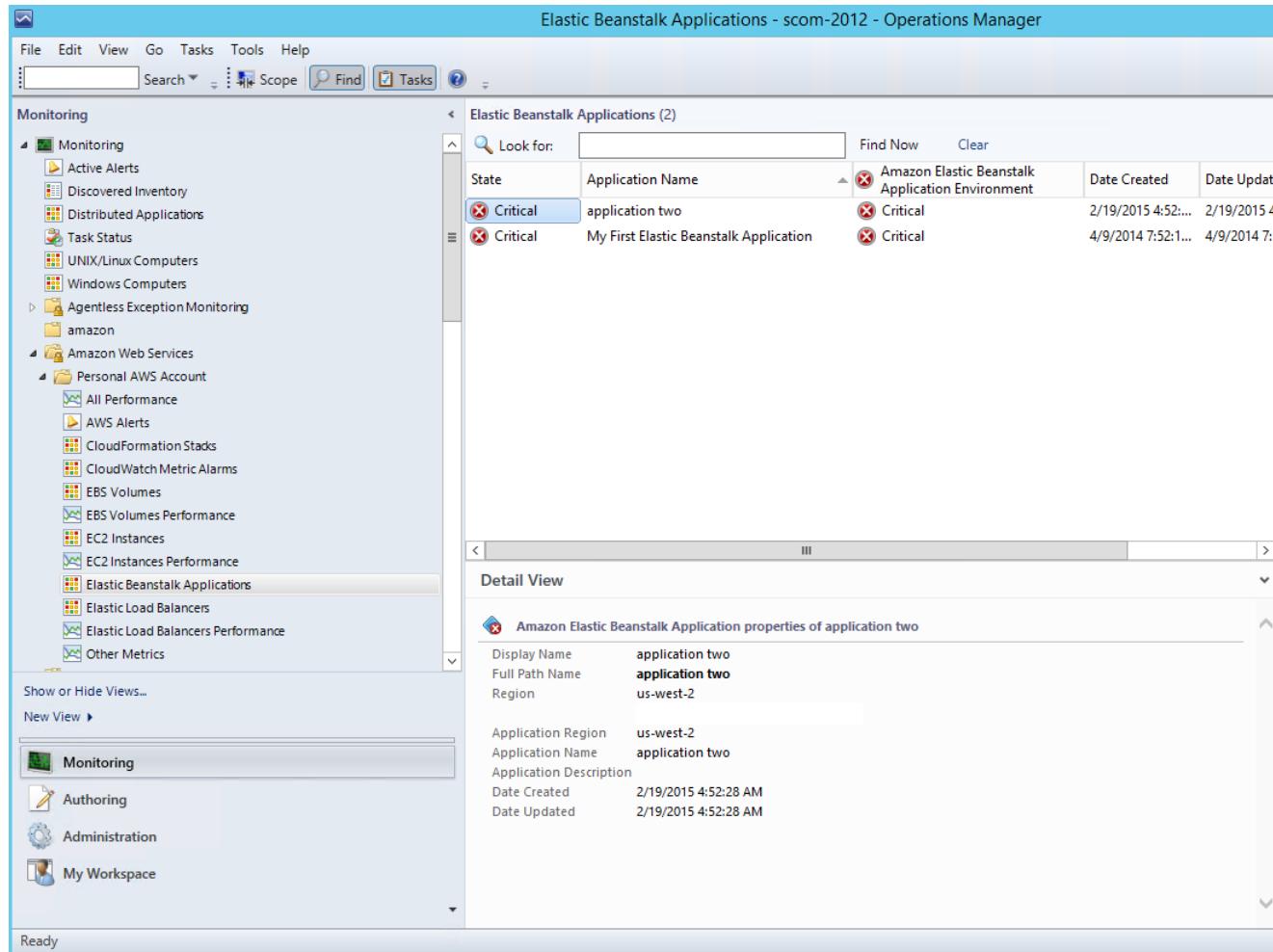
显示 Elastic Load Balancing 与其他组件之间的关系。下图显示了一个示例：



## AWS Elastic Beanstalk 应用程序

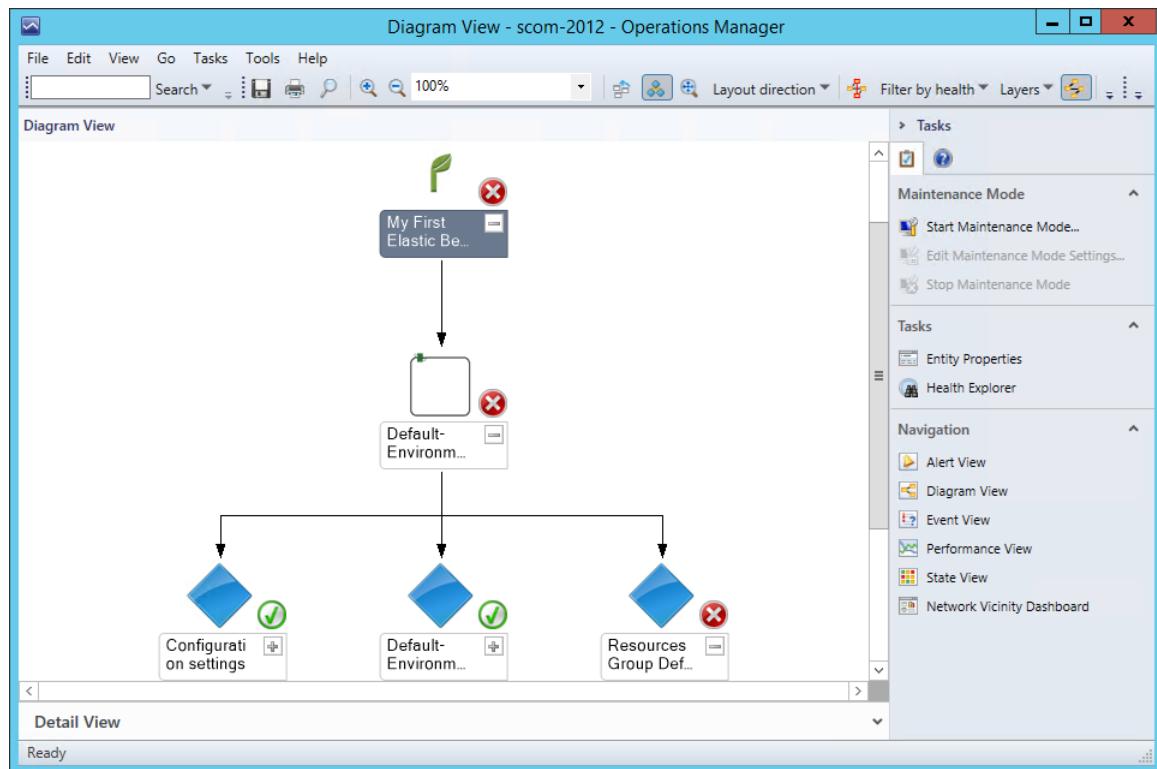
显示所有已发现的 AWS Elastic Beanstalk 应用程序的状态。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图



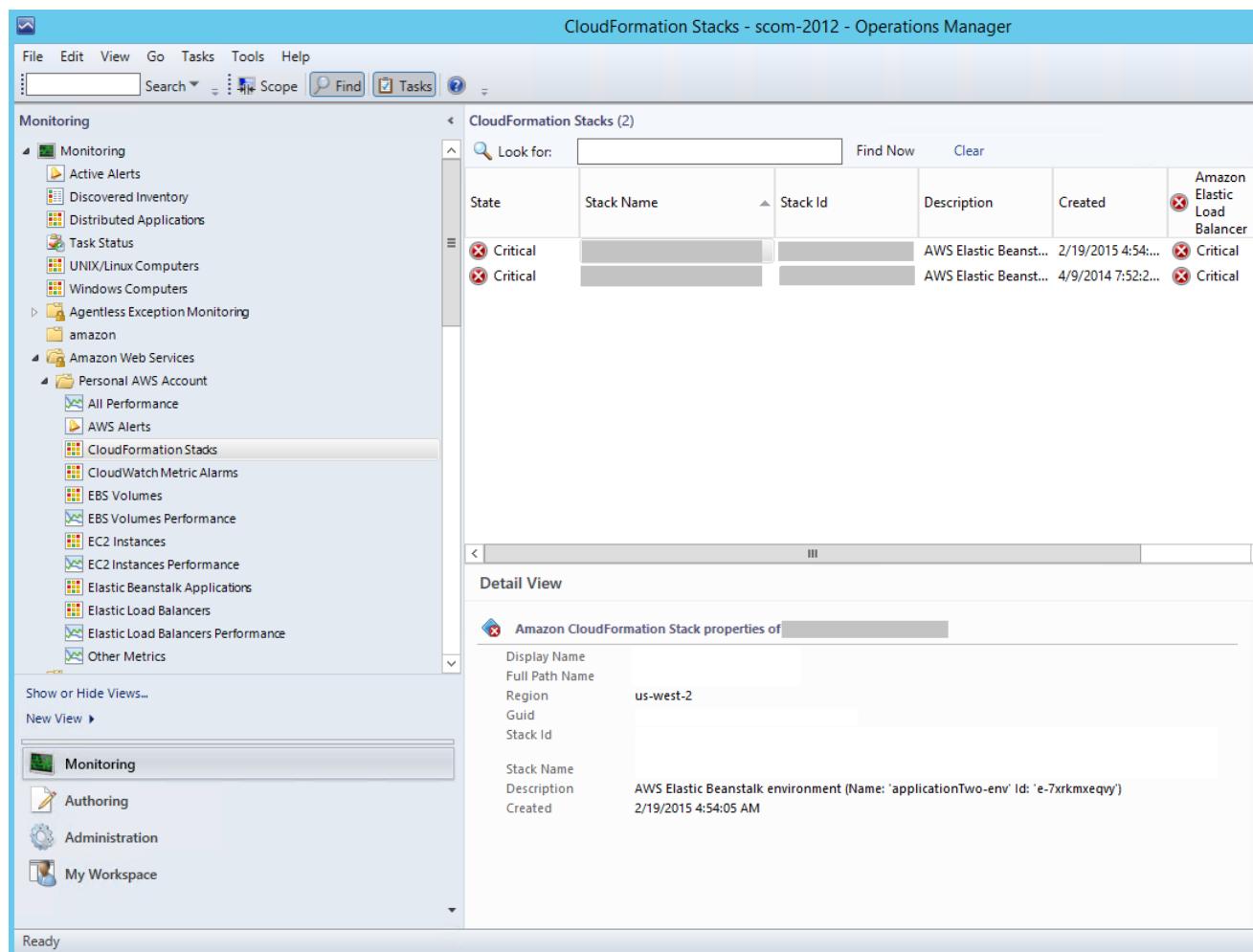
### AWS Elastic Beanstalk 应用程序关系图视图

显示 AWS Elastic Beanstalk 应用程序、应用程序环境、应用程序配置和应用程序资源对象。



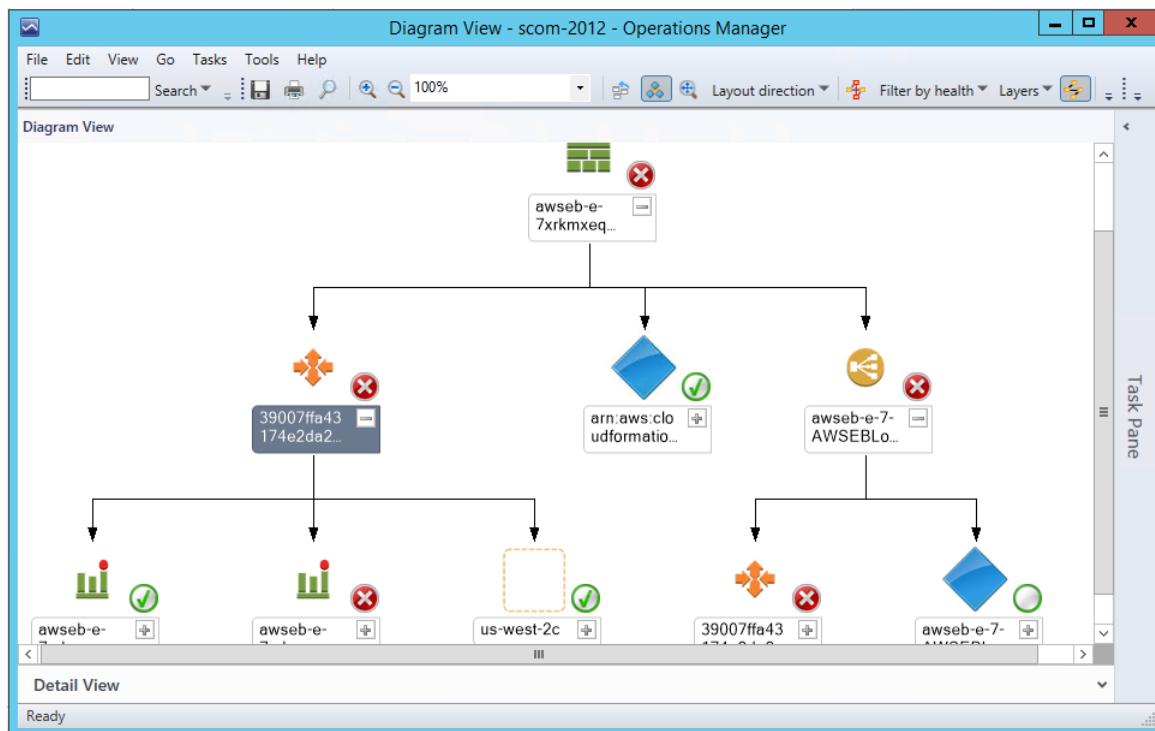
## AWS CloudFormation 堆栈

显示所有区域中属于某特定 AWS 账户的所有 AWS CloudFormation 堆栈的运行状态。



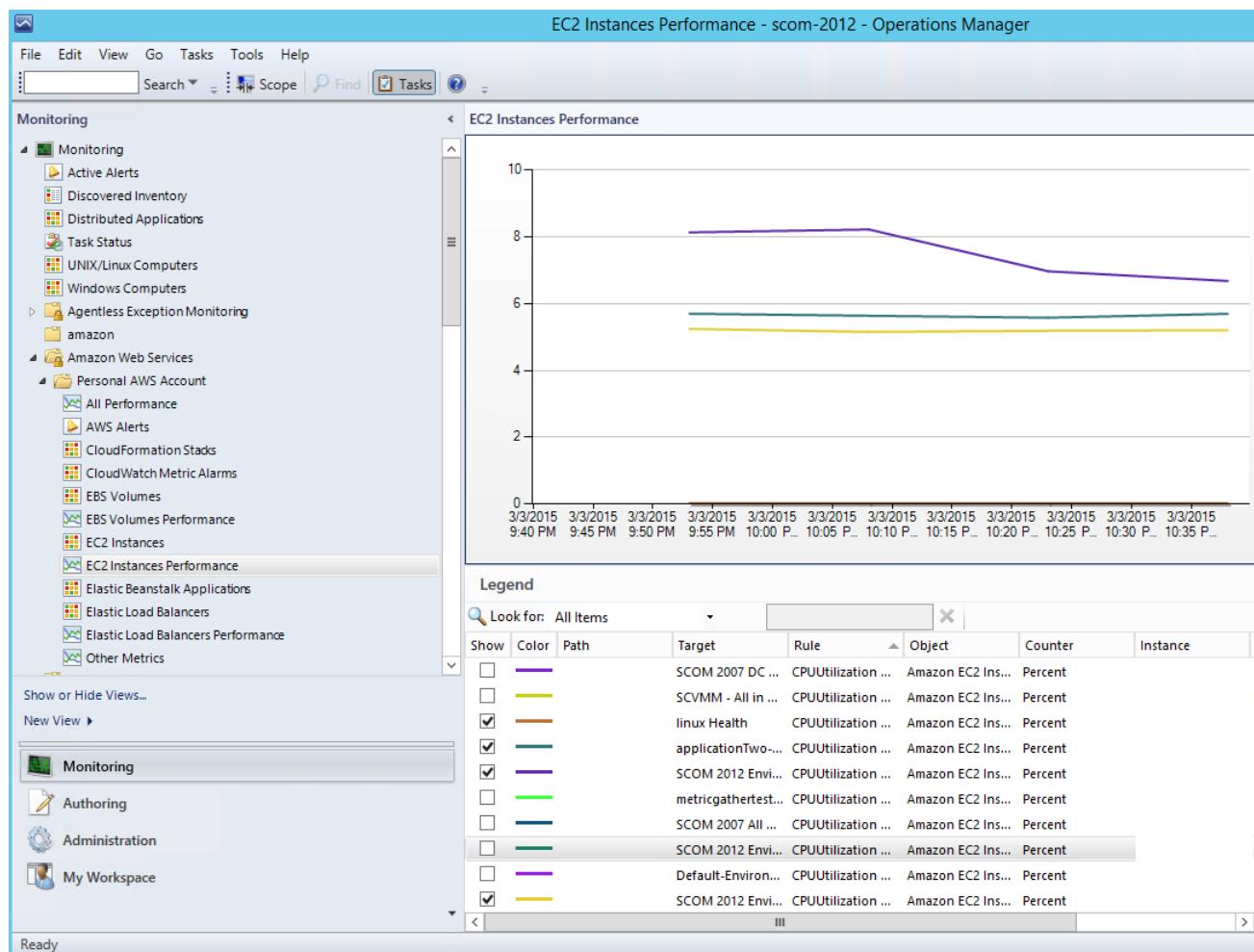
#### AWS CloudFormation 堆栈关系图视图

显示 AWS CloudFormation 堆栈与其他组件之间的关系。一个 AWS CloudFormation 堆栈可包含 Amazon EC2 或 Elastic Load Balancing 资源。下图显示了一个示例：



## Amazon 性能视图

显示 Amazon EC2、Amazon EBS 和 Elastic Load Balancing 的 Amazon CloudWatch 指标、自定义指标以及从 CloudWatch 警报创建的指标。此外，每个资源还有单独的性能视图。Other Metrics 性能视图包含自定义指标和从 CloudWatch 警报创建的指标。有关这些指标的更多信息，请参阅 [Amazon CloudWatch Developer Guide 中的 CloudWatch Metrics, Namespaces, and Dimensions Reference](#)。下图显示了一个示例。



## Amazon CloudWatch 指标警报

显示与已发现的 AWS 资源相关的 Amazon CloudWatch 警报。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图

The screenshot shows the Microsoft System Center Operations Manager interface with the title bar "CloudWatch Metric Alarms - scom-2012 - Operations Manager". The left navigation pane is titled "Monitoring" and includes sections for Active Alerts, Discovered Inventory, Distributed Applications, Task Status, UNIX/Linux Computers, Windows Computers, Agentless Exception Monitoring, Amazon Web Services, Personal AWS Account, and CloudWatch Metric Alarms. The "CloudWatch Metric Alarms" section is currently selected. The main pane displays a table titled "CloudWatch Metric Alarms (11)". The table columns are State, Alarm Name, Metric Name, Condition, and Description. The data is as follows:

| State    | Alarm Name                    | Metric Name                   | Condition                              | Description         |
|----------|-------------------------------|-------------------------------|----------------------------------------|---------------------|
| Critical | dynamo test alarm             | ProvisionedWriteCapacityUn... | ProvisionedWriteCapacityUnits <= 10... | should always alarm |
| Critical | scom-volume-exists-test       | VolumeReadBytes               | VolumeReadBytes >= 0                   |                     |
| Critical | awseb-e-qazu95f2zm-stack-A... | NetworkOut                    | NetworkOut < 2000000                   | Elastic...          |
| Critical | elb alarm                     | HealthyHostCount              | HealthyHostCount <= 10                 | Elastic...          |
| Critical | awseb-e-7xrkmxeqvy-stack-A... | NetworkOut                    | NetworkOut < 2000000                   | Elastic...          |
| Healthy  | awseb-e-qazu95f2zm-stack-A... | NetworkOut                    | NetworkOut > 6000000                   | Elastic...          |
| Healthy  | awseb-e-7xrkmxeqvy-stack-A... | NetworkOut                    | NetworkOut > 6000000                   | Elastic...          |
| Healthy  | testalarm                     | VolumeReadBytes               | VolumeReadBytes <= 50000               | hi                  |
| Healthy  | az_alarm                      | Latency                       | Latency <= 1                           | scom...             |
| Healthy  | awsec2-i-cc4811c4-High-CPU... | CPUUtilization                | CPUUtilization < 80                    | Create...           |
| Healthy  | scom-bug-alarm                | CPUUtilization                | CPUUtilization <= 80                   | check...            |

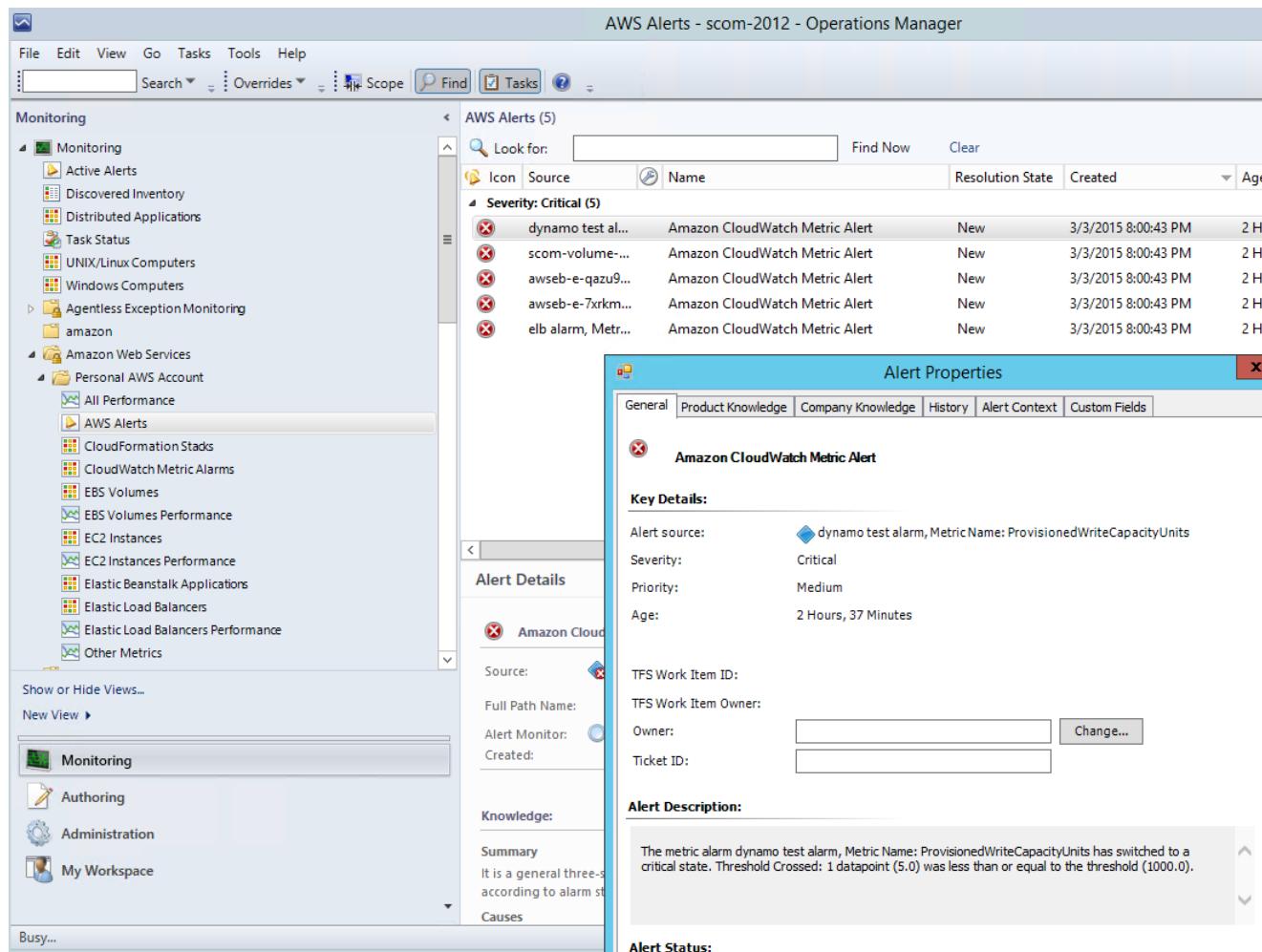
Below the table, a "Detail View" section is expanded for the "Amazon CloudWatch Alarm properties of dynamo test alarm, Metric Name: ProvisionedWriteCapacityUnits". The details are:

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| Display Name   | dynamo test alarm, Metric Name: ProvisionedWriteCapacityUnits     |
| Full Path Name | dynamo test alarm, Metric Name: ProvisionedWriteCapacityUnits     |
| Region         | us-west-2                                                         |
| Alarm ID       | arn:aws:cloudwatch:us-west-2:946130359068:alarm:dynamo test alarm |
| Description    | should always alarm                                               |
| Condition      | ProvisionedWriteCapacityUnits <= 1000                             |
| Alarm Name     | dynamo test alarm                                                 |
| Metric Name    | ProvisionedWriteCapacityUnits                                     |
| Namespace      | AWS/DynamoDB                                                      |
| Threshold      | 1000                                                              |
| Unit           |                                                                   |

## AWS 警报

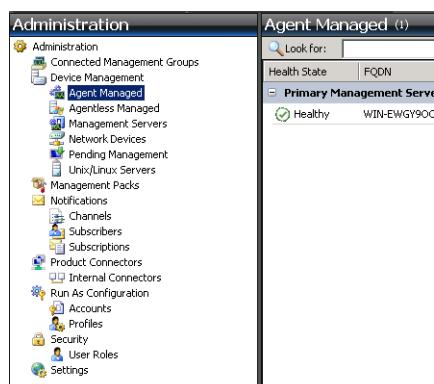
显示当对象的运行状况处于临界状态时 AWS 管理包产生的警报。

Amazon Elastic Compute Cloud Microsoft Windows 实例用  
户指南  
视图



## 观察程序节点 (System Center Operations Manager 2007 R2)

查看受监控的所有 AWS 账户上观察程序节点的运行状态。Healthy (正常) 状态表明观察程序节点已正确配置并且可以与 AWS 通信。



## 发现

发现结果是 AWS Management Pack 所监视的 AWS 资源。AWS Management Pack 发现以下对象：

- Amazon EC2 实例
- EBS 卷
- ELB 负载均衡器
- AWS CloudFormation 堆栈
- Amazon CloudWatch 警报
- AWS Elastic Beanstalk 应用程序
- Auto Scaling 组和可用区

Amazon CloudWatch 指标是针对以下资源生成的：

- Amazon EC2 实例
- EBS 卷
- Elastic Load Balancing
- 自定义 Amazon CloudWatch 指标
- 来自现有 Amazon CloudWatch 警报的指标

对于 Amazon CloudWatch 指标发现，以下指导适用：

- AWS CloudFormation 堆栈没有任何默认的 Amazon CloudWatch 指标。
- 已停止的 Amazon EC2 实例和未使用的 Amazon EBS 卷不会生成用于各自默认 Amazon CloudWatch 指标的数据。
- 启动 Amazon EC2 实例后，Amazon CloudWatch 指标最多需要 30 分钟才会显示在 Operations Manager 中。
- Amazon CloudWatch 会保留监控数据两周，即使您的 AWS 资源已被终止也会保留。此类数据会显示在 Operations Manager 中。
- 不支持的资源的现有 Amazon CloudWatch 警报将会创建指标并与 Amazon CloudWatch 警报关联。可以在“Other Metrics”性能视图中查看这些指标。

AWS Management Pack 还会发现以下关系：

- AWS CloudFormation 堆栈及其 Elastic Load Balancing 或 Amazon EC2 资源
- Elastic Load Balancing 负载均衡器与其 EC2 实例
- Amazon EC2 实例及其 EBS 卷
- Amazon EC2 实例及其操作系统
- AWS Elastic Beanstalk 应用程序及其环境、配置和资源

AWS Management Pack 会自动发现 EC2 实例与其上运行的操作系统之间的关系。要发现此类关系，实例上必须已安装和配置 Operations Manager 代理，且 Operations Manager 中必须已导入相应的操作系统管理包。

发现功能在资源池中的管理服务器 (System Center 2012) 或观察程序节点 (System Center 2007 R2) 上运行。

| 发现                                           | 间隔 ( 秒 ) |
|----------------------------------------------|----------|
| Amazon 资源发现 (SCOM 2012)                      | 14400    |
| 发现 EC2 实例、Amazon EBS 卷、负载均衡器和 CloudFront 堆栈。 |          |
| AWS Elastic Beanstalk 发现                     | 14400    |
| 发现 AWS Elastic Beanstalk 及其与环境、资源和配置的关系。     |          |
| CloudWatch 警报发现                              | 900      |
| 发现使用 CloudWatch 指标生成的警报。                     |          |
| 自定义 CloudWatch 指标发现                          | 14400    |
| 发现自定义 CloudWatch 指标。                         |          |
| 观察程序节点发现 (SCOM 2007 R2)                      | 14400    |
| 定位根管理服务器并创建观察程序节点对象。                         |          |

## 监视器

监视器用于衡量 AWS 资源的运行状况。监控功能在资源池中的管理服务器 (System Center 2012) 或观察程序节点 (System Center 2007 R2) 上运行。

| 监视器                                       | 间隔 ( 秒 ) |
|-------------------------------------------|----------|
| AWS CloudFormation 堆栈状态                   | 900      |
| Amazon CloudWatch 指标警报                    | 300      |
| Amazon EBS 卷状态                            | 900      |
| Amazon EC2 实例状态                           | 900      |
| Amazon EC2 实例系统状态                         | 900      |
| AWS Elastic Beanstalk 状态                  | 900      |
| 观察程序节点与 Amazon Cloud 的连接情况 (SCOM 2007 R2) | 900      |

## 规则

规则会创建警报 ( 依据 Amazon CloudWatch 指标 ) 并收集数据以用于分析和报告。

| 规则                                                                                                                                                                                   | 间隔 ( 秒 ) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| AWS 资源发现规则 (SCOM 2007 R2)<br><br>确定目标观察程序节点并借助 AWS API 发现以下 AWS 资源的对象 : EC2 实例、EBS 卷、负载均衡器和 AWS CloudFormation 堆栈。 ( 不发现 CloudWatch 指标或警报 ) 。发现完成后，查看处于 Not Monitored ( 未监视 ) 状态的对象。 | 14400    |
| Amazon Elastic Block Store 卷性能指标数据收集规则                                                                                                                                               | 900      |

| 规则                                  | 间隔 ( 秒 ) |
|-------------------------------------|----------|
| Amazon EC2 实例性能指标数据收集规则             | 900      |
| Elastic Load Balancing 均衡性能指标数据收集规则 | 900      |
| 自定义 CloudWatch 指标数据收集规则             | 900      |

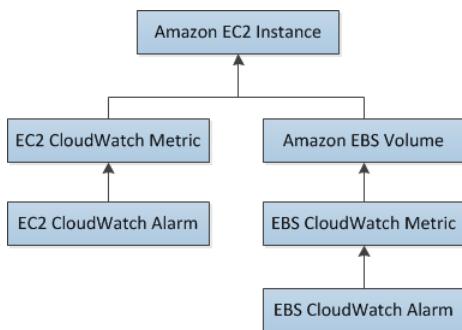
## 事件

事件会报告涉及受监视资源的活动。系统会将相关事件写入 Operations Manager 事件日志。

| 事件 ID | 说明                                                                        |
|-------|---------------------------------------------------------------------------|
| 4101  | Amazon EC2 实例发现 ( 常规发现 ) 已完成                                              |
| 4102  | Elastic Load Balancing 指标发现、<br>Amazon EBS 卷指标发现、<br>Amazon EC2 实例指标发现已完成 |
| 4103  | Amazon CloudWatch 指标警报发现已完成                                               |
| 4104  | Amazon Windows 计算机发现已完成                                                   |
| 4105  | Amazon 指标警报收集已完成                                                          |
| 4106  | EC2 实例计算机关系发现已完成                                                          |
| 4107  | AWS CloudFormation 堆栈状态收集已完成                                              |
| 4108  | 观察程序节点可用性状态收集已完成                                                          |
| 4109  | Amazon 指标收集规则已完成                                                          |
| 4110  | Amazon 实例状态更改任务已完成                                                        |
| 4111  | EC2 实例状态监视器状态已完成                                                          |
| 4112  | Amazon EBS 卷状态监视器状态已完成                                                    |
| 4113  | Amazon EC2 实例预定事件监视器状态已计算                                                 |
| 4114  | Amazon EBS 预定事件监视器状态已计算                                                   |
| 4115  | Elastic Beanstalk 发现已完成                                                   |
| 4116  | Elastic Beanstalk 环境状态已计算                                                 |
| 4117  | Elastic Beanstalk 环境操作状态已计算                                               |
| 4118  | Elastic Beanstalk 环境配置状态已计算                                               |

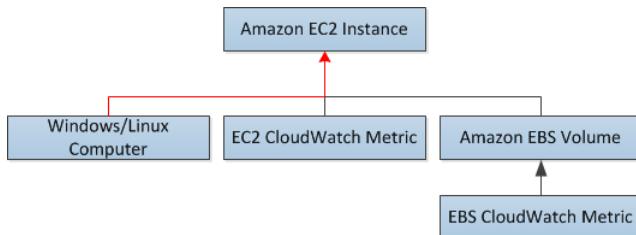
## 运行状况模型

下图显示了 AWS Management Pack 定义的运行状况模型。



CloudWatch 警报的运行状况汇总其相应 CloudWatch 指标。Amazon EC2 的 CloudWatch 指标的运行状况汇总到 EC2 实例。同样，Amazon EBS 的 CloudWatch 指标的运行状况汇总到 Amazon EBS 卷。EC2 实例所使用的 Amazon EBS 卷的运行状况汇总到 EC2 实例。

系统发现 EC2 实例与其操作系统之间的关系之后，操作系统运行状况汇总到 EC2 实例。

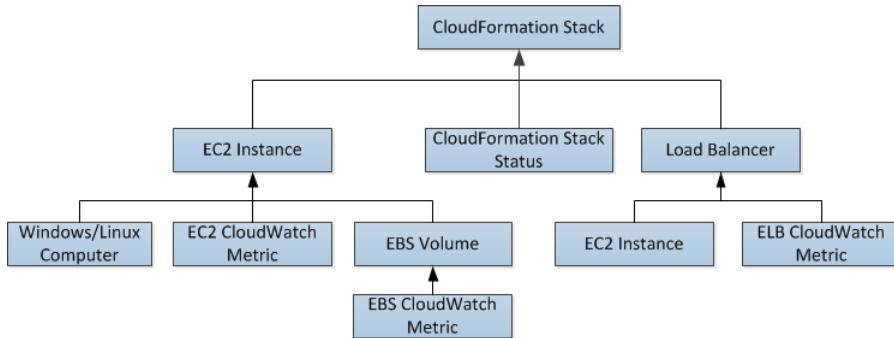


AWS CloudFormation 堆栈的运行状态取决于 AWS CloudFormation 堆栈本身的状态及其资源（即负载均衡器和 EC2 实例）的运行状态。

下表是 AWS CloudFormation 堆栈与其运行状态之间的对应关系。

| 运行状态 | AWS CloudFormation 堆栈状态                                                                                 | 备注         |
|------|---------------------------------------------------------------------------------------------------------|------------|
| 错误   | CREATE_FAILED<br>DELETE_IN_PROGRESS<br>DELETE_FAILED<br>UPDATE_ROLLBACK_FAILED                          | 可能可用       |
| 警告   | UPDATE_ROLLBACK_IN_PROGRESS<br>UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS<br>UPDATE_ROLLBACK_COMPLETE | 部分问题解决后会恢复 |
| 正常   | CREATE_COMPLETE<br>UPDATE_IN_PROGRESS<br>UPDATE_COMPLETE_CLEANUP_IN_PROGRESS<br>UPDATE_COMPLETE         | 可用         |

AWS CloudFormation 堆栈的完整健康模型如下所示：



## 自定义 AWS Management Pack

要更改发现、规则和监控器的频率，您可以覆盖间隔时间（以秒为单位）。

### 更改频率

1. 在 Operations Manager 工具栏中，单击 Go，然后单击 Authoring。
2. 在 Authoring 窗格中，展开 Management Pack Objects，然后单击要更改的对象（例如，Object Discoveries、Rules 或 Monitors）。
3. 在工具栏中，单击 Scope。
4. 在 Scope Management Pack Objects 对话框中，单击 View all targets。
5. 要将范围限制到 Amazon 对象，请在 Look for 字段中键入 Amazon。
6. 选择要配置的对象，然后单击 OK。
7. 在 Operations Manager 中心窗格中，右键单击要配置的对象，单击 Overrides，然后单击要配置的覆盖类型。
8. 使用 Override Properties 对话框可为对象配置不同的值和设置。



### Tip

要禁用发现、规则或监控对象，请在 Operations Manager 中心窗格中右键单击要禁用的对象，单击 Overrides，然后单击 Disable the Rule。您有时可能需要禁用规则，例如，在您不运行 AWS Elastic Beanstalk 应用程序或使用自定义 Amazon CloudWatch 指标的情况下。

有关创建覆盖的信息，请参阅 Microsoft TechNet 网站上的 [使用目标设定和替代来优化监视](#)。

有关创建自定义规则和监视器的信息，请参阅 Microsoft TechNet 网站上的 [Authoring for System Center 2012 - Operations Manager](#) 或 [System Center Operations Manager 2007 R2 Management Pack Authoring Guide](#)。

## 升级 AWS Management Pack

您将用于更新 AWS Management Pack 的过程取决于 System Center 的版本。

## System Center 2012

### 升级 AWS Management Pack

1. 在 [AWS Add-Ins for Microsoft System Center](#) 网站上，单击 SCOM 2012。将 AWS-SCOM-MP-2.0-2.5.zip 下载到您的计算机并解压缩。.zip 文件包括 Amazon.AmazonWebServices.mpb。
2. 在操作控制台的 Go 菜单上，依次单击 Administration 和 Management Packs。
3. 在 Tasks 窗格中，单击 Import Management Packs。
4. 在 Select Management Packs 页面中，依次单击 Add 和 Add from disk。
5. 在 Select Management Packs to import 对话框中，从下载 Amazon.AmazonWebServices.mpb 文件的位置选择该文件，然后单击 Open。
6. 在 Select Management Packs 页面的 Import list 下，选择 Amazon Web Services 管理包，然后单击 Install。

如果 Install 按钮已禁用，则不支持升级到最新版本。您必须先卸载 AWS Management Pack，然后才能安装最新版本。有关更多信息，请参阅 [卸载 AWS Management Pack \(p. 805\)](#)。

## System Center 2007 R2

### 升级 AWS Management Pack

1. 在管理服务器上，转到 [AWS Add-Ins for Microsoft System Center](#) 网站，然后单击 SCOM 2007。保存 AWS-MP-Setup-2.5.msi，然后运行该文件。
2. 单击 Next 并按照指示升级您之前安装的组件。
3. 如果根管理服务器、操作控制台和观察程序节点位于不同的计算机上，则必须在每台计算机上下载和运行安装程序。
4. 在观察程序节点上，以管理员身份打开命令提示符窗口并运行以下命令。

```
C:\> net stop HealthService
The System Center Management service is stopping.
The System Center Management service was stopped successfully.

C:\> net start HealthService
The System Center Management service is starting.
The System Center Management service was started successfully.
```

5. 在操作控制台的 Go 菜单上，依次单击 Administration 和 Management Packs。
6. 在 Actions 窗格中，单击 Import Management Packs。
7. 在 Select Management Packs 页面中，依次单击 Add 和 Add from disk。
8. 在 Select Management Packs to import 对话框中，将目录更改为 C:\Program Files (x86)\Amazon Web Services Management Pack，选择 Amazon.AmazonWebServices.mpb 文件，然后单击 Open。
9. 在 Select Management Packs 页面的 Import list 下，选择 Amazon Web Services 管理包，然后单击 Install。

如果 Install 按钮已禁用，则不支持升级到最新版本，您必须先卸载 AWS Management Pack。有关更多信息，请参阅 [卸载 AWS Management Pack \(p. 805\)](#)。

## 卸载 AWS Management Pack

如果需要卸载 AWS Management Pack，请按照以下过程操作。

### System Center 2012

#### 卸载 AWS Management Pack

1. 在操作控制台的 Go 菜单上，依次单击 Administration 和 Management Packs。
2. 右键单击 Amazon Web Services，并选择 Delete。
3. 在 Dependent Management Packs 对话框中，记下相关的管理包，然后单击 Close。
4. 右键单击相关管理包并选择 Delete。
5. 右键单击 Amazon Web Services 并选择 Delete。

### System Center 2007 R2

#### 卸载 AWS Management Pack

1. 完成上一部分中针对 System Center 2012 所述的步骤 1 到步骤 5。
2. 在控制面板中，打开“程序和功能”。选择 Amazon Web Services Management Pack，然后单击卸载。
3. 如果根管理服务器、操作控制台和观察程序节点位于不同的计算机上，则必须在每台计算机上重复此过程。

## 排查 AWS Management Pack方面的问题

### Abstract

排查 AWS Management Pack方面的问题。

以下是常见的错误、事件和故障排除步骤。

#### 内容

- [错误 4101 和 4105 \(p. 805\)](#)
- [错误 4513 \(p. 806\)](#)
- [事件 623 \(p. 806\)](#)
- [事件 2023 和 2120 \(p. 806\)](#)
- [事件 6024 \(p. 807\)](#)
- [System Center 2012 — Operations Manager 的一般故障排除 \(p. 807\)](#)
- [System Center 2007 R2 的一般故障排除 \(p. 807\)](#)

## 错误 4101 和 4105

如果您收到以下错误之一，则必须升级 AWS Management Pack。有关更多信息，请参阅 [升级 AWS Management Pack \(p. 803\)](#)。

```
Error 4101
Exception calling "DescribeVolumes" with "1" argument(s): "AWS was not able to
validate the
provided access credentials"
```

```
Error 4105
Exception calling "DescribeApplications" with "0" argument(s): "The security
token included
in the request is invalid"
```

## 错误 4513

如果您收到以下错误之一，则必须升级 AWS Management Pack。有关更多信息，请参阅 [升级 AWS Management Pack \(p. 803\)](#)。

```
Error 4513
The callback method DeliverDataToModule failed with exception "Resolution of
the dependency
failed, type = "Amazon.SCOM.SDK.Interfaces.IMonitorSdk", name = "(none)".
Exception occurred while: Calling constructor Amazon.SCOM.SDK.CloudWatch.AwsMon
itorSdk
(System.String awsAccessKey, System.String awsSecretKey).
Exception is: InvalidOperationException - Collection was modified; enumeration
operation
may not execute.
```

## 事件 623

如果您在 Windows 事件日志中找到以下事件，请遵循 [KB975057](#) 中所述的解决方案。

```
Event ID: 623
HealthService (process_id) The version store for instance instance ("name") has
reached
its maximum size of size MB. It is likely that a long-running transaction is
preventing
cleanup of the version store and causing it to build up in size. Updates will
be rejected
until the long-running transaction has been completely committed or rolled back.

Possible long-running transaction:
SessionId: id
Session-context: value
Session-context ThreadId: id
Cleanup: value
```

## 事件 2023 和 2120

如果您在 Windows 事件日志中找到以下事件，请参阅 [事件 ID 2023 和 2120](#) 了解更多信息。

```
Event ID: 2023
The Health Service has removed some items from the send queue for management
```

```
group "Servers"
since it exceeded the maximum allowed size of size megabytes.
```

```
Event ID: 2120
The Health Service has deleted one or more items for management group "Servers"
which could
not be sent in 1440 minutes.
```

## 事件 6024

如果您在 Windows 事件日志中找到以下事件，请参阅[运行状况服务重启](#)了解更多信息。

```
Event ID: 6024
LaunchRestartHealthService.js : Launching Restart Health Service. Health Service
exceeded
Process\Handle Count or Private Bytes threshold.
```

## System Center 2012 — Operations Manager 的一般故障排除

请尝试以下操作解决任何问题。

- 验证是否已安装 System Center 2012—Operations Manager 的最新 Update Rollup。AWS Management Pack 要求至少安装 Update Rollup 1。
- 确保您已通过运行添加监视向导，在导入 AWS Management Pack 之后对其进行了配置。有关更多信息，请参阅[步骤 1：安装 AWS Management Pack \(p. 775\)](#)。
- 确保您等待足够长的时间以发现 AWS 资源（10-20 分钟）。
- 验证管理服务器的配置是否正确。
  - 管理服务器必须具有 Internet 连接。
  - 管理服务器的操作账户必须在管理服务器上具有本地管理员特权。
  - 管理服务器必须有 .NET Framework 4.5 或更高版本。
- 验证 AWS 运行方式账户是有效的。
  - 访问密钥 ID 和秘密访问密钥的值准确无误。
  - 访问密钥是有效的：在 AWS 管理控制台中，在导航栏中单击您的姓名，然后单击 Security Credentials（安全证书）。
  - IAM 用户至少要具有只读访问权限。请注意，只读访问允许执行不改变资源状态的用户操作，如监控，但不允许类似启动或停止实例的用户操作。
    - 如果某个 Amazon CloudWatch 指标显示为 Not Monitored（未监视），请检查是否已为该 Amazon CloudWatch 指标至少定义一个 Amazon CloudWatch 警报。
    - 要进一步排查问题，请使用事件日志中的相关信息。
  - 查看管理服务器上的 Operations Manager 事件日志。有关更多信息，请参阅[事件 \(p. 801\)](#)以了解 AWS Management Pack 写入 Operations Manager 事件日志的事件列表。

## System Center 2007 R2 的一般故障排除

请尝试以下操作解决任何问题。

- 确保您已通过运行添加监视向导，在导入 AWS Management Pack 之后对其进行了配置。有关更多信息，请参阅 [步骤 1：安装 AWS Management Pack \(p. 775\)](#)。
- 确保您等待足够长的时间以发现 AWS 资源（10-20 分钟）。
- 验证观察程序节点的配置是否正确。
  - 代理程序已启用。有关更多信息，请参阅 [步骤 2：配置观察程序节点 \(p. 777\)](#)。
  - 观察程序节点具有 Internet 连接。
  - 观察程序节点的操作账户具有本地管理员特权。
  - 观察程序节点必须有 .NET Framework 3.5.1 或更高版本。
- 验证观察程序节点运行状况良好并处理所有警报。有关更多信息，请参阅 [视图 \(p. 785\)](#)。
- 验证 AWS 运行方式账户是有效的。
  - 访问密钥 ID 和秘密访问密钥的值准确无误。
  - 访问密钥是有效的：在 AWS 管理控制台中，在导航栏中单击您的姓名，然后单击 Security Credentials（安全证书）。
  - IAM 用户至少要具有只读访问权限。请注意，只读访问允许执行不改变资源状态的用户操作，如监控，但不允许类似启动或停止实例的用户操作。
    - 如果某个 Amazon CloudWatch 指标显示为 Not Monitored（未监视），请检查是否已为该 Amazon CloudWatch 指标至少定义一个 Amazon CloudWatch 警报。
    - 要进一步排查问题，请使用事件日志中的相关信息。
  - 在管理服务器以及观察程序节点上查看 Operations Manager 事件日志。有关更多信息，请参阅 [事件 \(p. 801\)](#) 以了解 AWS Management Pack 写入 Operations Manager 事件日志的事件列表。

# AWS Diagnostics for Microsoft Windows Server - Beta

---

## Abstract

诊断并排查您的 Amazon EC2 Windows 实例可能存在的问题。

AWS Diagnostics for Microsoft Windows Server 是一个易于使用的工具，可以在 Amazon EC2 Windows Server 实例上运行，以诊断和排查可能存在的问题。该工具很有价值，不仅会收集日志文件以及进行故障排除，还会主动搜索可能存在问题的区域。例如，该工具可以诊断 Windows 防火墙与 AWS 安全组之间的配置问题，这些问题可能会影响您的应用程序。它甚至还可以检测其他实例中的 EBS 启动卷，并收集相关日志以对使用该卷的 Windows Server 实例进行故障排除。

AWS Diagnostics for Microsoft Windows Server 的一个用处是诊断密钥管理服务 (KMS) 激活问题。如果您更换了 DNS 服务器并将实例添加到某个域，或者服务器时间并不同步，则 KMS 激活就会失败。在此情况下，请不要手动检测您的配置设置或是调试该问题，而是运行 AWS Diagnostics for Microsoft Windows Server 工具以提供您需要的有关可能问题的信息。

该工具还可以查找安全组与 Windows 防火墙在规则方面的区别。如果您提供自己的 AWS 用户证书以描述您的安全组，则 AWS Diagnostics for Microsoft Windows Server 工具可以验证安全组中所列的端口是否允许通过 Windows 防火墙。您不必手动查看防火墙规则并根据安全组规则对其进行验证。

AWS Diagnostics for Microsoft Windows Server 工具是免费的，可从 [AWS Diagnostics for Microsoft Windows Server - Beta](#) 下载和安装。

AWS Diagnostics for Microsoft Windows Server 有两个不同模块：数据收集器模块，用于收集各种不同源的数据；分析器模块，用于根据一系列预定义的规则分析所收集的数据，以识别问题并提供建议。

AWS Diagnostics for Microsoft Windows Server 工具只能在 EC2 实例上运行的 Windows Server 上运行。该工具在启动时会确定是否在 EC2 实例上运行。如果检查失败，该工具会显示 EC2InstanceCheckFailed 错误消息。

## 分析规则

AWS Diagnostics for Microsoft Windows Server 提供以下分析规则：

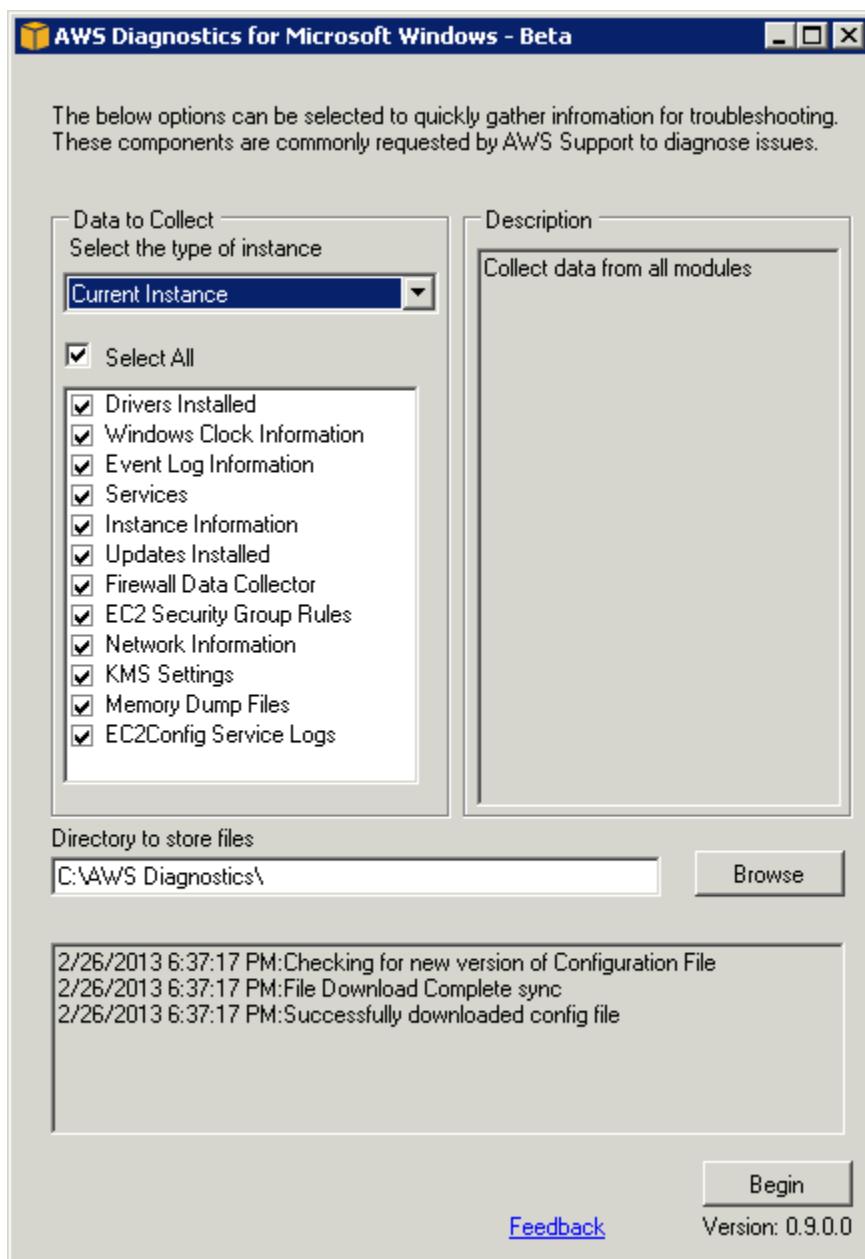
- 检查激活状态和 KMS 设置

- 检查关于元数据和 KMS 访问的合适路由表条目
- 将安全组规则与 Windows 防火墙规则进行比较
- 检查半虚拟化驱动程序 ( RedHat 或 Citrix ) 的版本
- 检查是否已设置 RealTimeIsUniversal 注册表项
- 检查默认网关设置 ( 如果使用多个 NIC )
- 检查小型转储文件中的错误代码

即使分析器没有报告任何问题，该工具收集到的数据仍可能有用。您可以查看该工具创建的数据文件以查找相关问题，也可以将这些文件提供给 AWS Support 以帮助解决支持案例。

## 分析当前实例

要分析当前实例，请运行 AWS Diagnostics for Microsoft Windows Server 工具，然后选择 Current Instance (当前实例) 作为实例类型。在主窗口的 Data to Collect (要收集的数据) 部分，您可以指定 AWS Diagnostics for Microsoft Windows Server 收集的数据。



| Data                      | 说明                      |
|---------------------------|-------------------------|
| Drivers Installed         | 收集实例上安装的所有驱动程序的相关信息。    |
| Windows Clock Information | 收集实例的当前时间和时区信息。         |
| Event Log Information     | 收集事件日志中的重要消息、错误消息和警告消息。 |
| 服务                        | 收集实例上所安装服务的相关信息。        |
| Instance Information      | 收集实例元数据和本地环境变量的信息。      |
| Updates Installed         | 收集实例上所安装更新的相关信息。        |

| Data                     | 说明                                |
|--------------------------|-----------------------------------|
| Firewall Data Collector  | 收集 Windows 防火墙设置的相关信息。            |
| EC2 Security Group Rules | 收集与实例相关联的 Amazon EC2 安全组中规则的相关信息。 |
| Network Information      | 收集实例的路由表和 IP 地址信息。                |
| KMS Settings             | 收集密钥管理服务的设置。                      |
| Memory Dump Files        | 收集实例上的所有内存转储文件。                   |
| EC2Config Service Logs   | 收集 EC2Config 服务生成的日志文件。           |

## 收集来自离线实例的数据

如果需要对无法启动或是阻止您在实例上运行 AWS Diagnostics for Microsoft Windows Server 工具的 Windows 实例调试问题，Offline Instance(离线实例) 选项会非常有用。在这种情况下，您可以将 EBS 启动卷从该相应实例分离并将其附加到另一 Windows 实例。

### 收集来自离线实例的数据

1. 停止出现故障的实例（如果目前尚未停止）。
2. 从出现故障的实例分离 EBS 启动卷。
3. 将 EBS 启动卷添加到其他已安装 AWS Diagnostics for Microsoft Windows Server 且正在运行的 Windows 实例。
4. 在正在运行的实例中装载该卷，并为其分配一个驱动器盘符（例如 F:）。
5. 在正在运行的实例上运行 AWS Diagnostics for Microsoft Windows Server 工具并选择 Offline Instance(离线实例)。
6. 选择新装载卷的驱动器盘符（例如 F:）。
7. 单击 Begin。

AWS Diagnostics for Microsoft Windows Server 工具会扫描该卷，并根据该卷上的日志文件收集故障排除信息。对于离线实例，收集的数据是个固定集，不会执行任何数据分析。

## 数据文件存储

默认情况下，AWS Diagnostics for Microsoft Windows Server 工具将其数据文件放在从中启动该工具的目录中。您可以选择保存 AWS Diagnostics for Microsoft Windows Server 工具所收集数据文件的位置。在所选目录中，该工具创建一个名为 DataCollected 的目录。每当该工具运行时，它还会创建具有当前日期和时间戳的单独目录。每个数据采集模块均会生成一个 XML 文件，其中包含关于该数据集的信息。最后，该工具会创建一个 ZIP 文件存档，其中包含生成的所有数据文件的副本。如果需要，您可以将此存档提供给 AWS Support 工程师。

# 对 Windows 实例进行故障排除

---

## Abstract

对 Windows 实例的问题进行故障排除。

以下程序和提示可以帮助您对 Amazon EC2 Windows 实例问题进行故障排除。

### 主题

- [对无法访问的实例进行故障排除 \(p. 813\)](#)
- [常见问题 \(p. 820\)](#)
- [常见消息 \(p. 827\)](#)

如果需要其他帮助，您可以将问题发布到 [Amazon EC2 forum](#)。请务必发布实例的 ID 以及所有错误消息，包括通过控制台输出提供的错误消息。

要获取有关对实例问题进行故障排除的其他信息，请使用 [AWS Diagnostics for Microsoft Windows Server - Beta \(p. 809\)](#)。有关对 PV 驱动程序问题进行故障排除的信息，请参阅 [对半虚拟化驱动程序进行故障排除 \(p. 281\)](#)。

## 对无法访问的实例进行故障排除

如果您无法通过 SSH 或 RDP 访问您的实例，您可以捕获实例的屏幕截图并将其作为图像查看。这可以让您了解实例的状态，更快地处理问题。

此屏幕截图不会产生数据传输费用。生成的图像为 JPG 格式，大小不超过 100kb。本节包含以下信息。

- [如何捕获无法访问的实例的屏幕截图 \(p. 813\)](#)
- [常见的屏幕截图 \(p. 814\)](#)

## 如何捕获无法访问的实例的屏幕截图

### 访问实例控制台

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。

2. 在左侧导航窗格中，选择 Instances。
3. 选择要捕获的实例。
4. 选择 Actions、Instance Settings。
5. 选择 Get Instance Screenshot。

右键单击图像，以下载并保存该图像。

#### 使用命令行捕获屏幕截图

您可以使用以下任一命令。返回的输出采用 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 \(Amazon EC2 查询 API \)](#)

对于 API 调用，返回的内容采用 base64 编码。对于命令行工具，系统会为您进行解码。

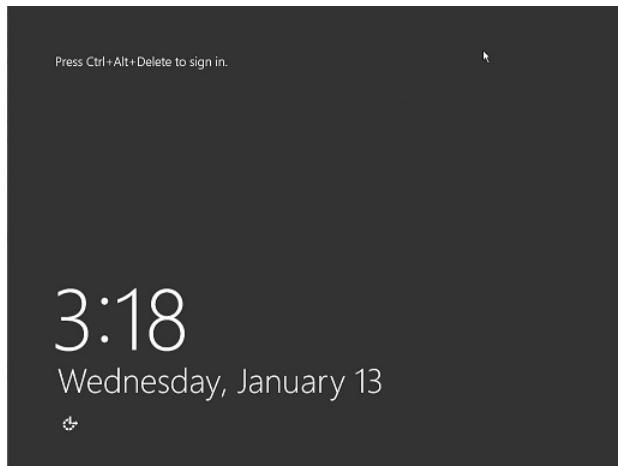
## 常见的屏幕截图

您可以根据服务返回的屏幕截图，利用以下信息帮助您对无法访问的实例进行故障排除。

- [登录屏幕 \(Ctrl+Alt+Delete\) \(p. 814\)](#)
- [恢复控制台屏幕 \(p. 816\)](#)
- [Windows 引导管理器屏幕 \(p. 818\)](#)
- [Sysprep 屏幕 \(p. 818\)](#)
- [Getting Ready 屏幕 \(p. 819\)](#)
- [Windows 更新屏幕 \(p. 819\)](#)
- [Chkdsk \(p. 820\)](#)

## 登录屏幕 (Ctrl+Alt+Delete)

控制台屏幕截图服务返回以下截图。



如果实例在登录时无法访问，可能是因为网络配置或 Windows 远程桌面服务存在问题。如果某个进程占用了大量 CPU，实例也可能没有响应。

## 网络配置

使用以下信息验证您的 AWS、Microsoft Windows 和本地（或内部）网络配置是否阻止了对实例的访问。

### AWS 网络配置

| 配置             | 验证                                                                                                                                 |
|----------------|------------------------------------------------------------------------------------------------------------------------------------|
| 安全组配置          | 验证端口 3389 是否向您的安全组开放。验证您是否连接到正确的公有 IP 地址。如果实例未与弹性 IP 关联，公有 IP 就会在实例停止或启动后发生更改。有关更多信息，请参阅 <a href="#">远程桌面无法连接到远程计算机 (p. 824)</a> 。 |
| VPC 配置（网络 ACL） | 验证您的 Amazon VPC 的访问控制列表（ACL）是否阻止访问。有关信息，请参阅 <a href="#">Amazon VPC 用户指南</a> 中的 <a href="#">网络 ACL</a> 。                            |
| VPN 配置         | 如果您使用虚拟专用网络（VPN）连接您的 VPC，请验证 VPN 隧道的连通性。有关更多信息，请参阅 <a href="#">如何对 Amazon VPC 的 VPN 隧道连通性问题进行故障排除？</a>                             |

### Windows 网络配置

| 配置                    | 验证                                                                                                         |
|-----------------------|------------------------------------------------------------------------------------------------------------|
| Windows 防火墙           | 验证 Windows 防火墙是否阻止与您的实例建立连接。按照远程桌面故障排除部分第 7 项的说明禁用 Windows 防火墙： <a href="#">远程桌面无法连接到远程计算机 (p. 824)</a> 。  |
| 高级 TCP/IP 配置（使用静态 IP） | 实例可能因您配置了静态 IP 地址而没有响应。对于 VPC，请 <a href="#">创建网络接口 (p. 617)</a> 并将其连接到实例 (p. 619)。对于 EC2 Classic，请启用 DHCP。 |

### 本地或内部网络配置

验证本地网络配置是否阻止访问。尝试连接无法访问的实例所在 VPC 中的其他实例。如果您无法访问其他实例，请联系本地网络管理员确定是否有本地策略限制了访问。

## 远程桌面服务问题

如果实例在登录时无法访问，可能是因为实例存在远程桌面服务（RDS）问题。

### 远程桌面服务配置

| 配置       | 验证                                                                                                                                                                                                                                                                                                   |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RDS 正在运行 | 验证实例上的 RDS 是否在运行。使用 Microsoft 管理控制台 (MMC) 的服务管理单元 (services.msc) 连接实例。在服务列表中，验证远程桌面服务是否处于 Running 状态。如果不是，请将其开启，然后将启动类型设置为 Automatic。如果使用服务管理单元无法连接到实例，请将根卷从该实例分离并为其创建快照或 AMI，将原始卷作为辅助卷挂载到同一个可用区中的其他实例，并修改 Start 注册表项。完成后，请重新将根卷挂载到原始实例。有关分离卷的更多信息，请参阅 <a href="#">从实例断开 Amazon EBS 卷 (p. 670)</a> 。 |
| RDS 已启用  | 即使该服务已启动，它也有可能被禁用。将根卷从实例分离并为其创建快照或 AMI，将原始卷作为辅助卷挂载到同一个可用区中的其他实例，然后按照 <a href="#">使用注册表远程启用远程桌面</a> 中的说明，通过修改 Terminal Server 注册表项来启用该服务。完成后，请重新将根卷挂载到原始实例。有关分离卷的更多信息，请参阅 <a href="#">从实例断开 Amazon EBS 卷 (p. 670)</a> 。                                                                               |

### 高 CPU 使用率

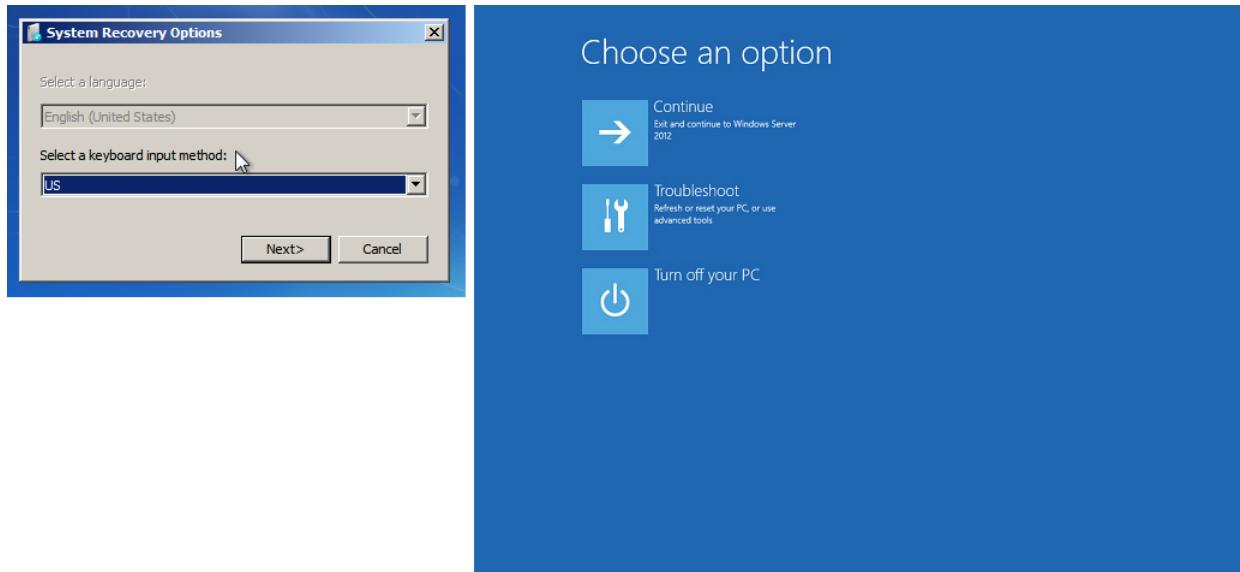
使用 Amazon CloudWatch 检查您实例上的 CPUUtilization (Maximum) 指标。如果 CPUUtilization (Maximum) 的值比较大，请等待 CPU 使用率下降后尝试重新连接。CPU 使用率高可能由以下原因导致：

- Windows 更新
- 安全软件扫描
- 自定义启动脚本
- 任务计划程序

有关 CPUUtilization (Maximum) 指标的更多信息，请参阅 [Amazon CloudWatch 开发者指南](#) 中的 [获取指定 EC2 实例的统计数据](#)。有关其他故障排除提示，请参阅 [Windows 启动后，CPU 使用率短时增高 \(p. 822\)](#)。

### 恢复控制台屏幕

控制台屏幕截图服务返回以下截图。



如果 `bootstatuspolicy` 未设置为 `ignoreallfailures`，操作系统可能启动至恢复控制台，并停滞在这一状态。请按照以下步骤将 `bootstatuspolicy` 配置更改为 `ignoreallfailures`。



#### Note

默认情况下，AWS 提供的公用 Windows AMI 的策略配置设置为 `ignoreallfailures`。

1. 停止无法访问的实例。
2. 创建根卷的快照。根卷是作为 `/dev/sda1` 挂载到实例的。

将根卷从无法访问的实例分离并为其创建快照或 AMI，然后将根卷作为辅助卷挂载到同一个可用区中的其他实例。有关更多信息，请参阅 [从实例断开 Amazon EBS 卷 \(p. 670\)](#)。



#### Warning

( 可选 ) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成额外的步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。或者，可以为临时实例选择不同的 AMI。例如，如果原始实例使用 Windows Server 2008 R2 的 AWS Windows AMI，则使用 Windows Server 2012 或 Windows Server 2003 的 AWS Windows AMI 来启动临时实例。( 要查找 Windows Server 2003 的 AMI，请搜索名称为 `Windows_Server-2003-R2_SP2` 的 AMI。) 如果您必须基于相同 AMI 创建一个临时实例，请参阅 [远程桌面无法连接到远程计算机 \(p. 824\)](#) 中的第 6 步，了解您必须完成哪些其他步骤才能避免磁盘签名冲突。

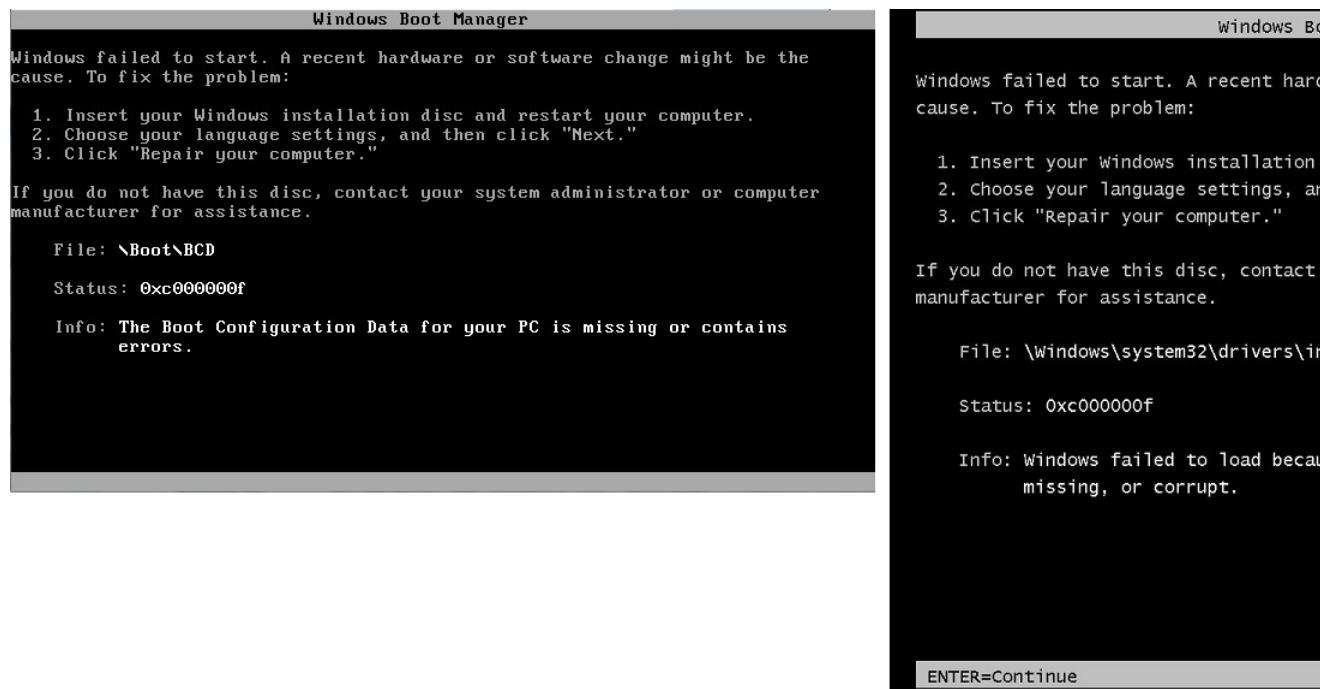
3. 登录实例并从命令提示符执行以下命令，以将 `bootstatuspolicy` 配置更改为 `ignoreallfailures`：

```
bcdeedit /store <Drive Letter>:\boot\bcd /set {default} bootstatuspolicy ignoreallfailures
```

4. 重新将卷挂载到无法访问的实例并重新启动实例。

## Windows 引导管理器屏幕

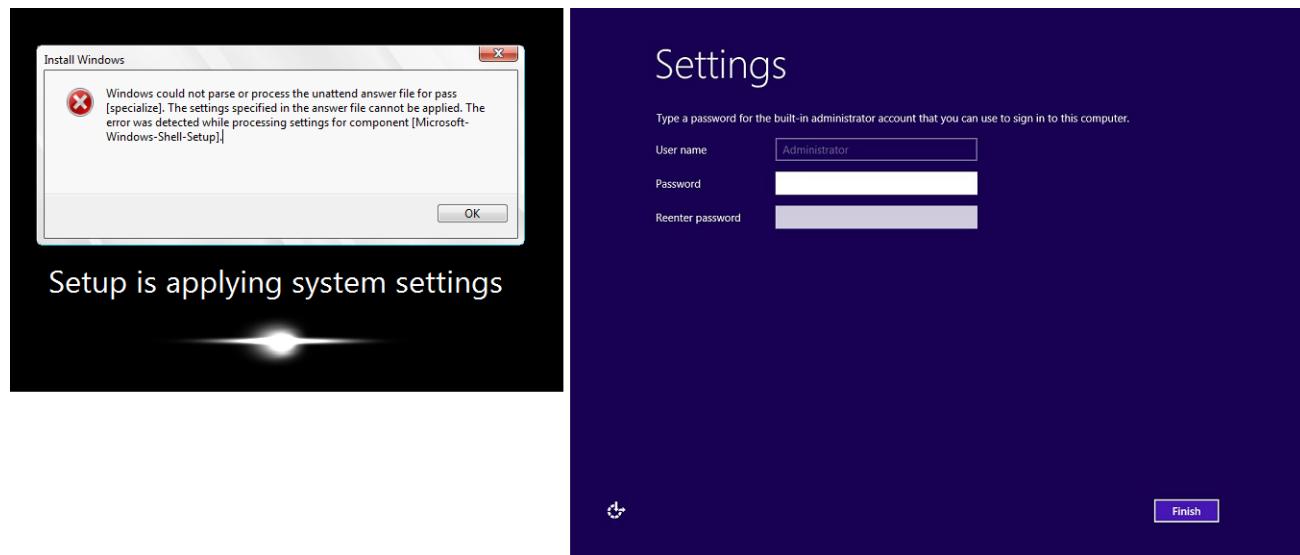
控制台屏幕截图服务返回以下截图。



操作系统的系统文件和/或注册表遭到严重损坏。当实例停滞在这一状态时，您应该从最近备份的 AMI 恢复实例或启动一个替代实例。如果您需要访问实例上的数据，请将所有根卷从无法访问的实例上分离并为这些卷创建快照或 AMI，然后将其作为辅助卷连接到同一个可用区中的其他实例。有关更多信息，请参阅[从实例断开 Amazon EBS 卷 \(p. 670\)](#)。

## Sysprep 屏幕

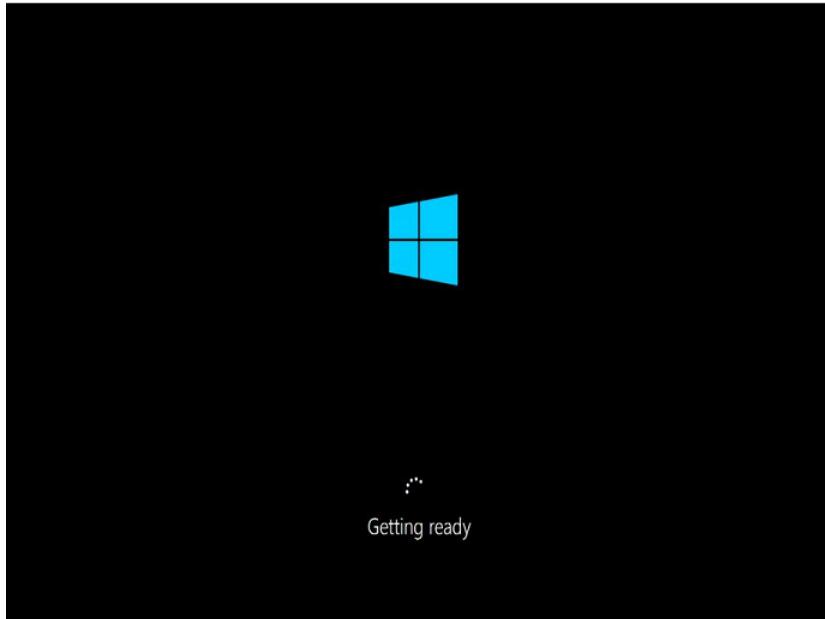
控制台屏幕截图服务返回以下截图。



如果您没有使用 EC2Config 服务调用 sysprep.exe，或者操作系统在运行 Sysprep 时出现故障，您可能会看到此屏幕。要解决此问题，请参阅 [使用 Sysprep 创建标准 Amazon 系统映像 \(AMI\) \(p. 105\)](#)。

## Getting Ready 屏幕

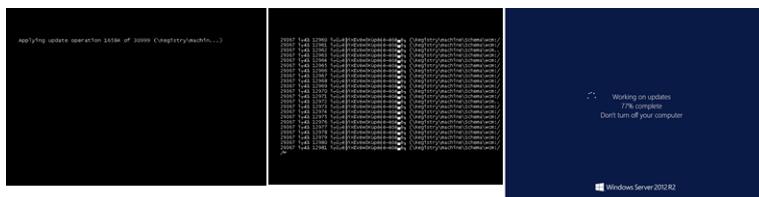
控制台屏幕截图服务返回以下截图。



反复刷新实例控制台屏幕截图服务，验证环形进度条是否转动。如果环形进度条转动，请等待操作系统启动。您也可以使用 Amazon CloudWatch 查看您实例上的 CPUUtilization (Maximum) 指标，以确认操作系统是否处于活动状态。如果环形进度条不转，则实例可能停滞在启动过程。重启实例。如果重新启动未能解决问题，请从最近备份的 AMI 中恢复实例或启动一个替代实例。如果需要访问实例上的数据，请将根卷从无法访问的实例中分离，并为其创建快照或 AMI。然后，将根卷作为辅助卷连接到同一个可用区中的其他实例。有关 CPUUtilization (Maximum) 的更多信息，请参阅 *Amazon CloudWatch 开发者指南* 中的 [获取指定 EC2 实例的统计数据](#)。

## Windows 更新屏幕

控制台屏幕截图服务返回以下截图。



Windows 更新进程正在更新注册表。请等待更新完成。请勿在更新期间重新启动或停止实例，因为这可能会导致数据损坏。

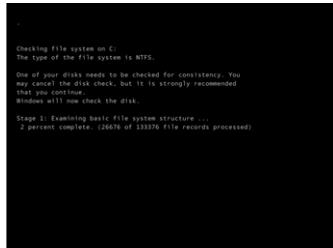


### Note

在更新时，Windows 更新进程会占用服务器上的资源。若您频繁遇到这一问题，可以考虑使用速度更快的实例类型和 EBS 卷。

## Chkdsk

控制台屏幕截图服务返回以下截图。



Windows 正在驱动器上运行 chkdsk 系统工具，以验证文件系统的完整性并修复逻辑文件系统错误。请等待该进程完成。

## 常见问题

本部分包含的故障排除提示可以帮助您解决常见问题。

### 主题

- [将 EC2 Windows 实例启动至目录服务还原模式 \(DSRM\) \(p. 820\)](#)
- [Windows 启动后，CPU 使用率短时增高 \(p. 822\)](#)
- [无控制台输出 \(p. 823\)](#)
- [实例立即终止 \(p. 823\)](#)
- [远程桌面无法连接到远程计算机 \(p. 824\)](#)
- [RDP 显示黑屏而不是桌面 \(p. 826\)](#)
- [实例失去网络连接或计划的任务不按预期方式运行 \(p. 826\)](#)
- [实例容量不足 \(p. 827\)](#)
- [超出实例限制 \(p. 827\)](#)
- [网络上不可用的 Windows Server 2012 R2 \(p. 827\)](#)

## 将 EC2 Windows 实例启动至目录服务还原模式 (DSRM)

如果运行 Microsoft Active Directory 的实例遇到系统故障或其他关键问题，您可以通过启动至特殊版本的安全模式（称为 [目录服务还原模式 \(DSRM\)](#)）对该实例进行故障排除。在 DSRM 中，您可以修复或恢复 Active Directory。

## DSRM 的驱动程序支持

您启用 DSRM 和启动至实例的方式取决于实例正在运行的驱动程序。在 EC2 控制台中，您可以从系统日志查看实例的驱动程序版本详细信息。下表显示了 DSRM 支持的驱动程序。

| 驱动程序版本              | 操作系统                      | DSRM 是否支持？ | 后续步骤                |
|---------------------|---------------------------|------------|---------------------|
| Citrix 半虚拟化驱动程序 5.9 | Windows Server 2008 或早期版本 | 否          | 从备份还原实例。您无法启用 DSRM。 |

|                             |                           |   |                                                                                           |
|-----------------------------|---------------------------|---|-------------------------------------------------------------------------------------------|
| AWS 半虚拟化驱动程序<br>7.2.0       | Windows Server 2012<br>R2 | 否 | 尽管该驱动程序不支持 DSRM，但您仍可以将根卷从实例分离并为其创建快照或 AMI，然后将其作为辅助卷挂载到同一个可用区中的其他实例。然后，您可以按照本部分的说明启用 DSRM。 |
| AWS 半虚拟化驱动程序<br>7.2.2 和更高版本 | Windows Server 2012<br>R2 | 是 | 分离根卷，将其挂载到其他实例，然后启用 DSRM（如本节中所述）。                                                         |
| 增强联网 ( Intel 82599 虚拟功能 )   | Windows Server 2012<br>R2 | 是 | 分离根卷，将其挂载到其他实例，然后启用 DSRM（如本节中所述）。                                                         |



#### Note

默认情况下，增强联网对以下 Windows Server 2012 R2 实例类型启用：

- C3
- C4
- D2
- I2
- R3

有关实例类型的更多信息，请参阅 [Amazon EC2 实例](#)。有关如何为其他 Windows Server 实例启用增强联网的信息，请参阅在 [VPC 中对 Windows 实例启用增强联网](#)。

## 将实例配置为启动至 DSRM

在操作系统运行前，EC2 Windows 实例没有网络连接。因此，您无法通过按键盘上的 F8 键来选择启动选项。您必须使用以下过程之一将 EC2 Windows Server 实例启动至 DSRM。

### 将在线实例启动至 DSRM

如果您怀疑 Active Directory 已损坏，但该实例仍在运行，则可以使用 System Configuration 对话框或命令提示符将该实例配置为启动至 DSRM。选择以下方法之一。如果您的实例未处于在线状态（不可用），请参阅下一节：

#### 使用 System Configuration 对话框将在线实例启动至 DSRM

1. 在 Run 对话框中，键入 `msconfig` 并选择 Enter。
2. 选择 Boot 选项卡。
3. 在 Boot options 下，选择 Safe boot。
4. 选择 Active Directory repair，然后选择 OK。系统将提示您重新启动服务器。

#### 使用命令提示符下将在线实例启动至 DSRM 实例

1. 打开命令提示符。

2. 键入 `bcdedit /set safeboot dsrepair`，然后选择 Enter。

## 将离线实例启动至 DSRM

如果某个实例处于离线状态并且无法访问，您必须先分离根卷并将其挂载到其他实例才能启用 DSRM 模式。

### 将离线实例启动至 DSRM

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 找到受影响的实例。打开实例的上下文（右键单击）菜单，选择 Instance State，然后选择 Stop。
4. 选择 Launch Instance 并在与受影响实例相同的可用区中创建临时实例。选择使用其他 Windows 版本的实例类型。例如，如果您的实例是 Windows Server 2008 R1，则选择 Windows Server 2008 R2 实例。



#### Important

如果您未在与受影响实例相同的可用区中创建该实例，则无法将受影响的实例的根卷挂载到新实例。

5. 在导航窗格中，选择 Volumes。
6. 找到受影响的实例的根卷。分离该卷并将其挂载到早先创建的临时实例。使用默认设备名称(xvdf)挂载该卷。
7. 使用远程桌面连接临时实例，然后通过磁盘管理实用工具使该卷可供使用。
8. 打开命令提示符窗口并运行以下命令。将 *D* 替换为您刚刚挂载的辅助卷的实际驱动器号：  
`bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair`
9. 在磁盘管理实用工具中，选择您之前挂载的驱动器，打开上下文（右键单击）菜单，然后选择脱机。
10. 在 EC2 控制台中，将受影响的卷从临时实例分离，然后将其重新挂载到设备名称为 /dev/sda1 的原始实例。您必须指定此设备名称才能将卷指派为根卷。
11. 启动实例。
12. 在实例将健康检查传入 EC2 控制台后，使用远程桌面连接到实例，然后验证实例是否启动至 DSRM 模式。



#### Note

删除或停止您在本过程中创建的临时实例。

## Windows 启动后，CPU 使用率短时增高

如果将 Windows Update 设置为 Check for updates but let me choose whether to download and install them（默认实例设置），则此检查可能会在实例上消耗 50 - 99% 的 CPU。如果此 CPU 消耗会导致您的应用程序出现问题，您可手动在 Control Panel 中更改 Windows Update 设置或者使用 Amazon EC2 用户数据字段中的以下脚本：

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

执行此脚本时，为 /d 指定一个值。默认值为 3。可能的值包括：

1. 从未检查更新
2. 检查更新，但允许我选择是否下载并安装它们
3. 下载更新，但允许我选择是否安装它们
4. 自动安装更新

为 Amazon EBS 支持的实例修改用户数据

1. 打开 Amazon EC2 控制台 <https://console.amazonaws.cn/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Instance State 和 Stop。
4. 在确认对话框中，选择 Yes, Stop。停止实例可能需要几分钟时间。
5. 在实例仍处于选中状态的情况下，选择 Actions，选择 Instance Settings，然后选择 View/Change User Data。请注意，如果实例正在运行，您不能更改用户数据，但是可以查看。
6. 在 View/Change User Data 对话框中，更新用户数据，然后选择 Save。

在为您的实例修改用户数据后，可执行它。有关更多信息，请参阅 [使用用户数据执行脚本 \(p. 242\)](#)。

## 无控制台输出

针对 Windows 实例，实例控制台会显示在实例上运行的 EC2Config 服务的输出。该输出会记录 Windows 启动期间执行的任务的状态。如果 Windows 成功启动，则最后记录的消息是 Windows is Ready to use。请注意，您也可以在控制台中显示事件日志消息，但默认情况下未启用此功能。有关更多信息，请参阅 [Ec2 服务属性 \(p. 251\)](#)。

要使用 Amazon EC2 控制台获取您的实例的控制台输出，请选择该实例，单击 Actions，选择 Instance Settings，然后单击 Get System Log。要使用命令行获取控制台输出，请使用以下命令之一：  
`get-console-output` (AWS CLI) 或 `Get-EC2ConsoleOutput` (适用于 Windows PowerShell 的 AWS 工具)。

如果控制台输出是空的，说明 EC2Config 服务可能存在问题，例如，配置文件的配置不正确或 Windows 无法正确启动。要修复该问题，请下载并安装最新版本的 EC2Config。有关更多信息，请参阅 [安装最新版的 EC2Config \(p. 258\)](#)。

## 实例立即终止

在启动实例之后，建议您检查其状态，确认从 pending 状态变为 running 状态而不是 terminated 状态。

如果实例立即终止，您可以使用 Amazon EC2 控制台或命令行获取有关实例终止原因的信息。

使用控制台了解实例终止的原因

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances 以显示实例详细信息。
3. 选择实例。
4. 在 Description (描述) 选项卡上，找到标签 State transition reason (状态转换原因) 旁边的原因。如果实例仍在运行，则通常不会列出原因。如果您已明确停止或终止实例，则原因为 User initiated shutdown。

使用命令行了解实例终止的原因

对实例 ID 使用 `describe-instances` 命令 (AWS CLI)。在输出中查找 StateReason 元素。

## 远程桌面无法连接到远程计算机

尝试以下操作以解决与连接实例有关的问题：

- 确认您使用的是正确的公有 DNS 主机名。（在 Amazon EC2 控制台中，请选择实例并在详细信息窗格中检查 Public DNS（公有 DNS）。）如果您的实例是在 VPC 中，并且您没有看到公有 DNS 名称，则必须启用 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](#)。
- 验证您的实例是否具有公有 IP 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 \(p. 606\)](#)。
- 确认您的安全组具有允许 RDP 访问的规则。有关更多信息，请参阅 [创建安全组 \(p. 17\)](#)。
- 如果您输入复制的密码，然后收到错误消息 Your credentials did not work，请尝试根据系统提示手动键入密码。可能是复制密码时丢失了字符或添加了额外空格。
- 确认实例已通过状态检查。有关更多信息，请参阅 [实例的状态检查 \(p. 444\)](#) 和 [通过故障状态检查排查实例故障 \(Amazon EC2 用户指南 \(适用于 Linux 实例\)\)](#)。
- [EC2-VPC] 确认子网的路由表具有这样一个路由，该路由将发往 VPC 外部 (0.0.0.0/0) 的所有流量发送到该 VPC 的 Internet 网关。有关更多信息，请参阅 [Amazon VPC 用户指南 中的创建自定义路由表 \(Internet 网关\)](#)。
- 确认 Windows 防火墙或其他防火墙软件没有阻止到实例的 RDP 流量。我们建议您禁用 Windows 防火墙，使用安全组规则来控制对实例的访问。

### 在无法连接到的 Windows 实例上禁用 Windows 防火墙

- 停止受影响的实例并断开其根卷。
- 在受影响的实例所在的可用区中启动临时实例。



#### Warning

( 可选 ) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成额外的步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。或者，可以为临时实例选择不同的 AMI。例如，如果原始实例使用 Windows Server 2008 R2 的 AWS Windows AMI，则使用 Windows Server 2012 或 Windows Server 2003 的 AWS Windows AMI 来启动临时实例。( 要查找适用于 Windows Server 2003 的 AMI，请使用名称 Windows\_Server-2003-R2\_SP2 来搜索 AMI。 )

- 将根卷从受影响的实例连接到此临时实例。连接到临时实例，打开 Disk Management (磁盘管理) 实用工具，将驱动器联机。
- 打开 Regedit，选择 HKEY\_LOCAL\_MACHINE。从 File 菜单中，选择 Load Hive。选择驱动器，打开文件 Windows\System32\config\SYSTEM，在出现提示时指定键名（您可以使用任何名称）。
- 选择刚刚加载的键并导航至 ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy。对于名称格式为 xxxxProfile 的各个键，请选择该键并将 EnableFirewall 从 1 更改为 0。再次选择该键，在 File 菜单中，选择 Unload Hive。
- ( 可选 ) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成以下步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。



#### Warning

以下过程介绍了如何使用注册表编辑器编辑 Windows 注册表。如果您不熟悉注册表或不知道如何使用注册表安全地做出更改，请阅读 [Microsoft TechNet 上的注册表](#)。

- a. 打开命令提示符，键入 regedit.exe，并按“Enter”键。
- b. 在注册表编辑器中，从上下文菜单中选择 HKEY\_LOCAL\_MACHINE（右击），然后选择“查找”。
- c. 键入 Windows Boot Manager，然后选择“查找下一个”。
- d. 选择名为 11000001 的密钥。此密钥与您在之前步骤中找到的密钥处于同一层级。
- e. 在右侧窗格中，选择“”，然后从上下文菜单中选择“修改”（右击）。
- f. 在数据中的偏移 0x38 处查找四字节磁盘签名。颠倒这些字节以创建磁盘签名并将其记下。例如，由以下数据表示的磁盘签名 E9EB3AA5：

```
...
0030 00 00 00 00 01 00 00 00
0038 A5 3A EB E9 00 00 00 00
0040 00 00 00 00 00 00 00 00
...
```

- g. 在命令提示符窗口中，运行以下命令以启动 Microsoft DiskPart。

```
C:\> diskpart
```

- h. 运行以下 DiskPart 命令以选择卷。（您可以使用 Disk Management（磁盘管理）实用工具来验证磁盘编号为 1。）

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

- i. 运行以下 DiskPart 命令以获取磁盘签名。

```
DISKPART> uniqueid disk

Disk ID: 0C764FA8
```

- j. 如果上一步骤中显示的磁盘签名与前面记下的 BCD 中的磁盘签名不匹配，请使用以下 DiskPart 命令更改磁盘签名以使其匹配：

```
DISKPART> uniqueid disk id=E9EB3AA5
```

## 7. 使用 Disk Management（磁盘管理）实用工具，将驱动器脱机。



### Note

如果临时实例运行的操作系统与受影响实例相同，则驱动器将自动脱机，因此您无需手动使其脱机。

8. 将该卷从临时实例分离。如果您不再使用临时实例，则可以将其终止。
9. 通过将受影响的实例的根卷挂载为 /dev/sda1 将其还原。
10. 启动实例。

- 确认密码没有过期。如果密码已过期，可以重置密码。有关更多信息，请参阅 [重置丢失或过期的管理员密码 \(p. 288\)](#)。
- 如果您尝试使用在实例上创建的用户账户进行连接并收到错误消息 The user cannot connect to the server due to insufficient access privileges，请确认您已为该用户授予从本地登录的权限。有关更多信息，请参阅 <http://technet.microsoft.com/en-us/library/ee957044.aspx>。
- 如果尝试次数超过所允许的并发 RDP 会话的最大数目，则会终止会话，并显示消息 Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.。默认情况下，实例可以有两个并发 RDP 会话。

## RDP 显示黑屏而不是桌面

请尝试以下操作解决该问题：

- 检查控制台输出有无其他信息。要使用 Amazon EC2 控制台获取您的实例的控制台输出，请选择该实例，然后依次选择 Actions、Instance Settings、Get System Log。
- 确认您正在运行最新版本的 RDP 客户端。
- 尝试使用 RDP 客户端的默认设置。有关更多信息，请参阅 [Microsoft TechNet 库 中的远程会话环境](#)。
- 如果您要使用远程桌面连接，请尝试使用 /admin 选项，通过以下方式将其启动。

```
C:\> mstsc /v:instance /admin
```

- 如果服务器正在运行全屏应用程序，则它可能会停止响应。使用 Ctrl+Shift+Esc 以启动 Windows 任务管理器，然后关闭应用程序。
- 如果过度使用服务器，则服务器可能已停止响应。要使用 Amazon EC2 控制台来监控实例，请选择实例，然后选择 Monitoring (监控) 选项卡。如果需要将实例类型更改为更大大小，请参阅 [调整您的实例大小 \(p. 133\)](#)。

## 实例失去网络连接或计划的任务不按预期方式运行

如果您重新启动实例而该实例失去网络连接，则可能该实例的时间不正确。

默认情况下，Windows 实例使用协调世界时 (UTC)。如果将实例的时间设置为不同的时区，然后再重新启动实例，则时间会发生偏移，该实例暂时失去其 IP 地址。实例最终会重新获取网络连接，但这可能要用数小时的时间。实例重新获取网络连接所用的时间取决于 UTC 与其他时区之间的差异。

这种时间问题也可能导致计划的任务不如期运行。在这种情况下，计划的任务会因实例的时间不正确而不如期运行。

要持久使用 UTC 以外的时区，您必须设置 RealTimelsUniversal 注册表项。若不设置此项，则实例会在重新启动后使用 UTC。



### Important

Windows Server 2003 不支持 RealTimelsUniversal 注册表项。因此，实例始终在重新启动后使用 UTC。

### 解决造成网络连接丢失的时间问题

- 确保所运行的是建议的半虚拟化驱动程序。有关更多信息，请参阅 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。
- 验证以下注册表项存在并且已设置为 1：  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimelsUniversal`

## 实例容量不足

如果您在启动实例时看到 `InsufficientInstanceCapacity` 错误，则表示 AWS 当前没有足够的可用容量来服务您的请求。

尝试以下操作：

- 等待几分钟，然后再次提交您的请求；容量可能经常转移。
- 提交减少了实例数的新请求。例如，如果您要提交 1 个启动包含 15 个实例的请求，请改为尝试提交 3 个包含 5 个实例的请求或 15 个包含 1 个实例的请求。
- 提交新请求而不指定可用区。
- 使用其他实例类型（可在后期调整大小）提交新请求。有关更多信息，请参阅 [调整您的实例大小 \(p. 133\)](#)。
- 尝试购买预留实例。预留实例是长期的容量预留。有关更多信息，请参阅 [Amazon EC2 预留实例](#)。

## 超出实例限制

如果您在启动实例时看到 `InstanceLimitExceeded` 错误，这表示您已达到并行运行的实例数上限。对于新的 AWS 账户，默认限制为 20。如果需要更多运行实例，请在[请求提高 Amazon EC2 实例限制](#)上填写表单。

## 网络上不可用的 Windows Server 2012 R2

有关对网络上不可用的 Windows Server 2012 R2 实例进行故障排除的信息，请参阅 [Windows Server 2012 R2 在实例重启后丢失网络和存储连接 \(p. 282\)](#)。

## 常见消息

本部分包含的提示可以帮助您根据常见消息进行故障排除。

### 主题

- "密码不可用" (p. 827)
- "密码尚不可用" (p. 828)
- "无法检索 Windows 密码" (p. 828)
- "等待元数据服务" (p. 828)
- "无法激活 Windows" (p. 831)
- "Windows 不是正版 (0x80070005)" (p. 832)
- "没有终端服务器许可服务器可提供许可证" (p. 832)

## "密码不可用"

要使用远程桌面连接到 Windows 实例，必须指定账户和密码。提供的账户和密码基于用于启动实例的 AMI。您可以为管理员账户检索自动生成的密码，也可以使用在创建该 AMI 的原始实例中所用的账户和密码。

如果未将 Windows 实例配置为生成随机密码，则在使用控制台检索自动生成的密码时会收到以下消息：

Password is not available.  
The instance was launched from a custom AMI, or the default password has changed.

A password cannot be retrieved for this instance. If you have forgotten your password, you can reset it using the Amazon EC2 configuration service. For more information, see Passwords for a Windows Server instance.

检查实例的控制台输出，查看用于启动实例的 AMI 是不是在禁用了密码生成的情况下创建的。如果禁用了密码生成，则控制台输出包含以下内容：

Ec2SetPassword: Disabled

如果禁用了密码生成并且您未记住原始实例的密码，则可以重置该实例的密码。有关更多信息，请参阅[重置丢失或过期的管理员密码 \(p. 288\)](#)。

## "密码尚不可用"

要使用远程桌面连接到 Windows 实例，必须指定账户和密码。提供的账户和密码基于用于启动实例的 AMI。您可以为管理员账户检索自动生成的密码，也可以使用在创建该 AMI 的原始实例中所用的账户和密码。

您的密码应在几分钟内可用。如果密码不可用，则在使用控制台检索自动生成的密码时会收到以下消息：

Password not available yet.  
Please wait at least 4 minutes after launching an instance before trying to retrieve the auto-generated password.

如果在超过四分钟后您仍无法获取密码，则 EC2Config 可能已被禁用。请根据控制台输出是否为空，对此进行验证。有关更多信息，请参阅[无控制台输出 \(p. 823\)](#)。

此外，请确认用于访问管理门户的 AWS Identity and Access Management (IAM) 账户是否已允许 ec2:GetPasswordData 操作。有关 IAM 权限的更多信息，请参阅[什么是 IAM？](#)。

## "无法检索 Windows 密码"

要为管理员账户检索自动生成的密码，您必须针对启动实例时指定的密钥对使用私有密钥。如果在启动实例时未指定密钥对，您将会收到以下消息。

Cannot retrieve Windows password

您可以终止该实例并使用相同的 AMI 启动新实例，并确保指定密钥对。

## "等待元数据服务"

Windows 实例必须包含其实例元数据中的信息才能将自身激活。默认情况下，WaitForMetaDataAvailable 设置可确保 EC2Config 服务等待实例元数据可以访问，然后继续启动过程。有关更多信息，请参阅[实例元数据和用户数据 \(p. 239\)](#)。

如果实例未通过实例可到达性测试，请尝试以下操作来解决此问题。

- [EC2-VPC] 检查您的 VPC 的 CIDR 块。如果 Windows 实例启动至 IP 地址范围为 224.0.0.0 - 255.255.255.255 (D 类和 E 类 IP 地址范围) 的 VPC，则其无法正确启动。这些 IP 地址范围是预

留的，不应分配给主机设备。我们建议您创建一台 CIDR 块来自私有（非公共可路由）IP 地址范围（如 [RFC 1918 所指](#)）的 VPC。

- 系统有可能配置了静态 IP 地址。尝试以下操作：
  - [EC2-VPC] [创建网络接口 \(p. 617\)](#) 并将其连接到实例 (p. 619)。
  - [EC2-Classic] 启用 DHCP。
- 在无法连接到的 Windows 实例上启用 DHCP
  1. 停止受影响的实例并断开其根卷。
  2. 在受影响的实例所在的可用区中启动临时实例。



#### Warning

(可选) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成额外的步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。或者，可以为临时实例选择不同的 AMI。例如，如果原始实例使用 Windows Server 2008 R2 的 AWS Windows AMI，则使用 Windows Server 2012 或 Windows Server 2003 的 AWS Windows AMI 来启动临时实例。（要查找适用于 Windows Server 2003 的 AMI，请使用名称 Windows\_Server-2003-R2\_SP2 来搜索 AMI。）

3. 将根卷从受影响的实例连接到此临时实例。连接到临时实例，打开 Disk Management (磁盘管理) 实用工具，将驱动器联机。
4. 从临时实例，打开 Regedit 并选择 HKEY\_LOCAL\_MACHINE。从 File 菜单中，选择 Load Hive。选择驱动器，打开文件 Windows\System32\config\SYSTEM，在出现提示时指定键名（您可以使用任何名称）。
5. 选择刚加载的注册表项，然后导航至 ControlSet001\Services\Tcpip\Parameters\Interfaces。每个网络接口均按 GUID 列出。选择正确的网络接口。如果禁用了 DHCP 且分配了静态 IP 地址，则 EnableDHCP 设置为 0。要启用 DHCP，请将 EnableDHCP 设置为 1，并且删除以下键（如果存在）：NameServer、SubnetMask、IPAddress 和 DefaultGateway。再次选择该键，在 File 菜单中，选择 Unload Hive。
6. (可选) 如果已启用 DHCP，则可能是您没有通向该元数据服务的路由。更新 EC2Config 可以解决此问题。
  - a. 下载最新的 [Amazon Windows EC2Config 服务](#)。将文件从 .zip 文件提取到所连接的驱动器上的 Temp 目录。
  - b. 打开 Regedit，选择 HKEY\_LOCAL\_MACHINE。从 File 菜单中，选择 Load Hive。选择驱动器，打开文件 Windows\System32\config\SOFTWARE，在出现提示时指定键名（您可以使用任何名称）。
  - c. 选择刚加载的注册表项，然后导航至 Microsoft\Windows\CurrentVersion。选择 RunOnce 键。（如果此键不存在，请右键单击 CurrentVersion，指向 New(新建)，选择 Key(键)，然后将该键命名为 RunOnce。）右键单击，指向 New(新建)，选择 String Value(字符串值)。输入 Ec2Install 作为名称并输入 C:\Temp\Ec2Install.exe -q 作为数据。
  - d. 再次选择该键，在 File 菜单中，选择 Unload Hive。
7. (可选) 如果您的临时实例与原始实例基于相同的 AMI，且操作系统版本高于 Windows Server 2003，则您必须完成以下步骤，否则在您恢复原始实例的根卷之后，由于磁盘签名冲突，您将无法启动原始实例。



#### Warning

以下过程介绍了如何使用注册表编辑器编辑 Windows 注册表。如果您不熟悉注册表或不知道如何使用注册编辑器安全地做出更改，请阅读 [Microsoft TechNet](#) 上的注册表。

- a. 打开命令提示，键入 regedit.exe，并按“Enter”键。
- b. 在注册表编辑器中，从上下文菜单中选择 HKEY\_LOCAL\_MACHINE（右击），然后选择“查找”。
- c. 键入 Windows Boot Manager，然后选择“查找下一个”。
- d. 选择名为 11000001 的密钥。此密钥与您在之前步骤中找到的密钥处于同一层级。
- e. 在右侧窗格中，选择“”，然后从上下文菜单中选择“修改”（右击）。
- f. 在数据中的偏移 0x38 处查找四字节磁盘签名。颠倒这些字节以创建磁盘签名并将其记下。例如，由以下数据表示的磁盘签名 E9EB3AA5：

```
...
0030 00 00 00 00 01 00 00 00
0038 A5 3A EB E9 00 00 00 00
0040 00 00 00 00 00 00 00 00
...
```

- g. 在命令提示符窗口中，运行以下命令以启动 Microsoft DiskPart。

```
C:\> diskpart
```

- h. 运行以下 DiskPart 命令以选择卷。（您可以使用 Disk Management（磁盘管理）实用工具来验证磁盘编号为 1。）

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

- i. 运行以下 DiskPart 命令以获取磁盘签名。

```
DISKPART> uniqueid disk

Disk ID: 0C764FA8
```

- j. 如果上一步骤中显示的磁盘签名与前面记下的 BCD 中的磁盘签名不匹配，请使用以下 DiskPart 命令更改磁盘签名以使其匹配：

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. 使用 Disk Management（磁盘管理）实用工具，将驱动器脱机。



#### Note

如果临时实例运行的操作系统与受影响实例相同，则驱动器将自动脱机，因此您无需手动使其脱机。

9. 将该卷从临时实例分离。如果您不再使用临时实例，则可以将其终止。
10. 将受影响实例的根卷作为 /dev/sda1 挂载，从而将其还原。
11. 启动受影响的实例。

如果您已连接到实例，请从该实例打开 Internet 浏览器，然后输入元数据服务器的以下 URL：

```
http://169.254.169.254/latest/meta-data/
```

如果您无法连接到元数据服务器，请尝试以下操作解决问题：

- 下载并安装最新版本的 EC2Config。有关更多信息，请参阅 [安装最新版的 EC2Config \(p. 258\)](#)。
- 检查 Windows 实例是否正在运行 RedHat 半虚拟化驱动程序。如果正在运行这种驱动程序，请更新至 Citrix 半虚拟化驱动程序。有关更多信息，请参阅 [在 Windows AMI 上升级半虚拟化驱动程序 \(p. 275\)](#)。
- 验证防火墙、IPSec 和代理设置没有阻止到元数据服务 (169.254.169.254) 或 KMS 服务器（地址在 C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml 中的 TargetKMServer 元素中指定）的传出流量。
- 使用以下命令验证您拥有到元数据服务 (169.254.169.254) 的路由。

```
C:\> route print
```

- 检查可能影响您的实例的可用区的网络问题。转到 <http://status.amazonaws.cn/>。

## "无法激活 Windows"

Windows 实例使用 AWS Key Management Service (AWS KMS) 进行激活。如果您的实例无法访问 KMS 服务器，您可能会收到此消息：A problem occurred when Windows tried to activate. Error Code 0xC004F074。必须每隔 180 天激活一次 Windows。在激活期限到期之前，EC2Config 会尝试连接 KMS 服务器以确保 Windows 仍处于激活状态。

如果您遇到 Windows 激活问题，请使用以下过程来解决此问题。

1. 下载并安装最新版本的 EC2Config 服务。有关更多信息，请参阅 [Amazon Windows EC2Config 服务](#)。
2. 登录到实例并打开以下文件：C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml。
3. 在 config.xml 文件中找到 Ec2WindowsActivate 插件。将状态更改为 Enabled 并保存您的更改。
4. 在 Windows 服务管理单元中，重新启动 EC2Config 服务或者重启实例。

如果这没有解决激活问题，请按照下面这些额外步骤操作。

1. 设置 KMS 目标：C:\> slmgr.vbs /skms 169.254.169.250:1688
2. 激活 Windows：C:\> slmgr.vbs /ato

如果您仍然收到激活错误，则验证以下信息。

- 确认您除了使用任何其他 DNS 服务器外还使用 Amazon DNS 服务器，或确认 Amazon DNS 服务器已列出为 DNS 转发服务器。Amazon DNS 服务器位于 EC2-Classic 实例的 172.16.0.23，或者位于 VPC 网络以及 VPC 中的两个实例的基点，例如，在带有 CIDR 10.0.0.0/16 的 VPC 中，Amazon DNS 服务器位于 10.0.0.2。
- 确认您有到 KMS 服务器的路由。打开 C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml，找到 TargetKMServer 元素。运行以下命令，检查是否列出了这些 KMS 服务器的地址。

```
C:\> route print
```

- 确认已设置 KMS 客户端密钥。运行以下命令并检查输出。

```
C:\> C:\Windows\System32\slmgr.vbs /dlv
```

如果输出包含 Error: product key not found，则说明未设置 KMS 客户端密钥。如果未设置 KMS 客户端密钥，请按 Microsoft TechNet 文章 <http://technet.microsoft.com/en-us/library/jj612867.aspx> 中的说明查找客户端密钥，然后运行以下命令以设置 KMS 客户端密钥。

```
C:\> C:\Windows\System32\slmgr.vbs /ipk client_key
```

- 确认系统的时间和时区是正确的。如果您使用的是 Windows Server 2008 或更高版本以及 UTC 以外的时区，请添加以下注册表项并将其设置为 1 以确保时间正确：  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal。
- 如果启用了 Windows 防火墙，请使用以下命令临时将其禁用。

```
C:\> netsh advfirewall set allprofiles state off
```

## "Windows 不是正版 (0x80070005)"

Windows 实例使用 KMS 进行激活。如果实例无法完成激活过程，则会报告该 Windows 副本不是正版。

请尝试有关 "无法激活 Windows" (p. 831) 的建议。

## "没有终端服务器许可服务器可提供许可证"

默认情况下，Windows Server 已获得授权，允许两个用户通过远程桌面同时使用。如果需要允许两个以上用户通过远程桌面同时访问您的 Windows 实例，您可以购买远程桌面服务客户端访问许可证 (CAL)，并安装“Remote Desktop Session Host (远程桌面会话主机)”和“Remote Desktop Licensing Server (远程桌面许可服务器)”角色。

检查有无以下问题：

- 已超过并发 RDP 会话的最大数目。
- 已安装 Windows 远程桌面服务角色。
- 许可已过期。如果许可已过期，那么您无法作为用户连接到您的 Windows 实例。您可以尝试以下操作：
  - 使用 /admin 参数从命令行连接到实例，例如：

```
C:\> mstsc /v:instance /admin
```

有关更多信息，请参阅以下 Microsoft 文章：[在远程桌面连接中使用命令行参数](#)。

- 停止该实例，断开其 Amazon EBS 卷，然后将这些卷挂载到同一可用区中的另一个实例以恢复数据。

# 文档历史记录

---

## Abstract

查找 Amazon EC2 文档的修订日期、相关版本和重要更改。

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：2016-04-01。

| 功能                            | API 版本     | 说明                                                                                                         | 发行日期            |
|-------------------------------|------------|------------------------------------------------------------------------------------------------------------|-----------------|
| 针对托管实例的 Run Command 支持        | 2016-04-01 | Amazon EC2 Run Command 现在支持对本地服务器和虚拟机 (VM) 以及来自其他云提供商的虚拟机进行管理。有关更多信息，请参阅 <a href="#">设置托管实例 (p. 335)</a> 。 | 2016 年 6 月 30 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 <a href="#">增强联网类型 (p. 630)</a> 。                                             | 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 <a href="#">资源 ID (p. 730)</a> 。                        | 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 <a href="#">复制 Amazon EBS 快照 (p. 679)</a> 。                         | 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 <a href="#">对无法访问的实例进行故障排除 (p. 813)</a> 。                                | 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 <a href="#">X1 实例 (p. 130)</a> 。               | 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 <a href="#">Amazon EBS 卷类型 (p. 641)</a> 。           | 2016 年 4 月 19 日 |

| 功能                                                           | API 版本     | 说明                                                                                                                                                              | 发行日期             |
|--------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 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 <a href="#">实例指标 (p. 454)</a> 。                                                         | 2016 年 3 月 23 日  |
| 竞价型队列的 CloudWatch 指标                                         |            | 您现在可以获取竞价型队列的 CloudWatch 指标。有关更多信息，请参阅 <a href="#">竞价型队列的 CloudWatch 指标 (p. 191)</a> 。                                                                          | 2016 年 3 月 21 日  |
| 计划实例                                                         | 2015-10-01 | 利用计划的预留实例（计划实例），您可以购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的容量预留。有关更多信息，请参阅 <a href="#">计划的预留实例 (p. 157)</a> 。                                                           | 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 <a href="#">资源 ID (p. 730)</a> 。                                           | 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 实例和 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。有关更多信息，请参阅 <a href="#">启用 ClassicLink DNS 支持 (p. 584)</a> 。 | 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 <a href="#">T2 实例 (p. 113)</a> 。                                            | 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 <a href="#">专用主机 (p. 201)</a> 。                                                                                      | 2015 年 11 月 23 日 |
| 竞价型实例持续时间                                                    | 2015-10-01 | 现在，您可以为竞价型实例指定持续时间。有关更多信息，请参阅 <a href="#">指定竞价型实例的持续时间 (p. 171)</a> 。                                                                                           | 2015 年 10 月 6 日  |
| 竞价型队列修改请求                                                    | 2015-10-01 | 您现在可以修改竞价型队列请求的目标容量。有关更多信息，请参阅 <a href="#">修改竞价型队列请求 (p. 181)</a> 。                                                                                             | 2015 年 9 月 29 日  |
| 竞价型队列多样化分配策略                                                 | 2015-04-15 | 您现在可以使用单个竞价型队列请求在多个竞价池中分配竞价型实例。有关更多信息，请参阅 <a href="#">竞价型队列分配策略 (p. 165)</a> 。                                                                                  | 2015 年 9 月 15 日  |
| 竞价型队列实例权重                                                    | 2015-04-15 | 您现在可以定义每个实例类型对应用程序性能贡献的容量单位，并相应地为每个竞价池调整出价。有关更多信息，请参阅 <a href="#">竞价型队列实例权重 (p. 166)</a> 。                                                                      | 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 <a href="#">创建停止、终止、重启或恢复实例的警报 (p. 483)</a> 。                                                                           | 2015 年 7 月 23 日  |

| 功能                                          | API 版本     | 说明                                                                                                                                                                                                                                                                                      | 发行日期            |
|---------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 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 <a href="#">T2 实例 (p. 113)</a> 。                                                                                                                                                                    | 2015 年 6 月 16 日 |
| M4 实例                                       |            | 实现了计算、内存和网络资源平衡的下一代通用型实例。M4 实例由带 AVX2 的自定义 Intel 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器支持。                                                                                                                                                                                        | 2015 年 6 月 11 日 |
| 竞价型队列                                       | 2015-04-15 | 您可以管理竞价型实例的集合或队列，而不必管理单独的竞价型实例请求。有关更多信息，请参阅 <a href="#">竞价型队列的工作方式 (p. 165)</a> 。                                                                                                                                                                                                       | 2015 年 5 月 18 日 |
| 将弹性 IP 地址迁移至 EC2-Classic                    | 2015-04-15 | 您可将分配为在 EC2-Classic 平台中使用的弹性 IP 地址迁移至 EC2-VPC 平台。有关更多信息，请参阅 <a href="#">将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC (p. 608)</a> 。                                                                                                                                                               | 2015 年 5 月 15 日 |
| 将具有多个磁盘的 VM 作为 AMI 导入                       | 2015-03-01 | VM Import 过程现在支持将具有多个磁盘的 VM 作为 AMI 导入。有关更多信息，请参阅 <a href="#">导入和导出虚拟机 (p. 401)</a> 。                                                                                                                                                                                                    | 2015 年 4 月 23 日 |
| 新 g2.8xlarge 实例类型                           |            | 新 g2.8xlarge 实例受四种高性能 NVIDIA GPU 支持，非常适合 GPU 计算工作负载，包括大规模呈现、转码、机器学习以及其他需要大规模并行处理能力的服务器端工作负载。                                                                                                                                                                                            | 2015 年 4 月 7 日  |
| D2 实例                                       |            | <p>新一代 Amazon EC2 密集存储实例，经过优化，适用于需要顺序访问直接连接实例存储上大量数据的应用程序。D2 实例适合在密集存储系列中提供最佳性价比。由 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器提供支持，通过提供额外的计算能力、更多内存和增强联网功能，HS1 上的 D2 实例得到了极大改进。此外，D2 实例有四种实例大小可供选择，存储容量分别是 6TB、12TB、24TB 和 48TB。</p> <p>有关更多信息，请参阅 <a href="#">D2 实例 (p. 121)</a>。</p> | 2015 年 3 月 24 日 |
| Amazon EC2 Simple Systems Manager (SSM)     |            | SSM 使您可以配置和管理您的 EC2 实例。有关更多信息，请参阅 <a href="#">管理 Windows 实例配置 (p. 294)</a> 和 <a href="#">将 Windows 实例加入 AWS Directory Service 域 (p. 299)</a> 。                                                                                                                                          | 2015 年 2 月 17 日 |
| AWS Systems Manager for Microsoft SCVMM 1.5 |            | 您现在可以使用 AWS Systems Manager for Microsoft SCVMM 启动实例，并将 VM 从 SCVMM 导入 Amazon EC2。有关更多信息，请参阅 <a href="#">创建 EC2 实例 (p. 763)</a> 和 <a href="#">导入您的虚拟机 (p. 767)</a> 。                                                                                                                     | 2015 年 1 月 21 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 <a href="#">恢复您的实例 (p. 237)</a>。</p>                                                                                                 | 2015 年 1 月 12 日 |

| 功能                                      | API 版本     | 说明                                                                                                                                                                                                                                                                                                                                                     | 发行日期             |
|-----------------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C4 实例                                   |            | <p>新一代计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C4 实例基于自定义 2.9 GHz Intel® Xeon® E5-2666 v3 (Haswell) 处理器。C4 实例采用睿频加速技术，单核或双核经睿频加速后，处理器时钟频率可高达 3.5Ghz。C4 实例扩展自 C3 计算优化型实例的功能，可为客户在 EC2 实例中提供最高的处理器性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体动力学。</p> <p>有关更多信息，请参阅 <a href="#">C4 实例 (p. 116)</a>。</p>                                            | 2015 年 1 月 11 日  |
| ClassicLink                             | 2014-10-01 | <p>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 <a href="#">ClassicLink (p. 578)</a>。</p>                                                                                                                                                                      | 2015 年 1 月 7 日   |
| 竞价型实例终止通知                               |            | <p>防范竞价型实例中断的最佳方法是为应用程序设计容错能力。此外，您还可以利用竞价型实例终止通知，该通知可在 Amazon EC2 必须终止您的竞价型实例时，提前两分钟发出警告。</p> <p>有关更多信息，请参阅 <a href="#">竞价型实例终止通知 (p. 197)</a>。</p>                                                                                                                                                                                                    | 2015 年 1 月 5 日   |
| AWS Systems Manager for Microsoft SCVMM |            | <p>AWS Systems Manager for Microsoft SCVMM 可为从 Microsoft SCVMM 管理 AWS 资源（如 EC2 实例）提供简单易用的界面。有关更多信息，请参阅 <a href="#">AWS Systems Manager for Microsoft System Center VMM (p. 758)</a>。</p>                                                                                                                                                               | 2014 年 10 月 29 日 |
| DescribeVolumes 分页支持                    | 2014-09-01 | <p>DescribeVolumes API 调用现在可使用 MaxResults 和 NextToken 参数支持结果分页。有关详细信息，请参阅 <a href="#">Amazon EC2 API Reference</a> 中的 <a href="#">DescribeVolumes</a>。</p>                                                                                                                                                                                             | 2014 年 10 月 23 日 |
| 增加了对 Amazon CloudWatch Logs 的支持         |            | <p>您可以使用 Amazon CloudWatch Logs 来监控、存储和访问您的系统、应用程序以及来自实例或其他来源的自定义日志文件。然后可以使用 Amazon CloudWatch 控制台、AWS CLI 中的 CloudWatch Logs 命令或使用 CloudWatch Logs 软件开发工具包，从 CloudWatch Logs 检索关联的日志数据。有关更多信息，请参阅 <a href="#">使用 EC2Config 服务配置 Windows 实例 (p. 250)</a>。更多有关 CloudWatch Logs 的信息，请参阅 Amazon CloudWatch 开发者指南中的 <a href="#">监控系统、应用程序和自定义日志文件</a>。</p> | 2014 年 7 月 10 日  |
| T2 实例                                   | 2014-06-15 | <p>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 <a href="#">T2 实例 (p. 113)</a>。</p>                                                                                                                                                                                                                             | 2014 年 6 月 30 日  |

| 功能                                 | API 版本     | 说明                                                                                                                                                                                                       | 发行日期             |
|------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 新 EC2 Service Limits (EC2 服务限制) 页面 |            | 使用 Amazon EC2 控制台中的 EC2 Service Limits (EC2 服务限制) 页面可按区域查看 Amazon EC2 和 Amazon VPC 提供的资源的当前限制。                                                                                                           | 2014 年 6 月 19 日  |
| Amazon EBS 通用型 SSD 卷               | 2014-05-01 | 通用型 SSD 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷的延迟通常不超过十毫秒，能突增至 3000 IOPS 很长时间，基本性能为 3 IOPS/GiB。通用型 SSD 卷的大小范围是 1 GiB 到 1 TiB。有关更多信息，请参阅 <a href="#">通用型 SSD (gp2) 卷 (p. 643)</a> 。                                  | 2014 年 6 月 16 日  |
| Windows Server 2012 R2             |            | Windows Server 2012 R2 AMI 使用新的 AWS 半虚拟化驱动程序。有关更多信息，请参阅 <a href="#">AWS 半虚拟化驱动程序 (p. 273)</a> 。                                                                                                          | 2014 年 6 月 3 日   |
| AWS 管理包                            |            | AWS 管理包现在支持 System Center Operations Manager 2012 R2。有关更多信息，请参阅 <a href="#">AWS Management Pack for Microsoft System Center (p. 771)</a> 。                                                               | 2014 年 5 月 22 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 <a href="#">Amazon EBS Encryption (p. 686)</a> 。 | 2014 年 5 月 21 日  |
| R3 实例                              | 2014-02-01 | 新一代内存优化型实例具有最佳的每 GiB RAM 价格点和高性能。这些实例十分适合于关系数据库和 NoSQL 数据库、内存分析解决方案、科学计算以及其他可受益于 R3 实例的 vCPU 高内存、高计算性能和增强的联网功能的内存密集型应用程序。<br><br>有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。      | 2014 年 4 月 9 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 <a href="#">Amazon EC2 使用率报告 (p. 747)</a> 。                                                                                                            | 2014 年 1 月 28 日  |
| 额外 M3 实例                           | 2013-10-15 | 现在支持 M3 实例大小 m3.medium 和 m3.large。<br>有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。                                                                                                 | 2014 年 1 月 20 日  |
| I2 实例                              | 2013-10-15 | 这些实例提供极高的 IOPS。I2 实例还支持增强型联网，从而减小实例间延迟、降低网络抖动，显著提高每秒数据包(PPS)性能。有关更多信息，请参阅 <a href="#">I2 实例 (p. 119)</a> 。                                                                                               | 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。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。                                                                                      | 2013 年 12 月 19 日 |

| 功能                     | API 版本     | 说明                                                                                                                                                                                                                         | 发行日期             |
|------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| RunInstances 的资源级别权限   | 2013-10-15 | 您现在可以在 AWS Identity and Access Management 中创建策略以控制 Amazon EC2 RunInstances API 操作的资源级别权限。有关更多信息以及示例策略，请参阅 <a href="#">控制对 Amazon EC2 资源的访问 (p. 522)</a> 。                                                                  | 2013 年 11 月 20 日 |
| C3 实例                  | 2013-10-15 | 计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C3 实例还支持增强型联网，这种联网可减小实例间延迟、降低网络抖动并显著提高每秒数据包 (PPS) 性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体动力学。<br><br>有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。 | 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 <a href="#">启动 AWS Marketplace 实例 (p. 223)</a> 。                                                                                                                  | 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 <a href="#">Windows GPU 实例 (p. 118)</a> 。                                                                                                          | 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 <a href="#">启动实例 (p. 216)</a> 。                                                                                                                                                            | 2013 年 10 月 10 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。                                                                                                                                                                                                           | 2013 年 9 月 11 日  |
| 分配公有 IP 地址             | 2013-07-15 | 在 VPC 中启动实例时，现在可以分配公有 IP 地址。有关更多信息，请参阅 <a href="#">分配公有 IP 地址 (p. 601)</a> 。                                                                                                                                               | 2013 年 8 月 20 日  |
| 授予资源级别权限               | 2013-06-15 | Amazon EC2 支持新的 Amazon 资源名称 (ARN) 和条件键。有关更多信息，请参阅 <a href="#">Amazon EC2 的 IAM 策略 (p. 525)</a> 。                                                                                                                           | 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 <a href="#">复制 Amazon EBS 快照 (p. 679)</a> 。                                                                                                                                                       | 2013 年 6 月 11 日  |
| AWS 管理包                |            | AWS 管理包会将 Amazon EC2 实例与其内部运行的 Microsoft 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。有关更多信息，请参阅 <a href="#">AWS Management Pack for Microsoft System Center (p. 771)</a> 。         | 2013 年 5 月 8 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 <a href="#">标记 Amazon EC2 资源 (p. 737)</a> 。                                                                                                                                  | 2013 年 4 月 4 日   |

| 功能                                           | API 版本     | 说明                                                                                                                                                                                                                       | 发行日期             |
|----------------------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| EBS 优化的额外实例类型                                | 2013-02-01 | <p>以下实例类型现在可作为 EBS 优化的实例启动：c1.xlarge、m2.2xlarge、m3.xlarge 和 m3.2xlarge。</p> <p>有关更多信息，请参阅 <a href="#">Amazon EBS 优化实例 (p. 683)</a>。</p>                                                                                  | 2013 年 3 月 19 日  |
| 半虚拟化驱动程序                                     |            | <p>要了解如何升级 Windows AMI 上的半虚拟化 (PV) 驱动程序，请参阅 <a href="#">在 Windows AMI 上升级半虚拟化驱动程序 (p. 275)</a>。</p>                                                                                                                      | 2013 年 3 月       |
| AWS Diagnostics for Microsoft Windows Server |            | <p>主题 <a href="#">AWS Diagnostics for Microsoft Windows Server - Beta (p. 809)</a> 介绍如何通过 AWS Diagnostics for Microsoft Windows Server 诊断可能存在的问题，并且对其进行故障排除。</p>                                                         | 2013 年 3 月       |
| 将 AMI 从一个区域复制到另一个区域                          | 2013-02-01 | <p>您可以将 AMI 从一个区域复制到另一个区域，以便快速轻松地在多个 AWS 区域启动一致的实例。</p> <p>有关更多信息，请参阅 <a href="#">复制 AMI (p. 84)</a>。</p>                                                                                                                | 2013 年 3 月 11 日  |
| 在默认 VPC 中启动实例                                | 2013-02-01 | <p>您的 AWS 账户可以将实例启动为 EC2-Classic 或 EC2-VPC 平台，也可以根据各区域间的差异仅仅启动为 EC2-VPC 平台。如果您只能将实例启动为 EC2-VPC，我们会为您创建一个默认 VPC。当您启动实例时，我们会将其启动为默认 VPC，除非您创建了非默认 VPC 并在启动实例时对其进行指定。</p> <p>有关更多信息，请参阅 <a href="#">支持的平台 (p. 577)</a>。</p> | 2013 年 3 月 11 日  |
| 内存增强型群集 (cr1.8xlarge) 实例类型                   | 2012-12-01 | <p>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。</p>                                                                                                                                                                 | 2013 年 1 月 21 日  |
| 高存储 (hs1.8xlarge) 实例类型                       | 2012-12-01 | <p>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。有关更多信息，请参阅 <a href="#">HS1 实例 (p. 123)</a>。</p>                                                                                                | 2012 年 12 月 20 日 |
| EBS 快照副本                                     | 2012-12-01 | <p>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 <a href="#">复制 Amazon EBS 快照 (p. 679)</a>。</p>                                                                                                      | 2012 年 12 月 17 日 |
| 已更新 Provisioned IOPS 卷的 EBS 指标和状态检查          | 2012-10-01 | <p>已更新 EBS 指标，以便包含 Provisioned IOPS 卷的两项新指标。有关更多信息，请参阅 <a href="#">使用 CloudWatch 监控卷 (p. 660)</a>。还添加了 Provisioned IOPS 卷的新状态检查。有关更多信息，请参阅 <a href="#">使用状态检查来监控卷 (p. 663)</a>。</p>                                      | 2012 年 11 月 20 日 |

| 功能                                                                     | API 版本          | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                | 发行日期             |
|------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 适用于 Microsoft Windows Server 2012 的支持                                  |                 | <p>Amazon EC2 为您提供了几个预先配置的 Windows Server 2012 AMI。这些 AMI 对所有区域的每个 64 位实例类型即时可用。这些 AMI 支持以下语言：</p> <ul style="list-style-type: none"> <li>• 英语</li> <li>• 简体中文</li> <li>• 繁体中文</li> <li>• 繁体中文（香港）</li> <li>• 日语</li> <li>• 韩语</li> <li>• 葡萄牙语</li> <li>• 巴西葡萄牙语</li> <li>• 捷克语</li> <li>• 荷兰语</li> <li>• 法语</li> <li>• 德语</li> <li>• 匈牙利语</li> <li>• 意大利语</li> <li>• 波兰语</li> <li>• 俄语</li> <li>• 西班牙语</li> <li>• 瑞典语</li> <li>• 土耳其语</li> </ul> | 2012 年 11 月 19 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 <a href="#">Amazon EC2 实例</a> 。                                                                                                                                                                                                                                                                                                                                                      | 2012 年 10 月 31 日 |
| 竞价型实例请求状态                                                              | 2012-10-01      | 竞价型实例请求状态简化了确定您的竞价请求状态的过程。                                                                                                                                                                                                                                                                                                                                                                                                                        | 2012 年 10 月 14 日 |
| Amazon EC2 预留实例市场                                                      | 2012-08-15      | 预留实例市场 将想要出售不再需要的 Amazon EC2 预留实例的卖方与正在寻找购买额外容量的买方匹配起来。通过 预留实例市场 购买和出售的预留实例与其他预留实例一样工作，不同的是他们受标准条款限制更少，并能以不同价格出售。                                                                                                                                                                                                                                                                                                                                 | 2012 年 9 月 11 日  |
| 适用于 Amazon EBS 的 Provisioned IOPS (input/output operations per second) | 2012-07-20      | Provisioned IOPS 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 <a href="#">Amazon EBS 卷类型 (p. 641)</a> 。                                                                                                                                                                                                                                                                                                                           | 2012 年 7 月 31 日  |
| 适用于 Amazon EC2 的高 I/O 实例                                               | 2012-06-15      | 高 I/O 实例通过使用基于 SSD 的本地实例存储提供低延时、高性能的磁盘 I/O。有关更多信息，请参阅 <a href="#">H1 实例 (p. 122)</a> 。                                                                                                                                                                                                                                                                                                                                                            | 2012 年 7 月 18 日  |

| 功能                                                                           | API 版本     | 说明                                                                                                                                                                                                                                                                                       | 发行日期             |
|------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| IAM 对 Amazon EC2 实例的作用                                                       | 2012-06-01 | <p>适用于 Amazon EC2 实例的 IAM 角色提供：</p> <ul style="list-style-type: none"> <li>在 Amazon EC2 实例上运行的应用程序的 AWS 访问密钥。</li> <li>Amazon EC2 实例上的 AWS 访问密钥的自动交替。</li> <li>为 Amazon EC2 实例上请求 AWS 服务的运行应用程序细调权限。</li> </ul>                                                                          | 2012 年 6 月 11 日  |
| 让启动和处理中断可能性变得更加容易的竞价型实例功能                                                    |            | <p>现在您可以按照以下方式管理您的竞价型实例：</p> <ul style="list-style-type: none"> <li>使用 Auto Scaling 启动配置为竞价型实例竞价，并为竞价型实例的竞价设置日程表。有关更多信息，请参阅 <i>Auto Scaling 用户指南</i> 中的<a href="#">在 Auto Scaling 组中启动竞价型实例</a>。</li> <li>实例启动或终止时获得通知。</li> <li>在 AWS 资源堆栈中使用 AWS CloudFormation 模板来启动竞价型实例。</li> </ul> | 2012 年 6 月 7 日   |
| 用于 Amazon EC2 状态检查的 EC2 实例导出和时间戳                                             | 2012-05-01 | <p>已添加将您原先导入到 EC2 的 Windows Server 实例导出的支持。</p> <p>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。</p>                                                                                                                                                                                            | 2012 年 5 月 25 日  |
| Amazon VPC 实例和系统状态检查中的 EC2 实例导出和时间戳                                          | 2012-05-01 | <p>已添加将实例导出至 Citrix Xen、Microsoft Hyper-V 和 VMware vSphere 的支持。</p> <p>已添加多实例和系统状态检查中的时间戳的支持。</p>                                                                                                                                                                                        | 2012 年 5 月 25 日  |
| 八倍超大型群集计算                                                                    | 2012-04-01 | 添加了对 VPC 中的 cc2.8xlarge 实例的支持。                                                                                                                                                                                                                                                           | 2012 年 4 月 26 日  |
| AWS Marketplace AMIs                                                         | 2012-04-01 | 已添加对 AWS Marketplace AMIs 的支持。                                                                                                                                                                                                                                                           | 2012 年 4 月 19 日  |
|                                                                              | 2011-12-15 | 已添加一种新的实例类型和 64 位信息的支持。                                                                                                                                                                                                                                                                  | 2012 年 3 月 7 日   |
| 预留实例定价套餐                                                                     | 2011-12-15 | 已添加一个章节来讨论如何充分享用预留实例定价套餐自带的折扣价格。                                                                                                                                                                                                                                                         | 2012 年 3 月 5 日   |
| Amazon Virtual Private Cloud 中的适用于 EC2 实例的 Elastic Network Interfaces (ENIs) | 2011-12-01 | 已添加有关 VPC 中适用于 EC2 实例的 Elastic Network Interfaces (ENIs) 的新章节。有关更多信息，请参阅 <a href="#">弹性网络接口 (ENI) (p. 612)</a> 。                                                                                                                                                                         | 2011 年 12 月 21 日 |
| Amazon EC2 预留实例的新产品类型                                                        | 2011-11-01 | 您可以选择各种各样的预留实例产品，以满足您对实例的预期使用要求：高利用率、中利用率和低利用率。                                                                                                                                                                                                                                          | 2011 年 12 月 1 日  |

| 功能                                               | API 版本     | 说明                                                                                                                                                                                                                                                                               | 发行日期             |
|--------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Amazon EC2 实例状态                                  | 2011-11-01 | 您可以查看您的实例状态的其他详细信息，包括 AWS 计划的可能会影响您的实例的事件。这些操作活动包括，执行软件更新和安全性补丁程序所要求的实例重启，和出现硬件问题时所需的实例停止。有关更多信息，请参阅 <a href="#">“监控实例状态 (p. 443)”</a> 。                                                                                                                                         | 2011 年 11 月 16 日 |
| Amazon EC2 群集计算实例类型                              |            | Amazon EC2 八倍超大型群集计算 (cc2.8xlarge) 的补充支持。                                                                                                                                                                                                                                        | 2011 年 11 月 14 日 |
| Amazon VPC 中的竞价型实例                               | 2011-07-15 | 添加了 Amazon VPC 中的竞价型实例支持的有关信息。通过此更新，用户可以在 Virtual Private Cloud (VPC) 中启动竞价型实例。通过在 VPC 中启动竞价型实例，竞价型实例的用户可以享用 Amazon VPC 的优势。                                                                                                                                                     | 2011 年 10 月 11 日 |
| 适用于 CLI 工具用户的简化的 VM import 程序                    | 2011-07-15 | 使用 <code>ec2-import-instance</code> 和 <code>ec2-import-volume</code> 的增强功能将适用于 CLI 工具用户的 VM Import 程序进行简化，现在，创建导入任务后，系统会执行上传图片到 Amazon EC2 上的操作。此外，通过引入 <code>ec2-resume-import</code> 命令，用户可以在任务停止时即刻重新启动未完成的上传。有关更多信息，请参阅 <a href="#">步骤 4：将您的 VM 导入 Amazon EC2 (p. 425)</a> 。 | 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，VM Import 现在支持 RAW、VHD 和 VMDK（与 VMware ESX 兼容的）图像格式。有关更多信息，请参阅 <a href="#">步骤 1：安装 Amazon EC2 CLI (p. 422)</a> 。                                                                         | 2011 年 8 月 24 日  |
| 适用于 Microsoft Windows Server 2003 R2 的支持         |            | VM Import 现在支持 Windows Server 2003 (R2)。通过这种新产品，VM Import 支持所有 Amazon EC2 支持的 Microsoft Windows Server 版本。                                                                                                                                                                       | 2011 年 8 月 24 日  |
| 更新至适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器 |            | 适用于 VMware vCenter 虚拟设备（连接器）的 1.1 版本的 EC2 VM Import 连接器的有关补充信息。此次更新包括访问因特网的代理支持、更好的错误处理方法、任务进度栏准确性的提高以及一些 bug 修复。有关更多信息，请参阅 <a href="#">将 VM 作为实例导入 Amazon EC2 (p. 418)</a> 。                                                                                                    | 2011 年 6 月 27 日  |
| 竞价型实例可用区定价更改                                     | 2011-05-15 | 添加了竞价型实例可用区定价功能的有关信息。在本版本中，我们添加了新的可用区定价选项，当您查询竞价型实例请求和现货价格历史记录时，返回的信息中包括这些新的定价选项。通过这些新增功能，可以更方便地确定将竞价型实例启动到特定可用区所需的价格。                                                                                                                                                           | 2011 年 5 月 26 日  |
| AWS Identity and Access Management               |            | 已添加 AWS Identity and Access Management (IAM) 的有关信息，使用户可以指定借助 Amazon EC2 资源一般能使用哪些 Amazon EC2 功能。有关更多信息，请参阅 <a href="#">控制对 Amazon EC2 资源的访问 (p. 522)</a> 。                                                                                                                       | 2011 年 4 月 26 日  |

| 功能                                             | API 版本     | 说明                                                                                                                                                                                                                               | 发行日期             |
|------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 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，请参阅如何使用 <a href="#">Amazon VPC 用户指南中的 EC2 专用实例</a> 。             | 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。                                                                                                                                                                             | 2011 年 3 月 27 日  |
| 支持 Windows Server 2008 R2                      |            | Amazon EC2 现在为您提供了几个预先配置的 Windows Server 2008 R2 AMI。这些 AMI 对所有区域的大多数 64 位实例类型即时可用，不包括 t1.micro 和 HPC 系列。这些 AMI 支持多种语言。                                                                                                          | 2011 年 3 月 15 日  |
| 元数据信息                                          | 2011-01-01 | 已添加元数据的有关信息，将反映 2011-01-01 版本中的更改。有关更多信息，请参阅 <a href="#">实例元数据和用户数据 (p. 239)</a> 和 <a href="#">实例元数据类别 (p. 245)</a> 。                                                                                                            | 2011 年 3 月 11 日  |
| 适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器。 |            | 已添加适用于 VMware vCenter 虚拟设备（连接器）的 EC2 VM Import Connector 的有关信息。这个连接器是一个用于 VMware vCenter 的插件，集成了 VMware vSphere 客户端，并提供了一个图形用户界面，您可以用它来将 VMware 虚拟机导入到 Amazon EC2 中。有关更多信息，请参阅 <a href="#">将 VM 作为实例导入 Amazon EC2 (p. 418)</a> 。 | 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 <a href="#">从实例断开 Amazon EBS 卷 (p. 670)</a> 。                                                                                                                          | 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 <a href="#">为实例启用终止保护 (p. 234)</a> 。                                                                                                                                                         | 2011 年 2 月 23 日  |
| VM Import                                      | 2010-11-15 | 已添加有关 VM Import 的信息，允许您将虚拟机或卷导入到 Amazon EC2 中。有关更多信息，请参阅 <a href="#">步骤 1：安装 Amazon EC2 CLI (p. 422)</a> 。                                                                                                                       | 2010 年 12 月 15 日 |
| 实例的基本监控                                        | 2010-08-31 | 已添加有关 EC2 实例的基本监控的信息。                                                                                                                                                                                                            | 2010 年 12 月 12 日 |
| 群集 GPU 实例                                      | 2010-08-31 | Amazon EC2 为高性能计算 (HPC) 应用程序提供了 GPU 群集实例(cg1.4xlarge)。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。                                                                                                         | 2010 年 11 月 14 日 |
| 筛选条件和标记                                        | 2010-08-31 | 已添加列举、筛选和标记资源的有关信息。有关更多信息，请参阅 <a href="#">列出并筛选您的资源 (p. 734)</a> 和 <a href="#">标记 Amazon EC2 资源 (p. 737)</a> 。                                                                                                                   | 2010 年 9 月 19 日  |

| 功能                                                  | API 版本     | 说明                                                                                                                   | 发行日期            |
|-----------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------|-----------------|
| 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。                                                                                                 | 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 <a href="#">T1 微型实例 (p. 124)</a> 。                                  | 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 <a href="#">控制对 Amazon EC2 资源的访问 (p. 522)</a> 。 | 2010 年 9 月 2 日  |
| 群集实例                                                | 2010-06-15 | Amazon EC2 为您的高性能计算 (HPC) 应用程序提供了群集计算实例。有关每种 Amazon EC2 实例类型的硬件规格的更多信息，请参阅 <a href="#">Amazon EC2 实例</a> 。           | 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 <a href="#">使用 CloudWatch 监控卷 (p. 660)</a> 。                     | 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 <a href="#">Amazon EC2 实例</a> 。          | 2010 年 2 月 22 日 |
| Windows 预留实例                                        |            | Amazon EC2 现在支持 Windows 预留实例。                                                                                        | 2010 年 2 月 22 日 |

# AWS 词汇表

---

## Abstract

列出最新 AWS 术语和用法。

有关最新的 AWS 术语，请参阅 *AWS General Reference*中的 [AWS 术语表](#)。