



用户指南

# Amazon EBS



# Amazon EBS: 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

# Table of Contents

什么是 Amazon EBS ? .....	1
Amazon EBS 的功能 .....	1
相关服务 .....	2
访问 Amazon EBS .....	2
定价 .....	3
为 Amazon EBS 进行设置 .....	4
注册获取 AWS 账户 .....	4
创建具有管理访问权限的用户 .....	4
( 可选 ) 创建和使用用于 Amazon EBS 加密的客户托管密钥 .....	5
( 可选 ) 启用阻止公开访问 Amazon EBS 快照 .....	6
EBS 卷 .....	8
使用 EBS 卷的优势 .....	8
数据可用性 .....	9
数据持久性 .....	9
数据加密 .....	10
数据安全性 .....	10
快照 .....	10
弹性 .....	11
EBS 卷类型 .....	11
固态硬盘 ( SSD ) 卷 .....	12
硬盘驱动器 ( HDD ) 卷 .....	13
上一代卷 .....	14
通用型 SSD 卷 .....	15
预置 IOPS SSD 卷 .....	19
吞吐量优化型 HDD 和 Cold HDD 卷 .....	23
大小和配置限制 .....	32
存储容量 .....	32
服务限制 .....	33
分区方案 .....	34
数据块大小 .....	35
EBS 卷和 NVMe .....	35
安装或升级 NVMe 驱动程序 .....	36
识别 EBS 设备 .....	38
使用 NVMe EBS 卷 .....	41

I/O 操作超时 .....	42
Abort 命令 .....	43
卷生命周期 .....	43
创建卷 .....	45
将卷挂载到实例 .....	49
将卷挂载到多个实例 .....	51
使卷可用 .....	60
查看卷详细信息 .....	72
修改卷 .....	76
从实例分离卷 .....	99
删除卷 .....	103
替换卷 .....	104
监控卷 .....	106
EBS 卷状态检查 .....	106
EBS 卷事件 .....	109
使用受损的卷 .....	111
使用自动启用 IO 卷属性 .....	113
故障测试 .....	114
EBS 快照 .....	117
快照的工作原理 .....	118
复制和共享快照 .....	122
快照的加密支持 .....	123
快照生命周期 .....	123
创建 快照 .....	124
查看快照信息 .....	129
复制快照 .....	131
共享快照 .....	137
归档快照 .....	143
删除快照 .....	174
自动化快照生命周期 .....	178
快速快照还原 .....	178
注意事项 .....	179
卷创建积分 .....	179
管理快速快照还原 .....	180
监控快速快照还原 .....	184
快速快照还原配额 .....	184

定价和计费 .....	184
快照锁定 .....	185
概念 .....	185
注意事项 .....	188
所需的权限 .....	188
使用快照锁定 .....	191
监视器使用 CloudTrail .....	195
监视器使用 EventBridge .....	195
阻止公开访问快照 .....	198
注意事项 .....	198
IAM 权限 .....	199
启用阻止公开访问快照 .....	200
监控事件 .....	203
回收站 .....	204
使用回收站中的快照的权限 .....	205
在回收站中查看快照 .....	206
从回收站中还原快照 .....	208
Outposts 上的 本地快照 .....	209
常见问题 .....	209
先决条件 .....	211
注意事项 .....	52
使用 IAM 控制访问 .....	212
使用本地快照 .....	214
EBS 加密 .....	223
EBS 加密的工作原理 .....	223
快照加密时 EBS 加密的工作原理 .....	224
快照未加密时 EBS 加密的工作原理 .....	224
不可用的 KMS 密钥如何影响数据密钥 .....	225
要求 .....	225
支持的卷类型 .....	226
支持的实例类型 .....	226
用户的权限 .....	226
实例的权限 .....	227
使用 Amazon EBS 加密 .....	228
选择 EBS 加密的 KMS 密钥 .....	228
默认启用加密 .....	229

默认使用 API 和 CLI 管理加密 .....	232
加密 EBS 资源 .....	232
在创建时加密空卷 .....	233
加密未加密的资源 .....	233
旋转 AWS KMS 钥匙 .....	234
示例 .....	234
还原未加密的卷 ( 未启用默认加密 ) .....	235
还原未加密的卷 ( 启用了默认加密 ) .....	235
复制未加密的快照 ( 未启用默认加密 ) .....	236
复制未加密的快照 ( 启用了默认加密 ) .....	236
重新加密已加密卷 .....	237
重新加密已加密快照 .....	237
在加密卷与未加密卷之间迁移数据 .....	238
加密结果 .....	238
EBS 性能 .....	241
Amazon EBS 性能提示 .....	241
使用 EBS 优化的实例 .....	241
了解如何计算性能 .....	241
了解工作负载 .....	242
请注意, 从快照中初始化卷时, 性能将会下降 .....	242
可能导致 HDD 性能下降的因素 .....	242
为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值 ( 仅限 Linux 实例 ) .....	242
使用现代 Linux 内核 ( 仅限 Linux 实例 ) .....	243
使用 RAID 0 以最大限度利用实例资源 .....	244
使用 Amazon 追踪绩效 CloudWatch .....	244
优化性能 .....	244
I/O 特性和监控 .....	244
IOPS .....	245
卷队列长度和延迟 .....	246
I/O 大小和卷吞吐量限制 .....	246
使用监控 I/O 特性 CloudWatch .....	247
相关资源 .....	249
初始化 卷 .....	249
RAID 配置 .....	253
RAID 配置选项 .....	254
创建 RAID 0 阵列 .....	254

创建 RAID 阵列中卷的快照 .....	262
对 EBS 卷进行基准测试 .....	263
设置实例 .....	263
安装基准测试工具 .....	264
选择卷队列长度 .....	266
禁用 C 状态 .....	266
执行基准测试 .....	267
Amazon Data Lifecycle Manager .....	271
配额 .....	272
Amazon Data Lifecycle Manager 的工作原理 .....	272
策略 .....	272
政策计划 .....	273
定位资源标签 .....	274
快照 .....	274
EBS 支持的 AMI .....	274
Amazon Data Lifecycle Manager 标签 .....	275
默认策略与自定义策略 .....	275
EBS 快照策略比较 .....	275
EBS 支持的 AMI 策略比较 .....	277
默认策略 .....	278
注意事项 .....	279
EBS 快照的默认策略 .....	279
EBS 支持的 AMI 的默认策略 .....	283
启用跨账户和地区的默认政策 .....	286
自定义策略 .....	290
自动化快照生命周期 .....	290
自动化 AMI 生命周期 .....	355
自动执行跨账户快照副本 .....	364
查看、修改和删除生命周期策略 .....	375
查看生命周期策略 .....	376
修改生命周期策略 .....	376
删除生命周期策略 .....	56
AWS Identity and Access Management .....	380
AWS 托管策略 .....	380
IAM 服务角色 .....	387
用户的权限 .....	393

加密权限 .....	395
监控快照和 AMI 的生命周期 .....	395
控制台和 AWS CLI .....	395
AWS CloudTrail .....	396
使用“CloudWatch 事件”监控您的政策 .....	396
使用 Amazon 监控您的政策 CloudWatch .....	398
故障排除 .....	410
错误: Role with name already exists .....	410
Amazon EBS 直接 API .....	412
了解 EBS direct API .....	412
快照 .....	412
数据块 .....	413
数据块索引 .....	413
数据块令牌 .....	413
校验和 .....	413
加密 .....	413
API 操作 .....	413
EBS 直接 API 的 IAM 权限 .....	414
使用 EBS 直接 API .....	420
读取快照 .....	421
写入快照 .....	428
使用加密 .....	434
使用签名版本 4 签名 .....	437
使用校验和 .....	437
API 的等性 StartSnapshot .....	438
错误重试 .....	439
优化性能 .....	441
EBS 直接 API 服务端点 .....	441
EBS 直接 API 的定价 .....	445
API 的定价 .....	445
联网成本 .....	445
接口 VPC 端点 .....	446
关于 EBS direct API VPC 终端节点的注意事项 .....	446
为 EBS direct API 创建接口 VPC 终端节点 .....	447
使用记录 API 调用 AWS CloudTrail .....	447
EBS 直接 API 中的信息 CloudTrail .....	448



了解 EBS direct API 日志文件条目 .....	449
常见问题 .....	455
安全性 .....	458
数据保护 .....	458
Amazon EBS 数据安全 .....	459
静态和动态加密 .....	459
KMS 密钥管理 .....	460
Identity and Access Management .....	460
受众 .....	461
使用身份进行身份验证 .....	461
使用策略管理访问 .....	464
Amazon Elastic Block Store 如何与 IAM 配合使用 .....	465
基于身份的策略示例 .....	472
故障排除 .....	489
合规性验证 .....	491
恢复能力 .....	492
监控 .....	493
AWS CloudTrail .....	493
CloudTrail 中的 Amazon EBS 信息 .....	448
了解 Amazon EBS 日志文件条目 .....	449
Amazon CloudWatch .....	496
Amazon EBS 卷的指标 .....	496
Nitro 实例的指标 .....	506
快速快照还原的指标 .....	509
Amazon EC2 控制台图表 .....	510
Amazon EventBridge .....	512
EBS 卷事件 .....	513
EBS 卷修改事件 .....	518
EBS 快照事件 .....	519
EBS 快照归档事件 .....	524
EBS 快速快照还原事件 .....	524
AWS Lambda 用于处理 EventBridge 事件 .....	526
Amazon GuardDuty .....	529
配额 .....	530
文档历史记录 .....	540
.....	dxlv

# 什么是 Amazon Elastic Block Store ?

Amazon Elastic Block Store ( Amazon EBS ) 提供了可扩展、高性能的数据块存储资源，与 Amazon Elastic Compute Cloud ( Amazon EC2 ) 实例一起使用。使用 Amazon Elastic Block Store 时，您可以创建和管理以下数据块存储资源：

- Amazon EBS 卷 – 挂载到 Amazon EC2 实例的存储卷。将卷挂载到实例后，您可以像使用挂载到计算机上的本地硬盘一样使用卷，例如用于存储文件或安装应用程序。
- Amazon EBS 快照 – 独立于卷本身持续存在的 Amazon EBS 卷的时间点备份。您可以通过创建快照来备份 Amazon EBS 卷上的数据。而后可以随时从这些快照还原新卷。

## 主题

- [Amazon EBS 的功能](#)
- [相关服务](#)
- [访问 Amazon EBS](#)
- [定价](#)

## Amazon EBS 的功能

Amazon EBS 提供以下功能和优势：

- 多种卷类型 – Amazon EBS 提供多种卷类型，可优化各种应用程序的存储性能和成本。卷类型分为两大类：用于交易工作负载的 SSD 支持型存储，以及用于吞吐量密集型工作负载的 HDD 支持型存储。
- 可扩展性 – 您可以创建容量和性能规范都满足需求的 Amazon EBS 卷。随着需求的变化，您可以在不必停机的情况下使用弹性卷操作来动态增加容量或调整性能。
- 备份和恢复 – 使用 Amazon EBS 快照来备份存储在卷上的数据。然后，您可以使用这些快照立即还原卷或跨 AWS 账户、AWS 区域或可用区迁移数据。
- 数据保护 – 使用 Amazon EBS 加密来加密 Amazon EBS 卷和 Amazon EBS 快照。加密操作在托管 Amazon EC2 实例的服务器上进行，用于确保静态数据的安全性，以及在实例和其挂载的卷与后续快照之间的传输中数据的安全性。
- 数据可用性和持久性 – io2 Block Express 卷持久性为 99.999%，年故障率为 0.001%。其他卷类型持久性为 99.8% 到 99.9%，年故障率为 0.1% 到 0.2%。另外，卷的数据可在可用区内多个服务器间进行自动复制，以防任何单个组件故障导致数据丢失。

- 数据存档 – EBS 快照归档提供了低成本的存储层，用于存档 EBS 快照的完整时间点副本，留存出于监管和合规原因或为了发布未来版本必须保留 90 天或更长时间的 EBS 快照。

## 相关服务

Amazon EBS 适用于以下服务：

- Amazon Elastic Compute Cloud – 此为允许您在 AWS Cloud 中启动和管理虚拟机 ( Amazon EC2 实例 ) 的服务。您可以将 EBS 卷挂载到这些实例，并像使用本地硬盘一样使用 EBS 卷，例如用于存储文件或安装应用程序。有关更多信息，请参阅[什么是 Amazon EC2 ?](#)
- AWS Key Management Service – 此为允许您创建和管理加密密钥的托管服务。您可以使用 AWS KMS 加密密钥，对存储在 Amazon EBS 卷和 Amazon EBS 快照中的数据进行加密。有关更多信息，请参阅[Amazon EBS 如何使用 AWS KMS](#)。
- Amazon Data Lifecycle Manager – 此为自动创建、保留和删除 EBS 快照及 EBS 支持的 AMI 的托管服务。您可以使用 Amazon Data Lifecycle Manager 自动备份 Amazon EBS 卷和 Amazon EC2 实例。有关更多信息，请参阅[Amazon Data Lifecycle Manager](#)。
- EBS 直接 API – 此为允许您创建 EBS 快照、将数据直接写入快照、读取快照上的数据，以及标识两个快照之间的差异或变化的服务。有关更多信息，请参阅[使用 EBS direct API 访问 EBS 快照的内容](#)。
- 回收站 – 此为数据恢复服务，支持您还原意外删除的 EBS 快照和 EBS 支持的 AMI。有关更多信息，请参阅[回收站](#)。

## 访问 Amazon EBS

您可以使用以下界面创建和管理 Amazon EBS 资源：

### Amazon EC2 控制台

此为用于创建和管理卷与快照的 Web 界面。如果已注册 AWS 账户，可以通过 <https://console.aws.amazon.com/ec2/> 访问 Amazon EC2 控制台。

### AWS Command Line Interface

此为命令行工具，允许您在命令行 Shell 中使用命令管理 Amazon EBS 资源。它在 Windows、Mac 和 Linux 上受支持。有关更多信息，请参阅 [AWS Command Line Interface 用户指南](#)和 [AWS CLI 命令参考](#)。

## AWS Tools for PowerShell

此为一组 PowerShell 模块，允许您从 PowerShell 命令行针对 Amazon EBS 资源的操作编写脚本。有关更多信息，请参阅 [AWS Tools for Windows PowerShell 用户指南](#) 和 [AWS Tools for PowerShell Cmdlet 参考](#)。

## AWS CloudFormation

此为完全托管式 AWS 服务，允许创建用于描述 AWS 资源的可重用 JSON 或 YAML 模板，然后预调配和配置这些资源。有关更多信息，请参阅 [AWS CloudFormation 用户指南](#)。

## Amazon EC2 查询 API

Amazon EC2 查询 API 提供使用 HTTP 动词 GET 或 POST 以及一个名为 Action 的查询参数的 HTTP 或 HTTPS 请求。有关更多信息，请参阅 [Amazon EC2 API Reference](#)。

## AWS SDK

特定语言的 API 支持您构建与 AWS 服务集成的应用程序。AWS 软件开发工具包适用于许多常用编程语言。有关更多信息，请参阅 [用于在 AWS 上进行构建的工具](#)。

# 定价

使用 Amazon EBS，您可以按实际预置量付费。有关更多信息，请参阅 [Amazon EBS 定价](#)。

# 为 Amazon EBS 进行设置

完成本部分中的任务，为使用 Amazon EBS 资源做好准备。

## 任务

- [注册获取 AWS 账户](#)
- [创建具有管理访问权限的用户](#)
- [\( 可选 \) 创建和使用用于 Amazon EBS 加密的客户托管密钥](#)
- [\( 可选 \) 启用阻止公开访问 Amazon EBS 快照](#)

## 注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

### 要注册 AWS 账户

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

在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建 AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 <https://aws.amazon.com/> 并选择我的账户来查看当前的账户活动并管理您的账户。

## 创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以不会使用 root 用户执行日常任务。

### 保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS Management Console](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的[以根用户身份登录](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台\)](#)。

### 创建具有管理访问权限的用户

1. 启用 IAM Identity Center

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

### 以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

### 将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[创建权限集](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[添加组](#)。

## ( 可选 ) 创建和使用用于 Amazon EBS 加密的客户托管密钥

Amazon EBS 加密是一种加密解决方案，它使用 AWS KMS 加密密钥来加密您的亚马逊 EBS 卷和亚马逊 EBS 快照。Amazon EBS 会自动为每个地区的亚马逊 EBS 加密创建唯一的 AWS 托管 KMS 密

钥。此 KMS 密钥具有 `aws/ebs` 别名。您无法轮换默认 KMS 密钥或管理其权限。为了提高灵活性和更好地控制用于 Amazon EBS 加密的 KMS 密钥，您可考虑创建和使用客户托管密钥。

创建和使用用于 Amazon EBS 加密的客户托管密钥

1. [创建对称加密 KMS 密钥。](#)
2. [选择将 KMS 密钥作为用于 Amazon EBS 加密的默认 KMS 密钥。](#)
3. [授予用户使用用于 Amazon EBS 加密的 KMS 密钥的权限。](#)

## ( 可选 ) 启用阻止公开访问 Amazon EBS 快照

要防止公开共享您的快照，您可以启用阻止公开访问快照。在为一个区域阻止公开访问快照之后，将自动阻止任何尝试在此区域公开共享快照的行为。这样可以帮您提高快照的安全性，并保护您的快照数据免遭未经授权的访问或意外访问。

有关更多信息，请参阅 [阻止公开访问快照](#)。

### Console

启用阻止公开访问快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 EC2 控制面板，然后在 ( 右侧的 ) 账户属性中，选择数据保护和安全。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 选择阻止公开访问，然后选择以下选项之一：
  - 阻止所有公开访问 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
  - 阻止新的公开共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。
5. 选择更新。

### AWS CLI

启用阻止公开访问快照

使用 [enable-snapshot-block-public-access](#) 命令。对于 `--state`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing/block-new-sharing
```



# Amazon EBS 卷

Amazon EBS 卷是一种耐用的数据块级存储设备，您可以将其附加到您的实例。将卷附加到实例后，您可以像使用其他物理硬盘一样使用它。EBS 卷非常灵活。对于附加到当前一代实例类型的当前一代卷，您可以动态增加大小、修改预配置 IOPS 容量以及更改实际生产卷上的卷类型。

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）。还可以将其用于执行连续磁盘扫描的吞吐量密集型应用程序。EBS 卷始终不受 EC2 实例运行时间的影响。

您可以将多个 EBS 卷附加到单个实例。该卷与实例必须位于同一可用区。根据卷和实例类型，您可以使用[多重挂载](#)将卷同时挂载到多个实例。

Amazon EBS 提供以下卷类型：通用型 SSD（gp2 和 gp3）、预调配 IOPS SSD（io1 和 io2）、吞吐量优化型 HDD（st1）、Cold HDD（sc1）以及磁介质卷（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](#)。

您的账户对可用的总存储空间有限制。有关这些限制以及如何请求提高限制的更多信息，请参阅[Amazon EBS 端点和限额](#)。

有关定价的更多信息，请参阅[Amazon EBS 定价](#)。

## 目录

- [使用 EBS 卷的优势](#)
- [Amazon EBS 卷类型](#)
- [针对 EBS 卷的大小和配置的限制](#)
- [Amazon EBS 和 NVMe](#)
- [Amazon EBS 卷的生命周期](#)
- [使用以前的快照替换 Amazon EBS 卷](#)
- [监控 Amazon EBS 卷](#)
- [在 Amazon EBS 上进行故障测试](#)

## 使用 EBS 卷的优势

EBS 卷具有实例存储卷不具备的优势。

## 优势

- [数据可用性](#)
- [数据持久性](#)
- [数据加密](#)
- [数据安全性](#)
- [快照](#)
- [弹性](#)

## 数据可用性

当您创建 EBS 卷时，系统会在其可用区内自动复制该卷，以防止因任何一个硬件组件出现故障而导致数据丢失。您可以将 EBS 卷附加到同一可用区中的任何 EC2 实例。附加后，该卷显示为类似于硬盘或其他物理设备的本机块储存设备。这时，实例就像与本地驱动器交互一样与该卷交互。您可以连接到实例并使用文件系统 [例如 Ext4 (Linux 实例) 或 NTFS (Windows 实例)] 格式化 EBS 卷，然后安装应用程序。

如果您将多个卷附加到您指定的一个设备，则可以在卷内将数据条带化，以增强 I/O 性能和吞吐量。

您可以将 io1 和 io2 EBS 卷挂载到最多 16 个基于 Nitro 的实例。有关更多信息，请参阅 [使用 Amazon EBS 多重挂载将卷挂载到多个实例](#)。或者，也可以将 EBS 卷附加到单个实例。

您可以获取针对 EBS 卷 (包括 EBS 支持的实例的根设备卷) 的监控数据，而无需额外付费。有关监控指标的更多信息，请参阅 [亚马逊 EBS 的亚马逊 CloudWatch 指标](#)。有关跟踪卷状态的信息，请参阅 [Amazon f EventBridge or Amazon EBS](#)。

## 数据持久性

EBS 卷是一种实例外存储，其数据的保存期限不受实例使用寿命的影响。只要数据存在，您就要继续支付卷的使用费用。

如果您在 EC2 控制台中为您的实例配置 EBS 卷时取消选中了终止时删除复选框，则在运行的实例终止时，附加到该实例的 EBS 卷会自动从该实例分离，并保持数据完整。然后，可将卷重新附加到新的实例，从而快速恢复数据。如果选中终止时删除复选框，则在 EC2 实例终止时删除卷。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其附加的卷中存储的数据。在从停止到启动的整个周期中，该卷均为已附加状态。这使您能够无限期地在卷上处理和存储数据，并只在需要时使用处理和存储资源。数据将一直保存在该卷上，直至将其显式删除。删除的 EBS 卷所使用的物理块存储在分配给新卷之前，会被零或加密的伪随机数据覆盖。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与 Amazon EBS 加密保护的卷上。有关更多信息，请参阅 [Amazon EBS 加密](#)。

默认情况下，当一个实例终止时，将删除在启动时创建并附加到该实例的根 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `false`。修改值后，即使实例终止，也可将该卷保留下来并附加到其他实例。

默认情况下，当一个实例终止时，不会删除在启动时创建并附加到该实例的额外 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `true`。此修改的值会导致在实例终止时删除卷。

## 数据加密

为简化数据加密，您可以使用 Amazon EBS 加密功能创建加密 EBS 卷。所有 EBS 卷类型都支持加密。您可以使用加密的 EBS 卷来满足监管/审计的数据和应用程序的各种 data-at-rest 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。加密发生在托管 EC2 实例的服务器上，从而提供 data-in-transit 从 EC2 实例到 Amazon EBS 存储的加密。有关更多信息，请参阅 [Amazon EBS 加密](#)。

Amazon EBS 加密 AWS KMS keys 在创建加密卷以及从您的加密卷创建的任何快照时使用。首次在该区域中创建加密 EBS 卷时，系统会自动为您创建默认的 AWS 托管 KMS 密钥。此密钥用于 Amazon EBS 加密，除非您创建和使用客户自主管理型密钥。创建您自己的客户自主管理型密钥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等功能。有关更多信息，请参见 [AWS Key Management Service 开发人员指南](#)。

## 数据安全性

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说​​明的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

## 快照

Amazon EBS 提供为任何 EBS 卷创建快照（备份）并将卷中数据的副本写入 Amazon S3（其中数据以冗余方式存储在多个可用区中）的功能。不必将该卷附加到运行中的实例，也可以制作快照。因为您不断向卷写入数据，则可定期创建该卷的快照，以用作创建新卷的基准。也可利用这些快照创建多个新的 EBS 卷或在可用区间移动卷的位置。加密 EBS 卷的快照会自动加密。

从快照创建新卷时，新卷是制作快照时的原始卷的精确副本。通过加密快照创建的 EBS 卷会自动加密。通过指定不同的可用区（可选），您可以使用此功能在该区域中创建重复的卷。快照可以与特定 AWS 账户共享或公开。创建快照时，会根据备份数据的大小（而不是源卷的大小）收取 Amazon S3 费用。同一卷的后续快照为增量快照。这些快照仅包含自上次创建快照以来写入卷的已更改数据和新数据，您只需为这些已更改数据和新数据付费。

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，但快照删除过程仅要求保留最新的快照。

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。

要自动备份卷，您可以使用 [Amazon Data Lifecycle Manager](#) 或 [AWS Backup](#)。

## 弹性

EBS 卷支持生产期间的实时配置更改。您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。有关更多信息，请参阅 [使用 Amazon EBS 弹性卷修改卷](#)。

## Amazon EBS 卷类型

Amazon EBS 提供以下卷类型，各种类型性能特点和价格不同，因此您可根据应用程序要求定制您所需的存储性能和相应成本。

### Important

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。为了充分利用 EBS 卷上预调配的 IOPS，请使用 EBS 优化实例。有关充分利用 EBS 卷的更多信息，请参阅 [Amazon EBS 卷性能](#)。

有关定价的更多信息，请参阅 [Amazon EBS 定价](#)。

### 卷类型

- [固态硬盘 \(SSD\) 卷](#)
- [硬盘驱动器 \(HDD\) 卷](#)
- [上一代卷](#)

## 固态硬盘 ( SSD ) 卷

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。由 SSD 支持的卷类型包括通用型 SSD 和预调配 IOPS SSD。下面是 SSD 支持的卷的使用案例和特征摘要。

	通用型 SSD 卷		预置 IOPS SSD 卷	
卷类型	gp3	gp2	io2 Block Express <sup>3</sup>	io1
持久性	99.8% - 99.9% 耐用性 ( 0.1% - 0.2% 的年故障率 )		99.999% 的耐用性 ( 0.001% 的年故障率 )	99.8% - 99.9% 耐用性 ( 0.1% - 0.2% 的年故障率 )
使用案例	<ul style="list-style-type: none"> <li>事务性工作负载</li> <li>虚拟桌面</li> <li>中型单实例数据库</li> <li>低延迟交互式应用程序</li> <li>引导卷</li> <li>开发和测试环境</li> </ul>		需要以下工作负载： <ul style="list-style-type: none"> <li>亚毫秒级延迟</li> <li>持续 IOPS 绩效</li> <li>超过 64,000 IOPS 或 1,000 MiB/s 吞吐量</li> </ul>	<ul style="list-style-type: none"> <li>需要持续 IOPS 性能或超过 16,000 IOPS 性能的工作负载</li> <li>I/O 密集型数据库工作负载</li> </ul>
卷大小	1 GiB - 16 TiB		4GiB - 64TiB <sup>4</sup>	4 GiB - 16 TiB
每个卷的最大 IOPS	16,000 (64 KiB I/O)	16,000 (16 KiB I/O)	256,000 (16 KiB I/O) <sup>5</sup>	64,000 (16 KiB I/O)
每个卷的最大吞吐量	1,000 MiB/s	250MiB/s <sup>1</sup>	4,000 MiB/s	1000MiB/s <sup>2</sup>
Amazon EBS 多重挂载	不支持		支持	

	<a href="#">通用型 SSD 卷</a>	<a href="#">预置 IOPS SSD 卷</a>	
NVMe 预留	不支持	支持	不支持
引导卷	支持		

<sup>1</sup> 吞吐量限制介于 128MiB/s 到 250MiB/s 不等，具体情况取决于卷大小。有关更多信息，请参阅 [gp2 卷性能](#)。除非您[修改卷](#)，否则在 2018 年 12 月 3 日之前创建并且自创建以来未经修改的卷可能无法实现完全性能。

<sup>2</sup> 要实现 1000 MiB/s 的最大吞吐量，必须为卷预调配 64000 IOPS，而且必须将卷挂载到[基于 Nitro 系统构建的实例](#)。除非[修改卷](#)，否则在 2017 年 12 月 6 日之前创建且自创建以来未经修改的卷可能无法实现完全性能。

<sup>3</sup> 在 2023 年 11 月 21 日之后创建的所有 io2 卷都是 io2 Block Express 卷。通过[修改卷的 IOPS 或大小](#)，可以将 2023 年 11 月 21 日之前创建的 io2 卷转换为 io2 Block Express 卷。

<sup>4</sup> 大小超过 16 TiB 的卷只能连接到基于 [Nitro 系统构建的实例](#)。

<sup>5</sup> 超过 64,000 IOPS 的卷只能连接到基于 [Nitro 系统构建的实例](#)。最多 64,000 IOPS 的卷可以连接到非 Nitro 实例，但它们最多只能实现 32,000 IOPS。

有关 SSD 支持的卷类型的更多信息，请参阅以下文件：

- [通用型 SSD 卷](#)
- [预置 IOPS SSD 卷](#)

## 硬盘驱动器 (HDD) 卷

HDD 支持的卷针对大型流式处理工作负载进行了优化，其中主要的性能属性是吞吐量。HDD 容量类型包括吞吐量优化型 HDD 和冷 HDD。下面是 HDD 支持的卷的使用案例和特征摘要。

	<a href="#">吞吐量优化型 HDD 卷</a>	<a href="#">Cold HDD 卷</a>
卷类型	st1	sc1
持久性	99.8% - 99.9% 耐用性 ( 0.1% - 0.2% 的年故障率 )	

	<a href="#">吞吐量优化型 HDD 卷</a>	<a href="#">Cold HDD 卷</a>
使用案例	<ul style="list-style-type: none"> <li>• 大数据</li> <li>• 数据仓库</li> <li>• 日志处理</li> </ul>	<ul style="list-style-type: none"> <li>• 适用于访问频率较低的数据的高吞吐量存储</li> <li>• 最低存储成本至关重要的情形</li> </ul>
卷大小	125 GiB - 16 TiB	
每个卷的最大 IOPS ( 1 MiB I/O )	500	250
每个卷的最大吞吐量	500 MiB/s	250 MiB/s
Amazon EBS 多重挂载	不支持	
引导卷	不支持	

有关硬盘驱动器 ( HDD ) 卷的更多信息，请参阅 [吞吐量优化型 HDD 和 Cold HDD 卷](#)。

## 上一代卷

磁性 ( standard ) 卷是采用磁性驱动器的上一代卷。它们适用于具有较小数据集的工作负载，在这些工作负载中，数据访问不频繁，性能不是最重要的。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。

### Tip

磁介质卷是上一代卷类型。如果您需要比上一代卷更高的性能或性能一致性，建议您考虑使用一种更新的卷类型。

下表列出了上一代 EBS 卷类型。

	磁介质
卷类型	standard
使用案例	数据不常访问的工作负载
卷大小	1 GiB - 1 TiB
每个卷的最大 IOPS	40–200
每个卷的最大吞吐量	40–90 MiB/s
引导卷	支持

有关更多信息，请参阅[上一代卷](#)。

## 通用型 SSD 卷

固态硬盘 (SSD) 支持通用型 SSD (gp2 和 gp3) 卷。通用型 SSD 卷在各种事务性工作负载的价格和性能之间实现平衡。其中包括虚拟桌面、中型单实例数据库、延迟敏感型交互式应用程序、开发和测试环境以及启动卷。建议为大多数工作负载使用这种卷。

Amazon EBS 提供以下类型的通用型 SSD 卷：

### 类型

- [通用型 SSD \(gp3\) 卷](#)
- [通用型 SSD \(gp2\) 卷](#)

## 通用型 SSD (gp3) 卷

通用型 SSD (gp3) 卷是最新一代通用型 SSD 卷，也是 Amazon EBS 提供的成本最低的 SSD 卷。这种卷类型有助于为大多数应用程序提供合理得当的价格和性能。其还可以帮助您独立于卷大小扩展卷的性能。这意味着您可以预置所需性能，而无需预置额外的块存储容量。此外，gp3 卷每 GiB 价格比通用型 SSD (gp2) 卷低了 20%。

gp3 卷提供个位数的毫秒延迟和 99.8% 至 99.9% 的卷持久性，年故障率 (AFR) 不高于 0.2%，这意味着在一年内每 1,000 个运行卷中最多有两次卷故障。AWS 设计 gp3 卷以在 99% 的时间内提供其预配置的性能。



## 内容

- [gp3 卷性能](#)
- [gp3 卷大小](#)
- [从 gp2 迁移到 gp3](#)

## gp3 卷性能

### Tip

gp3 卷不使用突增性能。其可以无限期地维持其完全预调配 IOPS 和吞吐量性能。

## IOPS 性能

gp3 卷提供 3000 IOPS 的一致基准 IOPS 性能，这包含在存储价格中。您可以按每 GiB 卷大小 500 IOPS 的比例预置额外的 IOPS（最大 16000 IOPS），但需支付额外费用。可为 32 GiB 或更大的卷预置最大 IOPS（每 GiB 500 IOPS × 32 GiB = 16000 IOPS）。

## 吞吐量性能

gp3 卷提供 125 MiB/s 的一致基准吞吐量性能，这包含在存储价格中。您可以按每个预调配 IOPS 0.25 MiB/s 的比例预置额外的吞吐量（最高 1000 MiB/s），但需支付额外费用。最大吞吐量可预置为 4000 IOPS 或更高以及 8 GiB 或更大（4000 IOPS × 每 IOPS 0.25 MiB/s = 1000 MiB/s）。

## gp3 卷大小

gp3 卷的大小范围为 1 GiB 到 16 TiB。

## 从 gp2 迁移到 gp3

如果您当前正在使用 gp2 卷，则可以使用 [使用 Amazon EBS 弹性卷修改卷](#) 操作将卷迁移到 gp3。您可以使用 Amazon EBS 弹性卷操作修改现有卷的卷类型、IOPS 和吞吐量，而不中断 Amazon EC2 实例。当使用控制台创建卷或从快照中创建 AMI 时，卷类型的默认选择是“通用型 SSD gp3”。在其他情况下，默认选择是 gp2。在这些情况下，可以选择 gp3 作为卷类型而不是使用 gp2。

若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 [Amazon EBS gp2 至 gp3 迁移成本节省计算器](#)。

## 通用型 SSD ( gp2 ) 卷

这种卷类型可提供经济实惠的存储，是广泛事务性工作负载的理想选择。使用 gp2 卷，性能随卷大小而扩展。

### Tip

gp3 卷是最新一代通用型 SSD 卷。其提供更加可预测的性能扩展，而且价格比 gp2 卷低 20%。有关更多信息，请参阅 [通用型 SSD \( gp3 \) 卷](#)。

若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 [Amazon EBS gp2 至 gp3 迁移成本节省计算器](#)。

gp2 卷提供个位数的毫秒延迟和 99.8% 至 99.9% 的卷持久性，年故障率 (AFR) 不高于 0.2%，也就是说，在一年内每 1,000 个运行卷中最多有两次卷故障。AWS 设计 gp2 卷以在 99% 的时间内提供其预配置的性能。

### 内容

- [gp2 卷性能](#)
- [gp2 卷大小](#)

## gp2 卷性能

### IOPS 性能

基准 IOPS 性能以每 GiB 卷大小 3 IOPS 的速度，在最小 100 IOPS 和最大 16000 IOPS 之间进行线性扩缩。IOPS 性能预置如下：

- 33.33 GiB 及更小的卷预置至少 100 IOPS。
- 大于 33.33 GiB 的卷预置每 GiB 卷大小 3 IOPS，最高可达 16000 IOPS，达到 5334 GiB ( 3 X 5334 )。
- 5334 GiB 及更大的卷预置 16000 IOPS。

小于 1 TiB 的 gp2 卷 ( 且预置的 IOPS 低于 3000 ) 可在需要较长时间时突增至 3000 IOPS。卷的突增能力受 I/O 积分的控制。I/O 需求大于基准性能时，卷花费 I/O 积分以突增至所需的性能级别 ( 最多 3000 IOPS )。突增时，I/O 积分不会累积，而是按照高于基准 IOPS 的 IOPS 速率进行消费 ( 费用率

= 突增 IOPS - 基准 IOPS )。卷累积的 I/O 积分越多，其维持突增性能的时间就越长。您可以按如下方式计算突增持续时间：

$$\text{Burst duration} = \frac{(\text{I/O credit balance})}{(\text{Burst IOPS}) - (\text{Baseline IOPS})}$$

I/O 需求降至基准性能水平或更低时，卷开始以每 GiB 卷大小每秒 3 个 I/O 积分的速率获得 I/O 积分。每个卷都有 540 万 I/O 积分的 I/O 积分累积限制，这足以在至少 30 分钟内维持 3000 IOPS 的最大突增性能。

#### Note

每个卷都有 540 万 I/O 积分的初始 I/O 积分余额，这为启动卷提供了快速初始启动循环，并为其他应用程序提供良好的引导过程。

下表列出了示例卷大小和卷的相关基准性能、突增持续时间（从 540 万 I/O 积分开始时）以及重填空 I/O 积分余额所需的时间。

卷大小 (GiB)	基准性能 (IOPS)	3000 IOPS 时的最大突增持续时间 (秒)	重填空 I/O 积分余额所需的时间 (秒)
1 至 33.33	100	1862	54000
100	300	2000	18000
334 (最大吞吐量的最小大小)	1,002	2,703	5,389
750	2250	7200	2400
1000	3000	不适用*	不适用*
5334 (最大 IOPS 的最小大小) 及更大	16000	不适用*	不适用*

\*卷的基准性能超过了最大突发性能。

您可以使用亚马逊中的 Amazon EBS BurstBalance 指标监控卷的 I/O 积分余额。CloudWatch 此指标显示 gp2 剩余的 I/O 积分百分比。有关更多信息，请参阅 [Amazon EBS I/O 特性和监控](#)。您可以设置警报，以便在 BurstBalance 值降到特定水平时获取通知。有关更多信息，请参阅 [创建 CloudWatch 警报](#)。

## 吞吐量性能

gp2 提供介于 128 MiB/s 和 250 MiB/s 之间的吞吐量，具体取决于卷大小。吞吐量性能预置如下：

- 170 GiB 或更小的卷提供最大 128 MiB/s 的吞吐量。
- 大于 170 GiB 但小于 334 GiB 的卷可以突增至 250 MiB/s 的最大吞吐量。
- 334 GiB 及更大的卷提供 250 MiB/s 的吞吐量。

gp2 卷的吞吐量可以使用以下公式计算，吞吐量上限为 250 MiB/s：

$$\text{Throughput in MiB/s} = \text{IOPS performance} \times \text{I/O size in KiB} / 1,024$$

## gp2 卷大小

gp2 卷的大小范围为 1 GiB 到 16 TiB。请记住，卷性能随卷大小呈线性扩缩。

## 预置 IOPS SSD 卷

固态硬盘 (SSD) 支持预调配 IOPS SSD 卷。这种卷是性能最高的 Amazon EBS 存储卷，专为需要低延迟的 IOPS 密集型和吞吐量密集型关键工作负载而设计。预调配 IOPS SSD 卷在 99.9% 的时间里可提供预置 IOPS 性能。

Amazon EBS 提供了两种类型的预调配 IOPS SSD 卷：

- [预调配 IOPS SSD \(io2\) Block Express 卷](#)
- [预调配 IOPS SSD \(io1\) 卷](#)

## 预调配 IOPS SSD (io2) Block Express 卷

io2 Block Express 卷基于下一代 Amazon EBS 存储服务器架构而构建。它旨在满足[基于 Nitro 系统构建的实例](#)上运行的最苛刻 I/O 密集型应用程序的性能要求。Block Express 具有最高耐用性和最低延迟，非常适合运行性能密集、任务关键型工作负载，例如 Oracle、SAP HANA、Microsoft SQL Server 和 SAS Analytics。

Block Express 架构提高了 io2 卷的性能和规模。Block Express 服务器利用可扩展的可靠数据报 (SRD) 网络协议与[基于 Nitro 系统构建的实例](#)通信。此接口在专用于实例主机硬件上 Amazon EBS I/O 功能的 Nitro Card 中实现。它最大限度地减少 I/O 延迟和延迟变化 (网络抖动)，从而为应用程序提供更快、更一致的性能。

io2 Block Express 卷可提供 99.999% 的卷耐用性，年故障率 (AFR) 不超过 0.001%，这意味着在一年时间内，每 10 万个正在运行的卷最多发生一次卷故障。io2 Block Express 卷非常适合可以从达到亚毫秒级延迟的单个卷受益的工作负载，并支持比 gp3 卷更多的 IOPS、更高的吞吐量和更大的容量。

预调配 IOPS SSD (io2) Block Express 卷在 99.9% 的时间里可提供预调配的 IOPS 性能。

所有[基于 Nitro 系统构建的实例](#)都支持 io2 Block Express 卷。有关更多信息，请参阅 [io2 Block Express 卷](#)。

## 主题

- [注意事项](#)
- [Performance](#)

## 注意事项

- io2 Block Express 卷已在以下区域提供：美国东部 (俄亥俄州) | 美国东部 (弗吉尼亚州北部) | 美国西部 (北加利福尼亚) | 美国西部 (俄勒冈州) | 亚太地区 (香港) | 亚太地区 (孟买) | 亚太地区 (首尔) | 亚太地区 (新加坡) | 亚太地区 (悉尼) | 亚太地区 (东京) | 加拿大 (中部) | 欧洲地区 (法兰克福) | 欧洲地区 (爱尔兰) | 欧洲地区 (伦敦) | 欧洲地区 (斯德哥尔摩) | 中东 (巴林)。
- 在 2023 年 11 月 21 日之后创建的所有 io2 卷都是 io2 Block Express 卷。通过[修改卷的 IOPS 或大小](#)，可以将 2023 年 11 月 21 日之前创建的 io2 卷转换为 io2 Block Express 卷。
- 可以将[基于 Nitro 系统构建的实例](#)挂载到最大 64 TiB 的卷。其他实例类型可以挂载到最大 16 TiB 的卷。
- 可以将[基于 Nitro 系统构建的实例](#)挂载到预调配了最多 256000 IOPS 的卷。其他实例类型可以挂载到预置了最多 64000 IOPS 的卷，但可以实现最多 32000 IOPS。
- 要从未加密的快照或共享的加密快照创建一个大小大于 16 TiB 或 IOPS 大于 64000 的加密 io2 卷，您必须：
  1. 在您的账户中，创建此快照的加密副本
  2. 使用此快照副本创建卷

## Performance

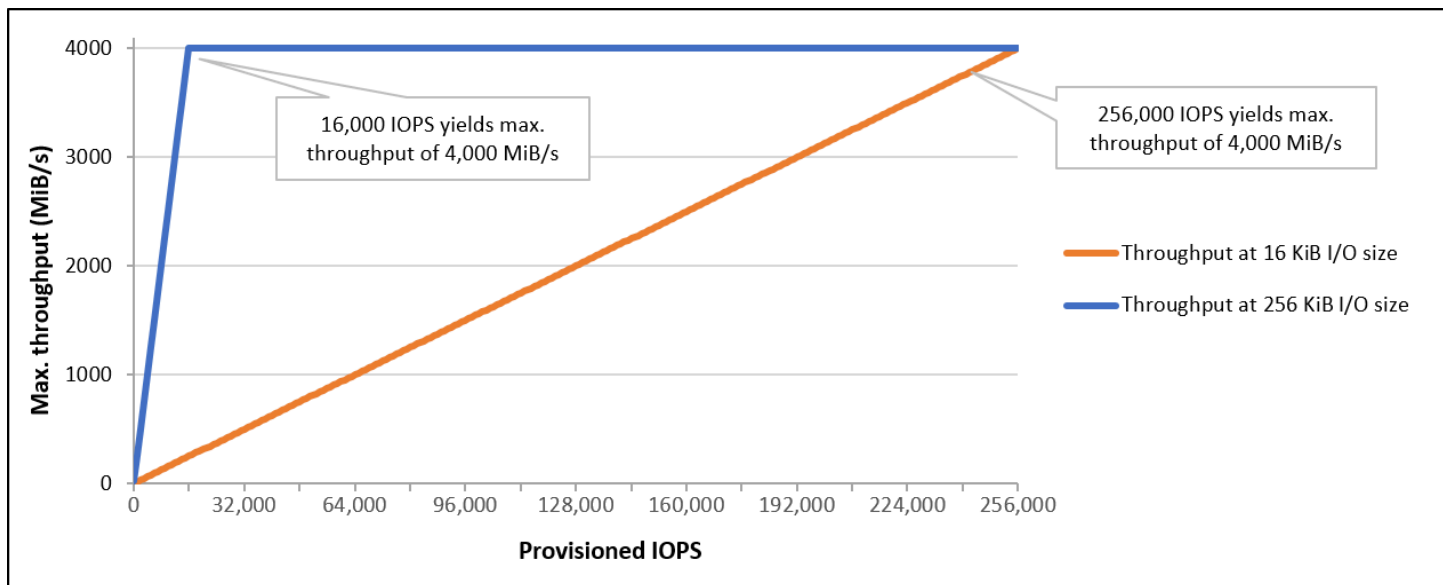
借助 io2 Block Express 卷，您可以通过以下方式预置卷：

- 亚毫秒级平均延迟
- 存储容量高达 64TiB ( 65536GiB )
- 预置 IOPS 高达 256,000，IOPS:GiB 比率为 1,000:1。可以为 256GiB 和更大的卷预置最多 IOPS (  $1000\text{IOPS} \times 256\text{GiB} = 256000\text{IOPS}$  )。

### Note

使用[基于 Nitro 系统构建的实例](#)，可以实现最多 256000 IOPS。在其他实例中，可以实现最高 32000IOPS 的性能。

- 卷吞吐量高达 4,000 MiB/s。吞吐量按比例扩展至每个预置 IOPS 0.256 Mib/s。最大吞吐量可在 16,000 IOPS 或更高的情况下实现。



## 预调配 IOPS SSD ( io1 ) 卷

预调配 IOPS SSD ( io1 ) 卷旨在满足 I/O 密集型工作负载（尤其是数据库工作负载）的需求，这些工作负载对存储性能和一致性非常敏感。预置 IOPS SSD 卷使用一致的 IOPS 速率（在创建卷时指定），而 Amazon EBS 在 99.9% 的时间里可提供预置性能。

io1 卷可提供 99.8% 到 99.9% 的卷耐用性，年故障率 ( AFR ) 不超过 0.2%，这意味着在一年时间内，每 1000 个正在运行的卷最多发生两次卷故障。

io1 卷可用于所有 Amazon EC2 实例类型。

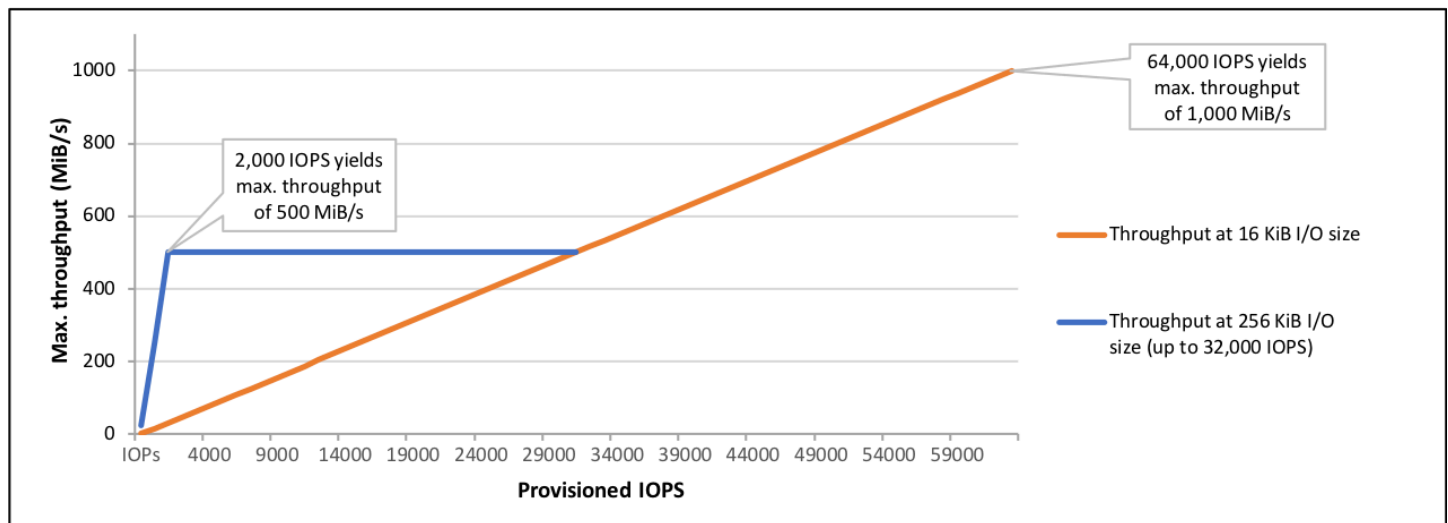
## Performance

io1 卷的大小介于 4GiB 到 16TiB 不等，可以为每个卷预置 100IOPS 到最多 64000IOPS。预调配 IOPS 与请求的卷大小（以 GiB 为单位）的最大比率为 50:1。例如，可以为一个 100GiB io1 卷预置最多 5000IOPS。

可以为 1280GiB 或更大的卷预置最多的 IOPS（ $50 \times 1280\text{GiB} = 64000\text{IOPS}$ ）。

- 预置了最高 32000 IOPS 的 io1 卷支持 256 KiB 的最大 I/O 大小，可以达到最高 500 MiB/s 的吞吐量。当 I/O 大小达到最大时，吞吐量也将达到峰值 2000 IOPS。
- 预调配超过 32000IOPS（最高可达 64000IOPS）的 io1 卷以每个预调配 IOPS 16KiB 的速率线性增大吞吐量。例如，预置了 48,000 IOPS 的卷可以支持高达 750 MiB/s 的吞吐量（每个预置 IOPS 16 KiB x 48,000 个预置 IOPS = 750 Mib/s）。
- 要实现 1,000 MiB/s 的最大吞吐量，必须为卷预置 64,000 IOPS（每个预置 IOPS 16 KiB x 64,000 个预置 IOPS = 1,000 Mib/s）。
- 只有在[基于 Nitro 系统构建的实例](#)上，才能实现最多 64000 IOPS。在其他实例中，可以实现最高 32000IOPS 的性能。

下图说明了这些性能特性：



您的每 I/O 延迟体验取决于预置 IOPS 以及您的工作负载模式。要获得最佳 I/O 延迟体验，请确保您预配置 IOPS 以满足工作负载的 I/O 配置文件。

## 吞吐量优化型 HDD 和 Cold HDD 卷

Amazon EBS 提供的 HDD 卷分为以下几个类别：

- 吞吐量优化型 HDD – 适用于访问频率较高的吞吐量密集型工作负载的低成本 HDD。
- Cold HDD – 适用于访问频率较低的工作负载的最低成本 HDD。

### 主题

- [每实例吞吐量限制](#)
- [吞吐量优化型 HDD 卷](#)
- [Cold HDD 卷](#)
- [使用 HDD 卷时的性能注意事项](#)
- [监控卷的突发存储桶余额](#)

### 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 优化型 EC2 实例来避免网络瓶颈。

### 吞吐量优化型 HDD 卷

吞吐量优化型 HDD ( st1 ) 卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。该卷类型是大型顺序工作负载（例如 Amazon EMR、ETL、数据仓库和日志处理）的理想之选。不支持可启动的 st1 卷。

吞吐量优化型 HDD ( st1 ) 卷虽然与 Cold HDD ( sc1 ) 卷类似，但其旨在支持频繁访问的数据。

该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅 [HDD 上的小型读/写效率低下问题](#)。

附加到 EBS 优化型实例的吞吐量优化型 HDD ( st1 ) 卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

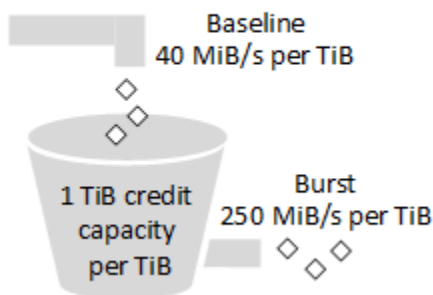


## 吞吐量积分和突增性能

与 gp2 类似，st1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。

下图显示 st1 的突增存储桶行为。

### ST1 burst bucket



st1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

对于 1 TiB st1 卷，突增吞吐量限制为 250 MiB/s，存储桶以 40 MiB/s 的速度填充，最多可容纳 1 TiB 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 500 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 40 MiB/s。

在从 0.125 TiB 到 16 TiB 的卷大小范围内，基准吞吐量从 5 MiB/s 到上限 500 MiB/s 变化，12.5 TiB 时达到上限，如下所示：

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

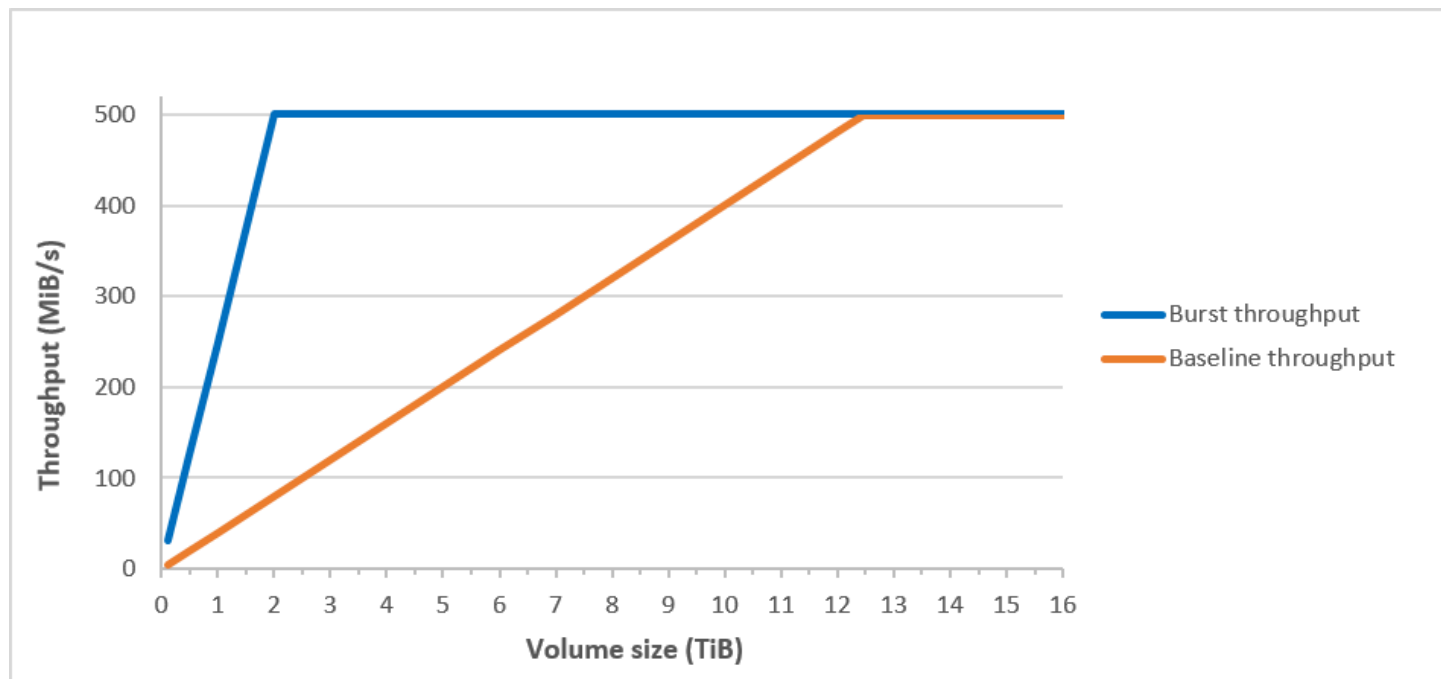
突增吞吐量从 31 MiB/s 到上限 500 MiB/s 变化，2 TiB 时达到上限，如下所示：

$$2 \text{ TiB} \times \frac{250 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

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 )
0.125	5	31
0.5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12.5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

下图绘制了表值：



#### Note

如果创建吞吐量优化型 HDD ( st1 ) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报监控突发存储桶余额的信息，请参阅[监控卷的突发存储桶余额](#)。

## Cold HDD 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。st1 的吞吐量限制比 sc1 更低，是大型顺序冷数据工作负载的绝佳选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的块存储。不支持可启动的 sc1 卷。

Cold HDD ( sc1 ) 卷虽然与吞吐量优化型 HDD ( st1 ) 卷类似，但其旨在支持不频繁访问的数据。

#### Note

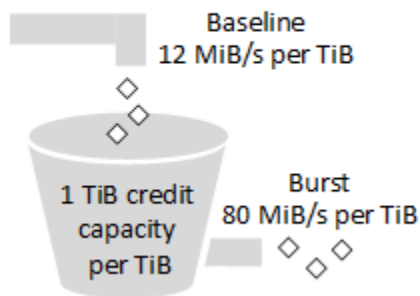
该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅[HDD 上的小型读/写效率低下问题](#)。

附加到 EBS 优化型实例的 Cold HDD ( `sc1` ) 卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

## 吞吐量积分和突增性能

与 `gp2` 类似，`sc1` 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。

### SC1 burst bucket



`sc1` 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

对于 1 TiB `sc1` 卷，突增吞吐量限制为 80 MiB/s，存储桶以 12 MiB/s 的速度填充，最多可容纳 1 TiB 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 250 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 12 MiB/s。

在从 0.125 TiB 到 16 TiB 的卷大小范围内，基准吞吐量从 1.5 MiB/s 到最大 192 MiB/s 变化，16 TiB 时达到上限，如下所示：

$$16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

突增吞吐量从 10 MiB/s 到上限 250 MiB/s 变化，3.125 TiB 时达到上限，如下所示：

$$3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

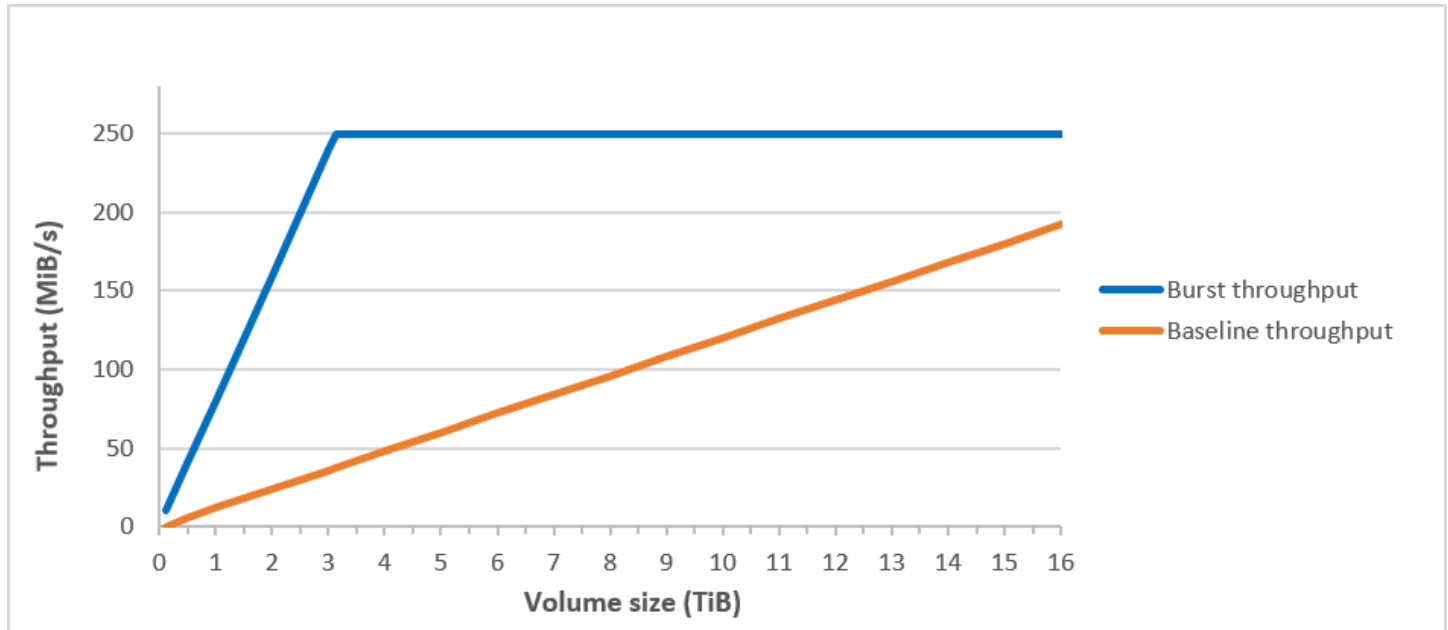
## 1 TiB

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 )
0.125	1.5	10
0.5	6	40
1	12	80
2	24	160
3	36	240
3.125	37.5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250

卷大小 ( TiB )	SC1 基准吞吐量 ( MiB/s )	SC1 突增吞吐量 ( MiB/s )
16	192	250

下图绘制了表值：



#### Note

如果创建 Cold HDD ( sc1 ) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报监控突发存储桶余额的信息，请参阅[监控卷的突发存储桶余额](#)。

## 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。

### 比较吞吐量优化型 HDD 和 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 专为在 99% 的时间内实现 90% 的突发吞吐量性能一致性而设计。不合规时间段大致均匀分布，目标是达到 99% 的每小时预计总吞吐量。

一般来说，扫描时间可由此公式表示：

$$\frac{\text{Volume size}}{\text{Throughput}} = \text{Scan time}$$

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。

- 最佳扫描时间

$$\frac{5 \text{ TiB}}{500 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.00047684 \text{ TiB/s}} = 10,486 \text{ seconds} = 2.91 \text{ hours}$$

- 最长扫描时间

$$\frac{2.91 \text{ hours}}{(0.90)(0.99)} = 3.27 \text{ hours}$$

(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。

- 最佳扫描时间

$$\frac{5 \text{ TiB}}{250 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} = 20972 \text{ seconds} = 5.83 \text{ hours}$$

- 最长扫描时间

$$\frac{5.83 \text{ hours}}{(0.90)(0.99)} = 6.54 \text{ hours}$$

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。

卷大小 (TiB)	带突增的 ST1 扫描时间 (小时) *	带突增的 SC1 扫描时间 (小时) *
1	1.17	3.64
2	1.17	3.64
3	1.75	3.64
4	2.33	4.66
5	2.91	5.83
6	3.50	6.99
7	4.08	8.16
8	4.66	9.32
9	5.24	10.49
10	5.83	11.65
11	6.41	12.82
12	6.99	13.98
13	7.57	15.15
14	8.16	16.31
15	8.74	17.48
16	9.32	18.64

\* 这些扫描时间在执行 1 MiB 顺序 I/O 时采取平均队列深度 (四舍五入到最近的整数) 四或更多。



因此，如果您有面向吞吐量的工作负载需要快速完成扫描（最快 500MiB/s）或一天查询几个整卷，请使用 st1。如果您针对成本进行了优化，数据访问相对不频繁，而且不需要超过 250 MiB/s 的扫描性能，请使用 sc1。

### HDD 上的小型读/写效率低下问题

st1 和 sc1 卷的性能模型针对顺序 I/O 进行了优化，支持高吞吐量工作负载，对具有混合 IOPS 和吞吐量的工作负载提供可接受的性能，不建议使用具有小型随机 I/O 的工作负载。

例如，1 MiB 或更小的 I/O 请求计为 1 MiB I/O 积分。但是，如果是顺序 I/O，则会合并为 1 MiB I/O 数据块，并且只计为 1 MiB I/O 积分。

### 监控卷的突发存储桶余额

您可以使用亚马逊上提供的 Amazon EBS BurstBalance 指标监控 st1 和 sc1 卷的突发存储桶级别。CloudWatch 此指标显示 st1 和 sc1 在突增存储桶中剩余的吞吐量积分。有关指标和其他与 I/O 相关的指标的更多信息，请参阅 [Amazon EBS I/O 特性和监控](#)。BurstBalance CloudWatch 还允许您设置警报，当该 BurstBalance 值降至一定水平时会通知您。有关更多信息，请参阅 [创建 CloudWatch 警报](#)。

## 针对 EBS 卷的大小和配置的限制

Amazon EBS 卷的大小受块数据存储的物理和算术以及操作系统 (OS) 和文件系统设计者的实施决策的限制。AWS 对卷大小施加了额外的限制，以保障其服务的可靠性。

以下部分介绍了限制 EBS 卷的可用大小并提供配置 EBS 卷的建议的最重要因素。

### 目录

- [存储容量](#)
- [服务限制](#)
- [分区方案](#)
- [数据块大小](#)

## 存储容量

下表总结了 Amazon EBS 上的最常用文件系统的理论和实现存储容量（假定 4096 字节块大小）。

分区方案	最大可寻址块数	理论最大大小 (块数 x 块大小)	Ext4 实现的最大大小*	XFS 实现的最大大小**	NTFS 实现的最大大小	EBS 支持的最大大小
MBR	$2^{32}$	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	$2^{64}$	64 ZiB	1 EiB = 242 <sup>10</sup> TiB  (在 RHEL7 上认证的 50TiB)	500 TiB  (在 RHEL7 上认证)	256 TiB	64 TiB †

、 [https://ext4.wiki.kernel.org/index.php/Ext4\\_Howto](https://ext4.wiki.kernel.org/index.php/Ext4_Howto) 和 <https://access.redhat.com/solutions/1532>

\*\* <https://access.redhat.com/solutions/1532>

† io2 Block Express 卷最高支持 64TiB 的 GPT 分区。有关更多信息，请参阅 [预调配 IOPS SSD \( io2 \) Block Express 卷](#)。

## 服务限制

Amazon EBS 将数据中心的大规模分布式存储提取到虚拟硬盘中。对安装在 EC2 实例上的操作系统而言，附加的 EBS 卷似乎是包含 512 字节磁盘扇区的物理硬盘驱动器。操作系统通过其存储管理实用程序对数据块（或集群）分配到这些虚拟扇区进行管理。分配与卷分区方案（例如主启动记录 [MBR] 或 GUID 分区表 [GPT]）一致，并且属于已安装文件系统（ext4、NTFS 等）的功能。

EBS 不知道其虚拟磁盘扇区中包含的数据；它只会确保扇区的完整性。这意味着 AWS 操作和操作系统操作是相互独立的。在您选择卷大小时，请注意二者的功能和限制，如以下情况中所示：

- EBS 当前支持最大卷大小 64 TiB。这意味着您可以创建一个大小为 64 TiB 的 EBS 卷，但操作系统是否能够识别该容量的全部取决于其自身的设计特征以及该卷的分区方式。
- 启动卷必须使用 MBR 或 GPT 分区方案。您从中启动实例的 AMI 决定了启动模式以及随后用于启动卷的分区方案。

使用 MBR 时，启动卷的大小限制为 2 TiB。

使用 GPT 时，如与 GRUB2 ( Linux ) 或 UEFI 启动模式 ( Windows ) 配合使用，启动卷的大小最多可达 64 TiB。

有关更多信息，请参阅 [使 Amazon EBS 卷可供使用](#)。

- 2 TiB ( 2048 GiB ) 或更大的非启动卷必须使用 GPT 分区表才能访问整个卷。

## 分区方案

除其他影响之外，分区方案还确定了可以在单个卷中唯一寻址的逻辑数据块的数量。有关更多信息，请参阅[数据块大小](#)。正在使用的常见分区方案是主启动记录 ( MBR ) 和 GUID 分区表 ( GPT )。这两个方案之间的重要差别可归纳如下。

### MBR

MBR 使用 32 位数据结构来存储块地址。这意味着，每个数据块会映射到  $2^{32}$  个可能整数之一。卷的最大可寻址大小由以下公式给出：

$$2^{32} \times \text{Block size}$$

MBR 卷的块大小通常限制为 512 字节。因此：

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

工程解决办法是提高 MBR 卷的这个 2 TiB 限制，但还没有被行业广泛采用。因此，Linux 和 Windows 永远不会检测到 MBR 体积大于 2 TiB，AWS 即使显示其大小更大。

### GPT

GPT 使用 64 位数据结构来存储块地址。这意味着，每个数据块会映射到  $2^{64}$  个可能整数之一。卷的最大可寻址大小由以下公式给出：

$$2^{64} \times \text{Block size}$$

GPT 卷的块大小通常限制为 4,096 字节。因此：

$$\begin{aligned} 2^{64} \times 4,096 \text{ bytes} \\ = 2^{64} \times 2^{12} \text{ bytes} \end{aligned}$$

$$\begin{aligned} &= 2^{70} \times 2^6 \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

现实世界中的计算机系统不支持任何接近这个理论最大值的值。实施的文件系统大小目前上限为 50TiB ( 对于 ext4 ) 和 256TiB ( 对于 NTFS )。

## 数据块大小

现代硬盘驱动器上的数据存储是通过逻辑块寻址来管理的，逻辑块寻址是一个抽象层，它允许操作系统在逻辑块中读取和写入数据，而无需详细了解底层硬件。操作系统依赖存储设备将块映射到其物理扇区。EBS 将 512 字节的扇区公告给操作系统，操作系统使用数据块 ( 是扇区大小的数倍 ) 将数据读写到磁盘。

逻辑数据块的行业默认大小当前为 4096 字节 ( 4 KiB )。由于某些工作负载受益于较小或较大的块大小，因此文件系统支持可在格式化期间指定的非默认块大小。应使用非默认块大小的情况不在本主题的范围之内，但块大小的选择会对卷的存储容量产生影响。下表显示了存储容量随不同块大小的变化：

块大小	最大卷大小
4KiB ( 默认 )	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64KiB ( 最大 )	256 TiB

EBS 实施的卷大小限制 ( 64TiB ) 目前等于 16KiB 数据块支持的最大大小。

## Amazon EBS 和 NVMe

EBS 卷作为 NVMe 块存储设备在基于 [Nitro 系统](#) 构建的实例上公开。

无论块设备接口如何，[Amazon EBS 产品详细信息](#) 中所述的 EBS 性能指南都有效。

### Linux 实例

设备名称为 `/dev/nvme0n1`、`/dev/nvme1n1`，以此类推。您在块设备映射中指定的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。块储存设备驱动程序可以使用不同于您在块储存设备映射中为卷指定的顺序来分配 NVMe 设备名称。

## Windows 实例

当您将卷附加到实例时，需要为卷提供设备名称。该设备名称由 Amazon EC2 使用。实例的块设备驱动程序会在挂载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 使用的名称不同。

## 内容

- [安装或升级 NVMe 驱动程序](#)
- [识别 EBS 设备](#)
- [使用 NVMe EBS 卷](#)
- [I/O 操作超时](#)
- [Abort 命令](#)

## 安装或升级 NVMe 驱动程序

要访问 NVMe 卷，必须安装 NVMe 驱动程序。实例可以支持 NVMe EBS 卷和 NVMe 实例存储卷（要么两种类型的 NVMe 卷均支持，要么均不支持）。有关更多信息，请参阅[联网和存储功能摘要](#)。

## Linux 实例

以下 AMI 包含所需的 NVMe 驱动程序：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

### Note

AWS 基于 Graviton 的实例类型需要带内核的 Ubuntu 18.04 或更高版本 `linux-aws`

- Red Hat Enterprise Linux 6.5 或更高版本
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本

- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

## 确认实例具有 NVMe 驱动程序

您可以使用以下命令确认您的实例是否具有 NVMe 驱动程序。

- Amazon Linux、RHEL、CentOS 和 SUSE Linux Enterprise Server

```
$ modinfo nvme
```

如果实例具有 NVMe 驱动程序，则该命令将返回有关该驱动程序的信息。

- Amazon Linux 2 和 Ubuntu

```
$ ls /sys/module/ | grep nvme
```

如果实例具有 NVMe 驱动程序，该命令将返回已安装的驱动程序。

## 更新 NVMe 驱动程序

如果您的实例具有 NVMe 驱动程序，您可以使用以下过程将驱动程序更新到最新版本。

1. 连接到您的实例。
2. 更新程序包缓存以获取必需程序包更新，如下所示。
  - 对于 Amazon Linux 2、Amazon Linux、CentOS 和 Red Hat Enterprise Linux :

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

- 对于 Ubuntu 和 Debian :

```
[ec2-user ~]$ sudo apt-get update -y
```

3. Ubuntu 16.04 及更高版本包含 `linux-aws` 程序包，该程序包包含基于 Nitro 的实例所需的 NVMe 和 ENA 驱动程序。升级 `linux-aws` 程序包以接收最新版本，如下所示：

```
[ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
```

对于 Ubuntu 14.04，您可以安装最新的 `linux-aws` 程序包，如下所示：

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. 重启实例以加载最新内核版本。

```
sudo reboot
```

5. 重启之后重新连接到实例。

## Windows 实例

AWS 适用于 Windows Server 2008 R2 及更高版本的 Windows AMI 包括 AWS NVMe 驱动程序。如果您使用的不是亚马逊提供的最新 AWS Windows AMI，请参阅亚马逊 EC2 用户指南 PowerShell 中的 [使用安装或升级 AWS NVMe 驱动程序](#)。

## 识别 EBS 设备

EBS 使用单一根 I/O 虚拟化 (SR-IOV) 在使用 NVMe 规范的基于 Nitro 的实例上提供卷附加。这些设备依赖于操作系统上的标准 NVMe 驱动程序。这些驱动程序通常在实例启动期间发现附加的设备，然后根据设备响应的顺序创建设备节点，而不是按照在块设备映射中指定设备的顺序。

## Linux 实例

在 Linux 中，NVMe 设备名称遵循 `/dev/nvme<x>n<y>` 模式，其中 `<x>` 是枚举顺序，对于 EBS，`<y>` 为 1。有时候，在接下来的实例启动时，设备会以不同顺序响应发现过程，这会导致设备名称更改。此外，块储存设备驱动程序分配的设备名称可以不同于块储存设备映射中指定的名称。

建议您在实例中为 EBS 卷使用静态标识符，例如以下之一：

- 对基于 Nitro 的实例，您在附加 EBS 卷或者在 `AttachVolume` 或 `RunInstances` API 调用期间通过 Amazon EC2 控制台指定的块储存设备映射，将在 NVMe 控制器标识的供应商特定数据字段中捕获。对版本高于 2017.09.01 的 Amazon Linux AMI，我们提供了 `udev` 规则，该规则读取此数据并创建指向块储存设备映射的符号链接。
- EBS 卷 ID 和挂载点在实例状态更改之间保持稳定。NVMe 设备名称可以根据设备在实例启动期间响应的顺序进行更改。我们建议使用 EBS 卷 ID 和挂载点以实现一致的设备标识。
- NVMe EBS 卷在设备标识中将 EBS 卷 ID 设置为序列号。使用 `lsblk -o +SERIAL` 命令列出序列号。

- NVMe 设备名称格式可能会有所不同，具体取决于 EBS 卷是在实例启动期间还是之后附上。实例启动后附上卷的 NVMe 设备名称包括 `/dev/` 前缀，而实例启动期间附上卷的 NVMe 设备名称不包括 `/dev/` 前缀。如果您使用的是 Amazon Linux 或 FreeBSD AMI，请使用 `sudo ebsnvme-id /dev/nvme0n1 -u` 命令获得一致的 NVMe 设备名称。对于其他发布版本，请使用 `sudo nvme id-ctrl -v /dev/nvme0n1` 命令确定 NVMe 设备名称。
- 格式化设备时，将生成在文件系统的使用寿命内保持的 UUID。此时可指定设备标签。有关更多信息，请参阅[使 Amazon EBS 卷可供使用](#)和[从错误的卷启动](#)。

## Amazon Linux AMI

利用 Amazon Linux AMI 2017.09.01 或更高版本（包括 Amazon Linux 2），您可以按下面所示运行 `ebsnvme-id` 命令以将 NVMe 设备名称映射到卷 ID 和设备名称：

以下示例显示实例启动期间附上的卷的命令和输出。请注意，NVMe 设备名称不包括 `/dev/` 前缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

以下示例显示实例启动后附上的卷的命令和输出。请注意，NVMe 设备名称包括 `/dev/` 前缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux 还将创建从块储存设备映射中的设备名称（例如，`/dev/sdf`）到 NVMe 设备名称的符号链接。

## FreeBSD AMI

从 FreeBSD 12.2-RELEASE 开始，您可以运行如上所示的 `ebsnvme-id` 命令。传递 NVMe 设备的名称（例如，`nvme0`）或磁盘设备的名称（例如，`nvd0` 或 `nda0`）。FreeBSD 还创建到磁盘设备的符号链接（例如，`/dev/aws/disk/ebs/volume_id`）。

## 其他 Linux AMI

利用内核版本 4.2 或更高版本，您可以按下面所示运行 `nvme id-ctrl` 命令以将 NVMe 设备映射到卷 ID。首先，使用您的 Linux 发行版的程序包管理工具安装 NVMe 命令行程程序包 `nvme-cli`。有关其他发行版的下载和安装说明，请参阅特定于您的发行版的文档。



以下示例将获取实例启动期间附上的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称不包括 `/dev/` 前缀。设备名称通过特定于 NVMe 控制器供应商的扩展（控制器标识的字节 384:4095）提供：

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn       : vol01234567890abcdef
mn       : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

以下示例将获取实例启动后附上的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称包括 `/dev/` 前缀。

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn       : volabcdef01234567890
mn       : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

`lsblk` 命令可列出可用设备及其挂载点（如果适用）。这有助于确定要使用的正确设备名称。在本示例中，`/dev/nvme0n1p1` 作为根设备挂载，`/dev/nvme1n1` 会附加但不会挂载。

```
[ec2-user ~]$ lsblk
NAME                MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1             259:3   0 100G  0 disk
nvme0n1             259:0   0   8G  0 disk
  nvme0n1p1         259:1   0   8G  0 part /
  nvme0n1p128       259:2   0    1M  0 part
```

## Windows 实例

您可以运行 `ebsnvme-id` 命令以将 NVMe 设备磁盘编号映射到 EBS 卷 ID 和设备名称。默认情况下，枚举所有 EBS NVMe 设备。您可以传递磁盘编号以枚举特定设备的信息。该 `ebsnvme-id` 工具包含在最新 AWS 提供的 Windows 服务器 AMI 中，位于 `C:\PROGRAMDATA\AMAZON\Tools`

从 AWS NVMe 驱动程序包 1.5.0 开始，该 `ebsnvme-id` 工具的最新版本由驱动程序包安装。最新版本仅在驱动程序包中可用。`ebsnvme-id` 工具的独立下载链接将不再接收更新。通过独立链接提供的最新版本是 1.1.0，可使用 [ebsnvme-id.zip](#) 链接下载，并将内容提取到 Amazon EC2 实例以访问 `ebsnvme-id.exe`。

```
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb

Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

## 使用 NVMe EBS 卷

要格式化并挂载 NVMe EBS 卷，请参阅 [使 Amazon EBS 卷可供使用](#)。

### Linux 实例

如果您使用的是 Linux 内核 4.2 或更高版本，您对 NVMe EBS 卷的卷大小进行的所有更改将自动在实例中反映。对于旧版 Linux 内核，您可能需要分离然后附加 EBS 卷或者重启实例才能反映大小更改。对于 Linux 内核 3.19 或更高版本，您可以按下面所示使用 `hdparm` 命令强制重新扫描 NVMe 设备：

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

当您分离 NVMe EBS 卷时，实例在分离卷之前将没有机会刷新文件系统缓存或元数据。在分离 NVMe EBS 卷之前，您应该首先同步并卸载它。如果卷无法分离，您可以按照 `force-detach` 中所述尝试执行 [将 Amazon EBS 卷与实例分离](#) 命令。

## Windows 实例

最新的 AWS Windows AMI 包含将 EBS 卷作为 AWS NVMe 块储存设备的实例类型所必需的 NVMe 驱动程序。但是，如果您调整了 Windows 系统上的根卷的大小，则必须重新扫描该卷才能在实例中体现此更改。如果您从其他 AMI 启动实例，则该实例可能不包含所需的 AWS NVMe 驱动程序。如果您的实例没有最新的 AWS NVMe 驱动程序，则必须安装它。有关更多信息，请参阅 [适用于 Windows 实例的 AWS NVMe 驱动程序](#)。

## I/O 操作超时

大多数操作系统为提交到 NVMe 设备的 I/O 操作指定一个超时。

### Linux 实例

在 Linux 上，挂载到基于 Nitro 系统的实例的 EBS 卷使用操作系统提供的默认 NVMe 驱动程序。大多数操作系统为提交到 NVMe 设备的 I/O 操作指定一个超时。默认超时为 30 秒，可以使用 `nvme_core.io_timeout` 引导参数更改该超时。对于 4.6 版之前的大多数 Linux 内核版本，此参数为 `nvme.io_timeout`。

如果 I/O 延迟超过了此超时参数的值，则 Linux NVMe 驱动程序会使 I/O 失败，并将错误返回文件系统或应用程序。根据 I/O 操作，您的文件系统或应用程序可以重试错误。在某些情况下，您的文件系统可能会通过只读方式重新挂载。

为了获得与附加到 Xen 实例的 EBS 卷类似的体验，我们建议将 `nvme_core.io_timeout` 设置为可能的最大值。对于当前内核，最大值为 4294967295，而对于较早的内核，最大值为 255。根据 Linux 版本的不同，超时时间可能已设置为支持的最大值。例如，对于 Amazon Linux AMI 2017.09.01 以及更高的版本，超时时间默认设置为 4294967295。

您可以通过将高于建议最大值的值写入 `/sys/module/nvme_core/parameters/io_timeout` 并在尝试保存文件时检查数值结果超出范围错误，以此来验证您的 Linux 发行版的最大值。

### Windows 实例

在 Windows 上，默认超时时间为 60 秒，最大值为 255 秒。您可以使用 [SCSI 微端口驱动程序的注册表项](#) 中所述的步骤修改 `TimeoutValue` 磁盘类注册表设置。

## Abort 命令

Abort 命令是一个 NVMe 管理员命令，用于中止之前提交给控制器的特定命令。此命令通常由设备驱动程序向超过输入/输出操作超时阈值的存储设备发出。默认支持 Abort 命令的 Amazon EC2 实例类型，将中止先前提交给已向其发出 Abort 命令的所附加 Amazon EBS 设备的控制器的特定命令。

默认情况下，以下实例类型支持所有附加的 Amazon EBS 卷的 Abort 命令：R5b、R6i、M6i、M6a、C6gn、C6i、X2gd、X2iezn、Im4gn、Is4gen。

向附加的 Amazon EBS 卷发出 Abort 命令时，其他实例类型不采取任何操作。

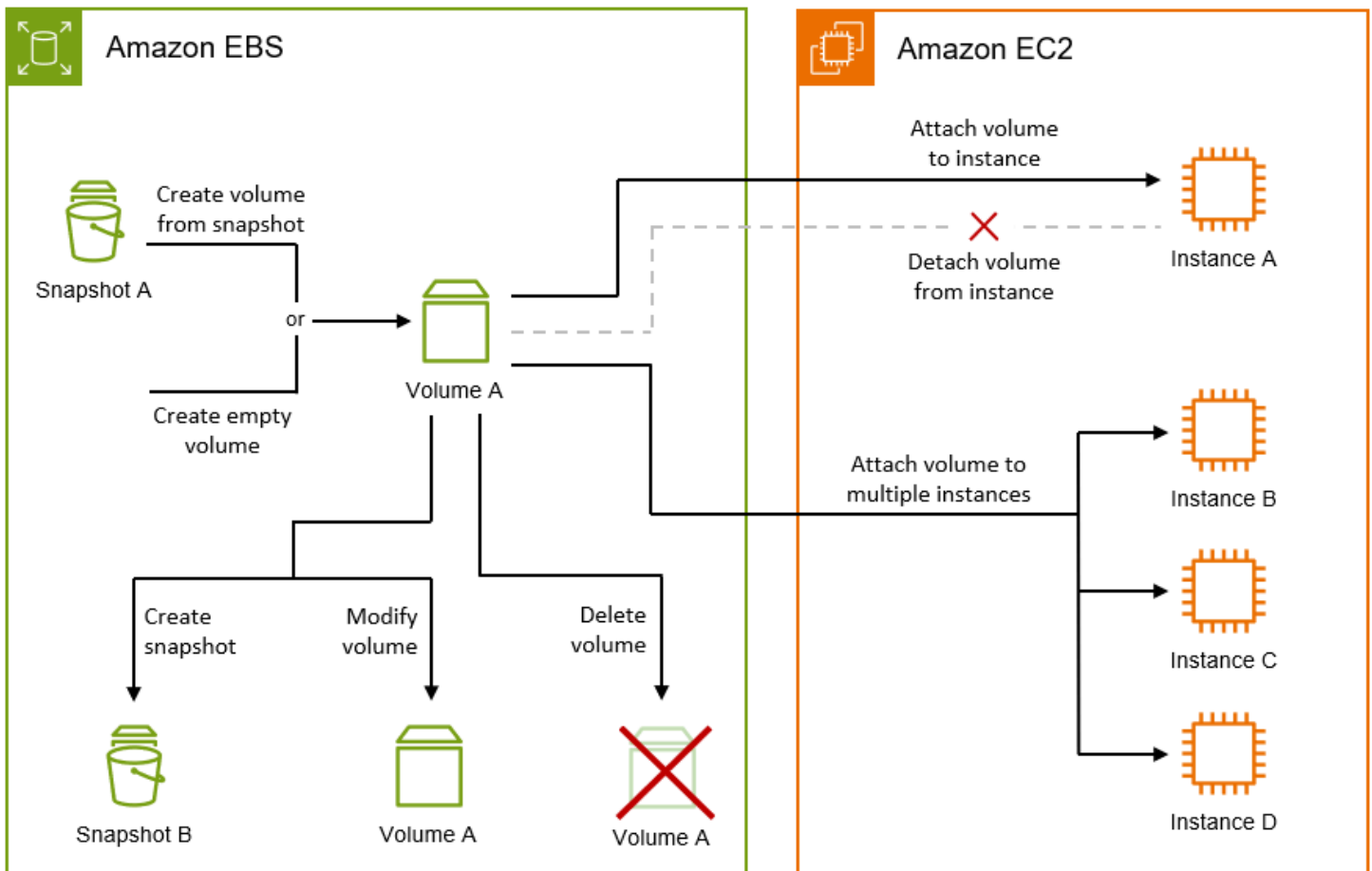
NVMe 设备为 1.4 版本或更高版本的 Amazon EBS 设备支持 Abort 命令。

有关更多信息，请参阅 [NVMe Express 基本规范](#) 的 5.1 Abort 命令部分。

## Amazon EBS 卷的生命周期

Amazon EBS 卷的生命周期始于创建过程。您可以通过 Amazon EBS 快照创建卷，也可以创建空卷。必须先将其挂载到与该卷位于相同可用区中的一个或多个 Amazon EC2 实例。您可以将多个卷挂载到一个实例。如有需要，您也可以将卷从实例中分离，随后将其挂载到另一个实例。如果存储需求发生变化，则可以随时修改卷的大小或性能。您可以通过创建 Amazon EBS 快照来创建卷的 point-in-time 备份。如果不再需要卷，则可将其删除，以免产生相关存储成本。

下图显示了可以在卷生命周期中对卷执行的操作。



您还可以通过连接到实例并运行操作系统命令来执行某些任务。例如，格式化卷、挂载卷、管理分区和查看可用磁盘空间。

## 任务

- [创建 Amazon EBS 卷](#)
- [将 Amazon EBS 卷挂载到实例](#)
- [使用 Amazon EBS 多重挂载将卷挂载到多个实例](#)
- [使 Amazon EBS 卷可供使用](#)
- [查看关于 Amazon EBS 卷的信息](#)
- [使用 Amazon EBS 弹性卷修改卷](#)
- [将 Amazon EBS 卷与实例分离](#)
- [删除 Amazon EBS 卷](#)

## 创建 Amazon EBS 卷

您可以创建一个 Amazon EBS 卷，然后将它附加到同一可用区内的任何 EC2 实例。如果您创建加密的 EBS 卷，则只能将其附加到支持的实例类型。有关更多信息，请参阅 [支持的实例类型](#)。

如果您要针对一种高性能存储情形来创建卷，应确保使用预置 IOPS SSD 卷 ( io1 或 io2 ) 并将它挂载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。此建议同样适用于吞吐量优化型 HDD ( st1 ) 和 Cold HDD ( sc1 ) 卷。

### Note

如果您创建了一个用于 Windows 实例的卷，并且该卷大于 2048 GiB ( 或者小于 2048 GiB 但以后可能会增加 )，请确保将该卷配置为使用 GPT 分区表。有关更多信息，请参阅 [Windows 对大于 2 TB 的硬盘的支持](#)。

空的 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，从快照创建的卷上的存储块必须先进行初始化 ( 从 Amazon S3 提取并写入到卷 )，然后您才能访问该块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。为了避免最初在生产环境中出现这种性能下降，您可以强制立即初始化整个卷或启用快速快照还原。有关更多信息，请参阅 [初始化 Amazon EBS 卷](#)。

### 创建卷的方法

- 在指定块储存设备映射以启动实例时，创建并附加 EBS 卷。有关更多信息，请参阅[使用新启动实例向导启动实例](#)和[块设备映射](#)。
- 创建空 EBS 卷并将其附加到运行的实例。有关更多信息，请参阅下面的 [创建空卷](#)。
- 从以前创建的快照中创建 EBS 卷，并将其附加到运行的实例。有关更多信息，请参阅下面的 [从快照创建卷](#)。

### 主题

- [创建空卷](#)
- [从快照创建卷](#)

## 创建空卷

空卷一旦可用便能实现其最高性能，而不需要初始化。

您可以使用以下方法之一创建空的 EBS 卷。

### Console

#### 使用控制台创建空 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择创建卷。
4. 对于 Volume Type（卷类型），选择需要创建的卷类型。有关更多信息，请参阅 [Amazon EBS 卷类型](#)。

默认选择是“通用型 SSD gp3”。

5. 对于大小，以 GiB 为单位输入卷的大小。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制](#)。
6. （仅限于 io1、io2 及 gp3）对于 IOPS，输入该卷应提供的每秒进行读写操作的次数（IOPS）的最大值。
7. （仅限于 gp3）对于吞吐量，以 MiB/s 为单位输入卷应提供的吞吐量。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。一个卷只能附加到同一可用区中的实例。
9. 对于快照 ID，保留默认值，即不要从快照中创建卷。
10. （仅限于 io1 和 io2）要为 Amazon EBS 多重挂载启用卷，请选择 Enable Multi-Attach（启用多重挂载）。有关更多信息，请参阅 [使用 Amazon EBS 多重挂载将卷挂载到多个实例](#)。
11. 设置卷的加密状态。

如果您的账户已启用 [encryption by default](#)（默认加密），那么加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

如果默认情况下您的账户未启用加密，则加密是可选的。要加密卷，请为 Encryption（加密）选择 Encrypt this volume（加密此卷），然后选择要用于加密卷的 KMS 密钥。

**Note**

加密卷只能附加到支持 Amazon EBS 加密的实例。有关更多信息，请参阅 [Amazon EBS 加密](#)。

12. (可选) 要为卷分配自定义标签，请在标签部分中选择添加标签，然后输入标签键和值对。
13. 选择创建卷。

**Note**

Volume state (卷状态) 为 available (可用) 时，卷即可供使用。

14. 要使用卷，请将其附加到实例。有关更多信息，请参阅 [将 Amazon EBS 卷挂载到实例](#)。

## AWS CLI

要使用创建空的 EBS 卷 AWS CLI

使用 [create-volume](#) 命令。

state 状态为 available 时，卷即可供使用。

## Tools for Windows PowerShell

使用适用于 Windows 的工具创建空的 EBS 卷 PowerShell

使用 [New-EC2Volume](#) 命令。

state 状态为 available 时，卷即可供使用。

## 从快照创建卷

从快照创建的新卷在后台延时加载。这意味着在实例开始访问附加的卷及其所有数据之前，无需等待所有数据从 Amazon S3 传输到 EBS 卷。如果您的实例访问尚未加载的数据，卷会立即从 Amazon S3 下载请求的数据，然后在后台继续加载卷数据的剩余部分。在下载所有块并将其写入到卷后，才会实现卷性能。为避免在生产环境中影响初始性能，请参阅 [初始化 Amazon EBS 卷](#)。

从加密快照创建的新 EBS 卷会自动加密。您也可以在从未加密的快照中恢复卷的 on-the-fly 同时对其进行加密。加密的卷只能附加到支持 EBS 加密的实例类型。有关更多信息，请参阅 [支持的实例类型](#)。



您可以使用以下方法之一从快照创建卷。

## Console

### 使用控制台从快照中创建 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择创建卷。
4. 对于 Volume Type（卷类型），选择需要创建的卷类型。有关更多信息，请参阅 [Amazon EBS 卷类型](#)。

默认选择是“通用型 SSD gp3”。

5. 对于大小，以 GiB 为单位输入卷的大小。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制](#)。
6. （仅限于 io1、io2 及 gp3）对于 IOPS，输入该卷应提供的每秒进行读写操作的次数（IOPS）的最大值。
7. （仅限于 gp3）对于吞吐量，以 MiB/s 为单位输入卷应提供的吞吐量。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。一个卷只能附加到位于相同可用区中的实例。
9. 对于 Snapshot ID（快照 ID），选择快照并从中创建卷。
10. 设置卷的加密状态。

如果选定的快照已加密，或者您的账户已启用[默认加密](#)，则加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

如果选定的快照未加密，且默认情况下账户未启用加密，则加密是可选的。要加密卷，请为 Encryption（加密）选择 Encrypt this volume（加密此卷），然后选择要用于加密卷的 KMS 密钥。

#### Note

加密卷只能附加到支持 Amazon EBS 加密的实例。有关更多信息，请参阅 [Amazon EBS 加密](#)。

11. （可选）要为卷分配自定义标签，请在标签部分中选择添加标签，然后输入标签键和值对。
12. 选择 Create Volume。

**Note**

Volume state ( 卷状态 ) 为 available ( 可用 ) 时，卷即可供使用。

13. 要使用卷，请将其附加到实例。有关更多信息，请参阅 [将 Amazon EBS 卷挂载到实例](#)。

## AWS CLI

使用快照创建 EBS 卷 AWS CLI

使用 [create-volume](#) 命令。

state 状态为 available 时，卷即可供使用。

## Tools for Windows PowerShell

使用适用于 Windows 的工具从快照创建 EBS 卷 PowerShell

使用 [New-EC2Volume](#) 命令。

state 状态为 available 时，卷即可供使用。

## 将 Amazon EBS 卷挂载到实例

您可以将可用的 EBS 卷附加到与该卷处于同一可用区中的一个或多个实例。

有关在启动时向实例添加 EBS 卷的信息，请参阅[实例块设备映射](#)。

### 注意事项

- 确定您可以将多少个卷附加到您的实例。您可以挂载到实例的最大 Amazon EBS 卷数取决于实例类型和实例规模。有关更多信息，请参阅[实例卷限制](#)。
- 确定是否可以将卷附加到多个实例并启用多重挂载。有关更多信息，请参阅[使用 Amazon EBS 多重挂载将卷挂载到多个实例](#)。
- 如果卷已加密，只能将它附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅[支持的实例类型](#)。
- 如果卷有 AWS Marketplace 产品代码：
  - 卷只能附加到已停止的实例。

- 您必须订阅卷上的 AWS Marketplace 代码。
- 实例的配置（例如其类型和操作系统）必须支持该特定 AWS Marketplace 代码。例如，您不能从 Windows 实例取用卷，然后将其附加到 Linux 实例。
- AWS Marketplace 产品代码从卷复制到实例。

您可以使用以下方法之一将卷挂载到实例。

## Console

### 使用控制台将 EBS 卷附加到实例

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择需要附加的卷，然后选择 Actions（操作）、Attach volume（附加卷）。

#### Note

您只能附加处于 Available 状态中的卷。

4. 对于 Instance（实例），输入实例的 ID 或从选项列表中选择实例。

#### Note

- 卷必须附加到位于同一可用区的实例上。
- 如果卷已加密，只能将它附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅 [Amazon EBS 加密](#)。

5. 对于“设备名称”，执行以下任一操作：

- 对于根卷，请从列表的“为根卷保留”部分中选择所需的设备名称。通常是 /dev/sda1/ dev/xvda 针对基于 AMI 的 Linux 实例，或者 /dev/sda1 适用于 Windows 实例。
- 对于数据卷，请从列表的“推荐用于数据量”部分中选择一个可用的设备名称。
- 要使用自定义设备名称，请选择“指定自定义设备名称”，然后输入要使用的设备名称。

该设备名称由 Amazon EC2 使用。在挂载卷时，实例的块储存设备驱动程序将分配不同的卷名称。有关更多信息，请参阅 [Linux 实例上的设备名称或 Windows 实例上的设备名称](#)。

6. 选择附加卷。
7. 连接到实例并挂载卷。有关更多信息，请参阅 [使 Amazon EBS 卷可供使用](#)。

## AWS CLI

使用 EBS 卷连接到实例 AWS CLI

使用 [attach-volume](#) 命令。

## Tools for Windows PowerShell

使用适用于 Windows 的工具将 EBS 卷连接到实例 PowerShell

使用 [Add-EC2Volume](#) 命令。

### Note

- 如果您尝试连接的卷数量超出了实例类型的卷限制，则请求会失败。有关更多信息，请参阅 [实例卷限制](#)。
- 在某些情况下，您可能会发现某个并非附加到 `/dev/xvda` 或 `/dev/sda` 的卷成为了您的实例的根卷。当您将另一个实例的根卷或从某个根卷的快照中创建的卷附加到带有现有根卷的实例时，可能会发生这种情况。有关详细信息，请参阅 [从错误的卷启动](#)。

## 使用 Amazon EBS 多重挂载将卷挂载到多个实例

通过 Amazon EBS 多重挂载，您可以将单个预置 IOPS SSD ( `io1` 或 `io2` ) 卷挂载到位于同一可用区中的多个实例。您可以将多个启用多重挂载的卷附加到一个实例或一组实例。卷附加到的每个实例都对共享卷拥有完全读取和写入权限。通过多重挂载，您可以更轻松地在管理并发写入操作的应用程序中实现更高的应用程序可用性。

### 内容

- [注意事项和限制](#)
- [Performance](#)
- [使用多重挂载](#)
- [监控启用多重挂载的卷](#)

- [定价和计费](#)
- [NVMe 预留](#)

## 注意事项和限制

- 启用多重挂载的卷最多可以挂载到位于相同可用区内的基于 [Nitro 系统](#) 构建的 16 个实例。
- Linux 实例支持启用多重挂载的 io1 和 io2 卷。Windows 实例仅支持启用多重挂载的 io2 卷。
- 您可以挂载到实例的最大 Amazon EBS 卷数取决于实例类型和实例规模。有关更多信息，请参阅 [实例卷限制](#)。
- 仅在 [预调配 IOPS SSD \( io1 和 io2 \) 卷](#) 上才支持多重挂载。
- io1 卷的多重挂载仅在以下区域可用：美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）和亚太地区（首尔）。

适用于 io2 的多重挂载功能已在所有支持 io2 的区域中提供。

### Note

为了以更低的成本获得更好的性能、一致性和耐用性，我们建议您使用 io2 卷。

- 当 [基于 Nitro System 而构建的实例](#) 仅支持可扩展的可靠数据报（SRD）网络协议时，将不支持启用了多重挂载的 io1 卷。要将多重挂载与这些实例类型结合使用，必须使用 io2 Block Express 卷。
- 标准文件系统（例如 XFS 和 EXT4）不能被多个服务器（例如 EC2 实例）同时访问。您应使用集群文件系统来确保生产工作负载的数据恢复能力和可靠性。
- 启用多重挂载的 io2 卷支持 I/O 隔离栏。I/O 隔离栏协议控制共享存储环境中的写入访问，以保持数据一致性。您的应用程序必须为附加的实例提供写入顺序，以保持数据一致性。有关更多信息，请参阅 [NVMe 预留](#)。

启用多重挂载的 io1 卷不支持 I/O 隔离栏。

- 无法将启用多重挂载的卷创建为引导卷。
- 可以将启用多重挂载的卷附加到每个实例的一个块储存设备映射。
- 在实例启动期间，无法使用 Amazon EC2 控制台或 RunInstances API 启用多重连接。
- 在 Amazon EBS 基础结构层存在问题的启用多重挂载的卷对于所有附加的实例都不可用。Amazon EC2 或网络层的问题可能仅影响某些挂载的实例。
- 下表显示了创建后对启用多重挂载的 io1 和 io2 卷的卷修改支持。

	io2 卷	io1 卷
修改卷类型	X	X
修改卷大小	✓	X
修改预置 IOPS	✓	X
启用多重挂载	✓ *	X
禁用多重挂载	✓ *	X

\*当卷挂载到实例时，您无法启用或禁用多重挂载。

## Performance

每个附加的实例都能够将其最大 IOPS 性能提升到卷的最大预置性能。但是，所有附加的实例的总体性能不能超过卷的最大预置性能。如果附加实例的 IOPS 需求高于卷的预置 IOPS，则卷不会超过其预置性能。

例如，假设您使用 io2 预置 IOPS 创建 80,000 启用了多重挂载的卷，然后将其挂载到最高支持 40,000 IOPS 的 m7g.large 实例和最高支持 60,000 IOPS 的 r7g.12xlarge 实例。每个实例都可以提升其最大 IOPS，因为它小于卷的预置 IOPS 80,000。但是，如果两个实例同时提升对卷的 I/O，则其组合 IOPS 不能超过卷的预置性能 80,000 IOPS。

为了实现一致的性能，最佳做法是在启用多重挂载的卷的扇区间平衡由附加实例提升的 I/O。

## 使用多重挂载

启用了多重挂载的卷的管理方式与管理任何其他 Amazon EBS 卷的方式大致相同。但是，为了使用多重挂载功能，您必须为卷启用它。当您创建新卷时，默认情况下，多重挂载处于禁用状态。

### 目录

- [启用多重挂载](#)
- [禁用多重挂载](#)
- [将卷挂载到实例](#)
- [终止时删除](#)

## 启用多重挂载

您可以在创建期间启用多重挂载功能。使用以下方法之一。

### Console

在卷创建过程中启用多重挂载

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择创建卷。
4. 对于卷类型，选择预调配 IOPS SSD ( **io1** ) 或预调配 IOPS SSD ( **io2** ) 。
5. 对于大小和 IOPS，选择所需的卷大小和要预置的 IOPS 数。
6. 对于可用区，请选择实例所在的相同可用区。
7. 对于 Amazon EBS Multi-Attach ( Amazon EBS 多重挂载 ) ，选择 Enable Multi-Attach ( 启用多重挂载 ) 。
8. ( 可选 ) 对于快照 ID，选择快照并从中创建卷。
9. 设置卷的加密状态。

如果选定的快照已加密，或者您的账户已启用[默认加密](#)，则加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

如果选定的快照未加密，且默认情况下账户未启用加密，则加密是可选的。要加密卷，请为 Encryption ( 加密 ) 选择 Encrypt this volume ( 加密此卷 ) ，然后选择要用于加密卷的 KMS 密钥。

#### Note

加密卷只能附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅 [Amazon EBS 加密](#)。

10. ( 可选 ) 要为卷分配自定义标签，请在标签部分中选择添加标签，然后输入标签键和值对。
11. 选择创建卷。

### Command line

在卷创建过程中启用多重挂载

使用 [create-volume](#) 命令并指定 `--multi-attach-enabled` 参数。

```
$ C:\> aws ec2 create-volume --volume-type io2 --multi-attach-enabled --size 100 --  
iops 2000 --region us-west-2 --availability-zone us-west-2b
```

您还可以在创建 io2 卷之后，仅在那些卷没有挂载到任何实例的情况下，为其启用多重挂载。

#### Note

在创建之后，您不能为 io1 卷启用多重挂载。

使用以下方法之一为已创建的 io2 卷启用多重挂载功能。

### Console

在创建后启用多重挂载

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions (操作)、Modify Volume (修改卷)。
4. 对于 Amazon EBS Multi-Attach (Amazon EBS 多重挂载)，选择 Enable Multi-Attach (启用多重挂载)。
5. 选择修改。

### Command line

在创建后启用多重挂载

使用 [modify-volume](#) 命令并指定 `--multi-attach-enabled` 参数。

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --multi-attach-  
enabled
```

### 禁用多重挂载

只有当 io2 卷挂载到不超过一个实例时，您才能对其禁用多重挂载。



**Note**

在创建之后，您不能为 io1 卷禁用多重挂载。

使用以下方法之一为 io2 卷禁用多重挂载。

### Console

在创建后禁用多重挂载

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions ( 操作 )、Modify Volume ( 修改卷 )。
4. 对于 Amazon EBS 多重挂载，清除 Enable Multi-Attach ( 启用多重挂载 )。
5. 选择修改。

### Command line

在创建后禁用多重挂载

使用 [modify-volume](#) 命令并指定 `-no-multi-attach-enabled` 参数。

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --no-multi-attach-enabled
```

### 将卷挂载到实例

您可以将启用多重挂载的卷附加到实例，方式与挂载任何其他 EBS 卷相同。有关更多信息，请参阅[将 Amazon EBS 卷挂载到实例](#)。

### 终止时删除

如果最后一个附加的实例终止，并且该实例配置为在终止时删除卷，则启用多重挂载的卷将在实例终止时被删除。如果卷附加到多个实例，而这些实例在其卷块储存设备映射中具有不同的终止时删除设置，则最后一个附加的实例的块储存设备映射设置决定终止时删除行为。

要确保对终止行为进行可预测删除，为卷挂载到的所有实例启用或禁用“终止时删除”。

默认情况下，当卷挂载到实例时，数据块设备映射的终止时删除设置会设为 `false`。如果要对启用多重挂载的卷开启终止时删除功能，请修改块储存设备映射。

如果您希望在终止附加的实例时删除卷，请在块储存设备映射中为所有附加的实例启用终止时删除。如果您要在附加的实例终止后保留卷，请在块储存设备映射中为所有附加的实例禁用终止时删除操作。有关更多信息，请参阅[实例终止时保留数据](#)。

您可以在启动时或启动后修改实例的终止时删除设置。如果您在实例启动期间启用或禁用终止时删除功能，则设置仅应用于在启动时附加的卷。如果您在启动后将卷附加到实例，则必须显式设置该卷的终止时删除行为。

您只能使用命令行工具修改实例的终止时删除设置。

### 修改现有实例的终止时删除设置

使用 [modify-instance-attribute](#) 命令并在 `DeleteOnTermination` 中指定 `--block-device-mappings option` 属性。

```
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/sdf",
    "Ebs": {
      "DeleteOnTermination": true/false
    }
  }
]
```

### 监控启用多重挂载的卷

您可以使用 Amazon EBS 卷的 CloudWatch 指标监控启用了多重连接的卷。有关更多信息，请参阅[亚马逊 EBS 的亚马逊 CloudWatch 指标](#)。

在所有附加的实例之间聚合数据。您无法监控单个附加的实例的指标。

## 定价和计费

使用 Amazon EBS 多重挂载不会产生额外费用。您需要按照适用于预置 IOPS SSD ( io1 和 io2 ) 卷的标准计费。有关更多信息，请参阅 [Amazon EBS 定价](#)。

## NVMe 预留

启用多重挂载的 io2 卷支持 NVMe 预留，这是一组行业标准的存储隔离栏协议。这些协议可让您创建和管理预留，以控制和协调多个实例对共享卷的访问。共享存储应用程序使用预留来确保数据一致性。

### 主题

- [要求](#)
- [启用对 NVMe 预留的支持](#)
- [支持的 NVMe 预留命令](#)
- [定价](#)

### 要求

仅启用多重挂载功能的 io2 卷支持 NVMe 预留。启用多重挂载的卷仅可以连接到基于 Nitro 系统构建的实例。

以下操作系统上支持 NVMe 预留：

- SUSE Linux Enterprise 12 SP3 和更高版本
- RHEL 8.3 和更高版本
- Amazon Linux 2 和更高版本
- Windows Server 2016 及更高版本

#### Note

对于日期为 2023.09.13 及之后的受支持 Windows Server AMI，包括所需的 NVMe 驱动程序。对于早期的 AMI，您必须更新到 NVMe 驱动程序版本 1.5.0 或更高版本。有关更多信息，请参阅 [适用于 Windows 实例的 AWS NVMe 驱动程序](#)。

如果您使用 EC2Launch v2 初始化磁盘，则必须升级到版本 2.0.1521 或更高版本。有关更多信息，请参阅 [使用 EC2Launch v2 配置 Windows 实例](#)。

## 启用对 NVMe 预留的支持

2023 年 9 月 18 日之后创建的所有启用多重挂载的 io2 卷均默认启用对 NVMe 预留的支持。

要为 2023 年 9 月 18 日之前创建的现有 io2 卷启用对 NVMe 预留的支持，您必须将所有实例与该卷分离，然后重新连接所需的实例。在分离所有实例后创建的所有附件都将启用 NVMe 预留。

### 支持的 NVMe 预留命令

Amazon EBS 支持以下 NVMe 预留命令：

#### Reservation Register

注册、取消注册或替换预留密钥。注册密钥用于识别和验证实例。向卷注册预留密钥会在实例和卷之间建立关联。您必须先向卷注册实例，然后该实例才能获得预留。

#### Reservation Acquire

获取卷上的预留，抢占命名空间上保存的预留，以及中止在卷上保存的预留。可以获取以下预留类型：

- 写专属预留
- 专属访问预留
- 写专属 - 仅限注册者预留
- 专属访问 - 仅限注册者预留
- 写专属 - 所有注册者预留
- 专属访问 - 所有注册者预留

#### Reservation Release

释放或清除卷上保存的预留。

#### Reservation Report

描述卷的注册和预留状态。

## 定价

启用和使用多重挂载不会产生额外费用。

## 使 Amazon EBS 卷可供使用

将某个 Amazon EBS 卷挂载到实例后，该卷将显示为块设备。您可以使用任何文件系统将卷格式化，然后进行挂载。在使 EBS 卷可供使用后，您可以像访问其他所有卷一样访问该卷。任何写入此文件系统的数据均写入 EBS 卷，并且对使用该设备的应用程序是透明的。

您可以制作 EBS 卷的快照以进行备份或在您创建其他卷时作为基准。有关更多信息，请参阅 [Amazon EBS 快照](#)。

如果您准备使用的 EBS 卷大于 2TiB，则必须使用 GPT 分区方案才能访问整个卷。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制](#)。

### Linux 实例

#### 格式化并挂载附加的卷

假设您的根设备 `/dev/xvda` 拥有一个具有 EBS 卷的 EC2 实例，并且您已使用 `/dev/sdf` 将一个空的 EBS 卷添加到了该实例。按照以下过程使新附加的卷可用。

#### 在 Linux 上格式化并挂载 EBS 卷

1. 使用 SSH 连接到实例。有关更多信息，请参阅[连接到您的 Linux 实例](#)。
2. 设备可附加到设备名称与您在块储存设备映射中指定的设备名称不同的实例。有关更多信息，请参阅[Linux 实例上的设备名称](#)。使用 `lsblk` 命令可查看可用磁盘设备及其挂载点（如果适用），以帮助确定要使用的正确设备名称。`lsblk` 的输出从完整的设备路径中去掉了 `/dev/` 前缀。

以下是基于 [Nitro 系统](#) 构建的实例的示例输出，该实例将 EBS 卷公开为 NVMe 块设备。根设备为 `/dev/nvme0n1`，它有两个名为 `nvme0n1p1` 和 `nvme0n1p128`。如果没有分区且尚未附加，则附加卷为 `/dev/nvme1n1`。

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM  SIZE RO  TYPE MOUNTPOINT
nvme1n1       259:0   0  10G  0  disk
nvme0n1       259:1   0   8G  0  disk
-nvme0n1p1    259:2   0   8G  0  part /
-nvme0n1p128  259:3   0   1M  0  part
```

以下是 T2 实例的示例输出。根设备为 `/dev/xvda`，它有一个名为 `xvda1` 的分区。如果没有分区且尚未附加，则附加卷为 `/dev/xvdf`。

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

```

NAME      MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
xvda      202:0    0    8G  0 disk
-xvda1    202:1    0    8G  0 part /
xvdf      202:80   0   10G  0 disk

```

3. 确定卷上是否存在文件系统。新卷为原始的块储存设备，您必须先在这种设备上创建文件系统，然后才能够挂载并使用它们。从快照创建的卷可能已经含有文件系统；如果您在现有的文件系统上创建新的文件系统，则该操作将覆盖您的数据。

使用以下一种或两种方法来确定卷上是否有文件系统：

- 使用 `file -s` 命令获取有关特定设备的信息，例如其文件系统类型。如果输出仅显示 `data`（如下示例输出所示），则说明设备上没有文件系统。

```

[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data

```

如果设备有文件系统，该命令会显示有关文件系统类型的信息。例如，以下示例输出显示具有 XFS 文件系统的根设备。

```

[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)

```

- 使用 `lsblk -f` 命令获取有关连接到实例的所有设备的信息。

```

[ec2-user ~]$ sudo lsblk -f

```

例如，以下输出显示有三个设备连接到实例 – `nvme1n1`、`nvme0n1` 和 `nvme2n1`。第一列列出了设备及其分区。FSTYPE 列显示每个设备的文件系统类型。如果该列对于特定设备为空，则表示该设备没有文件系统。在这种情况下，设备 `nvme1n1` 和设备 `nvme0n1` 上的分区 `nvme0n1p1` 都使用 XFS 文件系统进行格式化，而设备 `nvme2n1` 和设备 `nvme0n1` 上的分区 `nvme0n1p128` 没有文件系统。

```

NAME      FSTYPE LABEL UUID                                MOUNTPOINT
nvme1n1           xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
nvme0n1
##nvme0n1p1 xfs      / 90e29211-2de8-4967-b0fb-16f51a6e464c  /
##nvme0n1p128
nvme2n1

```

如果这些命令的输出显示设备上没有文件系统，则必须创建一个文件系统。

4. (有条件) 如果您在上一步中发现设备上存在文件系统，请跳过此步骤。如果您有一个空卷，请使用 `mkfs -t` 命令在该卷上创建一个文件系统。

**⚠ Warning**

如果要挂载已具有数据的卷（例如，从快照创建的卷），请勿使用此命令。否则，您会格式化卷并删除现有数据。

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

如果出现“找不到 `mkfs.xfs`”错误，请使用以下命令安装 XFS 工具，然后重复上一命令：

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. 使用 `mkdir` 命令创建卷的挂载点目录。挂载点是卷在文件系统树中的位置，以及您在安装卷之后读写文件的位置。下面的示例创建一个名为 `/data` 的目录。

```
[ec2-user ~]$ sudo mkdir /data
```

6. 在您于上一步创建的挂载点目录中挂载卷或分区。

如果该卷没有分区，请使用以下命令并指定设备名称来挂载完整的卷。

```
[ec2-user ~]$ sudo mount /dev/xvdf /data
```

如果该卷有分区，请使用以下命令并指定分区名称来挂载分区。

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /data
```

7. 检查新卷挂载的文件权限，确保您的用户和应用程序可以向该卷写入数据。有关文件权限的更多信息，请参阅 Linux 文档项目 [文件安全性](#)。
8. 重启实例后，挂载点不会自动保留。要在重启后自动挂载此 EBS 卷，请使用 [重启后自动挂载附加的卷](#)。

## 重启后自动挂载附加的卷

要在每次系统重启时附加附加的 EBS 卷，可在 `/etc/fstab` 文件中为该设备添加一个条目。

您可以在 `/dev/xvdf` 中使用设备名称（例如 `/etc/fstab`），但建议改为使用设备的 128 位通用唯一标识符（UUID）。设备名称可以更改，但 UUID 会在整个分区的使用寿命期间保留。通过使用 UUID，您可以减少系统在硬件重新配置后无法启动的机会。有关更多信息，请参阅[识别 EBS 设备](#)。

### 重启后自动附加附加卷

1. （可选）创建 `/etc/fstab` 文件的备份，以便在编辑时误损坏或删除此文件时使用。

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. 使用 `blkid` 命令查找设备的 UUID。记下要在重新启动后挂载的设备的 UUID。在下一步中您将需要用到它。

例如，以下命令显示有两个设备挂载到实例上，并显示了两个设备的 UUID。

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

对于 Ubuntu 18.04，请使用 `lsblk` 命令。

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. 使用任何文本编辑器（如 `/etc/fstab` 和 `nano`）打开 `vim` 文件。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. 将以下条目添加到 `/etc/fstab` 以在指定的挂载点挂载设备。这些字段是 `blkid`（或用于 Ubuntu 18.04 的 `lsblk`）返回的 UUID 值、挂载点、文件系统以及建议的文件系统挂载选项。有关必填字段的更多信息，请运行 `man fstab` 以打开 `fstab` 手册。

在以下示例中，我们将 UUID 为 `aebf131c-6957-451e-8d34-ec978d9581ae` 的设备挂载到挂载点 `/data`，然后我们使用 `xfs` 文件系统。我们还使用 `defaults` 和 `nofail` 标志。我们指定 `0` 以防止文件系统被转储，并且我们指定 `2` 以指示它是非根设备。



```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2
```

### Note

如果您要在未附加此卷的情况下启动实例（例如，将卷移动到另一个实例之后），`nofail` 附加选项允许该实例即使在卷附加过程中出现错误时也可启动。Debian 衍生物（包括早于 16.04 的 Ubuntu 版本）还必须添加 `nobootwait` 挂载选项。

5. 要检查条目是否有效，请在 `/etc/fstab` 中运行以下命令以卸载设备，然后挂载所有文件系统。如果未产生错误，则说明 `/etc/fstab` 文件正常，您的文件系统会在重启后自动挂载。

```
[ec2-user ~]$ sudo umount /data  
[ec2-user ~]$ sudo mount -a
```

如果收到错误消息，请解决文件中的错误。

### Warning

`/etc/fstab` 文件中的错误可能显示系统无法启动。请勿关闭 `/etc/fstab` 文件中有错误的系统。

如果您无法确定如何更正 `/etc/fstab` 中的错误并且您在此过程的第一步中创建了一个备份文件，则可以使用以下命令从您的备份文件还原。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

## Windows 实例

使用以下任一方法在 Windows 实例上启用卷。

### PowerShell

使所有带有原始分区的 EBS 卷都可用于 Windows PowerShell

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅[连接到 Windows 实例](#)。
2. 在任务栏上，打开“开始”菜单，然后选择“Windows PowerShell”。

3. 在打开的 PowerShell 提示符下使用提供的一系列 Windows PowerShell 命令。此脚本会默认执行以下操作：
  1. 停止 ShellHWDetection 服务。
  2. 枚举分区样式为原始的磁盘。
  3. 创建一个涵盖磁盘和分区类型将支持的最大大小的新分区。
  4. 分配一个可用的驱动器盘符。
  5. 使用指定的文件系统标注将文件系统格式化为 NTFS。
  6. 重新启动 ShellHWDetection 服务。


```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
-PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
Start-Service -Name ShellHWDetection
```

## DiskPart command line tool

### 使 EBS 卷可用于 DiskPart 命令行工具

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅[连接到 Windows 实例](#)。
2. 确定要开放使用的磁盘编号：
  1. 打开“开始”菜单，然后选择“窗口”PowerShell。
  2. 使用 Get-Disk Cmdlet 来检索可用磁盘列表。
  3. 在命令输出中，记下您开放使用的磁盘对应的 Number ( 编号 )。
3. 创建脚本文件来执行 DiskPart 命令：
  1. 打开 Start ( 开始 ) 菜单，然后选择 File Explorer ( 文件管理器 )。
  2. 导航到某个目录 ( 例如 C:\ ) 以存储脚本文件。
  3. 选择或右键单击文件夹中的空白区域以打开对话框，将光标置于 New ( 新建 ) 上方以访问上下文菜单，然后选择 Text Document ( 文本文档 )。
  4. 命名文本文件 diskpart.txt。
4. 将下列命令添加到脚本文件中。您可能需要修改磁盘编号、分区类型、卷标和驱动器盘符。此脚本会默认执行以下操作：

1. 选择磁盘 1 进行修改。
2. 将卷配置为使用主引导记录 ( MBR ) 分区结构。
3. 将卷格式化为 NTFS 卷。
4. 设置卷标。
5. 为卷分配一个驱动器盘符。

 Warning

如果您挂载其中已有数据的卷，请不要格式化卷，否则会删除现有数据。

```
select disk 1
attributes disk clear readonly
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

有关更多信息，请参阅[DiskPart 语法和参数](#)。

5. 打开命令提示符，导航到脚本所在的文件夹，然后运行以下命令以使该卷可用于指定的磁盘：

```
C:\> diskpart /s diskpart.txt
```

## Disk Management utility

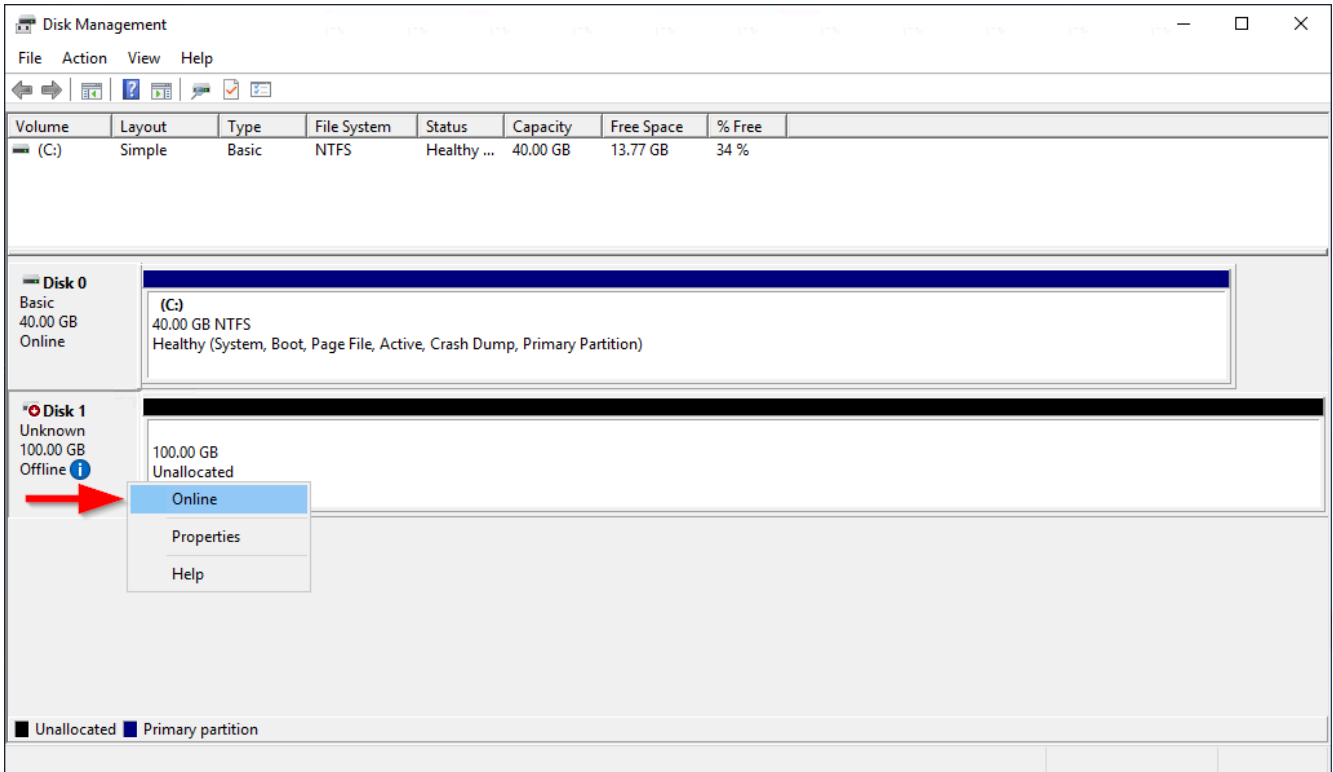
借助磁盘管理实用工具使 EBS 卷可供使用

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅[连接到 Windows 实例](#)。
2. 开启磁盘管理实用工具。在任务栏上，打开 Windows 徽标的上下文（右键单击）菜单，然后选择磁盘管理。

**Note**

在 Windows Server 2008 中，依次选择 Start (开始)、Administrative Tools (管理工具)、Computer Management (计算机管理) 和 Disk Management (磁盘管理)。

3. 将卷联机。在下面的窗格中，在左侧面板中打开 EBS 卷磁盘的上下文 (右键单击) 菜单。选择联机。



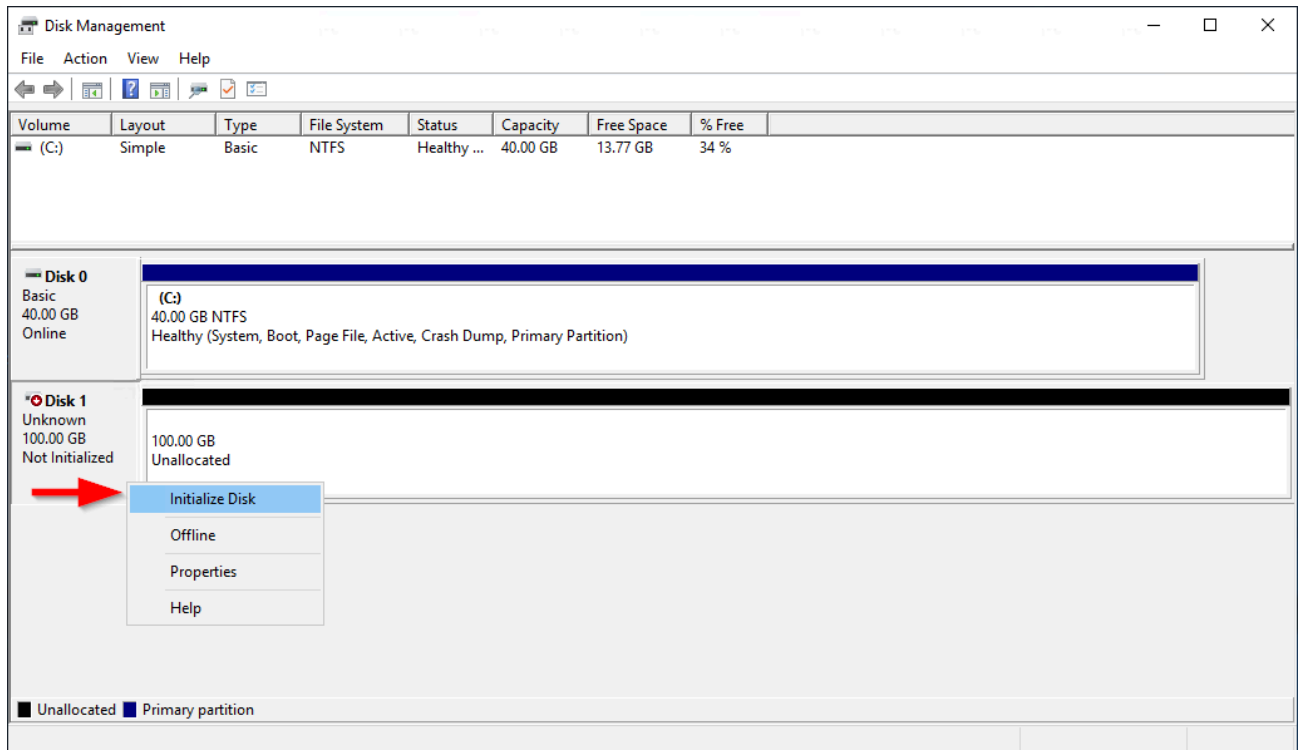
4. (视情况而定) 若未初始化磁盘，您必须初始化磁盘然后才能使用。如果磁盘已初始化，请跳过此步骤。

**Warning**

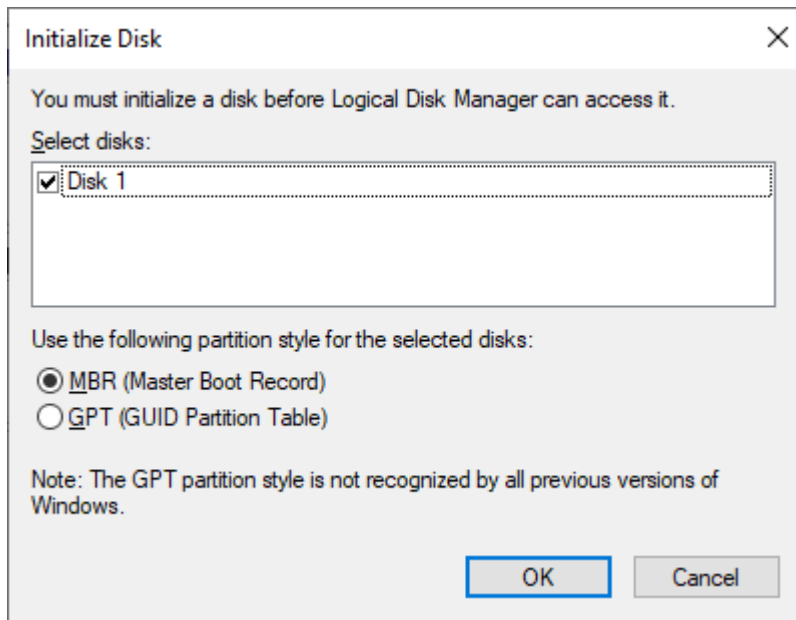
如果在挂载的卷上已包含数据 (例如，公用数据集或通过快照创建的卷)，请不要重新格式化卷，否则，将删除现有的数据。

如果未初始化磁盘，请按以下方式将其初始化：

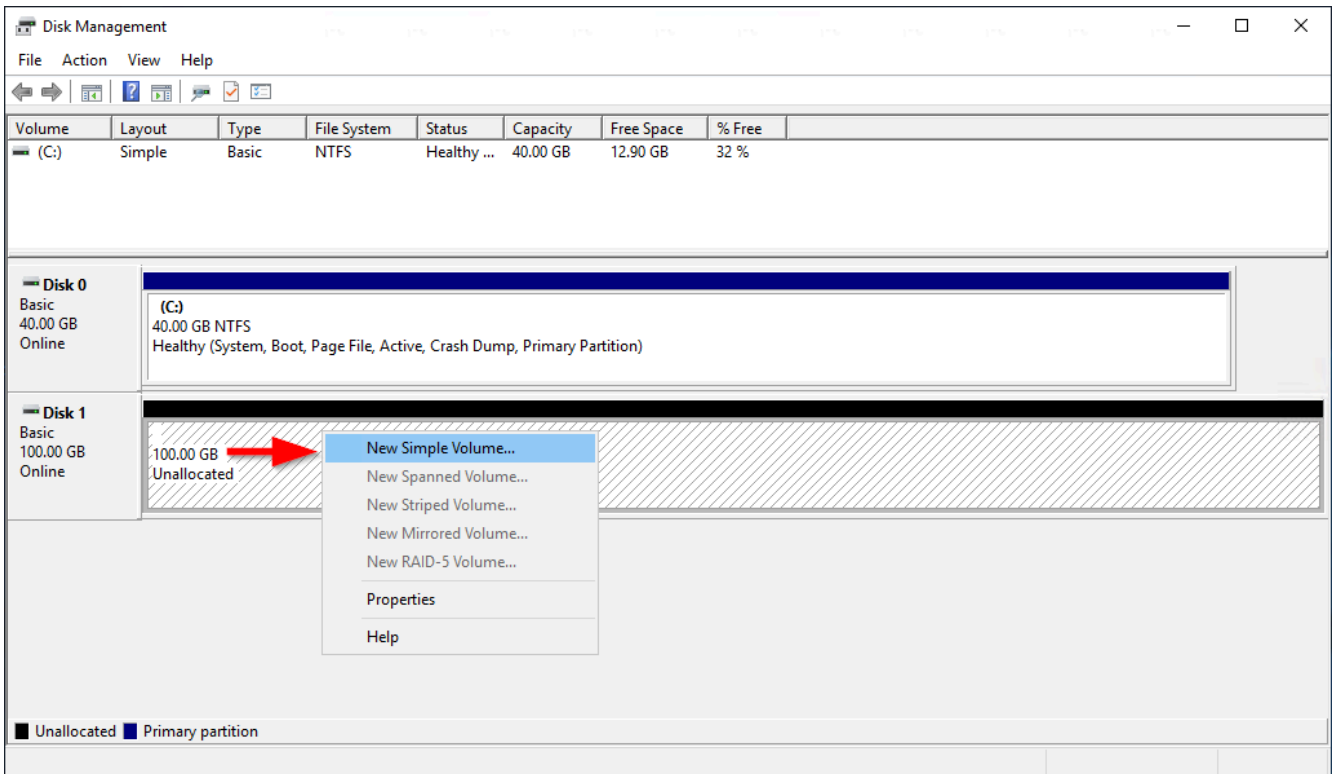
1. 在左侧面板中打开磁盘的上下文 (右键单击) 菜单，然后选择初始化磁盘。



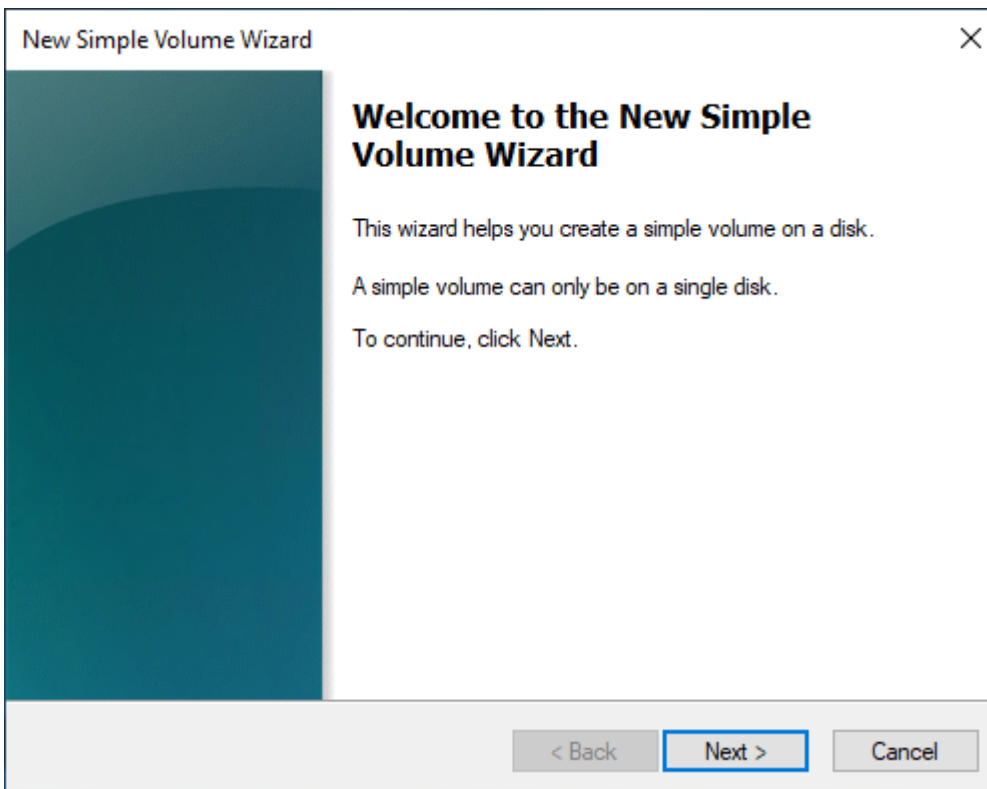
2. 在 Initialize Disk ( 初始化磁盘 ) 对话框中，选择一种分区格式，然后选择 OK ( 确定 )。



5. 在右侧面板中打开磁盘的上下文 ( 右键单击 ) 菜单，然后选择新建简单卷。



- 在 New Simple Volume Wizard ( 新建简单卷向导 ) 中，选择 Next ( 下一步 ) 。



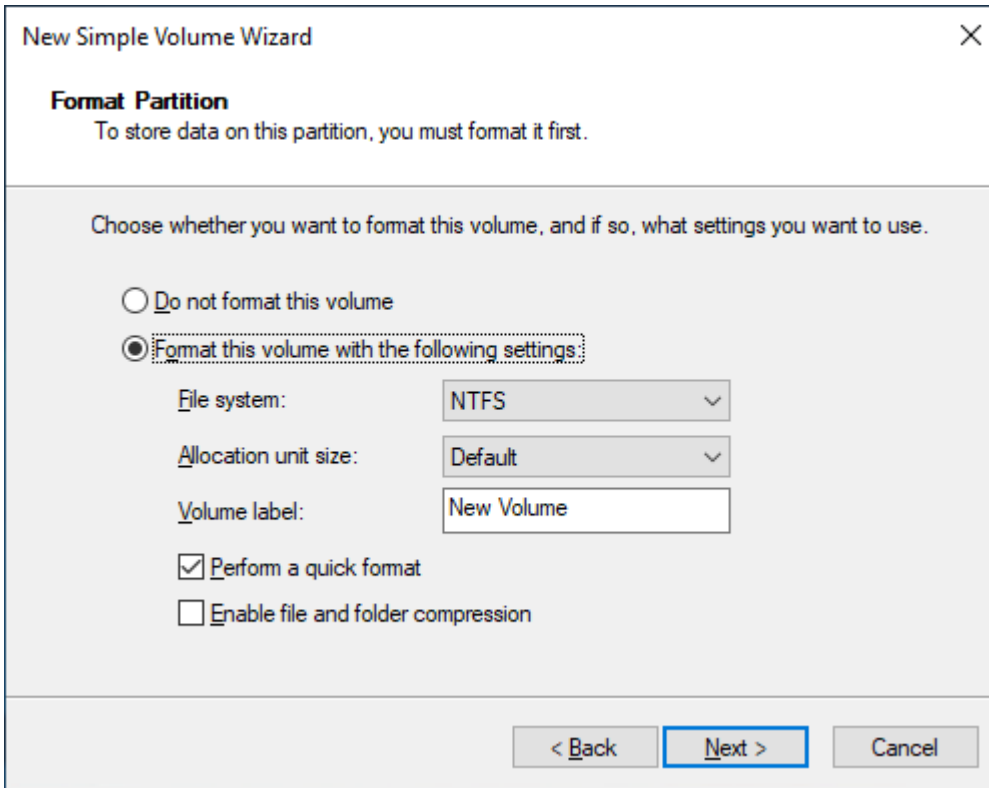
- 如果要原定设置的最大值，请指定 Simple volume size in MB [简单卷大小 ( MB ) ]，然后选择 Next ( 下一步 ) 。

The screenshot shows the 'New Simple Volume Wizard' dialog box with the 'Specify Volume Size' step selected. The title bar reads 'New Simple Volume Wizard' with a close button (X) on the right. Below the title, the section is titled 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three rows of information: 'Maximum disk space in MB:' with the value '102397', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text input field containing '102397' and a spinner control to its right. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

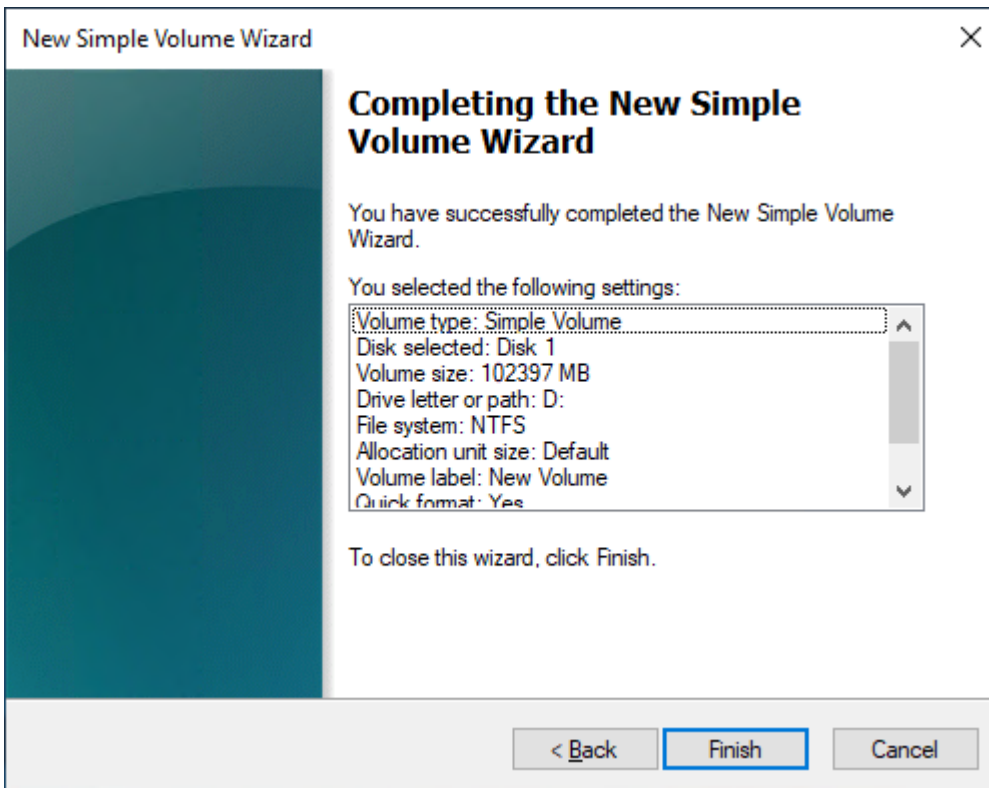
8. 如有必要，在 Assign the following drive letter ( 分配以下驱动器盘符 ) 下拉菜单中指定一个您偏好的驱动器盘符，然后选择 Next ( 下一步 )。

The screenshot shows the 'New Simple Volume Wizard' dialog box with the 'Assign Drive Letter or Path' step selected. The title bar reads 'New Simple Volume Wizard' with a close button (X) on the right. Below the title, the section is titled 'Assign Drive Letter or Path' with the instruction 'For easier access, you can assign a drive letter or drive path to your partition.' The main area contains three radio button options: the first is 'Assign the following drive letter:' with a dropdown menu showing 'D'; the second is 'Mount in the following empty NTFS folder:' with an empty text input field and a 'Browse...' button; the third is 'Do not assign a drive letter or drive path'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

9. 指定 Volume Label ( 卷标 ) 并根据需要调整原定设置 , 然后选择 Next ( 下一步 ) 。



10. 检查设置 , 然后选择 Finish ( 完成 ) 以应用修改并关闭新建简单卷向导。





## 查看关于 Amazon EBS 卷的信息

您可以查看有关您的 EBS 卷的描述信息。例如，您可以查看有关特定区域中所有卷的信息，或者查看有关单个卷的详细信息，包括其大小、卷类型、卷是否加密、加密卷所用的 KMS 密钥以及卷附加到的特定实例。

您可以获得有关您的 EBS 卷的其他信息，例如该实例的操作系统上有多少空间磁盘可用。

### 主题

- [查看卷信息](#)
- [卷状态](#)
- [查看卷指标](#)
- [查看可用磁盘空间](#)

## 查看卷信息

您可以使用以下方法之一查看有关卷的信息。

### Console

使用控制台查看有关卷的信息

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 要减少列表，您可以使用标签和卷属性来筛选卷。选择筛选条件字段，选择标签或卷属性，然后选择筛选条件值。
4. 要查看有关卷的更多信息，请选择其 ID。

使用控制台查看已附加到实例的 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 在 Storage ( 存储 ) 选项卡上，Block devices ( 块储存设备 ) 部分列出了已附加到实例的卷。要查看有关特定卷的信息，请在 Volume ID ( 卷 ID ) 列中选择卷 ID。

## Amazon EC2 Global View

您可以使用 Amazon EC2 全局视图查看启用 AWS 账户的所有区域中的卷。有关更多信息，请参阅 [Amazon EC2 全局视图](#)。

## AWS CLI

要查看有关 EBS 卷的信息，请使用 AWS CLI

使用 [describe-volumes](#) 命令。

## Tools for Windows PowerShell

使用适用于 Windows 的工具查看有关 EBS 卷的信息 PowerShell

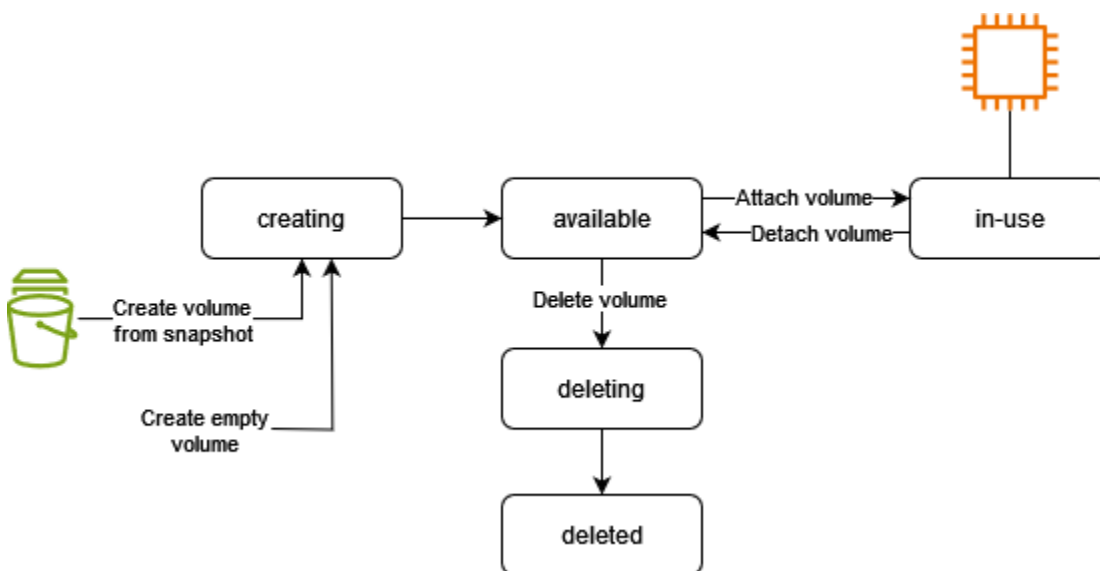
使用 [Get-EC2Volume](#) 命令。

## 卷状态

卷状态描述 Amazon EBS 卷的可用性。您可以在控制台的“卷”页面上的“状态”列中查看卷状态，也可以使用 `desc ribe- AWS CLI volumes` 命令查看卷状态。

从创建直至删除，Amazon EBS 卷会历经不同状态的转换。

下图阐释了卷状态之间的转换。您可以通过 Amazon EBS 快照创建卷，也可以创建空卷。创建卷时，其进入 `creating` 状态。当卷准备就绪后，其进入 `available` 状态。您可以将可用的卷挂载到与该卷位于相同可用区中的实例。必须先分离该卷，才能将其删除或挂载到其他实例。如果您不再需要某个卷，可以将其删除。



下表汇总了卷状态。

状态	描述
creating	正在创建卷。
available	卷未连接到实例。
in-use	卷已连接到实例。
deleting	正在删除卷。
deleted	卷被删除。
error	与 EBS 卷有关的底层硬件出现故障，与卷关联的数据不可恢复。有关如何还原卷或恢复卷上的数据的信息，请参阅 <a href="#">我的 EBS 卷的状态为“错误”</a> 。

## 查看卷指标

您可以从 Amazon CloudWatch 获取有关您的 EBS 卷的更多信息。有关更多信息，请参阅[亚马逊 EBS 的亚马逊 CloudWatch 指标](#)。

## 查看可用磁盘空间

### Linux 实例

您可以获得有关您的 EBS 卷的其他信息，例如该实例的 Linux 操作系统上有多少空间磁盘可用。例如，使用以下命令：

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

### Tip

您也可以使用 CloudWatch 代理从 Amazon EC2 实例收集磁盘空间使用率指标，而无需连接到该实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的[创建 CloudWatch CloudWatch 代理配置文件和安装代理](#)。如果您需要监控多个实例的磁盘空间使用情况，则可

以使用 Systems Manager 在这些实例上安装和配置 CloudWatch 代理。有关更多信息，请参阅[使用 Systems Manager 安装 CloudWatch 代理](#)。

有关在 Windows 实例上查看可用磁盘空间的信息，请参阅 Amazon EC2 用户指南中的[查看可用磁盘空间](#)。

## Windows 实例

您可以获得有关您的 EBS 卷的其他信息，例如该实例的 Windows 操作系统上有多少空间磁盘可用。例如，您可以通过打开文件浏览器并选择此 PC 以查看可用磁盘空间。

您还可以使用以下 `dir` 命令并检查输出的最后一行来查看可用磁盘空间：

```
C:\> dir C:
Volume in drive C has no label.
Volume Serial Number is 68C3-8081

Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
                0 File(s)                0 bytes
                13 Dir(s)  18,113,662,976 bytes free
```

您还可以使用以下 `fsutil` 命令查看可用磁盘空间：

```
C:\> fsutil volume diskfree C:
Total # of free bytes      : 18113204224
Total # of bytes          : 32210153472
```

```
Total # of avail free bytes : 18113204224
```

### Tip

您也可以使用 CloudWatch 代理从 Amazon EC2 实例收集磁盘空间使用率指标，而无需连接到该实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的[创建 CloudWatch CloudWatch 代理配置文件和安装代理](#)。如果您需要监控多个实例的磁盘空间使用情况，则可以使用 Systems Manager 在这些实例上安装和配置 CloudWatch 代理。有关更多信息，请参阅[使用 Systems Manager 安装 CloudWatch 代理](#)。

有关在 Linux 实例上查看可用磁盘空间的信息，请参阅 Amazon EC2 用户指南中的[查看可用磁盘空间](#)。

## 使用 Amazon EBS 弹性卷修改卷

通过使用 Amazon EBS 弹性卷，您可以增加卷大小，更改卷类型或调整 EBS 卷的性能。如果您的实例支持弹性卷，您可以执行这些操作，而无需分离卷或重新启动实例。这样，您就可以在更改生效时继续使用应用程序。

修改卷配置是免费的。卷修改开始后，您需要支付新卷配置的费用。有关更多信息，请参阅[Amazon EBS 定价](#)页面。

### 内容

- [EBS 卷修改要求](#)
- [请求对您的 EBS 卷进行修改](#)
- [监控 EBS 卷修改的进度](#)
- [调整 EBS 卷大小后扩展文件系统](#)

## EBS 卷修改要求

您修改 Amazon EBS 卷时存在以下要求和限制。若要了解有关 EBS 卷的常规要求的更多信息，请参阅[针对 EBS 卷的大小和配置的限制](#)。

### 主题

- [支持的实例类型](#)

- [操作系统](#)
- [限制](#)

## 支持的实例类型

以下实例上支持弹性卷：

- 所有[当前一代实例](#)
- 下面这些上一代的实例：C1、C3、C4、G2、I2、M1、M3、M4、R3 和 R4

如果您的实例类型不支持弹性卷，请参阅[在不支持弹性卷的情况下修改 EBS 卷](#)。

## 操作系统

以下操作系统要求适用：

### Linux

Linux AMI 需要将 GUID 分区表 ( GPT ) 和 GRUB 2 用于 2TiB ( 2048GiB ) 或更大的引导卷。现在的很多 Linux AMI 仍使用 MBR 分区方案，此方案仅支持最高 2 TiB 的引导卷大小。如果您的实例不通过大于 2 TiB 的引导卷启动，您要使用的 AMI 可能限制为小于 2 TiB 的引导卷大小。非引导卷对 Linux 实例没有这种限制。有关影响 Windows 卷的[要求，请参阅亚马逊 EC2 用户指南中的 Windows 卷要求](#)。

在尝试调整超过 2 TiB 的引导卷大小之前，您可以通过在您的实例上运行以下命令来决定该卷是使用 MBR 分区还是使用 GPT 分区：

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

使用 GPT 分区的 Amazon Linux 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.10
```

```
Partition table scan:  
  MBR: protective  
  BSD: not present  
  APM: not present  
  GPT: present
```

```
Found valid GPT with protective MBR; using GPT.
```

使用 MBR 分区的 SUSE 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.8
```

```
Partition table scan:
```

```
MBR: MBR only  
BSD: not present  
APM: not present  
GPT: not present
```

## Windows

默认情况下，Windows 使用主启动记录 ( MBR ) 分区表来初始化卷。由于 MBR 只支持小于 2TiB ( 2048GiB ) 的卷，Windows 会阻止您将 MBR 卷大小调整为超过此限制。在这种情况下，Windows 磁盘管理实用程序中的磁盘管理选项会禁用。如果您使用 AWS Management Console 或 AWS CLI 创建超出大小限制的 MBR 分区卷，Windows 将无法检测或使用额外的空间。有关影响 Linux 卷的[要求，请参阅 Amazon EC2 用户指南中的 Linux 卷要求](#)。

要克服此限制，您可以使用 GUID 分区表 ( GPT ) 创建新的较大的卷并从原始 MBR 卷复制数据。

### 创建 GPT 卷

1. 在 EC2 实例的可用区中创建新的具有所需大小的空卷，并将其附加到您的实例上。

#### Note

新卷不能是从快照恢复的卷。

2. 登录到您的 Windows 系统并打开磁盘管理 ( diskmgmt.exe )。
3. 打开新磁盘的上下文 ( 右键单击 ) 菜单并选择在线。
4. 在初始化磁盘窗口中，选择新磁盘，并依次选择 GPT ( GUID 分区表 )、确定。
5. 初始化完成后，使用 robocopy 或 teracopy 等工具将数据从原始卷复制到新卷。
6. 在 Disk Management 中，将盘符更改为适当的值，并使旧卷脱机。
7. 在 Amazon EC2 控制台中，从实例上分离旧卷，重启实例以验证它是否正常工作，然后删除旧卷。

## 限制

- 卷修改过程中可以请求的最大聚合存储空间存在限制。有关更多信息，请参阅 Amazon Web Services 一般参考中 [Amazon EBS 服务限额](#)。
- 修改卷后，必须等待至少六个小时并确保卷处于 in-use 或 available 状态，然后再对同一个卷进行其他修改。
- 修改 EBS 卷可能需要几分钟到几小时才能完成，具体视应用的配置更改而定。大小为 1TiB 的 EBS 卷通常最多可能需要六个小时即可得到修改。但是，在其他情况下，相同的卷可能需要 24 小时或更长时间。修改卷所需的时间并不总是线性扩展。因此，较大的卷可能需要较短时间，而较小的卷却可能需要较长时间。
- 如果卷是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的，您必须初始化弹性卷支持。有关更多信息，请参阅 [初始化弹性卷支持](#)。
- 如果在尝试修改 EBS 卷时遇到错误消息，或者要修改附加到上一代实例类型的 EBS 卷，请执行以下步骤之一：
  - 对于非根卷，将卷与实例分离，应用修改，然后重新附加卷。
  - 对于根卷，停止实例，应用修改，然后重新启动实例。
- 尚未完全初始化的卷的修改时间会增加。有关更多信息，请参阅 [初始化 Amazon EBS 卷](#)。
- 新卷大小不能超过其文件系统和分区方案所支持的容量。有关更多信息，请参阅 [针对 EBS 卷的大小和配置的限制](#)。
- 如果要修改卷类型，则大小和性能必须在目标卷类型的限制范围内。有关更多信息，请参阅 [Amazon EBS 卷类型](#)
- 您无法减小 EBS 卷的大小。但是，您可以创建较小的卷，然后使用应用程序级工具 [如 rsync ( Linux 实例 ) 或 robocopy ( Windows 实例 ) ] 将数据迁移到该卷。
- 在现有 io1 或 io2 卷预置超 32,000 IOPS 后，您可能需要分离并重新连接卷，或重新启动实例以查看完整的性能改进。
- 挂载到 [基于 Nitro 系统构建的实例](#) 的 io2 卷支持最大 64 TiB 的大小和最多 256000 的 IOPS。挂载到其他实例的 io2 卷支持最大 16 TiB 的大小和最多 64000 的 IOPS，但只能实现最高 32000 IOPS 的性能。
- 您不能修改启用多重挂载的 io2 卷的卷类型。
- 您无法修改启用了多重挂载的 io1 卷的卷类型、大小或预置 IOPS。
- 无法将类型 io1、io2、gp2、gp3 或 standard 的根卷修改为 st1 或 sc1 卷，即使已将它与实例分离也是如此。
- 虽然 m3.medium 实例完全支持卷修改，但 m3.large、m3.xlarge 和 m3.2xlarge 实例可能不支持所有卷修改功能。



## 请求对您的 EBS 卷进行修改

对于弹性卷，您可以在不分离 Amazon EBS 卷的情况下动态增加卷的大小或降低其性能，以及修改卷类型。

修改卷时使用以下过程：

1. ( 可选 ) 在修改包含有用数据的卷之前，最佳实践是创建卷的快照 ( 如果您需要回滚您的更改 )。有关更多信息，请参阅[创建 Amazon EBS 快照](#)。
2. 请求卷修改。
3. 监控卷修改进度。有关更多信息，请参阅[监控 EBS 卷修改的进度](#)。
4. 如果修改了卷的大小，请扩展卷的文件系统以利用增加的存储容量。有关更多信息，请参阅[调整 EBS 卷大小后扩展文件系统](#)。

### 目录

- [使用弹性卷修改 EBS 卷](#)
- [初始化弹性卷支持 \( 如果需要 \)](#)
- [在不支持弹性卷的情况下修改 EBS 卷](#)

### 使用弹性卷修改 EBS 卷

#### 注意事项

修改 卷时请牢记以下事项：

- 修改卷后，必须等待至少六个小时并确保卷处于 in-use 或 available 状态，然后再对同一个卷进行其他修改。
- 修改 EBS 卷可能需要几分钟到几小时才能完成，具体视应用的配置更改而定。大小为 1TiB 的 EBS 卷通常最多可能需要六个小时即可得到修改。但是，在其他情况下，相同的卷可能需要 24 小时或更长时间。修改卷所需的时间并不总是线性扩展。因此，较大的卷可能需要较短时间，而较小的卷却可能需要较长时间。
- 提交卷修改请求后，您将无法取消该请求。
- 您只能增加卷的大小。您无法减小卷的大小。
- 您可以提高或降低卷的性能。
- 如果您没有修改卷类型，则卷的大小和性能修改必须在当前卷类型的限制范围内。如果您更改卷类型，则卷的大小和性能修改必须在目标卷类型的限制范围内

- 如果您将卷类型从 gp2 更改为 gp3，并且您未指定 IOPS 或吞吐量性能，则 Amazon EBS 将自动预调配与源 gp2 卷的性能或基准 gp3 性能相当的性能（以二者中较高者为准）。

例如，如果您将具有 250 MiB/s 吞吐量和 1500 IOPS 的 500 GiB gp2 卷修改为 gp3，但未指定 IOPS 或吞吐量性能，Amazon EBS 会自动预调配具有 3000 IOPS（基准 gp3 IOPS）和 250 MiB/s（用于匹配源 gp2 卷吞吐量）的 gp3 卷。

要修改 EBS 卷，请使用以下方法之一。

## Console

### 使用控制台修改 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择要修改的卷，然后选择 Actions（操作）、Modify Volume（修改卷）。
4. Modify Volume（修改卷）窗口显示卷 ID 和卷的当前配置，包括类型、大小、IOPS 和吞吐量。设置新的配置值，如下所述：
  - 要修改类型，请为 Volume type（卷类型）选择一个值。
  - 要修改大小，请为大小输入新值。
  - （仅限于 gp3、io1 和 io2）要修改 IOPS，为 IOPS 输入新值。
  - （仅限于 gp3）要修改吞吐量，为 Throughput（吞吐量）输入新值。
5. 完成更改卷设置后，请选择修改。当系统提示您确认时，选择 Modify（修改）。

6.

#### Important

如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅 [调整 EBS 卷大小后扩展文件系统](#)。

7. （仅限 Windows 实例）如果您在没有 NVMe 驱动程序的实例上增加 AWS NVMe 卷的大小，则必须重启该实例才能让 Windows 看到新的卷大小。有关安装 AWS NVMe 驱动程序的更多信息，请参阅 [适用于 Windows 实例的 AWS NVMe 驱动程序](#)。

## AWS CLI

### 要使用修改 EBS 卷 AWS CLI

使用 `modify-volume` 命令修改卷的一个或多个配置设置。如果您有一个类型为 gp2 且大小为 100 GiB 的卷，以下命令会将其配置更改为类型为 io1、包含 10000 IOPS 且大小为 200 GiB 的卷。

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-id vol-111111111111111111
```

下面是示例输出：

```
{
  "VolumeModification": {
    "TargetSize": 200,
    "TargetVolumeType": "io1",
    "ModificationState": "modifying",
    "VolumeId": "vol-111111111111111111",
    "TargetIops": 10000,
    "StartTime": "2017-01-19T22:21:02.959Z",
    "Progress": 0,
    "OriginalVolumeType": "gp2",
    "OriginalIops": 300,
    "OriginalSize": 100
  }
}
```

#### Important

如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅 [调整 EBS 卷大小后扩展文件系统](#)。

### 初始化弹性卷支持（如果需要）

您必须先使用以下操作之一初始化卷修改支持，然后才能修改在 UTC 时间 2016 年 11 月 3 日 23:40 前附加到实例的卷：

- 分离和附加卷
- 停止和启动实例

使用以下过程之一来确定您的实例是否已准备好进行卷修改。

## Console

使用控制台确定您的实例是否已准备就绪

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择实例。
3. 选择显示/隐藏列图标（齿轮）。选择启动时间属性列，然后选择确认。
4. 按 Launch Time 列对实例列表进行排序。对于在截止日期之前启动的每个实例，选择存储选项卡，并检查连接时间列以查看其卷附加的时间。

## AWS CLI

使用 CLI 确定您的实例是否已准备就绪

使用以下 [describe-instances](#) 命令确定卷是否是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的。

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" --output text
```

每个实例的输出的第一行都将显示其 ID，无论实例是否在截止日期前启动（True 或 False）。第一行后跟一行或多行，以显示是否在截止日期前已附加每个 EBS 卷（True 或 False）。在以下示例输出中，您必须为第一个实例初始化卷修改，因为该实例是在截止日期前启动的，并且其根卷是在截止日期前附加的。其他实例已准备就绪，因为它们是在截止日期后启动的。

```
i-e905622e          True
True
i-719f99a8          False
True
i-006b02c1b78381e57  False
False
False
i-e3d172ed          False
True
```

## 在不支持弹性卷的情况下修改 EBS 卷

如果您使用的是支持的实例类型，则可以使用弹性卷来在不分离 Amazon EBS 卷的情况下动态修改卷的大小、性能和卷类型。

如果您无法使用弹性卷但需要修改根（启动）卷，则必须停止实例，修改卷，然后重新启动实例。

实例启动之后，可以检查文件系统大小，看实例是否识别这个更大的卷空间。在 Linux 上，请使用 `df -h` 命令检查文件系统大小。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      7.9G  943M  6.9G  12% /
tmpfs           1.9G   0    1.9G   0% /dev/shm
```

如果大小没有反映新扩展的卷，则必须扩展设备的文件系统，以便实例可以使用新的空间。有关更多信息，请参阅 [调整 EBS 卷大小后扩展文件系统](#)。

您可能需要将卷联机才能使用 Windows 实例。有关更多信息，请参阅 [使 Amazon EBS 卷可供使用](#)。您无需重新格式化卷。

## 监控 EBS 卷修改的进度

当您修改 EBS 卷时，它将经历一系列状态。卷将依次进入 `modifying` 状态、`optimizing` 状态和 `completed` 状态。此时，卷已准备好做进一步的修改。

### Note

在极少数情况下，瞬态 AWS 故障会导致 `failed` 状态。这并不指示卷的运行状况；它仅指示卷修改失败。如果发生这种情况，请重试卷修改。

当卷处于 `optimizing` 状态时，卷性能介于源配置规范和目标配置规范之间。过渡卷的性能将不会低于源卷的性能。如果您降级 IOPS，则过渡卷的性能不会低于目标卷的性能。

卷修改更改将生效，如下所示：

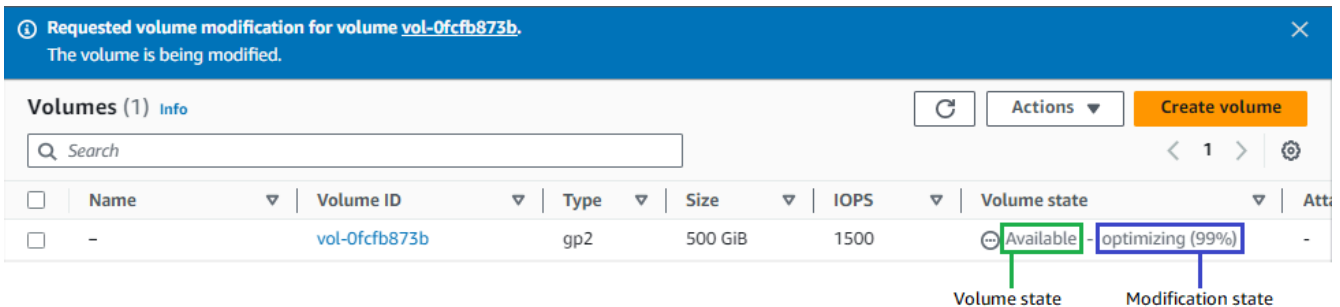
- 大小更改通常需要几秒钟才能完成，并在卷转为 `Optimizing` 状态后生效。
- 性能（IOPS）更改可能需要几分钟到几小时才能完成，具体视所做的配置更改而定。
- 在某些情况下，新配置生效最长需要 24 个小时，例如卷未完全初始化时。通常，完全使用的 1 TiB 卷需要约 6 个小时才能迁移到新的性能配置。

要监控卷修改的进度，请使用以下方法之一。

## Console

使用 Amazon EC2 控制台监控修改的进度

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 详细信息选项卡的卷状态列和卷状态字段包含如下格式的信息：**### - #####**（#####百分比）。下图显示了卷和卷修改状态。



可能的卷状态包括 creating、available、in-use、deleting、deleted 和 error。

可能的修改状态为 modifying、optimizing 和 completed。

修改完成后，仅显示卷状态。不再显示修改状态和进度。

## AWS CLI

要使用监控修改的进度 AWS CLI

使用 [describe-volumes-modifications](#) 命令查看一个或多个卷修改的进度。以下示例描述了两个卷的卷修改。

```
aws ec2 describe-volumes-modifications --volume-ids vol-11111111111111111111 vol-22222222222222222222
```

在以下示例输出中，卷修改仍处于 modifying 状态。以百分比形式报告进展情况。

```
{
```

```

"VolumesModifications": [
  {
    "TargetSize": 200,
    "TargetVolumeType": "io1",
    "ModificationState": "modifying",
    "VolumeId": "vol-11111111111111111",
    "TargetIops": 10000,
    "StartTime": "2017-01-19T22:21:02.959Z",
    "Progress": 0,
    "OriginalVolumeType": "gp2",
    "OriginalIops": 300,
    "OriginalSize": 100
  },
  {
    "TargetSize": 2000,
    "TargetVolumeType": "sc1",
    "ModificationState": "modifying",
    "VolumeId": "vol-22222222222222222",
    "StartTime": "2017-01-19T22:23:22.158Z",
    "Progress": 0,
    "OriginalVolumeType": "gp2",
    "OriginalIops": 300,
    "OriginalSize": 1000
  }
]
}

```

下一个示例描述了修改状态为 `optimizing` 或 `completed` 的所有卷，然后筛选和格式化结果以只显示于 2017 年 2 月 1 日及之后做出的修改：

```

aws ec2 describe-volumes-modifications --filters Name=modification-
state,Values="optimizing","completed" --query "VolumesModifications[?
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"

```

以下是包含有关两个卷的信息的示例输出：

```

[
  {
    "STATE": "optimizing",
    "ID": "vol-06397e7a0eEXAMPLE"
  },
  {
    "STATE": "completed",

```

```
    "ID": "vol-ba74e18c2aEXAMPLE"
  }
]
```

## CloudWatch Events console

使用“CloudWatch 事件”，您可以为卷修改事件创建通知规则。您可以使用规则生成使用 [Amazon SNS](#) 的通知消息，或调用 [Lambda 函数](#) 来响应匹配事件。尽最大努力发出事件。

使用“CloudWatch 事件”监控修改进度

1. 打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 依次选择 Events、Create rule。
3. 对于 Build event pattern to match events by service，选择 Custom event pattern。
4. 对于构建自定义事件模式，将内容替换为以下内容并选择保存。

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ],
  "detail": {
    "event": [
      "modifyVolume"
    ]
  }
}
```

下面是示例事件数据：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "2017-01-12T21:09:07Z",
  "region": "us-east-1",
  "resources": [
```



```
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
  ],
  "detail": {
    "result": "optimizing",
    "cause": "",
    "event": "modifyVolume",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
  }
}
```

## 调整 EBS 卷大小后扩展文件系统

[增加 EBS 卷的大小后](#)，您必须将分区和文件系统扩展到新的较大大小。您可以在卷进入 optimizing 状态后立即执行此操作。

### 开始前的准备工作

- 如果需要回滚更改，则创建卷的快照。有关更多信息，请参阅 [创建 Amazon EBS 快照](#)。
- 确认卷修改成功并且其处于 optimizing 或 completed 状态。有关更多信息，请参阅 [监控 EBS 卷修改的进度](#)。
- 确保卷已附加到实例，并且已格式化和挂载。有关更多信息，请参阅 [格式化并挂载附加的卷](#)。
- ( 仅限 Linux 实例 ) 如果在 Amazon EBS 卷上使用逻辑卷，则必须使用逻辑卷管理器 ( LVM ) 来扩展逻辑卷。有关如何执行此操作的说明，请参阅 [如何在整个 EBS 卷上创建 LVM 逻辑卷？](#) 中的扩展逻辑卷部分 AWS 知识中心文章。

### Linux 实例

#### Note

以下说明将引导您完成为 Linux 扩展 XFS 和 Ext4 文件系统的过程。有关扩展其他文件系统的信息，请参阅相关文档。

如果卷有分区，则必须先扩展分区，才能在 Linux 上扩展文件系统。

### 扩展 EBS 卷的文件系统

按照以下过程扩展调整大小后的卷的文件系统。

请注意，Xen 实例和[基于 Nitro 系统构建的实例](#)的设备和分区命名有所不同。要确定实例是基于 Xen 还是基于 Nitro，请使用 [describe-instance-types](#) AWS CLI 命令，如下所示：

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-type instance_type --query
"InstanceTypes[].Hypervisor"
```

nitro 表示实例基于 Nitro。xen 或 xen-on-nitro 则表示实例基于 Xen。

扩展 EBS 卷的文件系统

1. [连接到您的实例](#)。
2. 如果需要，调整分区的大小。为此，请执行以下操作：
  - a. 检查卷是否有分区。使用 lsblk 命令。

Nitro instance example

在以下示例输出中，根卷 (nvme0n1) 有两个分区 (nvme0n1p1 和 nvme0n1p128)，而额外的卷 (nvme1n1) 没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0   0  30G  0 disk /data
nvme0n1       259:1   0  16G  0 disk
##nvme0n1p1   259:2   0   8G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
```

Xen instance example

在以下示例输出中，根卷 (xvda) 有一个分区 (xvda1)，而额外的卷 (xvdf) 没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME     MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0   0  16G  0 disk
##xvda1  202:1   0   8G  0 part /
xvdf     202:80  0  24G  0 disk
```

如果该卷具有分区，则继续执行以下步骤 (2b)。如果该卷没有分区，请跳过步骤 2b、2c 和 2d，然后继续执行步骤 3。

**i** 故障排除技巧

如果没有在命令输出中看到该卷，请确保该卷已[附加到实例](#)并且[已格式化和挂载](#)。

- b. 检查是否需要扩展分区。在上一步的 `lsblk` 命令输出中，比较分区大小和卷大小。

如果分区大小小于卷大小，则继续执行下一步。如果分区大小等于卷大小，则无法扩展分区。

**i** 故障排除技巧

如果卷仍然反映原始大小，则请[确认卷修改成功](#)。

- c. 扩展分区。使用 `growpart` 命令并指定要扩展的分区。

Nitro instance example

例如，若要扩展名为 `nvme0n1p1` 的分区，请使用以下命令。

**⚠ Important**

请注意，设备名称 (`nvme0n1`) 和分区编号 (`1`) 之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Xen instance example

例如，若要扩展名为 `xvda1` 的分区，请使用以下命令。

**⚠ Important**

请注意，设备名称 (`xvda`) 和分区编号 (`1`) 之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

### 故障排除技巧

- `mkdir: cannot create directory '/tmp/growpart.31171': No space left on device FAILED: failed to make temp dir`: 表示卷上没有足够的可用磁盘空间供 `growpart` 创建执行调整大小所需的临时目录。请释放一些磁盘空间并重试。
- `must supply partition-number`: 表示您指定的分区不正确。使用 `lsblk` 命令以确认分区名称，并确保在设备名称和分区编号之间输入空格。
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown`: 表示分区已经扩展了整个卷，无法再扩展。[确认卷修改成功](#)。

- d. 验证是否已扩展分区。使用 `lsblk` 命令。分区大小现在应等于卷大小。

#### Nitro instance example

以下示例输出显示卷 (`nvme0n1`) 和分区 (`nvme0n1p1`) 的大小相同 (16 GB)。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0   30G  0 disk /data
nvme0n1       259:1    0   16G  0 disk
##nvme0n1p1   259:2    0   16G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
```

#### Xen instance example

以下示例输出显示卷 (`xvda`) 和分区 (`xvda1`) 的大小相同 (16 GB)。

```
[ec2-user ~]$ sudo lsblk
NAME     MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0   16G  0 disk
##xvda1  202:1    0   16G  0 part /
xvdf     202:80   0   24G  0 disk
```

### 3. 扩展文件系统。

- a. 获取需要扩展的文件系统的名称、大小、类型和挂载点。使用 `df -hT` 命令。

## Nitro instance example

以下示例输出显示了 `/dev/nvme0n1p1` 文件系统的大小为 8 GB，其类型为 `xfs`，其挂载点是 `/`。

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
...
```

## Xen instance example

以下示例输出显示了 `/dev/xvda1` 文件系统的大小为 8 GB，其类型为 `ext4`，其挂载点是 `/`。

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/xvda1      ext4  8.0G  1.9G  6.2G  24%   /
/dev/xvdf1      xfs   24.0G  45M  8.0G   1%   /data
...
```

- b. 扩展文件系统的命令因文件系统类型而异。根据您在上一步中记录的文件系统类型选择以下正确命令。
- [XFS 文件系统] 使用 `xfs_growfs` 命令并指定您在上一步中记录的文件系统的挂载点。

### Nitro and Xen instance example

例如，若要扩展挂载在 `/` 上的文件系统，请使用以下命令。

```
[ec2-user ~]$ sudo xfs_growfs -d /
```

#### 故障排除技巧

- `xfs_growfs: /data is not a mounted XFS filesystem`: 表示指定的挂载点不正确，或者文件系统不是 XFS。若要验证挂载点和文件系统类型，请使用 `df -hT` 命令。

- `data size unchanged, skipping`：表示文件系统已经扩展了整个卷。如果卷没有分区，则请[确认卷修改成功](#)。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [Ext4 文件系统] 使用 `resize2fs` 命令并指定您在上一步中记录的文件系统的名称。

Nitro instance example

例如，若要扩展名为 `/dev/nvme0n1p1` 的挂载文件系统，请使用以下命令。

```
[ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
```

Xen instance example

例如，若要扩展名为 `/dev/xvda1` 的挂载文件系统，请使用以下命令。

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
```

#### 故障排除技巧

- `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1`：表示文件系统不是 Ext4。若要验证文件系统类型，请使用 `df -hT` 命令。
- `open: No such file or directory while opening /dev/xvdb1`：表示您指定的分区不正确。若要验证分区，请使用 `df -hT` 命令。
- `The filesystem is already 3932160 blocks long. Nothing to do!`：表示文件系统已经扩展了整个卷。如果卷没有分区，则请[确认卷修改成功](#)。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [其他文件系统]，请参阅文件系统的文档，了解相关说明。

- c. 验证是否已扩展文件系统。使用 `df -hT` 命令并确认文件系统大小等于卷大小。

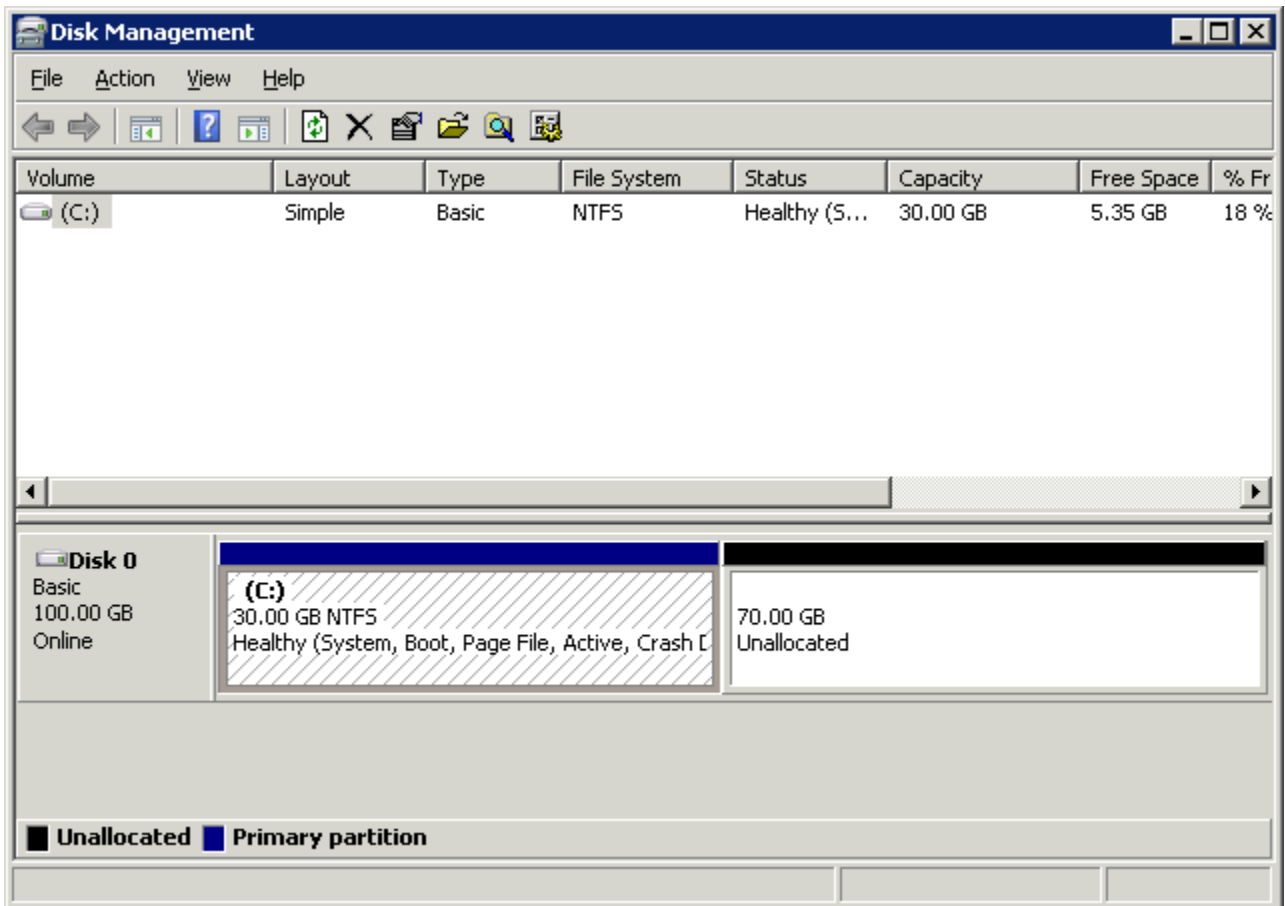
## Windows 实例

使用以下任一方法在 Windows 实例上扩展文件系统。

## Disk Management utility

### 使用磁盘管理扩展文件系统

1. 在扩展包含有用数据的文件系统之前，最佳实践是创建包含它的卷的快照 (如果您需要回滚您的更改)。有关更多信息，请参阅[创建 Amazon EBS 快照](#)。
2. 使用远程桌面登录 Windows 实例。
3. 在运行对话框中，输入 diskmgmt.msc 并按 Enter。然后，磁盘管理实例程序随之打开。



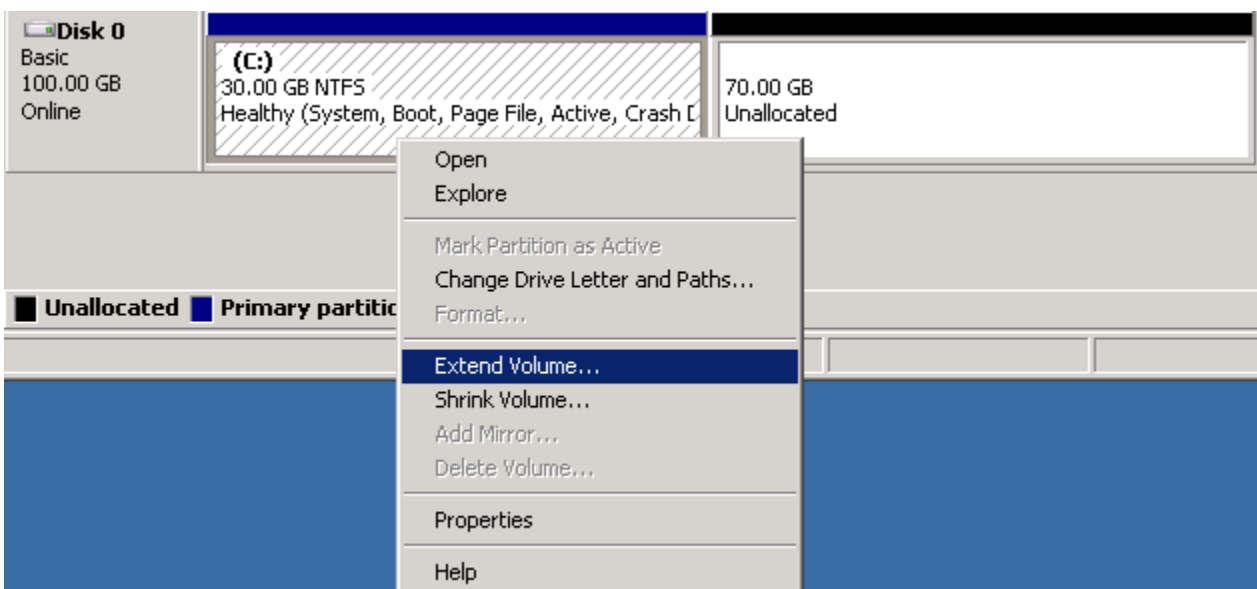
4. 在 Disk Management 菜单上，选择 Action、Rescan Disks。
5. 打开扩展驱动器的上下文 (右键单击) 菜单，然后选择扩展卷。

#### Note

如果出现以下情况，说明扩展卷可能已被禁用 (灰显)：

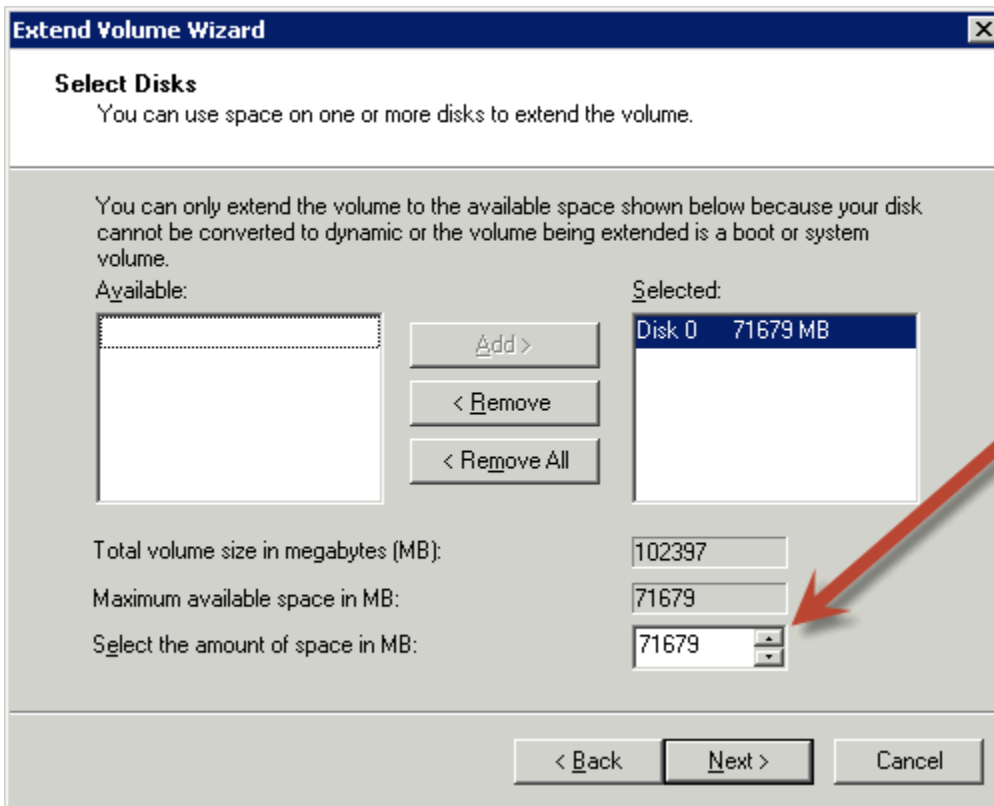
- 未分配的空间不在驱动器旁边。未分配的空间必须与要扩展的驱动器的右侧相邻。

- 卷使用主引导记录 ( MBR ) 分区样式，大小已经为 2TB。使用 MBR 的卷的大小不能超过 2TB。



6. 在扩展卷向导中，选择下一步。对于 Select the amount of space in MB，输入扩展卷的兆字节数。通常，您可指定最大可用空间。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。





- 如果您在没有 AWS NVMe 驱动程序的实例上增加了 NVMe 卷的大小，则必须重启实例才能使 Windows 发现新的卷大小。有关安装 AWS NVMe 驱动程序的更多信息，请参阅[适用于 Windows 实例的 AWS NVMe 驱动程序](#)。

## PowerShell

使用以下步骤使用扩展 Windows 文件系统 PowerShell。

### 使用扩展文件系统 PowerShell

- 在扩展包含有用数据的文件系统之前，最佳实践是创建包含它的卷的快照（如果您需要回滚您的更改）。有关更多信息，请参阅[创建 Amazon EBS 快照](#)。
- 使用远程桌面登录 Windows 实例。
- 以管理员 PowerShell 身份运行。
- 运行 Get-Partition 命令。PowerShell 返回每个分区的相应分区号、驱动器号、偏移量、大小和类型。请注意要扩展的分区的盘符。
- 运行以下命令重新扫描磁盘。

```
"rescan" | diskpart
```

6. 运行以下命令，使用您在步骤 4 中记下的驱动器号代替 **<drive-letter>**。PowerShell 返回允许的分区的最小和最大大小（以字节为单位）。

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

7. 要将分区扩展到指定的量，请运行以下命令，并在 **<size>** 的位置输入卷的新大小。您可以输入以 KB、MB 和 GB 为单位的大小，例如 50GB。

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

要将分区扩展到最大可用大小，请运行以下命令。

```
Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize  
-DriveLetter <drive-letter>).SizeMax
```

以下 PowerShell 命令显示了将文件系统扩展到特定大小的完整命令和响应流。

```

PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset                Size  Type
-----
1                 C             1048576              30 GB  IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset                Size  Type
-----
1                 D             1048576               8 MB  IFS

PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-----
8388608 107372085248

PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset                Size  Type
-----
1                 C             1048576              30 GB  IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset                Size  Type
-----
1                 D             1048576              50 GB  IFS

```

以下 PowerShell 命令显示了将文件系统扩展到最大可用大小的完整命令和响应流。

```

PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
PartitionNumber DriveLetter Offset Size Type
-----
1 C 1048576 30 GB IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
PartitionNumber DriveLetter Offset Size Type
-----
1 D 1048576 50 GB IFS

PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin SizeMax
-----
59047936 107372085248

PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
PartitionNumber DriveLetter Offset Size Type
-----
1 C 1048576 30 GB IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
PartitionNumber DriveLetter Offset Size Type
-----
1 D 1048576 100 GB IFS

```

## 将 Amazon EBS 卷与实例分离

您需要将 Amazon Elastic Block Store ( Amazon EBS ) 卷与实例分离，然后才能将其挂载到其他实例或删除该卷。分离卷不会影响卷上的数据。

### 主题

- [注意事项](#)
- [卸载并分离卷](#)
- [故障排除](#)

## 注意事项

- 您可以明确地将 Amazon EBS 卷与实例分离，或终止实例。但是，如果实例正在运行，您首先必须从实例卸载卷。
- 如果 EBS 卷是实例的根设备，则在分离卷之前必须停止该实例。
- 您可以重新附加分离的卷（无需卸载），但可能不能获得相同挂载点。如果分离时正在写入卷，那么卷上的数据可能不同步。
- 分离卷后，只要存储量超过 AWS 免费套餐的限制，您仍需要支付卷存储费用。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](#)。

## 卸载并分离卷

使用以下程序从实例卸载并分离卷。当您需要将卷挂载到不同实例时或当您需要删除卷时，此操作非常有用。

### 步骤

- [第 1 步：卸载卷](#)
- [第 2 步：从实例分离卷](#)
- [第 3 步：（仅限 Windows 实例）卸载离线设备位置](#)

### 第 1 步：卸载卷

#### Linux 实例

从 Linux 实例中，使用以下命令卸载 `/dev/sdh` 设备。

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

#### Windows 实例

按照以下步骤从 Windows 实例中卸载卷。

##### 1. 启动磁盘管理实用工具。

- （Windows Server 2012 及更高版本）在任务栏上，右键单击 Windows 徽标，然后选择磁盘管理。

- ( Windows Server 2008 ) 依次选择开始、管理工具、计算机管理和磁盘管理。
2. 右键单击磁盘 ( 例如, 右键单击磁盘 1 ), 然后选择脱机。等待磁盘状态变为脱机, 然后再打开 Amazon EC2 控制台。

## 第 2 步: 从实例分离卷

要将卷与实例分离, 请使用以下方法之一:

### Console

使用控制台将 EBS 卷分离

1. 通过以下网址打开 Amazon EC2 控制台: <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中, 选择 Volumes。
3. 选择需要分离的卷, 然后选择 Actions ( 操作 )、Detach Volume ( 分离卷 )。
4. 当系统提示进行确认时, 选择分离。

### AWS CLI

要将 EBS 卷与实例分离, 请使用 AWS CLI

卸载卷之后, 使用 [detach-volume](#) 命令。

### Tools for Windows PowerShell

使用适用于 Windows 的工具将 EBS 卷与实例分离 PowerShell

卸载卷后, 使用 [Dismount-EC2Volume](#) 命令。

## 第 3 步: ( 仅限 Windows 实例 ) 卸载离线设备位置

从实例卸载和分离卷时, Windows 会将该设备位置标记为脱机。重新启动后以及停止并重新启动实例后, 设备位置将保持脱机状态。重启实例时, Windows 可能会将其余卷之一挂载到脱机设备位置。这会导致卷在 Windows 中不可用。为了防止这种情况发生, 并确保下次启动 Windows 时所有卷都附加到在线设备位置, 请执行以下步骤:

1. 在实例上, 打开设备管理器。
2. 在设备管理器中, 依次选择查看、显示隐藏的设备。

### 3. 在设备列表中，展开存储控制器节点。

已分离卷挂载到的设备位置命名为 AWS NVMe Elastic Block Storage Adapter，且应显示为灰色。

### 4. 右键单击每个命名为 AWS NVMe Elastic Block Storage Adapter 的灰显设备位置，选择 Uninstall device（卸载设备），然后选择 Uninstall（卸载）。

#### Important

不要选中删除此设备的驱动程序软件复选框。

## 故障排除

以下内容介绍在分离卷时遇到的常见问题并以及如何解决这些问题。

#### Note

要防止出现数据丢失的可能性，请在尝试卸载之前为您的卷制作快照。强制分离一个状态卡住的卷可能对文件系统或其中包含的数据造成破坏，或者除非重启实例，否则无法使用同样的设备名称附加新卷。

- 如果在通过 Amazon EC2 控制台分离卷时遇到问题，您可使用 `describe-volumes` CLI 命令来诊断问题。有关更多信息，请参阅 [describe-volumes](#)。
- 如果您的卷处于 `detaching` 状态，您可以通过选择 `Force Detach` 强制执行分离操作。请将该选项仅用作在不得已的情况下从故障实例分离卷的方法，或是在要删除卷的情况下分离卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用该选项，则必须执行文件系统检查和修复流程。
- 如果在几分钟内多次尝试强制分离卷，并且该卷处于 `detaching` 状态，则可以向 [AWS re:Post](#) 发布帮助请求。为了帮助加快解决问题，请提供卷 ID 并描述已采取的步骤。
- 如果尝试分离仍挂载的卷，该卷可能在尝试分离时卡在 `busy` 状态。`describe-volumes` 的以下输出说明了这种情况：

```
"Volumes": [  
  {  
    "AvailabilityZone": "us-west-2b",  
    "Attachments": [  
      {  
        "Device": "/dev/xvdf",  
        "InstanceId": "i-12345678",  
        "VolumeId": "vol-12345678",  
        "State": "detaching",  
        "StateMessage": "The volume is being detached from the instance."  
      }  
    ]  
  }  
]
```

```
{
  "AttachTime": "2016-07-21T23:44:52.000Z",
  "InstanceId": "i-fedc9876",
  "VolumeId": "vol-1234abcd",
  "State": "busy",
  "DeleteOnTermination": false,
  "Device": "/dev/sdf"
}
...
}
```

如果遇到这种状态，可能无限期延迟分离，直到您卸载卷，强制分离，重启实例，或者执行前述全部三项操作。

## 删除 Amazon EBS 卷

如果您不再需要某个 Amazon EBS 卷，可以将其删除。删除后，卷上的数据都不复存在，并且再也不能附加到任何实例。然而，您可在删除之前保存卷的快照，以便以后可以使用该快照重新创建卷。

### Note

无法删除连接到实例的卷。要删除卷，必须先将其与实例分离。有关更多信息，请参阅[将 Amazon EBS 卷与实例分离](#)。

您可以检查卷是否已连接到实例。在控制台的卷页面上，可以查看卷的状态。

- 如果卷已连接到实例，则会处于in-use状态。
- 如果卷已与实例分离，则会处于available状态。您可以删除此卷。

您可以使用以下方法之一删除 EBS 卷。

### Console

#### 使用控制台删除 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择需要删除的卷，然后选择 Actions ( 操作 )、Delete Volume ( 删除卷 )。



**Note**

如果 Delete volume (删除卷) 显示为灰色, 则表示该卷已连接到实例。您必须先将卷与实例分离, 然后才能将其删除。

4. 在确认对话框中, 选择删除。

## AWS CLI

使用删除 EBS 卷 AWS CLI

使用 [delete-volume](#) 命令。

## Tools for Windows PowerShell

使用适用于 Windows 的工具删除 EBS 卷 PowerShell

使用 [Remove-EC2Volume](#) 命令。

## 使用以前的快照替换 Amazon EBS 卷

由于速度、便利性和成本, Amazon EBS 快照是 Amazon EC2 上的首选备份工具。当从快照中创建卷时, 您重新创建了它在过去特定时间点的状态, 并且所有数据完整无缺。通过将从快照中创建的卷附加到实例, 您可以在不同的区域之间复制数据, 创建测试环境, 完全替换受损或损坏的生产卷, 或检索特定文件和目录并将其传输到另一个附加的卷。有关更多信息, 请参阅 [Amazon EBS 快照](#)。

可以使用以下过程之一将 Amazon EBS 卷替换为从此卷的上一个快照创建的另一个卷。

### Console

要使用控制台替换一个卷

1. 从快照中创建一个卷, 并记下新卷的 ID。有关更多信息, 请参阅 [从快照创建卷](#)。

**Note**

确保在实例所在的可用区中创建卷。卷只能挂载到位于同一个可用区中的实例。

2. 在 Instances (实例) 页面上, 选择要替换卷的实例, 然后记下实例 ID。

在实例处于选中状态时，选择 Storage ( 存储 ) 选项卡。在 Block devices ( 块储存设备 ) 部分中，找到要替换的卷并记下该卷的设备名称，例如 /dev/sda1。

选择卷 ID。

3. 在 Volumes ( 卷 ) 屏幕上，选择该卷并选择 Actions ( 操作 )、Detach volume ( 分离卷 )、Detach ( 分离 )。
4. 选择在步骤 1 中创建的新卷，然后选择 Actions ( 操作 )、Attach volume ( 附加卷 )。

对于 Instance ( 实例 ) 和 Device name ( 设备名称 )，输入您在步骤 2 中记下的实例 ID 和设备名称，然后选择 Attach volume ( 附加卷 )。

5. 连接到您的实例并安装卷。有关更多信息，请参阅 [使 Amazon EBS 卷可供使用](#)。

## AWS CLI

### 要使用替换卷 AWS CLI

1. 从快照创建一个新卷。使用 [create-volume](#) 命令。对于 --snapshot-id，请定要使用的快照的 ID。对于 --availability-zone，指定与实例相同的可用区。根据需要配置剩余参数。

#### Note

确保在实例所在的可用区中创建卷。卷只能挂载到位于同一个可用区中的实例。

```
$ aws ec2 create-volume \  
--volume-type volume_type \  
--size volume_size \  
--snapshot-id snapshot_id \  
--availability-zone az_id
```

在命令输出中，记下新卷的 ID。

2. 获取要替换的卷的设备名称。可以使用 [describe-instances](#) 命令。对于 --instance-ids，指定要在其上替换卷的实例的 ID。

```
$ aws ec2 describe-instances --instance-ids instance_id
```

在命令输出中的 BlockDeviceMappings 中，记下要替换的卷的 VolumeId 和 DeviceName。

3. 从实例中分离要替换的卷。使用 [detach-volume](#) 命令。对于 --volume-id，指定要分离的卷的 ID。

```
$ aws ec2 detach-volume --volume-id volume_id
```

4. 将替换卷挂载到实例。使用 [attach-volume](#) 命令。对于 --volume-id，指定替换卷的 ID。对于 --instance-id，指定要为其挂载卷的实例的 ID。对于 --device，指定此前记下的设备名称。

```
$ aws ec2 attach-volume \  
--volume-id volume_id \  
--instance-id instance_id \  
--device device_name
```

5. 连接到您的实例并安装卷。有关更多信息，请参阅 [使 Amazon EBS 卷可供使用](#)。

## 监控 Amazon EBS 卷

AWS 会自动提供可用于监控 Amazon EBS 卷的数据。

内容

- [EBS 卷状态检查](#)
- [EBS 卷事件](#)
- [使用受损的卷](#)
- [使用自动启用 IO 卷属性](#)

有关其他监控信息，请参阅[亚马逊 EBS 的亚马逊 CloudWatch 指标](#)和[Amazon f EventBridge or Amazon EBS](#)。

### EBS 卷状态检查

通过卷状态检查，您可以更好地了解、追踪和管理 Amazon EBS 卷上数据的潜在不一致性。它们的作用是在您需要确定 Amazon EBS 卷是否损坏的时候为您提供信息，帮助您控制处理潜在不一致卷的方式。

卷状态检查为自动执行的测试，该测试每隔 5 分钟运行一次并返回通过或故障状态。如果所有的检查都通过，则卷的状态为 `ok`。如果一个检查返回故障，则卷的状态为 `impaired`。如果状态为 `insufficient-data`，那么该检查将在该卷上继续进行。您可以查看卷状态检查的结果来识别任意受损卷并进行所需操作。

当 Amazon EBS 判定一个卷中的数据具有潜在不一致性时，默认禁用从任何附加的 EC2 实例到该卷的 I/O，以此来防止数据损坏。禁用 I/O 后，下一个卷状态检查故障，并且卷状态为 `impaired`。此外，您还会看到一个通知您 I/O 被禁用的事件，并且您可以通过使能到该卷的 I/O 来解决卷的损坏状态。我们将等待您启用 I/O，期间您有机会决定是继续让实例使用该卷，还是在使用该卷之前先使用命令 [如 `fsck` (Linux 实例) 或 `chkdsk` (Windows 实例)] 运行一致性检查。

### Note

卷状况以卷状况检查为依据，并不反映卷状态。因此，卷状态并不表示卷处于 `error` 状态（例如，卷无法接受 I/O 时）。有关卷状态的信息，请参阅 [卷状态](#)。

如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是“受损”，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 IO 卷属性 (API 中的 `autoEnableIO`)，则卷状态检查会继续通过。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 不会自动启用。这使您能够检查卷的一致性 or 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。如果卷的表现低于预期，它会提醒您。此状态检查仅适用于挂载到实例的预调配 IOPS SSD (`io1` 和 `io2`) 和通用型 SSD (`gp3`) 卷。状态检查对于通用型 SSD (`gp2`)、吞吐量优化型 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。从您将 `io1` 或 `io2` 卷挂载到实例的那一刻起，可能需要 5 分钟来进行状态检查，以报告 I/O 性能状态。

### Important

在初始化已从快照还原的 Provisioned IOPS SSD 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 性能状态检查中显示 `warning` 状态。这是预期行为，并且您可在初始化 Provisioned IOPS SSD 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](#)。

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 ( 仅限 <b>io1</b> 、 <b>io2</b> 和 <b>gp3</b> 卷 )
ok	使能 ( I/O 使能或 I/O 自动使能 )	正常 ( 卷的期望性能 )
warning	使能 (I/O 使能或 I/O 自动使能)	降级 ( 卷的性能低于期望性能 )  严重降级 ( 卷的性能大大低于期望性能 )
impaired	使能 (I/O 使能或 I/O 自动使能)	停滞 ( 卷性能受到严重影响 )
	禁用 ( 卷脱机和挂起恢复, 或等待用户使能 I/O )	不可用 ( 由于 I/O 被禁用, 所以不能确定 I/O 性能 )
insufficient-data	使能 (I/O 使能或 I/O 自动使能)	数据不足
	数据不足	

您可以使用以下方法查看和处理状态检查。

## Console

查看状态检查，需要进行以下操作

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。

卷状态列显示每个卷的运行状态。

3. 要查看特定卷的详细状态信息，请在网格中选择该卷，然后选择 Status checks ( 状态检查 ) 选项卡。
4. 如果您的卷状态检查返回故障 ( 状态是 impaired )，请参阅 [使用受损的卷](#)。

另外，您还可以在导航器中选择事件来查看实例和卷所有的事件。有关更多信息，请参阅[EBS 卷事件](#)。

## AWS CLI

查看卷状态信息

使用 [describe-volume-status](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)。

## Tools for Windows PowerShell

查看卷状态信息

使用 [Get-EC2VolumeStatus](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)。

## EBS 卷事件

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何附加的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。

想要自动使能具有潜在不一致性卷上的 I/O，您可以改变自动启用 IO 卷属性（在 API 中为 `autoEnableIO`）的设置。更多关于改变这些属性的信息，请参阅[使用受损的卷](#)。

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：

### Awaiting Action: Enable IO

卷数据具有潜在一致性。在您明确的使能它之前，将一直禁用 I/O。当您明确启用 I/O 后，事件描述变为 IO Enabled。

### IO Enabled

明确地使能这些卷的 I/O 操作。

### IO Auto-Enabled

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。

### Normal

仅适用于 io1、io2 和 gp3 卷。卷执行其期望性能。

## Degraded

仅适用于 io1、io2 和 gp3 卷。卷性能低于期望性能。

## Severely Degraded

仅适用于 io1、io2 和 gp3 卷。卷性能大大地低于期望性能。

## Stalled

仅适用于 io1、io2 和 gp3 卷。卷的性能受到严重影响。

您可以使用以下方法查看卷的事件。

## Console

想要查看您的卷事件，需要执行以下操作

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Events。列出具有事件的所有实例和卷。
3. 可以按卷进行筛选以便仅查看卷状态。您也可以筛选指定的状态类型。
4. 选择一个卷以查看其特定事件。

## AWS CLI

想要查看您的卷事件，需要执行以下操作

使用 [describe-volume-status](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)。

## Tools for Windows PowerShell

想要查看您的卷事件，需要执行以下操作

使用 [Get-EC2VolumeStatus](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)。

如果您的卷 I/O 被禁用，请参阅[使用受损的卷](#)。如果您的卷 I/O 性能低于正常值，这可能是由于您之前的操作（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。

## 使用受损的卷

如果卷受损，请使用以下选项，因为卷的数据可能不一致。

### 选项

- [选项 1：对附加到其实例的卷执行一致性检查](#)
- [选项 2：使用其他实例对该卷执行一致性检查](#)
- [选项 3：如果您不再需要卷，请将其删除](#)

### 选项 1：对附加到其实例的卷执行一致性检查

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。使用以下方法之一。

#### Console

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Events。
3. 选择要使能 I/O 操作的卷。
4. 选择 Actions ( 操作 )、Enable I/O ( 启用输入/输出 )。

#### AWS CLI

要使用 AWS CLI 为一个卷启用 I/O

使用 [enable-volume-io](#) 命令。

#### Tools for Windows PowerShell

要使用 Tools for Windows PowerShell 为一个卷启用 I/O

使用 [Enable-EC2VolumeIO](#) 命令。

3. 检查卷上数据。



- a. 运行 fsck ( Linux 实例 ) 或 chkdsk ( Windows 实例 ) 命令。
- b. ( 可选 ) 查看所有适用的应用程序或系统日志以了解相关错误消息。
- c. 如果卷受损时间超过 20 分钟，您可以联系 AWS 支持中心。选择问题排查，然后在状态检查故障排除对话框上选择联系客服提交一个支持案例。

## 选项 2：使用其他实例对该卷执行一致性检查

按照以下程序在您的产品环境外检查该卷。

### Important

当卷 I/O 被禁用时，这些程序可能会导致挂起的写入 I/O 丢失。

想要在一个隔离环境中在一个卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 将该卷从实例中分离。有关更多信息，请参阅[将 Amazon EBS 卷与实例分离](#)。
3. 在该卷上使能 I/O。使用以下方法之一。

### Console

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Events。
3. 选择您在之前的步骤中分离的卷。
4. 选择 Actions ( 操作 )、Enable I/O ( 启用输入/输出 )。

### AWS CLI

要使用 AWS CLI 为一个卷启用 I/O

使用 [enable-volume-io](#) 命令。

### Tools for Windows PowerShell

要使用 Tools for Windows PowerShell 为一个卷启用 I/O

使用 [Enable-EC2VolumeIO](#) 命令。

4. 将该卷附加到另一个实例。有关更多信息，请参阅[启动实例](#)和[将 Amazon EBS 卷挂载到实例](#)。
5. 检查卷上数据。
  - a. 运行 fsck ( Linux 实例 ) 或 chkdsk ( Windows 实例 ) 命令。
  - b. ( 可选 ) 查看所有适用的应用程序或系统日志以了解相关错误消息。
  - c. 如果卷受损时间超过 20 分钟，您可以联系 AWS 支持中心。选择 Troubleshoot，然后在故障排除对话框中选择 Contact Support 以提交支持案例。

### 选项 3：如果您不再需要卷，请将其删除

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](#)。

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。有关更多信息，请参阅[从快照创建卷](#)。

## 使用自动启用 IO 卷属性

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何附加的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是受损，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 IO 卷属性 ( API 中的 autoEnableIO )，则卷和实例之间的 I/O 会自动重新启用，并且卷将通过状态检查。此外，您将会看到一个通知您该卷具有潜在不一致状态的事件，但它的 I/O 不会自动启用。如果发生此事件，您应该检查该卷的一致性，如有必要，可对其进行更换。有关更多信息，请参阅[EBS 卷事件](#)。

您可以使用以下方法查看和修改卷的 Auto-Enabled IO ( 自动启用输入/输出 ) 属性。

### Amazon EC2 console

#### 查看卷的“自动启用 IO”属性

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择卷，然后选择 Status checks ( 状态检查 ) 选项卡。

Auto-enabled I/O ( 自动启用输入/输出 ) 字段为所选择的卷显示当前设置：已启用或已禁用。

## 修改卷的“自动启用 I/O”属性

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions ( 操作 )、Manage auto-enabled I/O ( 管理自动启用的输入/输出 )。
4. 选中 Auto-enable I/O for impaired volumes ( 为受损卷自动启用输入/输出 ) 复选框，以便为受损卷自动启用输入/输出。想要禁用该功能，请清除复选框。
5. 选择更新。

## AWS CLI

查看卷的 autoEnableIO 属性

使用 [describe-volume-attribute](#) 命令。

要修改一个卷的 autoEnableIO 属性

使用 [modify-volume-attribute](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)

## Tools for Windows PowerShell

查看卷的 autoEnableIO 属性

使用 [Get-EC2VolumeAttribute](#) 命令。

要修改一个卷的 autoEnableIO 属性

使用 [Edit-EC2VolumeAttribute](#) 命令。

有关这些命令行界面的更多信息，请参阅[访问 Amazon EC2](#)

## 在 Amazon EBS 上进行故障测试

使用 AWS Fault Injection Service 和“暂停 I/O”操作可暂时停止 Amazon EBS 卷与其连接的实例之间的 I/O，以测试您的工作负载如何处理 I/O 中断。借 AWS FIS 助，您可以使用对照实验来测试您的架构和监控，例如 Amazon CloudWatch 警报和操作系统超时配置，并提高应对存储故障的弹性。

有关的更多信息 AWS FIS，请参阅《[AWS Fault Injection Service 用户指南](#)》。

## 注意事项

暂停卷 I/O 时请注意以下事项：

- 可以为挂载到[基于 Nitro 系统构建的实例](#)的所有 Amazon EBS 卷类型暂停 I/O。
- 可以为根卷暂停 I/O。
- 可以为启用多重挂载的卷暂停 I/O。如果为已启用多重挂载的卷暂停 I/O，则该卷及其所有附加实例之间将暂停 I/O。
- 要测试操作系统超时配置，请将实验持续时间设置为等于或大于为 `nvme_core.io_timeout` 指定的值。有关更多信息，请参阅 [I/O 操作超时](#)。
- 如果提升对已暂停 I/O 卷的 I/O，会发生以下情况：
  - 卷的状态将在 120 秒内转换为 `impaired`。有关更多信息，请参阅 [监控 Amazon EBS 卷](#)。
  - 队列长度 (`VolumeQueueLength`) 的 CloudWatch 指标将为非零。任何告警或监控都应监控非零队列深度。有关更多信息，请参阅 [Amazon EBS 卷的指标](#)。
  - `VolumeReadOps` 或的 CloudWatch 指标 `VolumeWriteOps` 将是 0，这表示该卷不再处理 I/O。

## 限制

暂停卷 I/O 时请注意以下限制：

- 不支持实例存储卷。
- 不支持基于 Xen 的实例类型。
- 您无法暂停在前哨基地 AWS Outposts、区域或本地 AWS Wavelength 区域中创建的卷的 I/O。

您可以从 Amazon EC2 控制台执行基本实验，也可以使用控制 AWS FIS 台进行更高级的实验。有关使用 AWS FIS 控制台执行高级实验的更多信息，请参阅《AWS Fault Injection Service 用户指南》AWS FIS 中的[教程](#)。

使用 Amazon EC2 控制台执行基础实验

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Volumes。
3. 选择要为其暂停 I/O 的卷，然后选择操作、错误注入、暂停卷 I/O。
4. 对于持续时间，输入要在卷和实例之间暂停 I/O 的持续时间。“持续时间”下拉列表旁边的字段将以 ISO 8601 格式显示持续时间。

5. 在服务访问权限部分，选择要代入的 [IAM 服务角色](#) AWS FIS 来执行实验。您可以使用默认角色，也可以使用您创建的现有角色。有关更多信息，请参阅 [AWS FIS 创建 IAM 角色](#)。
6. 选择暂停卷 I/O。系统提示时，在确认字段中输入 `start` 并选择开始实验。
7. 监控实验的进度和影响。有关更多信息，请参阅《AWS FIS 用户指南》中的 [监控 AWS FIS](#)。

# Amazon EBS 快照

您可以通过制作 point-in-time 副本（称为 Amazon EBS 快照）来备份 Amazon EBS 卷上的数据。快照是增量备份，这意味着我们仅保存设备上自最新快照之后发生更改的块。由于无需复制数据，这将最大限度缩短创建快照所需的时间和增加存储成本节省。

## Important

AWS 不会自动备份存储在 EBS 卷上的数据。为满足数据恢复能力和灾难恢复的需要，您应定期创建 EBS 快照，或者使用 [Amazon Data Lifecycle Manager](#) 或 [AWS Backup](#) 设置自动快照创建。

EBS 快照存储在 Amazon S3 中，在您无法直接访问的 S3 存储桶中。您可以使用 Amazon EC2 控制台或 Amazon EC2 API 创建和管理快照。您无法使用 Amazon S3 控制台或 Amazon S3 API 访问您的快照。

每个快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。当您基于快照创建 EBS 卷时，新卷将开始作为用于创建快照的卷的精确副本。复制的卷将在后台加载数据，让您可以立即开始使用数据。如果您访问尚未加载的数据，则卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的剩余数据。有关更多信息，请参阅 [创建 Amazon EBS 快照](#)。删除快照时，仅会删除该快照特有的数据。有关更多信息，请参阅 [删除 Amazon EBS 快照](#)。

有关更多信息，请参阅 [Amazon EBS 快照](#) 产品页面。

## 快照事件

您可以通过“CloudWatch 事件”跟踪 EBS 快照的状态。有关更多信息，请参阅 [EBS 快照事件](#)。

## 应用程序一致性快照（仅限 Windows 实例）

通过使用 Systems Manager Run Command，您可以为附加到 Amazon EC2 Windows 实例的所有 EBS 卷拍摄应用程序一致性快照。快照过程使用 Windows [卷影复制服务 \(VSS\)](#) 为 VSS 感知应用程序拍摄映像级备份，包括这些应用程序和磁盘之间的待处理事务中的数据。在备份所有已附加的卷时，您无需关闭实例或将其断开连接。有关更多信息，请参阅 [创建 VSS 应用程序一致性快照](#)。

## 多卷快照

快照可用于创建关键工作负载的备份，如跨多个 EBS 卷的大型数据库或文件系统。多卷快照允许您跨连接到 EC2 point-in-time 实例的多个 EBS 卷拍摄精确、数据协调和崩溃一致的快照。您不再需要停

止实例或在多个卷之间协调来确保崩溃一致性，因为快照将跨多个 EBS 卷自动进行拍摄。有关更多信息，请参阅[创建 Amazon EBS 快照](#)下创建多卷 EBS 快照的步骤。

## 快照定价

快照的费用取决于存储的数据量。由于快照是增量的，因此删除快照可能不会降低您的数据存储成本。删除快照时，专由某个快照引用的数据将被删除，但保留其他快照引用的数据。有关更多信息，请参阅 AWS Billing 用户指南中的 [Amazon Elastic Block Store 卷和快照](#)。

## 内容

- [快照的工作原理](#)
- [复制和共享快照](#)
- [快照的加密支持](#)
- [Amazon EBS 快照生命周期](#)
- [Amazon EBS 快速快照还原](#)
- [Amazon EBS 快照锁](#)
- [阻止公开访问快照](#)
- [快照回收站](#)
- [Amazon EBS local snapshots on Outposts](#)

## 快照的工作原理

您从卷创建的第一个快照始终是完整快照。它包括创建快照时写入卷的所有数据块。同一卷的后续快照为增量快照。这些快照仅包括自上次创建快照以来写入卷的已更改数据块和新数据块

完整快照的大小取决于备份数据的大小，而非源卷的大小。同样地，与完整快照相关的存储成本取决于快照的大小，而非源卷的大小。例如，您创建了仅包含 50 GiB 数据的 200 GiB Amazon EBS 卷的第一个快照。这会生成大小为 50 GiB 的完整快照，并且您需要为 50 GiB 快照存储付费。

同样，增量快照的大小和存储成本取决于自上次快照创建以来写入卷的任何数据的大小。继续此示例，如果您在更改 20 GiB 数据和添加 10 GiB 数据后创建 200 GiB 卷的第二个快照，则增量快照的大小为 30 GiB。然后，您需要为额外的 30 GiB 快照存储付费。

有关快照定价的更多信息，请参阅 [Amazon EBS 定价](#)。

### ⚠ Important

归档增量快照时，增量快照将转换为完整快照，其中包括创建快照时写入卷的所有块。然后，快照将移动到 Amazon EBS 快照归档层。归档层中的快照费率与标准层中的快照费率不同。有关更多信息，请参阅 [定价和计费](#)。

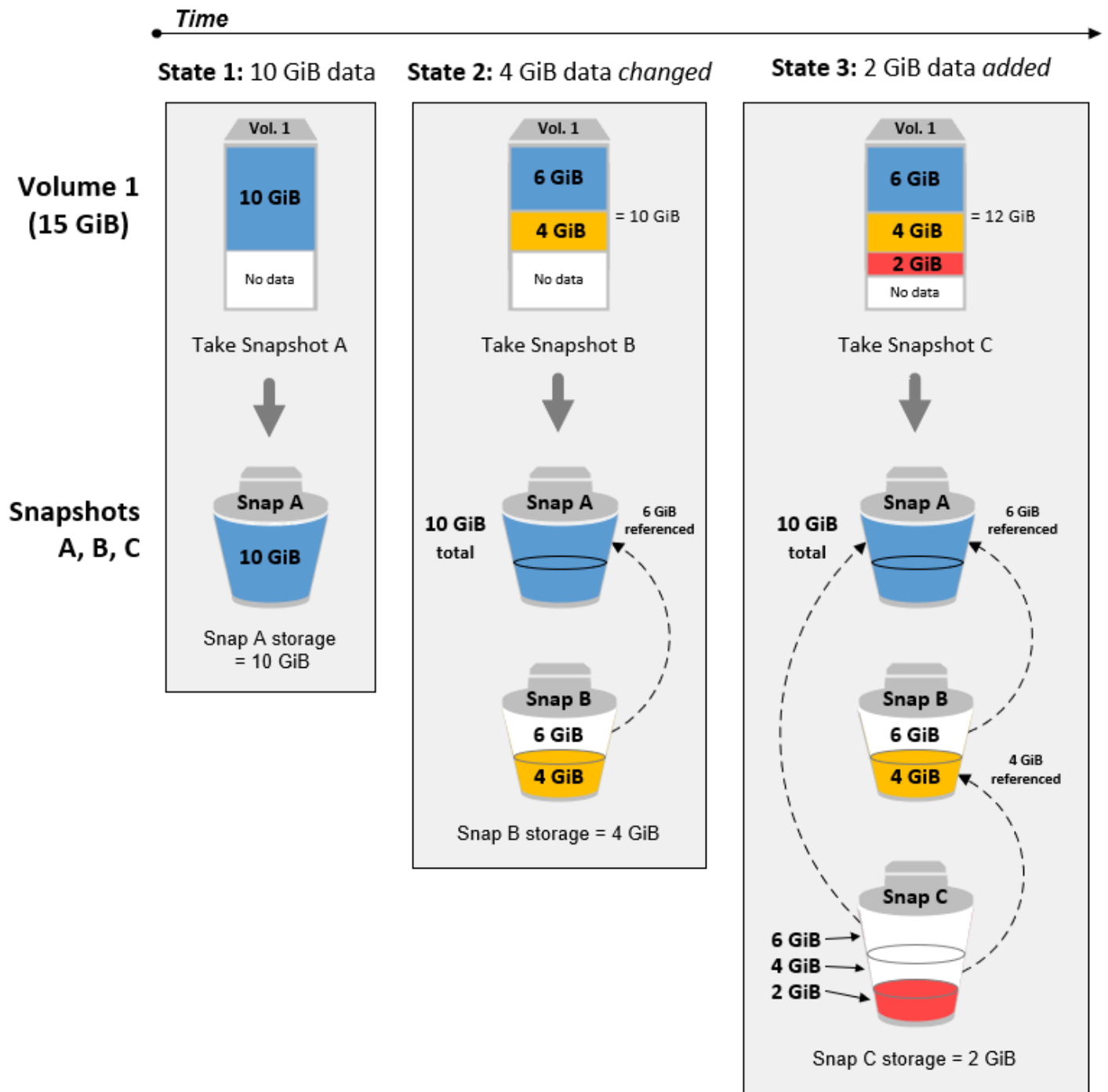
以下部分阐述了 EBS 快照如何捕获卷在某一时间点的状态，以及正在更改的卷的后续快照如何创建这些更改的历史记录。

### 同一卷的多个快照

在本部分的图表中，大小为 15 GiB 的卷 1 在 3 个时间点上显示。为这三个卷状态分别制作快照。该图表明显示以下内容：

- 在状态 1 中，该卷具有 10 GiB 数据。快照 A 是为该卷制作的第一个快照。快照 A 是完整快照，所有 10 GiB 数据均已备份。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，捕获快照 A 后仅 4 GiB 数据发生更改。快照 B 是增量快照。只需要备份已更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已在快照 A 中备份）将由快照 B 引用，而不会再次备份。这通过虚线箭头指示。
- 在状态 3 中，捕获快照 B 后，2 GiB 数据已添加到该卷中，共计 12 GiB 数据。快照 C 是增量快照。只需要对捕获快照 B 之后添加的 2 GiB 数据进行备份。如虚线箭头所示，快照 C 还引用了存储在快照 B 中的 4 GiB 数据和存储在快照 A 中的 6 GiB 数据。
- 三个快照共需 16 GiB 存储空间。这相当于快照 A 需要 10 GiB，快照 B 需要 4 GiB，快照 C 需要 2 GiB。





## 不同卷的增量快照

本节中的图表显示了如何从不同卷获取增量快照。

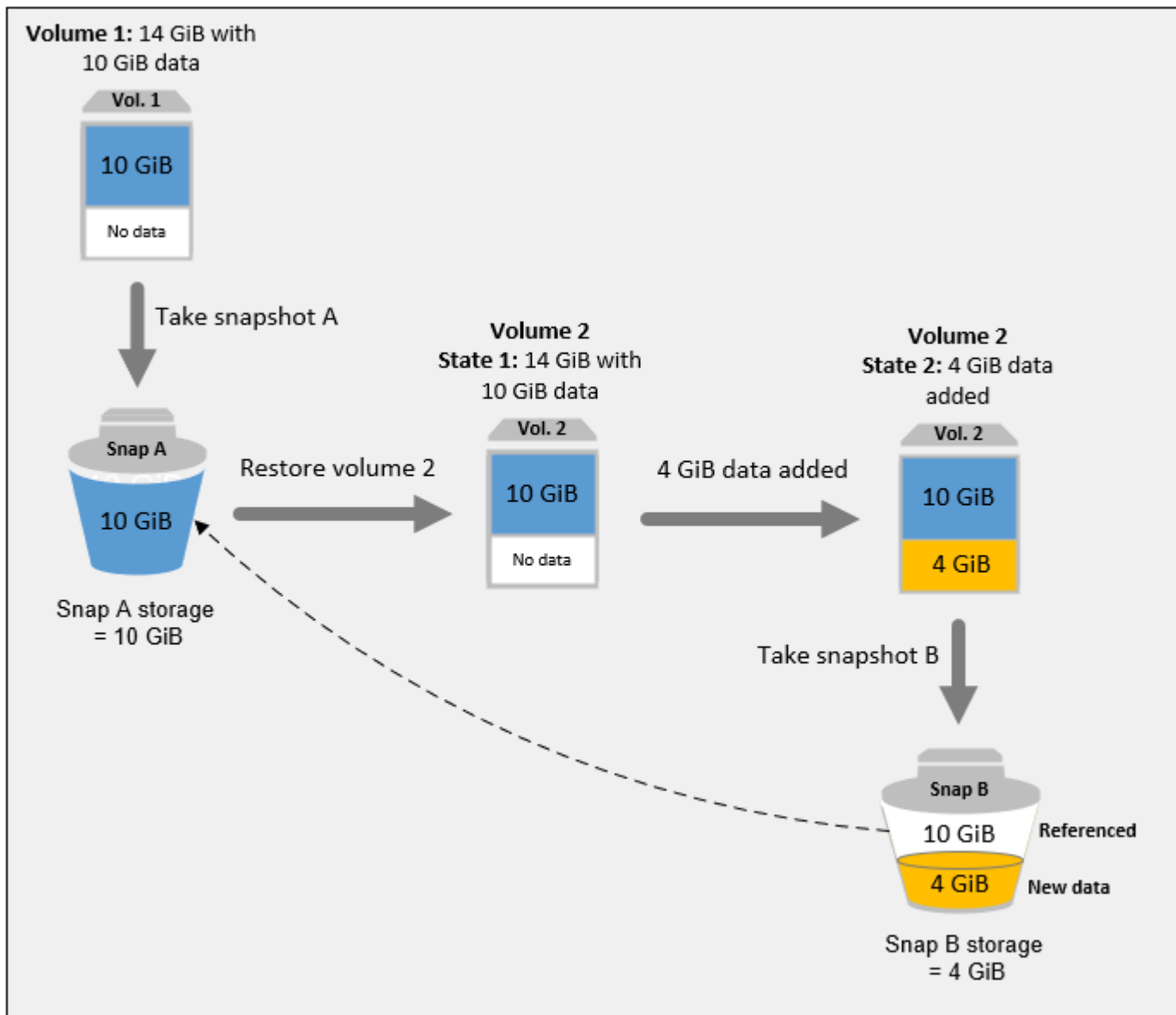
1. 大小为 14 GiB 的卷 1 包含 10 GiB 数据。因为快照 A 是为该卷捕获的首个快照，是完整快照，因此会备份所有 10 GiB 数据。

2. 卷 2 是从快照 A 创建的，所以它是卷 1 在拍摄快照时的精准副本。
3. 随着时间的推移，4 GiB 的数据将添加到卷 2，并且其数据总大小为 14 GiB。
4. 快照 B 是基于卷 2 制作的。对于快照 B，仅备份从快照 A 创建卷后添加的 4 GiB 数据。未更改的其他 10 GiB 数据（已存储在快照 A 中）将由快照 B 引用，而不会再次备份。

快照 B 是快照 A 的增量快照，即使它是从不同的卷创建的。

#### Important

该图表假定您拥有卷 1 和快照 A，并且卷 2 使用与卷 1 相同的 KMS 密钥进行加密。如果 Vol 1 归另一个 AWS 账户所有，并且该账户使用了 Snap A 并与你共享，那么 Snap B 将是完整快照。或者，如果卷 2 使用与卷 1 不同的 KMS 密钥进行加密，则快照 B 将是完整快照。



有关删除快照后如何管理数据的更多信息，请参阅[删除 Amazon EBS 快照](#)。

## 复制和共享快照

您可以通过修改快照的访问权限来跨 AWS 账户共享快照。您可以复制您拥有的快照以及与您共享的快照。有关更多信息，请参阅[共享 Amazon EBS 快照](#)。

快照仅限于创建快照的 AWS 区域。在您创建 EBS 卷的快照之后，可在同一个区域中使用它来创建新卷。有关更多信息，请参阅[从快照创建卷](#)。您还可以跨区域复制快照，从而能够使用多个区域进行地理扩展、数据中心迁移和灾难恢复。您可以复制具有 `completed` 状态的任何可访问快照。有关更多信息，请参阅[复制 Amazon EBS 快照](#)。

## 快照的加密支持

EBS 快照完全支持 EBS 加密。

- 加密卷的快照会自动加密。
- 通过加密快照创建的卷会自动加密。
- 根据您拥有或有权访问的未加密快照创建的卷可以加密 on-the-fly。
- 在复制您拥有的未加密快照时，您可以在复制过程中对其加密。
- 在复制您拥有或有权访问的加密快照时，可在复制过程中使用其他密钥对其重新加密。
- 对于从未加密的快照中创建的加密卷，拍摄的第一个快照始终是完整快照。
- 为重新加密的卷拍摄的第一个快照（具有与源快照不同的 CMK）始终是完整快照。

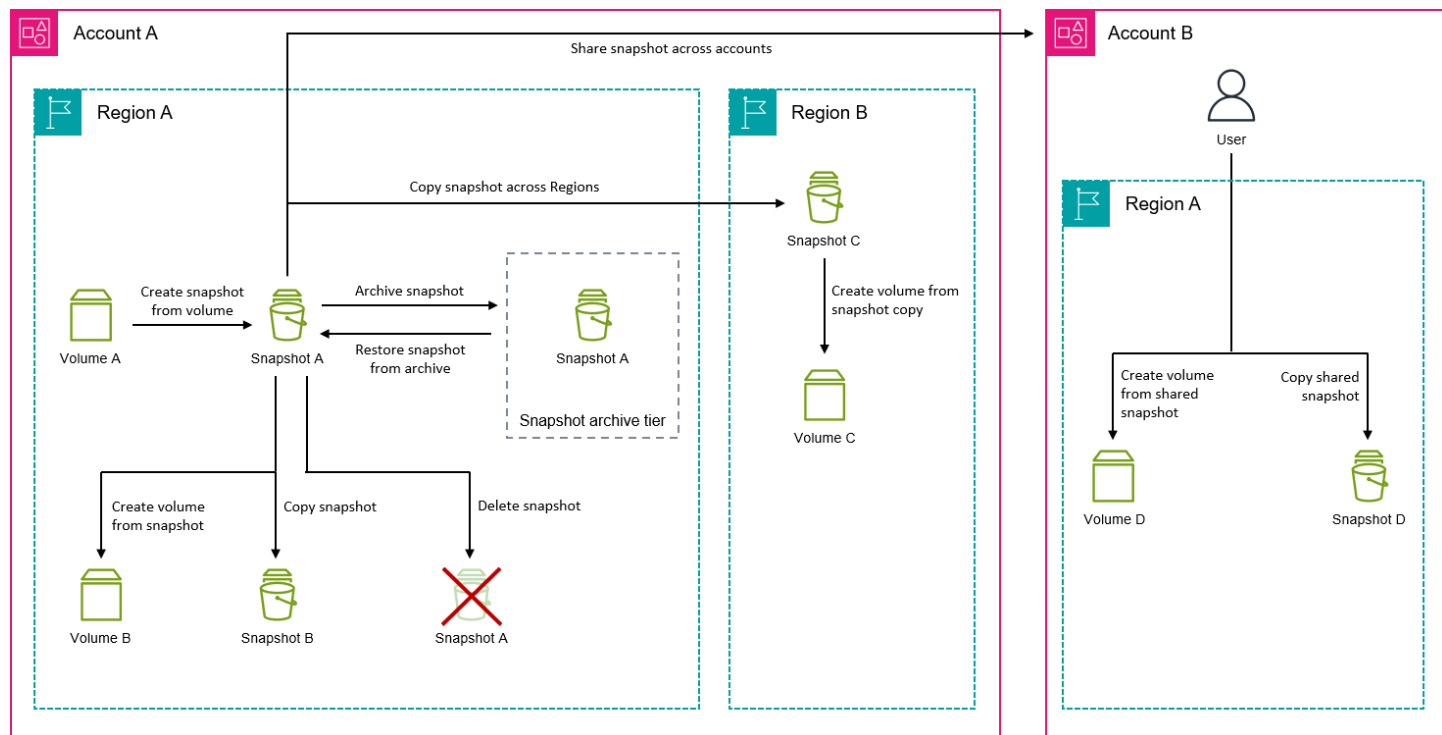
[创建 Amazon EBS 快照](#) 和 [复制 Amazon EBS 快照](#) 中提供了可能的快照加密方案的完整文档。

有关更多信息，请参阅 [Amazon EBS 加密](#)。

## Amazon EBS 快照生命周期

Amazon EBS 快照的生命周期始于创建过程。从 Amazon EBS 卷创建快照。可以使用快照还原新的 Amazon EBS 卷。可以在相同区域或不同区域创建快照副本。您可以公开或私下与其他 AWS 账户人共享快照。这些账户可以从共享快照还原卷，也可以在自有账户中创建共享快照的副本。如果不需要立即访问快照，则可以将其存档以节省存储成本。

下图显示了可以在快照生命周期中对快照执行的操作。



## 任务

- [创建 Amazon EBS 快照](#)
- [查看 Amazon EBS 快照信息](#)
- [复制 Amazon EBS 快照](#)
- [共享 Amazon EBS 快照](#)
- [归档 Amazon EBS 快照](#)
- [删除 Amazon EBS 快照](#)
- [自动化快照生命周期](#)

## 创建 Amazon EBS 快照

要在 Windows 实例上创建应用程序一致性快照，请参阅[创建 VSS 应用程序一致性快照](#)。

您可以创建 EBS 卷的 point-in-time 快照，并将其用作新卷或数据备份的基准。如果您定期为卷拍摄快照，则快照为增量快照，新快照上仅保存自上次快照后已更改的块。

快照是异步生成的；point-in-time 快照会立即创建，但是快照的状态是 pending 直到快照完成（当所有修改后的区块都已传输到 Amazon S3 时），对于大型初始快照或后续快照（其中许多块已更改），可能需要几个小时。执行期间，正在进行的快照不会受到同时发生的卷读写操作的影响。

您可以制作正在使用的已附加卷的快照。但是，快照只能捕获发出快照命令时已经写入您的 Amazon EBS 卷的数据。其中可能不包括已由任何应用程序或操作系统缓存的任何数据。如果您可以将该卷的所有文件写入暂停足够长的时间以制作快照，则快照应该是完整的。但是，如果您无法暂停该卷的所有文件写入，则应该从实例中卸载该卷、发出快照命令，然后重新安装该卷，以确保获得一致且完整的快照。当快照状态为 pending 时，您可以重新挂载并使用卷。

要简化快照的管理，您可以在创建期间为快照添加标签，也可在创建后添加。例如，您可以应用标记，描述该快照对应的原始卷，或描述用于将原始卷挂载到实例上的设备名称。

## 快照加密

从加密卷制作的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷及所有关联快照中的数据在静态或传输过程中均受到保护。有关更多信息，请参阅 [Amazon EBS 加密](#)。

默认情况下，只有您可以从您拥有的快照创建卷。但是，您可以与特定 AWS 账户共享未加密的快照，也可以通过公开快照与整个 AWS 社区共享。有关更多信息，请参阅 [共享 Amazon EBS 快照](#)。

您只能与特定 AWS 账户共享加密快照。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](#)。

## 多卷快照

您可以创建多卷快 point-in-time 照，即连接到实例的全部或部分卷的快照。

默认情况下，您从实例创建多卷快照时，Amazon EBS 会创建附加到该实例的所有卷 [根和数据 (非根)] 的快照。不过，您可以选择创建附加到实例的卷子集的快照。

您可以标记多卷快照，就像您使用单个卷快照执行的操作一样。我们建议您标记多个卷快照以在还原、复制或保留操作期间集中管理它们。还可以选择自动将标签从源卷复制到相应的快照。这将帮助您设置快照元数据 (如访问策略、附件信息和成本分配) 以匹配源卷。

创建快照后，每个快照将视为单个快照。您可以执行所有快照操作，如还原、删除和跨区域或账户复制，就像您使用单个卷快照执行的操作一样。

多卷、崩溃一致性快照通常以集的形式进行还原。这有助于通过使用实例 ID、名称或其他相关详细信息标记您的集，以标识位于崩溃一致性快照集中的快照。

创建快照后，它们会显示在您的 EC2 控制台中精确创建的快照中 point-in-time。

如果多卷快照集的任何快照失败，则所有其他快照都将显示错误状态，并将结果为 createSnapshots CloudWatch 的事件发送到您的 AWS 账户。failed 有关更多信息，请参阅 [创建多个快照 \( createSnapshots \)](#)。

## Amazon Data Lifecycle Manager

您可以创建快照生命周期策略来自动创建和保留单个卷快照和实例的多卷快照。有关更多信息，请参阅 [Amazon Data Lifecycle Manager](#)。

### 注意事项

创建快照时需考虑以下事项：

- 当您为充当根设备的 EBS 卷创建快照时，建议您在拍摄快照之前停止实例。
- 您不能从启用了休眠的实例或从已休眠实例创建快照。如果您从已休眠或已启用休眠的实例创建快照或 AMI，则可能无法连接到从该 AMI 启动的新实例，或者通过从快照创建的 AMI 启动的新实例。
- 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。
- 单个 pending 或 st1 卷限制为一个 sc1 快照，其他卷类型的单个卷限制为五个 pending 快照。如果您在尝试给同一个卷创建多个并发快照时收到 ConcurrentSnapshotLimitExceeded 错误，请等待一个或多个 pending 快照完成，然后再为该卷创建另一个快照。
- 从带有 AWS Marketplace 产品代码的卷创建快照时，产品代码会传播到快照中。
- 从实例创建多卷快照集时，最多可以指定 127 个要排除的数据（非根）卷。您可以挂载到实例的最大 Amazon EBS 卷数取决于实例类型和实例规模。有关更多信息，请参阅 [实例卷限制](#)。

### 创建快照

要从指定的卷中创建快照，请使用以下方法之一。

#### Console

##### 使用控制台创建快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Snapshots（快照）、Create snapshot（创建快照）。
3. 对于资源类型，选择卷。
4. 对于 Volume ID（卷 ID），选择需要从其创建快照的卷。

Encryption (加密) 字段指示所选卷的加密状态。如果选定的卷已加密, 则使用相同的 KMS 密钥自动加密快照。如果选定的卷未加密, 则不会对快照进行加密。

5. (可选) 对于描述, 输入对快照的简短描述。
6. (可选) 要为快照分配自定义标签, 请在标签部分中选择添加标签, 然后输入标签键和值对。最多可以添加 50 个标签。
7. 选择创建快照。

## AWS CLI

要使用创建快照 AWS CLI

使用 [create-snapshot](#) 命令。

## Tools for Windows PowerShell

使用适用于 Windows 的工具创建快照 PowerShell

使用 [New-EC2Snapshot](#) 命令。

## 创建多卷快照

从实例创建多卷快照集时, 您可以选择是否从源卷将标签复制到相应的快照。您可以指定是否创建根卷的快照。您还可以指定是为附加到实例的所有数据 (非根) 卷创建快照, 还是为这些卷的子集创建快照。

### 注意事项

- 多卷快照支持每个实例最多 128 个 Amazon EBS 卷, 其中包括根卷和最多 127 个数据 (非根) 卷。您可以挂载到实例的最大 Amazon EBS 卷数取决于实例类型和实例规模。有关更多信息, 请参阅[实例卷限制](#)。

要从实例的卷中创建快照, 请使用以下方法之一。

## Console

使用控制台创建多卷快照

1. 通过以下网址打开 Amazon EC2 控制台: <https://console.aws.amazon.com/ec2/>。



2. 在导航窗格中，选择 Snapshots ( 快照 )、Create snapshot ( 创建快照 )。
3. 对于资源类型，选择实例。
4. 对于 Description ( 描述 )，输入快照的简短描述。此描述适用于所有快照。
5. ( 可选 ) 默认情况下，Amazon EBS 会创建实例根卷的快照。如果您不想创建实例根卷的快照，请选择 Exclude root volume ( 排除根卷 )。
6. ( 可选 ) 默认情况下，Amazon EBS 会创建附加到实例的所有数据 ( 非根 ) 卷的快照。如果您想创建附加到实例的数据 ( 非根 ) 卷子集的快照，请选择排除特定数据卷。Attached data volumes ( 附加的数据卷 ) 部分列出了当前附加到所选实例的所有数据卷。

在 Attached data volumes ( 附加的数据卷 ) 部分，选择您不想为其创建快照的数据卷。只有未选中的卷才会包含在多卷快照集中。最多可以排除 127 个卷。

7. ( 可选 ) 若要自动将标签从源卷复制到相应快照，请为从源卷复制标签选择复制标签。这将设置快照元数据 ( 如访问策略、附件信息和成本分配 ) 以匹配源卷。
8. ( 可选 ) 若要为快照分配自定义标签，请在标签部分选择添加标签，然后输入键值对。最多可以添加 50 个标签。
9. 选择创建快照。

快照创建期间，将一起管理快照。如果卷集中的其中一个快照失败，则其他快照将移至卷集的错误状态。您可以使用“[CloudWatch事件](#)”监控快照的进度。快照创建过程完成后，CloudWatch 生成一个事件，其中包含受影响实例的状态和所有相关快照详细信息。

## AWS CLI

要使用创建多卷快照 AWS CLI，请使用 [create-snapshots](#) 命令。

如果您不想创建根卷的快照，请为 `--instance-specification ExcludeBootVolume` 指定 `true`。如果您不想创建附加到实例的所有数据 ( 非根 ) 卷的快照，对于 `--instance-specification ExcludeDataVolumes`，请指定不想为其创建快照的数据卷 ID。您最多可以指定 127 个要排除的数据 ( 非根 ) 卷。

## Tools for Windows PowerShell;

要使用适用于 Windows 的工具创建多卷快照 PowerShell，请使用 [New-EC2SnapshotBatch](#) 命令。

如果您不想创建根卷的快照，请为 `-InstanceSpecification_ExcludeBootVolume` 指定 `1`。如果您不想创建附加到实例的所有数据 ( 非根 ) 卷的快照，对于 `-InstanceSpecification_ExcludeDataVolumes`，请指定不想为其创建快照的数据卷 ID。您最多可以指定 127 个要排除的数据 ( 非根 ) 卷。

如果所有快照都成功完成，则会向您的 AWS 账户发送一个结果为 `createSnapshots CloudWatch` 的事件。如果多卷快照集的任何快照失败，则所有其他快照都将显示错误状态，并将结果为 `createSnapshots CloudWatch` 的事件发送到您的 AWS 账户。有关更多信息，请参阅 [创建多个快照 \( `createSnapshots` \)](#)。

## 使用 EBS 快照

您可以复制快照、共享快照和从快照创建卷。有关更多信息，请参阅下列内容：

- [复制 Amazon EBS 快照](#)
- [共享 Amazon EBS 快照](#)
- [从快照创建卷](#)

## 查看 Amazon EBS 快照信息

您可以使用以下方法之一查看有关快照的详细信息。

### Console

使用控制台查看快照信息

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 要仅查看您拥有的快照，请在屏幕左上角选择 `Owned by me ( 我拥有的 )`。您还可以使用标签和快照属性筛选快照列表。在 `Filter ( 筛选条件 )` 字段中，选择属性字段，然后选择或输入属性值。例如，要仅查看加密的快照，请选择 `Encryption ( 加密 )`，然后输入 `true`。
4. 要查看有关特定快照的更多信息，请在列表中选择其 ID。

### AWS CLI

要查看快照信息，请使用 AWS CLI

可以使用 [describe-hosts](#) 命令。

Example 示例 1：基于标签进行筛选

以下命令描述具有标签 `Stack=production` 的快照。

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

### Example 示例 2：基于卷进行筛选

以下命令描述从指定卷创建的快照。

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

### Example 示例 3：基于快照期限进行筛选

借助 AWS CLI，您可以使用 JMESPath 通过表达式筛选结果。例如，以下命令显示您的 AWS 账户在指定日期（由 `2020-03-31` 表示）之前创建的所有快照的 ID（由 `123456789012` 表示）。如果未指定所有者，则结果将包括所有公有快照。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

以下命令显示在指定日期范围内创建的所有快照的 ID。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --output text
```

## Tools for Windows PowerShell

使用适用于 Windows 的工具查看快照信息 PowerShell

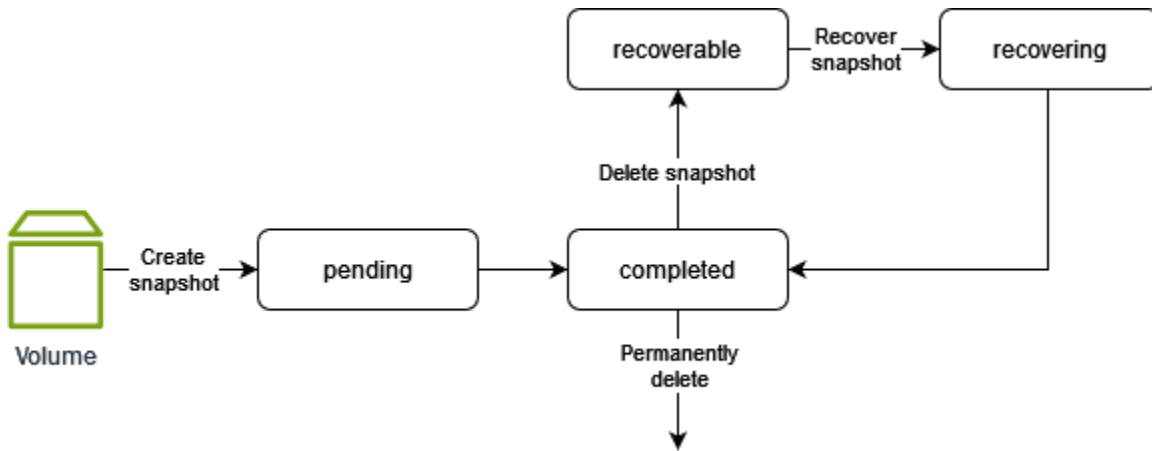
使用 [Get-EC2Snapshot](#) 命令。

```
PS C:\> Get-EC2Snapshot -SnapshotId snapshot_id
```

## 快照状态

从创建直至永久删除，Amazon EBS 快照会历经不同状态的转换。

下图阐释了快照状态之间的转换。创建快照时，其进入 pending 状态。当快照准备就绪后，其进入 completed 状态。若决定不再需要某个快照，可以删除该快照。如果删除与回收站保留规则匹配的快照，该快照会保留在回收站中并进入 recoverable 状态。如果从回收站还原快照，该快照会进入 recovering 状态，然后进入 completed 状态。否则，将永久删除此快照。



下表汇总了快照状态。

Status	描述
pending	快照创建过程仍在进行中。处于 pending 状态时，快照无法使用。
completed	快照创建过程已完成，快照可供使用。
recoverable	快照目前在回收站中。要使用快照，您必须首先从回收站中还原快照。
recovering	正在从回收站中还原快照。快照还原后会转换到 completed 状态并且可供使用。
error	快照创建过程已失败。处于 error 状态时，快照无法使用。

## 复制 Amazon EBS 快照

使用 Amazon EBS，您可以创建卷的 point-in-time 快照，我们将这些快照存储在 Amazon S3 中。创建快照并完成复制到 Amazon S3（当快照状态为 completed）后，您可以将其从一个 AWS 区域复制到另一个区域，或者复制到同一区域。Amazon S3 服务器端加密（256 位 AES）可在复制操作期间保护传输中的快照数据。快照副本将获得与原始快照 ID 不同的 ID。

要将多卷快照复制到另一个 AWS 区域，请使用您在创建多卷快照集时应用于该快照集的标签来检索快照。然后分别将快照复制到另一个区域。

如果您希望其他账户能够复制您的快照，则必须修改快照权限以允许访问该账户，或者将快照公开，以便所有 AWS 账户都能复制快照。有关更多信息，请参阅 [共享 Amazon EBS 快照](#)。

有关复制 Amazon RDS 快照的信息，请参阅 Amazon RDS 用户指南 中的 [复制数据库快照](#)。

## 使用案例

- 地理扩张：在新 AWS 地区启动您的应用程序。
- 迁移：将应用程序迁移到新区域，以实现更好的可用性以及最大限度地降低成本。
- 灾难恢复：在不同的地理位置定期备份您的数据和日志。发生灾难时，您可以使用存储在辅助区域中的 point-in-time 备份来恢复应用程序。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、更改用于加密快照的密钥，或创建您拥有的副本以从中创建卷（用于与您共享的加密快照）。
- 数据保留和审计要求：将您的加密 EBS 快照从一个 AWS 账户复制到另一个账户，以保留数据日志或其他文件，便于进行审计或数据保留。使用其他帐户有助于防止意外删除快照，并在主 AWS 帐户遭到盗用时保护您。

## 内容

- [先决条件](#)
- [注意事项](#)
- [定价](#)
- [增量快照复制](#)
- [加密和快照复制](#)
- [复制快照](#)

## 先决条件

- 您可以复制任何状态为 completed 的可访问快照，包括共享快照和您创建的快照。
- 您可以复制 AWS Marketplace、虚拟机导入/导出和 Storage Gateway 快照，但必须验证目标区域是否支持该快照。
- 要复制加密快照，您的用户必须具有以下权限才能使用 Amazon EBS 加密。
  - kms:DescribeKey
  - kms>CreateGrant
  - kms:GenerateDataKey

- kms:GenerateDataKeyWithoutPlaintext
  - kms:ReEncrypt
  - kms:Decrypt
- 要复制从其他 AWS 账户共享的加密快照，您必须有权使用用于加密快照的客户托管密钥。有关更多信息，请参阅 [共享 KMS 密钥](#)。

## 注意事项

- 每个目标区域限制并发快照复制请求不得超过 20 个。如果您超出此配额，会收到 ResourceLimitExceeded 错误。如果收到此错误，请等待一个或多个复制请求完成，然后再发出新的快照复制请求。
- 用户定义的标签不会从源快照复制到新快照。您可以在复制操作期间或之后添加用户定义的标签。
- 由快照复制操作创建的快照具有任意性的卷 ID，例如 vol-ffff 或 vol-ffffffff。这些任意性的卷 ID 不应用于任何目的。
- 为快照复制操作指定的资源级权限仅适用于新快照。您不能为源快照指定资源级权限。有关示例，请参阅 [示例：复制快照](#)。

## 定价

- 有关跨 AWS 区域和账户复制快照的定价信息，请参阅 [Amazon EBS 定价](#)。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 如果您将快照复制到新区域，则会创建完整（非增量）副本。这会产生额外的存储成本。同一快照的后续副本是增量副本。
- 如果使用外部或跨区域数据传输，则将收取额外的 [EC2 数据传输](#) 费用。而且，如果在启动后删除任何快照，仍需要为已传输的数据付费。

## 增量快照复制

快照副本是否为增量副本是由最近完成的快照复制决定的。在跨区域或账户复制快照时，如果满足以下条件，则副本为增量副本：

- 快照以前已复制到目标区域或账户。
- 最新的快照副本仍位于目标区域或账户中。

- 最新的快照副本尚未存档。
- 目标区域或账户中的所有快照副本均未加密，或者是使用同一 KMS 密钥加密的。

如果删除了最新的快照副本，则下一个副本是完整副本，而不是增量副本。如果某个副本在您启动另一个副本时仍处于挂起状态，则第二个副本仅在第一个副本完成后才开始。

使用相同的 KMS 密钥在同一账户和区域内执行快照复制操作会生成增量复制。

增量快照复制会缩短复制快照所需的时间，并且不会复制数据，从而节省数据传输和存储成本。

我们建议您使用卷 ID 和创建时间来标记快照，以便在目标区域或账户中跟踪卷的最新快照副本。

要查看您的快照副本是否为增量副本，请查看 CopySn [apshot 事件](#) CloudWatch。

## 加密和快照复制

在复制快照时，您可以加密副本，也可以指定一个与原始快照不同的 KMS 密钥，这样，生成的快照副本将使用新 KMS 密钥。但是，在复制操作过程中更改快照的加密状态可能会生成完整（非增量）副本，这可能产生更多的数据传输和存储费用。有关更多信息，请参阅 [增量快照复制](#)。

要复制从其他 AWS 账户共享的加密快照，您必须有权使用快照和用于加密快照的客户托管密钥 (CMK)。使用与您共享的加密快照时，我们建议您使用您拥有的 KMS 密钥复制快照以对其进行重新加密。这样，即使原始 KMS 密钥泄露或所有者将其撤销，您也不会失去对使用快照创建的任何加密卷的访问权限。有关更多信息，请参阅 [共享 Amazon EBS 快照](#)。

您可以将 Encrypted 参数设置为 true，以将加密应用到 EBS 快照副本。（如果启用了 [默认加密](#)，Encrypted 参数是可选的）。

或者，您可以使用 KmsKeyId 指定要用于加密快照副本的自定义密钥。（即使启用了默认加密，也必须将 Encrypted 参数设置为 true。）如果未指定 KmsKeyId，则用于加密的密钥取决于源快照的加密状态及其所有权。

下表描述了在复制您拥有的快照以及与您共享的快照时，每种可能设置组合的加密结果。

默认加密	是否设置了 Encrypted 参数？	源快照加密状态	默认值（未指定 KMS 密钥）	自定义（已指定 KMS 密钥）
已禁用	否	未加密	未加密	不适用

默认加密	是否设置了 <b>Encrypted</b> 参数？	源快照加密状态	默认值 ( 未指定 KMS 密钥 )	自定义 ( 已指定 KMS 密钥 )
		已加密	加密者为 AWS 托管式密钥	
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	
已启用	否	未加密	由默认 KMS 密钥加密	不适用
		已加密	由默认 KMS 密钥加密	
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	

\*\* 这是复制快照操作中所指定的 KMS 密钥。将为账户和区域使用此 KMS 密钥，而不是使用默认的 KMS 密钥。

## 复制快照

要复制快照，请使用以下方法之一。

### Console

#### 使用控制台复制快照

1. 打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择要复制的快照，然后选择 Actions ( 操作 )、Copy snapshot ( 复制快照 )。



4. (可选) 在 Description (描述) 中, 输入快照副本的简短描述。

在默认情况下, 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。您可以按需更改此描述。

5. 对于 Destination Region (目标区域), 选择要在其中创建快照副本的区域。
6. 指定快照副本的加密状态。

如果源快照已加密, 或者您的账户已启用[默认加密](#), 快照副本会自动加密, 您无法更改其加密状态。

如果源快照未加密, 并且在默认情况下未为您的账户启用加密, 则您可以选择启用或禁用加密。要加密快照副本, 请在 Encryption (加密) 中选择 Encrypt this snapshot (加密快照)。然后, 在 KMS key (KMS 密钥) 中, 选择要用于对目标区域中的快照进行加密的 KMS 密钥。

7. 选择复制快照。

## AWS CLI

要使用复制快照 AWS CLI

使用 [copy-snapshot](#) 命令。

## Tools for Windows PowerShell

使用适用于 Windows 的工具复制快照 PowerShell

使用 [Copy-EC2Snapshot](#) 命令。

## 检查是否失败

如果您在未获得加密密钥使用权限的情况下试图复制加密快照, 则操作将失败, 且系统不会提示。您刷新页面后, 控制台才会显示错误状态。您还可以通过命令行检查快照的状态, 如以下示例所示。

```
aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

如果由于密钥权限不足而导致复制失败, 您将看到以下消息: "StateMessage": "无法访问给定的密钥 ID"。

在复制加密的快照时, 您必须对默认 CMK 具有 DescribeKey 权限。显式拒绝这些权限将导致复制失败。有关管理 CMK 密钥的信息, 请参阅 [AWS KMS 身份验证和访问控制](#)。

## 共享 Amazon EBS 快照

如果您想与其他 AWS 账户共享快照，可以修改快照的权限。您可以与所有其他 AWS 账户公开共享快照，也可以与您指定的个人 AWS 账户私下共享快照。您已授权的用户可以使用您共享的快照来创建自己的 EBS 卷，同时您的原始快照不受影响。

### Important

共享快照时，您可以让其他人访问快照上的所有数据。仅与您信任的人共享所有快照数据的快照。

要防止公开共享您的快照，您可以启用快照的阻止公开访问权限。有关更多信息，请参阅[阻止公开访问 AMI](#)。

### 主题

- [共享快照之前](#)
- [共享快照](#)
- [共享 KMS 密钥](#)
- [查看与您共享的快照](#)
- [使用与您共享的快照](#)
- [确定共享快照的用途](#)

## 共享快照之前

共享快照时需考虑以下事项：

- 如果为此区域阻止公开访问快照，将阻止尝试公开共享快照的行为。仍然可以私下共享快照。
- 快照受限于在其中创建它们的区域。要与其他区域共享快照，请将快照复制到该区域，然后分享副本。有关更多信息，请参阅[复制 Amazon EBS 快照](#)。
- 您无法共享使用默认 AWS 托管式密钥加密的快照。您只能共享使用客户托管密钥加密的快照。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的[创建密钥](#)。
- 您只能公开共享未加密的快照。
- 共享加密快照时，还必须共享用于加密快照的客户托管密钥。有关更多信息，请参阅[共享 KMS 密钥](#)。

## 共享快照

您可以使用本节介绍的方法之一共享快照。

### Console

#### 共享快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择快照，然后依次选择 Actions ( 操作 )、Modify Permissions ( 修改权限 )。
4. 请指定快照的权限。Current setting ( 当前设置 ) 表示快照的当前共享权限。
  - 要与所有 AWS 账户公开共享快照，请选择公开。
  - 要与特定 AWS 账户私下共享快照，请选择“私人”。然后，在共享账户部分中，选择添加账户，接着输入要与之共享的账户的 12 位账户 ID ( 不带连字符 )。
5. 选择保存更改。

### AWS CLI

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要与特定 AWS 账户共享快照，请将用户设置为该 AWS 账户的 ID。

#### 公开共享快照

使用 [modify-snapshot-attribute](#) 命令。

对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于 `--group-names`，请指定 `all`。

```
$ aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute createVolumePermission --operation-type add --group-names all
```

#### 私密共享快照

使用 [modify-snapshot-attribute](#) 命令。

对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于 `--user-ids`，请指定要与之共享快照的 AWS 账户的 12 位 ID。

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

## Tools for Windows PowerShell

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要与特定 AWS 账户共享快照，请将用户设置为该 AWS 账户的 ID。

### 公开共享快照

使用 [Edit-EC2SnapshotAttribute](#) 命令。

对于 `-Attribute`，请指定 `CreateVolumePermission`。对于 `-OperationType`，请指定 `Add`。对于 `-GroupName`，请指定 `all`。

```
PS C:\> Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute  
CreateVolumePermission -OperationType Add -GroupName all
```

### 私密共享快照

使用 [Edit-EC2SnapshotAttribute](#) 命令。

对于 `-Attribute`，请指定 `CreateVolumePermission`。对于 `-OperationType`，请指定 `Add`。对于 `UserId`，请指定要与之共享快照的 AWS 账户的 12 位 ID。

```
PS C:\> Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute  
CreateVolumePermission -OperationType Add -UserId 123456789012
```

## 共享 KMS 密钥

共享加密快照时，还必须共享用于加密快照的客户托管密钥。您可以在创建客户托管密钥时或以后的某个时间向客户托管密钥应用跨账户权限。

必须为正在访问加密快照的共享客户托管密钥用户授予对密钥执行以下操作的权限：

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`

- kms:ReEncrypt
- kms:Decrypt

**i** Tip

为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用 kms:GrantIsForAWSResource 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权。

有关如何控制对客户托管密钥的访问权限的更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [使用 AWS KMS 中的密钥策略](#)。

### 使用 AWS KMS 控制台共享客户托管密钥

1. 打开 AWS KMS 控制台，[网址为 https://console.aws.amazon.com/kms](https://console.aws.amazon.com/kms)。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 在别名列中，选择用于加密快照的客户托管密钥的别名（文本链接）。密钥详细信息将在新页面中打开。
5. 在密钥策略部分中，您会看到策略视图或默认视图。策略视图显示密钥策略文档。默认视图显示密钥管理员、密钥删除、密钥使用和其他 AWS 账户几个部分。如果您在控制台中创建了策略，但尚未对其进行自定义，则会显示默认视图。如果默认视图不可用，则需要策略视图中手动编辑策略。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [查看密钥策略（控制台）](#)。

根据您可以访问的视图，使用策略视图或默认视图，向策略中添加一个或多个 AWS 账户 ID，如下所示：

- （策略视图）选择编辑。在以下语句中添加一个或多个 AWS 账户 ID："Allow use of the key"和"Allow attachment of persistent resources"。选择保存更改。在以下示例中，AWS 账户 ID 444455556666 已添加到策略中。

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
```

```

    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}

```

- (默认视图) 向下滚动到“其他 AWS 账户”。选择“添加其他 AWS 账户”，然后根据提示输入 AWS 账户 ID。要添加其他账户，请选择添加其他 AWS 账户并输入 AWS 账户 ID。添加完所有 AWS 账户后，选择 Save changes (保存更改)。

## 查看与您共享的快照

您可以使用以下方法之一查看与您共享的快照。

### Console

#### 使用控制台查看共享快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 筛选列出的快照。在屏幕的左上角，选择以下选项之一：

- 私有快照 – 仅查看与您私下共享的快照。
- 公有快照 – 仅查看与您公开共享的快照。

## AWS CLI

使用命令行查看快照权限

使用 [describe-snapshot-attribute](#) 命令。

## Tools for Windows PowerShell

使用命令行查看快照权限

使用 [Get-EC2SnapshotAttribute](#) 命令。

## 使用与您共享的快照

### 使用共享的未加密快照

按 ID 或描述查找共享快照。有关更多信息，请参阅[查看与您共享的快照](#)。您可以像使用账户中拥有的任何其他快照一样使用此快照。例如，您可以从快照中创建卷或将卷复制到其他区域。

### 使用共享的已加密快照

按 ID 或描述查找共享快照。有关更多信息，请参阅[查看与您共享的快照](#)。在您的账户中创建共享快照的副本，并使用您拥有的 KMS 密钥对副本进行加密。然后，您可以使用副本创建卷，也可以将其复制到不同的区域。

## 确定共享快照的用途

您可以使用 AWS CloudTrail 来监控您与他人共享的快照是否被复制或用于创建卷。记录了以下事件 CloudTrail：

- SharedSnapshotCopyInitiated— 正在复制共享快照。
- SharedSnapshotVolumeCreated— 正在使用共享快照来创建卷。

有关使用的更多信息 CloudTrail，请参阅使用[记录亚马逊 EC2 和 Amazon EBS API 调用 AWS CloudTrail](#)。

## 归档 Amazon EBS 快照

Amazon EBS 快照归档是一个新存储层，可用于长期低成本地存储很少访问且不需要频繁或快速检索的快照。

默认情况下，快照在创建时将存储在 Amazon EBS 快照标准层中（标准层）。存储在标准层中的快照可递增。这意味着只在卷上保存在最新快照之后发生更改的数据块。

归档快照时，增量快照将转换为完整快照，然后从标准层移动到 Amazon EBS 快照归档层（归档层）。完整快照包括创建快照时写入卷的所有数据块。

当您需要访问归档的快照时，可以将其从归档层还原到标准层，然后像使用账户中任何其它快照一样使用它。

Amazon EBS 快照归档为您存储极少需要访问的快照达 90 天或更长时间，同时存储成本降低 75%。

一些典型的使用案例包括：

- 归档卷的唯一快照，例如项目结束快照
- 出于合规性考虑，请将完整的时间点增量快照归档。
- 归档月度、季度或每年的增量快照。

### 主题

- [注意事项和限制](#)
- [定价和计费](#)
- [配额](#)
- [归档快照的准则和最佳做法](#)
- [所需的 IAM 权限](#)
- [使用快照归档](#)
- [监控快照归档](#)

## 注意事项和限制

### 注意事项

- 最短归档期为 90 天。如果您在最短 90 天的归档期限到来之前删除或永久还原已归档的快照，则需要为归档层的剩余天数付费（四舍五入到最接近的小时数）。有关更多信息，请参阅[定价和计费](#)。



- 将归档快照从归档层还原到标准层最长可能需要 72 小时，具体时间取决于快照的大小。
- 归档的快照始终是完整的快照。完整快照包含创建快照时写入卷的所有块。完整快照可能会大于它赖以创建的增量快照。但是，如果您在标准层上只有一个卷的增量快照，则归档层中的完整快照的大小将与标准层中的快照大小相同。这是因为卷的第一个快照始终是完整快照。
- 建议将月度、季度或每年快照存档。与将单个卷的每日增量快照保存在标准层中相比，将单个卷的每日增量快照存档可能会导致成本增加。
- 在归档快照时，快照谱系中其它快照引用的快照数据将保留在标准层中。与保留在标准层中的引用数据相关的数据和存储成本将分配给谱系中的下一个快照。这可以确保谱系中的后续快照不会受到归档的影响。
- 如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。要使用快照，您必须首先从回收站中恢复快照，然后从归档层中还原它。有关更多信息，请参阅[回收站](#)和[定价和计费](#)。
- 您不能在块设备映射中使用已归档快照或创建 Amazon EBS 卷。
- 您可以存档由 AWS Backup 使用 AWS Backup 控制台、API 或命令行工具创建的快照。有关更多信息，请参阅《AWS Backup 开发人员指南》中的[制定备份计划](#)。

## 限制

- 您只能归档状态为 `completed` 状态的快照。
- 您只能归档您在账户中拥有的快照。要归档与您共享的快照，首先将快照复制到您的账户，然后将快照副本归档。
- 在使用归档快照之前，必须先将其还原到标准层。要通过 `CreateVolume` 和 `RunInstances` API 操作从快照创建卷，以及共享或复制快照，都需要恢复到标准层。有关更多信息，请参阅[还原已归档的快照](#)。
- 只有禁用所有关联的 AMI 后，您才能归档与一个或多个 AMI 关联的快照。有关更多信息，请参阅[禁用 AMI](#)。
- 如果关联的快照已暂时恢复，则无法启用已禁用的 AMI。在启用 AMI 之前，必须永久恢复所有关联的快照。
- 在快照归档或快照还原过程启动后，您无法取消它。
- 您不能共享已归档的快照。如果归档了与其它账户共享的快照，则在归档快照后，与之共享快照的账户将失去访问权限。
- 您不能复制已归档的快照。如果需要复制归档的快照，则必须首先将其还原。
- 您不能为归档快照启用快速快照还原。快照归档后，快速快照还原会自动禁用。如果您需要使用快速快照还原，则必须在还原快照后手动启用该选项。

## 定价和计费

归档的快照按每 GB 每月 0.0125 美元的费率计费。例如，如果您归档 100GiB 快照，则每月需支付 1.25 美元 ( 100GiB x 0.0125 美元 ) 的费用。

快照还原的费率为每 GB 还原数据收费 0.03 美元。例如，如果您从归档层还原 100GiB 快照，则需要一次向您收取费用 3 美元 ( 100GiB x 0.03 美元 )。

快照还原到标准层后，快照按每 GB 每月 0.05 美元的标准费率计费。

有关更多信息，请参阅 [Amazon EBS 定价](#)。

### 按最短归档期收费

最短归档期为 90 天。如果您在最短 90 天的归档期限之前删除或永久还原归档的快照，则按比例收取的费用等于剩余天数的归档层存储费用 ( 四舍五入到最接近的小时数 )。例如，如果在 40 天之后删除或永久恢复归档快照，则将收取剩余 50 天的最小存档期的费用。

#### Note

在最短 90 天的归档期限之前暂时还原已归档的快照，不会产生此费用。

### 临时还原

当您临时还原快照时，快照将从归档层还原到标准层，并且快照的副本将保留在归档层中。在临时还原期间，您需要为标准层中的快照和归档层中的快照副本付费。从标准层中删除临时还原的快照时，您不再需要为其付费，而只需为归档层中的快照付费。

### 永久还原

当您永久还原快照时，快照将从归档层还原到标准层，并且快照将从归档层删除。您仅需为标准层中的快照付费。

### 删除快照

如果在归档快照时删除快照，则需要为已移动到归档层的快照数据付费。数据最短归档期限为 90 天，并要在删除时支付相应的费用。例如，如果您归档了 100GiB 快照，并且在仅归档 40GiB 之后删除快照，则对于已归档的 40GiB 而言，您需要支付最少 90 天的归档期费用 1.50 美元 ( 每 GB 每月费率 0.0125 美元 \* 40GB \* ( 90 天 \* 24 小时 ) / ( 24 小时/天 \* 每月 30 天 ) )。

如果在从归档层还原快照时删除快照，您需要为快照的完整大小（快照大小 x 0.03 美元）支付快照还原费用。例如，如果您从归档层还原 100GiB 快照，并且在快照还原完成之前的任何时候删除快照，则需支付 3 美元（100GiB 快照大小 x 0.03 美元）的费用。

## 回收站

归档的快照在回收站中时，按归档快照的费率计费。回收站中的归档快照的最短归档期限为 90 天，如果在最短归档期限到来之前被回收站删除，则会产生相应费用。换句话说，如果按照某保留规则，在最短期限 90 天之前从回收站中删除了归档的快照，则需要为剩余天数付费。

如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。它会按归档快照的费率计费。

如果在还原快照时删除与保留规则匹配的快照，则还原的快照将在保留期剩余时间内保留在回收站中，并按标准快照费率计费。要使用快照，您必须首先从回收站中恢复快照。

有关更多信息，请参阅[回收站](#)。

## 成本跟踪

归档的快照在 AWS 成本和使用情况报告 显示相同的资源 ID 和 Amazon 资源名称（ARN）。有关更多信息，请参阅[AWS 成本和使用情况报告 用户指南](#)。

您可以使用以下使用类型来确定相关成本：

- SnapshotArchiveStorage – 月度数据存储费
- SnapshotArchiveRetrieval – 快照还原的一次性费用
- SnapshotArchiveEarlyDelete – 在最短归档期限（90 天）之前删除或永久还原快照的费用

## 配额

本部分介绍了归档快照和正在进行的快照的默认配额。

限额	默认限额			
每卷的 已归档 快照	25			

限额	默认限额			
每个账户的正在并发进行的快照归档	25			
每个账户的正在并发进行的快照还原	5			

如果您需要的容量超出目标容量的默认限制，请填写 AWS Support 中心[创建案例](#)表格请求增加限制。

## 归档快照的准则和最佳做法

本部分提供了归档快照的准则和最佳做法。

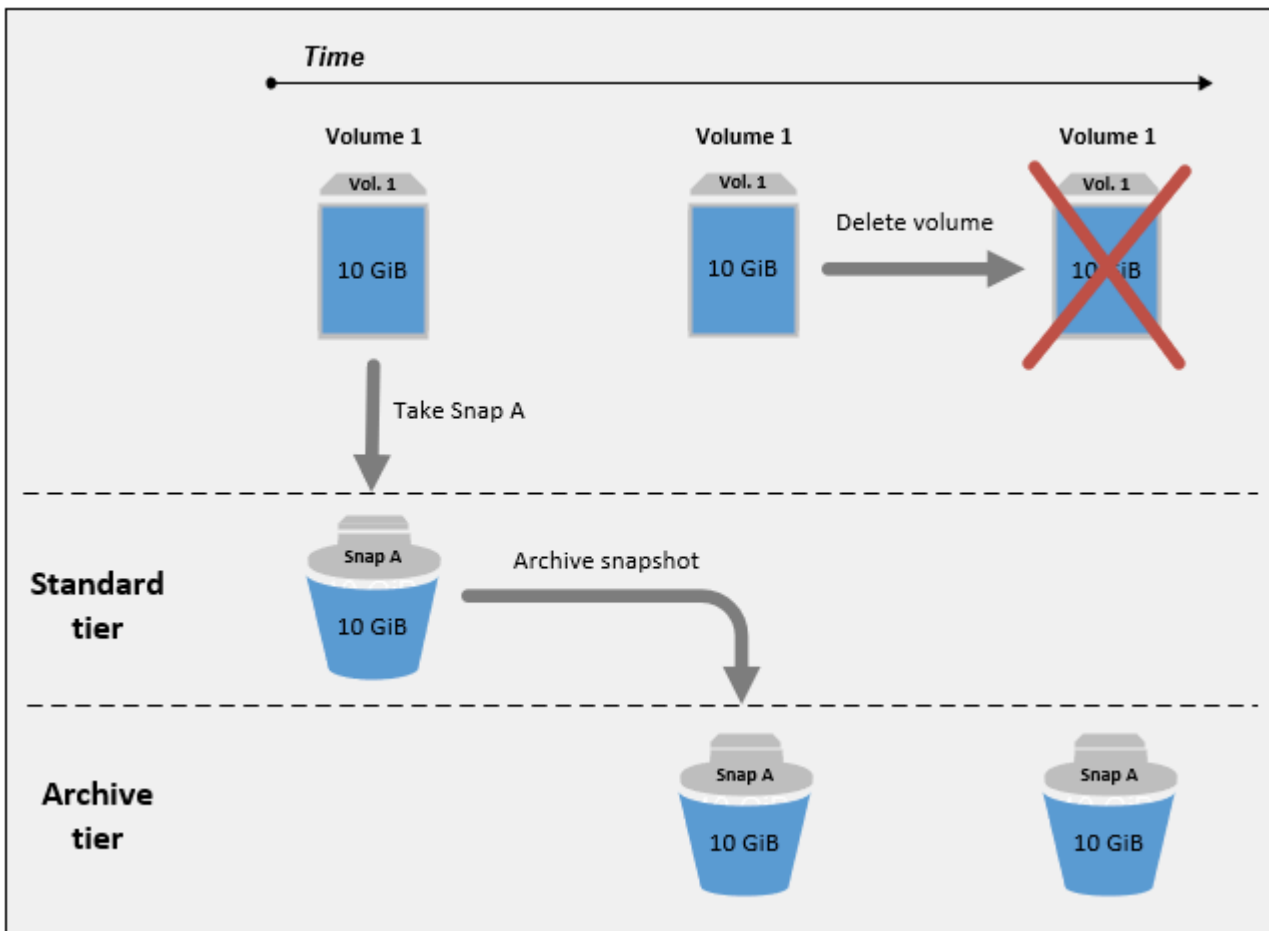
### 主题

- [归档卷的唯一快照](#)
- [归档单个卷的增量快照](#)
- [出于合规性原因归档完整快照](#)
- [确定标准层存储成本的减少程度](#)

### 归档卷的唯一快照

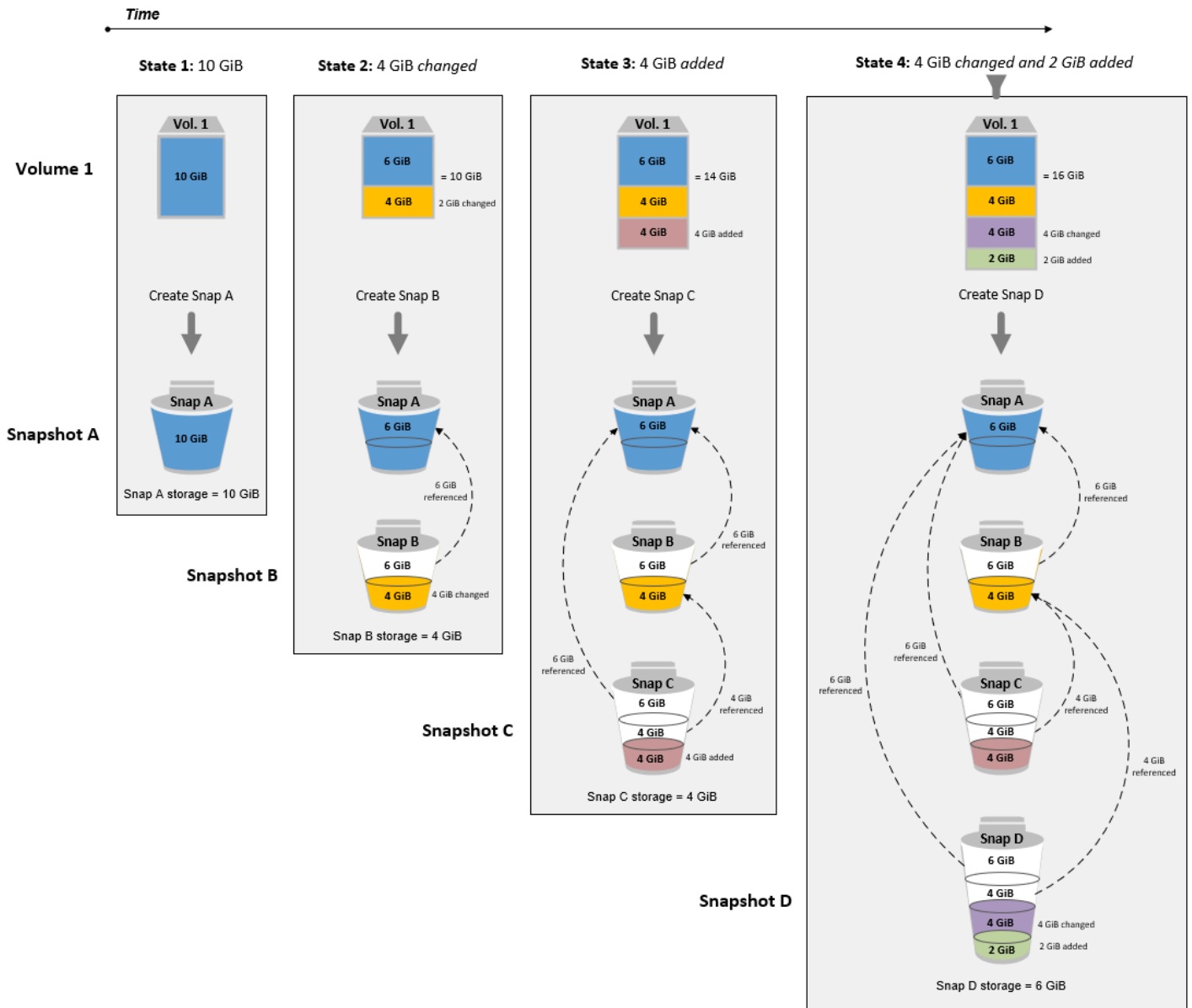
如果只存在卷的一个快照，则快照的大小始终与创建快照时写入卷的块的大小相同。归档此类快照时，标准层中的快照将转换为同等大小的完整快照，然后从标准层移动到归档层。

归档这些快照可以帮助您以更低的存储成本节省开支。如果不再需要源卷，则可以删除该卷以进一步节省存储成本。



### 归档单个卷的增量快照

归档增量快照时，增量快照将转换为完整快照，然后从标准层移动到归档层。例如，在下图中，如果您归档快照 B，快照将转换为大小为 10GiB 的完整快照并移动到归档层。同样，如果您归档快照 C，归档层中的完整快照大小为 14GiB。



如果要归档快照以降低标准层中的存储成本，您不应归档一组增量快照中的第一个快照。快照谱系中的后续快照引用了这些快照。在大多数情况下，归档这些快照不会降低存储成本。

**Note**

您不应归档一组增量快照中的最后一个快照。最后一个快照是卷的最新快照。如果要在卷损坏或丢失的情况下从快照中创建卷，则需要在标准层中使用此快照。

如果归档了一个快照，而该快照包含了谱系中后续快照所引用的数据，那么与所引用数据关联的数据存储和存储成本将分配给后续快照。在这种情况下，归档这些快照不会降低数据存储成本。例如，在上一张图片中，如果归档快照 B，它的 4GiB 的数据相当于由快照 C 产生。在这种情况下，总体存储成本将增加，因为您需要为归档层的快照 B 完整版付费，而标准层的存储成本保持不变。

如果归档快照 C，标准层存储将减少 4GiB，因为该数据未被谱系中任何其它后续快照引用。而且，由于快照已转换为完整快照，您的归档层存储将增加 14GiB。

### 出于合规性原因归档完整快照

出于合规性考虑，您可能需要每月、每季度或每年创建卷的完整备份。对于这些备份，您可能需要独立快照而不向后或向前引用快照谱系中的其它快照。使用 EBS 快照归档功能归档的快照是完整快照，它们没有引用谱系中的其它快照。此外，为了遵循合规性要求，您可能需要保留这些快照数年。EBS 快照归档使归档这些完整快照以长期保留具备良好的成本效益。

### 确定标准层存储成本的减少程度

如果要归档增量快照以降低存储成本，您应考虑归档层中完整快照的大小和标准层存储空间减少的程度。本部分介绍如何进行设置。

#### Important

在调用 API 的时间点，API 响应的数据是准确的。由于与快照相关的数据随着快照谱系的变化而发生变化，API 响应可能会有所不同。

要确定标准层存储空间和存储成本的降低，请使用以下步骤。

1. 检查完整快照的大小。要确定快照的完整大小，请使用 [list-snapshot-blocks](#) 命令。对于 `--snapshot-id`，请指定需归档快照 ID。

```
$ aws ebs list-snapshot-blocks --snapshot-id snapshot_id
```

这会返回有关指定快照中所有数据块的信息。该命令返回的最后一个数据块的 `BlockIndex` 表示快照中的数据块数。数据块数乘以 512KiB（即快照数据块大小），结果接近归档层中完整快照的大小（数据块数 x 512KiB = 完整快照大小）。

例如，以下命令会列出快照 `snap-01234567890abcdef` 的数据块。

```
$ aws ebs list-snapshot-blocks --snapshot-id snap-01234567890abcdef
```

以下是命令输出，其中省略了一些数据块。以下输出表明快照包括大约 16383 个数据块。这相当于约 8GiB 的完整快照大小 ( 16383 x 512KiB = 7.99GiB )。

```
{
  "VolumeSize": 8,
  "Blocks": [
    {
      "BlockToken": "ABgBAeShfa5RwG+RiWUg2pwmnCU/
YmNv7fGMxLbCwfEBEUmmuqac5RmoyVat",
      "BlockIndex": 0
    },
    {
      "BlockToken": "ABgBATdTONyThPUAbQhbUQXsn5TGoY/
J17GfE83j9WN7siupav0Tw9E1KpFh",
      "BlockIndex": 1
    },
    {
      "BlockToken": "EBEUmmuqXsn5TGoY/QwmnCU/YmNv74eKE2TSsn5TGoY/
E83j9WQhbUQXsn5T",
      "BlockIndex": 4
    },
    .....
    {
      "BlockToken": "yThPUAbQhb5V8xpwmnCU/
YmNv74eKE2TSFY1sKP/4r05y47WETdTONyThPUA",
      "BlockIndex": 12890
    },
    {
      "BlockToken":
"ABgBASHKD5V8xEbaRKdxdkZZS4eKE2TSFY1MG1sKP/4r05y47WEHqKaNPcLs",
      "BlockIndex": 12906
    },
    {
      "BlockToken": "ABgBARR0GMUJo6P9X3CFHQGZNQ7av9B6vZtTTqV89QqC
+Sk00HWMlwkGXjnA",
      "BlockIndex": 16383
    }
  ],
  "VolumeSize": 8,
  "ExpiryTime": 1637677800.845,
  "BlockSize": 524288
}
```



2. 找到需归档快照的源卷 ( 快照创建自此卷 )。可以使用 [describe-hosts](#) 命令。对于 `--snapshot-id`，请指定需归档快照 ID。响应参数 `VolumeId` 表示源卷 ID。

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

例如，以下命令返回有关快照 `snap-09c9114207084f0d9` 的信息。

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

以下是命令输出，它表示该快照 `snap-09c9114207084f0d9` 通过卷 `vol-0f3e2c292c52b85c3` 创建。

```
{
  "Snapshots": [
    {
      "Description": "",
      "Tags": [],
      "Encrypted": false,
      "VolumeId": "vol-0f3e2c292c52b85c3",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-11-16T08:29:49.840Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-09c9114207084f0d9"
    }
  ]
}
```

3. 查找通过该源卷创建的所有快照。可以使用 [describe-hosts](#) 命令。请指定 `volume-id` 筛选条件，并指定在上一步中得到的卷 ID 作为筛选条件值。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

例如，以下命令返回创建自卷的所有快照 `vol-0f3e2c292c52b85c3`。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
Values=vol-0f3e2c292c52b85c3"
```

以下是命令输出，表示三个快照通过卷创建 `vol-0f3e2c292c52b85c3`。

```
{
  "Snapshots": [
    {
      "Description": "",
      "Tags": [],
      "Encrypted": false,
      "VolumeId": "vol-0f3e2c292c52b85c3",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-11-14T08:57:39.300Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-08ca60083f86816b0"
    },
    {
      "Description": "",
      "Tags": [],
      "Encrypted": false,
      "VolumeId": "vol-0f3e2c292c52b85c3",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-11-15T08:29:49.840Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-09c9114207084f0d9"
    },
    {
      "Description": "01",
      "Tags": [],
      "Encrypted": false,
      "VolumeId": "vol-0f3e2c292c52b85c3",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-11-16T07:50:08.042Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-024f49fe8dd853fa8"
    }
  ]
}
```

4. 使用上一个命令的输出，按照创建时间（从最早到最新）对快照进行排序。每个快照的响应参数 `StartTime` 表示其创建时间（UTC 时间格式）。

例如，按创建时间（从最早到最新）排列的上一步返回的快照如下所示：

1. `snap-08ca60083f86816b0`（最早 – 在需归档快照产生之前创建）
  2. `snap-09c9114207084f0d9`（要归档的快照）
  3. `snap-024f49fe8dd853fa8`（最新 – 紧接着需归档的快照之后创建）
5. 确定在需归档快照产生之前和之后紧邻着创建的快照。在这种情况下，您要归档快照 `snap-09c9114207084f0d9`，这是在三个快照集中创建的第二个增量快照。快照 `snap-08ca60083f86816b0` 正好在其之前创建，而快照 `snap-024f49fe8dd853fa8` 紧接其后创建。
  6. 在需归档的快照中找到未引用的数据。首先，找出需归档快照以及正好在其之前创建的快照之间不同的数据块。使用 [list-changed-blocks](#) 命令。对于 `--first-snapshot-id`，请指定正好在需归档快照之前创建的快照 ID。对于 `--second-snapshot-id`，请指定需归档快照 ID。

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-snapshot-id snapshot_to_archive
```

例如，以下命令显示了以下两个快照之间不同数据块的块索引：快照 `snap-08ca60083f86816b0`（正好在需归档快照之前创建的快照），以及快照 `snap-09c9114207084f0d9`（需归档快照）。

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-snapshot-id snap-09c9114207084f0d9
```

下面显示了命令输出，其中省略了一些数据块。

```
{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1r0VeFbWXsH3W4z/",
      "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
      "BlockIndex": 4
    },
  ],
}
```

```

    {
      "FirstBlockToken": "ABgBAcfL
+EfmQm1NgstqrFnYgsAxR4SDS04LkNLY00ChGBWcfJnnpn90E9XX1",
      "SecondBlockToken": "ABgBAdX0mtX6aBAAt3EBy
+8jFCESMpig7csKjb020cd08m2iNJV2Ue+cRwUqF",
      "BlockIndex": 5
    },
    {
      "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUI3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
      "SecondBlockToken":
"ABgBADewWkHKTcrhZmsfm7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
      "BlockIndex": 13
    },
    {
      "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVn0qPxm9r7Wf60+i
+1tZ0dwPpGN39ijztLn",
      "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcw7CD9w4J2td",
      "BlockIndex": 14
    },
    {
      "FirstBlockToken":
"ABgBAZBFev4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICG1FmZCyJXzE4r3",
      "SecondBlockToken":
"ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVClndnpc91zBiNmSfW9ouIlbeXWy",
      "BlockIndex": 15
    },
    .....
    {
      "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5V05Q3rEEA
+ku50P498hjnTAgMhLG",
      "BlockIndex": 13171
    },
    {
      "SecondBlockToken":
"ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
      "BlockIndex": 13172
    },
    {
      "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWi0uj0AKcau0nUFC0
+eZ5ASVdWLXWwC04ijfoDTpTVZ",
      "BlockIndex": 13173
    },
  },

```

```

    {
      "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6t0vMoLBLJ14LKvavw4IiB1d0iykWe6b",
      "BlockIndex": 13174
    },
    {
      "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
      "BlockIndex": 13175
    }
  ],
  "ExpiryTime": 1637648751.813,
  "VolumeSize": 8
}

```

接下来，使用相同的命令查找需归档快照与紧接其后创建的快照之间不同的数据块。对于 `--first-snapshot-id`，请指定需归档快照 ID。对于 `--second-snapshot-id`，请指定紧接着需归档快照之后创建的快照 ID。

```

$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after

```

例如，以下命令显示了以下两个快照之间不同块的数据块索引：快照 `snap-09c9114207084f0d9`（在需归档快照之后立即创建的快照），以及快照 `snap-024f49fe8dd853fa8`（需归档快照）。

```

$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8

```

下面显示了命令输出，其中省略了一些数据块。

```

{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
      "SecondBlockToken":
"ABgBASEvi9x80m7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
      "BlockIndex": 4
    }
  ]
}

```

```

    },
    {
      "FirstBlockToken": "ABgBAeL0mtX6aBAAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
      "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLk0",
      "BlockIndex": 5
    },
    {
      "FirstBlockToken":
"ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
      "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrx0qGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
      "BlockIndex": 13
    },
    {
      "FirstBlockToken":
"ABgBAbRlitCVI7c6hGsT4cckKcW6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
      "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyv0wpozYII6UNCT",
      "BlockIndex": 14
    },
    {
      "FirstBlockToken": "ABgBAd+yxC026I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
      "SecondBlockToken": "ABgBACppnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
      "BlockIndex": 18
    },
    .....
    {
      "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV031U/lKCW
+CTxF13cQ5p2f2h1njpuUiGbqKGUa",
      "BlockIndex": 13190
    },
    {
      "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWvpBIshmeyeS5FD/M0i64U+a9",
      "BlockIndex": 13191
    },
    {
      "SecondBlockToken": "ABgBAZ8DhMk+rR0Xa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
      "BlockIndex": 13192
    }

```

```

    },
    {
      "SecondBlockToken":
"ABgBATH6MBVE90416sq0C27s1nVntFUPDwiMcRWGyJHy8sIgGL5yuYXHAvty",
      "BlockIndex": 13193
    },
    {
      "SecondBlockToken":
"ABgBARuZykaFBWpCWtJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn610Qyy+giN",
      "BlockIndex": 13194
    }
  ],
  "ExpiryTime": 1637692677.286,
  "VolumeSize": 8
}

```

7. 比较上一步中两个命令返回的输出。如果两个命令输出中都显示相同的数据块索引，则表示该数据块包含未引用的数据。

例如，上一步中的命令输出表明数据块 4、5、13 和 14 对于快照 `snap-09c9114207084f0d9` 来说是唯一的，而且快照谱系中的任何其他快照都不会引用这些数据块。

要确定标准层存储空间的减少多少，请将两个命令输出中出现的数据块数乘以 512KiB，即得出快照数据块大小。

例如，如果在两个命令输出中都出现 9950 个数据块索引，则表明您将减少标准层存储大约 4.85GiB ( 9950 个数据块 x 512KiB = 4.85GiB )。

8. 确定在标准层中存储未引用的数据块达 90 天的存储成本。将此值与归档层中的完整快照存储成本（如步骤 1 所述）进行比较。假设在最短 90 天的期限内没有从归档层还原完整快照，您可以通过比较这些值来确定节省的成本。有关更多信息，请参阅[定价和计费](#)。

## 所需的 IAM 权限

默认情况下，用户无权使用快照归档。要允许用户使用快照归档，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。有关更多信息，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

要使用快照归档，用户需要以下权限。

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`

- `ec2:RestoreSnapshotTier`

控制台用户可能还需要其他权限，例如 `ec2:DescribeSnapshots`。

要归档和恢复加密快照，需要以下 AWS KMS 额外权限。

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

以下是 IAM policy 示例，授予了 IAM 用户归档、恢复和查看加密及未加密快照的权限。其包括控制台用户的 `ec2:DescribeSnapshots` 权限。如果不需要某些上述权限，您可以从策略中将其删除。

#### Tip

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 AWS 服务代表用户创建授权时，才使用 `kms:GrantIsForAWSResource` 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSnapshotTierStatus",
      "ec2:ModifySnapshotTier",
      "ec2:RestoreSnapshotTier",
      "ec2:DescribeSnapshots",
      "kms:CreateGrant",
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": true
      }
    }
  ]
}
```



```
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和群组：

创建权限集。按照《AWS IAM Identity Center 用户指南》中[创建权限集](#)的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

创建适用于身份联合验证的角色。按照《IAM 用户指南》中[为第三方身份提供商创建角色 \( 联合身份验证 \)](#)的说明进行操作。

- IAM 用户：

- 创建您的用户可以代入的角色。按照《IAM 用户指南》中[为 IAM 用户创建角色](#)的说明进行操作。
- ( 不推荐使用 ) 将策略直接附加到用户或将用户添加到用户群组。按照《IAM 用户指南》中[向用户添加权限 \( 控制台 \)](#)中的说明进行操作。

## 使用快照归档

### 主题

- [归档快照](#)
- [还原已归档的快照](#)
- [修改临时还原快照的还原期或还原类型](#)
- [查看归档快照](#)

### 归档快照

您可以归档任何状态为 `completed` 的快照，以及自己账户中的快照。您无法归档状态为 `pending` 或 `error` 的快照，以及与您共享的快照。有关更多信息，请参阅[注意事项和限制](#)。

如果快照与一个或多个 AMI 关联，则必须先禁用这些关联的 AMI，然后才能归档快照。有关更多信息，请参阅[禁用 AMI](#)。

归档的快照保留其快照 ID、加密状态、AWS Identity and Access Management ( IAM ) 权限、所有者信息和资源标签。但是，快照还原和快照共享会在快照归档后自动禁用。

在归档处理过程中，您可以继续使用快照。一旦快照分层状态达到 `archival-complete` 状态，您无法再使用快照。

您可以使用以下方法归档快照。

## Console

### 归档快照

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 在快照列表中，选择需归档快照，然后选择 Actions ( 操作 )、Archive snapshot ( 归档快照 )。
3. 如要确认，请选择 Archive snapshot ( 归档快照 )。

## AWS CLI

### 归档快照

使用 [modify-snapshot-tier](#) AWS CLI 命令。对于 `--snapshot-id`，请指定需归档快照的 ID。对于 `--storage-tier`，请指定 `archive`。

```
$ aws ec2 modify-snapshot-tier \  
--snapshot-id snapshot_id \  
--storage-tier archive
```

例如，以下命令可以归档快照 `snap-01234567890abcdef`。

```
$ aws ec2 modify-snapshot-tier \  
--snapshot-id snap-01234567890abcdef \  
--storage-tier archive
```

该命令将显示以下输出。响应参数 `TieringStartTime` 以 UTC 时间格式 ( `YYYY-MM-DDTHH:MM:SSZ` ) 表示归档过程的启动日期和时间。

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "TieringStartTime": "2021-09-15T16:44:37.574Z"  
}
```

## 还原已归档的快照

在使用归档快照之前，必须先将其还原到标准层。还原的快照具有与归档之前相同的快照 ID、加密状态、IAM 权限、所有者信息和资源标签。还原后，您可以像使用账户中的任何其它快照一样使用它。还原的快照始终是完整快照。

还原快照时，可以选择使用以下两种方式还原快照：permanently（永久）或 temporarily（暂时）。

如果永久还原快照，则快照将从归档层永久移动到标准层。在手动重新归档或手动删除快照之前，快照将保持还原状态并可供使用。永久还原快照时，快照将从归档层中删除。

如果临时还原快照，则在您指定的还原期内，快照将从归档层复制到标准层。快照将保持还原状态，并且只能在还原期间使用。在还原期间，快照的副本将保留在归档层中。超过期限后，快照将自动从标准层中删除。在还原期间，您可以随时延长或缩短还原期，或将还原类型更改为永久。有关更多信息，请参阅[修改临时还原快照的还原期或还原类型](#)。

如果您要还原与已禁用的 AMI 关联的快照，并且打算使用该 AMI，则必须先永久还原所有关联的快照，再[重新启用已禁用的 AMI](#)，然后才能使用该 AMI。如果关联的快照已暂时恢复，则无法启用 AMI。您可以使用以下命令来查找与 AMI 关联的所有快照。

```
$ C:\> aws ec2 describe-images --image-id ami_id \  
--query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

您可以使用以下方法还原归档快照。

### Console

#### 从归档中还原快照

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 在快照列表中，选择要还原的归档快照，然后选择 Actions（操作）、Restore snapshot from archive（从归档还原快照）。
3. 指定要执行的还原类型。在 Restore type（还原类型）中，执行下列操作之一：
  - 要永久还原快照，请选择 Permanent（永久）。
  - 要临时还原快照，请选择 Temporary（临时），然后在 Temporary restore period（临时还原期）中，输入要还原快照的天数。

- 要确认，请选择 Restore snapshot ( 还原快照 )。

## AWS CLI

### 永久还原已归档的快照

使用 [restore-snapshot-tier](#) AWS CLI 命令。对于 `--snapshot-id`，请指定要还原的快照的 ID，并包括 `--permanent-restore` 选项。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snapshot_id \  
--permanent-restore
```

例如，以下命令可永久还原快照 `snap-01234567890abcdef`。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snap-01234567890abcdef \  
--permanent-restore
```

该命令将显示以下输出。

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "IsPermanentRestore": true  
}
```

### 临时还原已归档的快照

使用 [restore-snapshot-tier](#) AWS CLI 命令。忽略 `--permanent-restore` 选项。对于 `--snapshot-id`，请指定要还原的快照的 ID，以及在 `--temporary-restore-days` 中指定要还原快照的天数。

`--temporary-restore-days` 必须以天为单位指定。允许范围是 1 到 180。如果没有指定一个值，默认为 1 天。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snapshot_id \  
--temporary-restore-days number_of_days
```

例如，以下命令会临时还原快照 `snap-01234567890abcdef`，还原期为 5 天。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snap-01234567890abcdef \  
--temporary-restore-days 5
```

该命令将显示以下输出。

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "RestoreDuration": 5,  
  "IsPermanentRestore": false  
}
```

### 修改临时还原快照的还原期或还原类型

临时还原快照时，必须指定快照在账户中保持还原状态的天数。还原期到期后，快照将自动从标准层中删除。

您可以随时更改临时还原快照的还原期。

您可以选择增加或缩短还原期，也可以将还原类型从临时更改为永久。

如果更改还原期，则新的还原期将从当前日期开始生效。例如，如果指定新的还原期 5 天，快照将从当前日期开始到 5 天内保持还原状态。

#### Note

您可以通过将还原期设置为 1 天，提前结束临时还原。

如果将还原类型从临时更改为永久，则快照副本将从归档层中删除，并且在您手动重新归档或删除快照之前，该快照将保持在账户中并且可用。

您可以使用以下方法修改快照的还原期。

#### Console

##### 修改还原期或还原类型

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 在快照列表中，选择此前暂时还原的快照，然后选择 Actions ( 操作 )、Restore snapshot from archive ( 从归档还原快照 )。
3. 在 Restore type ( 还原类型 ) 中，执行下列操作之一：
  - 要将还原类型从临时更改为永久，请选择 Permanent ( 永久 )。
  - 要延长或缩短还原期，请保留 Temporary ( 临时 )，然后在 Temporary restore period ( 临时还原期 ) 中输入新的还原期 ( 以天为单位 )。
4. 要确认，请选择 Restore snapshot ( 还原快照 )。

## AWS CLI

### 修改还原期或还原类型

使用 [restore-snapshot-tier](#) AWS CLI 命令。对于 `--snapshot-id`，请指定之前临时还原的快照的 ID。要将还原类型从临时更改为永久性，请指定 `--permanent-restore` 并忽略 `--temporary-restore-days`。要延长或缩短还原期，请省略 `--permanent-restore`，而且对于 `--temporary-restore-days`，请指定新的还原期 ( 以天为单位 )。

例如：延长或缩短还原期

以下命令把快照还原期从 `snap-01234567890abcdef` 改到 10 天。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snap-01234567890abcdef \  
--temporary-restore-days 10
```

该命令将显示以下输出。

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "RestoreDuration": 10,  
  "IsPermanentRestore": false  
}
```

示例：将还原类型更改为永久

以下命令把快照 `snap-01234567890abcdef` 的还原类型从临时更改为永久。

```
$ aws ec2 restore-snapshot-tier \  
--snapshot-id snap-01234567890abcdef \  
--permanent-restore
```

该命令将显示以下输出。

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "IsPermanentRestore": true  
}
```

## 查看归档快照

您可以使用以下方法查看快照的存储层信息。

### Console

#### 查看快照的存储层信息

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 在快照列表中，选择快照，然后选择 Storage tier ( 存储层 ) 选项卡。

该表提供以下信息：

- Last tier change started on ( 上次层别更改始于 ) – 上次归档或还原的开始日期和时间。
- Tier change progress ( 层更改进展 ) – 以百分比表示的上次归档或还原操作的进度。
- Storage tier ( 存储层 ) – 快照的存储层。归档快照的状态始终为 archive，以及存储在标准层上的快照的状态始终为 standard，包括临时还原的快照。
- Tiering status ( 分层状态 ) – 上次归档或还原操作的状态。
- Archive completed on ( 归档完成时间 ) – 归档完成的日期和时间。
- Temporary restore expires on ( 临时还原到期时间 ) – 设置临时还原的快照过期的日期和时间。

## AWS CLI

### 查看有关归档快照的归档信息

使用 [describe-snapshot-tier-status](#) AWS CLI 命令。请指定 `snapshot-id` 筛选条件，请指定快照 ID 为筛选条件值。或者，要查看所有归档的快照，请省略筛选条件。

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
Values=snapshot_id"
```

输出包括以下响应参数：

- `Status` – 快照的状态。归档快照的状态始终为 `completed`。只有状态为 `completed` 的快照可以归档。
- `LastTieringStartTime` – 归档过程开始的日期和时间，采用 UTC 时间格式 ( `YYYY-MM-DDTHH:MM:SSZ` )。
- `LastTieringOperationState` – 归档过程的当前状态。可能的状态包括：`archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- `LastTieringProgress` – 快照归档过程的进度，以百分比表示。
- `StorageTier` – 快照的存储层。归档快照的状态始终为 `archive`，以及存储在标准层上的快照的状态始终为 `standard`，包括临时还原的快照。
- `ArchivalCompleteTime` – 归档过程完成的日期和时间，采用 UTC 时间格式 ( `YYYY-MM-DDTHH:MM:SSZ` )。

## 示例

以下命令显示有关快照 `snap-01234567890abcdef` 的信息。

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
Values=snap-01234567890abcdef"
```

该命令将显示以下输出。

```
{
  "SnapshotTierStatuses": [
    {
      "Status": "completed",
      "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
      "LastTieringProgress": 100,
```



```

    "Tags": [],
    "VolumeId": "vol-01234567890abcdef",
    "LastTieringOperationState": "archival-completed",
    "StorageTier": "archive",
    "OwnerId": "123456789012",
    "SnapshotId": "snap-01234567890abcdef",
    "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
  }
]
}

```

## 查看归档和标准层快照

使用 [describe-snapshot](#) AWS CLI 命令。对于 `--snapshot-ids`，请指定快照视图的 ID。

```
$ aws ec2 describe-snapshots --snapshot-ids snapshot_id
```

例如，以下命令显示有关快照 `snap-01234567890abcdef` 的信息。

```
$ aws ec2 describe-snapshots --snapshot-ids snap-01234567890abcdef
```

该命令将显示以下输出。响应参数 `StorageTier` 说明快照当前是否已归档。 `archive` 表示快照当前已归档并存储在归档层中，而 `standard` 表示快照当前尚未归档，并且存储在标准层中。

在以下示例输出中，只有 Snap A 已归档。Snap B 和 Snap C 尚未归档。

此外，响应参数 `RestoreExpiryTime` 仅为从归档中暂时还原的快照返回。它表示将何时从标准层中自动删除临时还原的快照。对于永久还原的快照，不会返回该值。

在以下示例输出中，Snap C 已暂时还原，它将在 2021-09-19T21:00:00.000Z (2021 年 9 月 19 日 UTC 21:00) 自动从标准级别中移除。

```

{
  "Snapshots": [
    {
      "Description": "Snap A",
      "Encrypted": false,
      "VolumeId": "vol-01234567890aaaaaa",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-09-07T21:00:00.000Z",
      "Progress": "100%",

```

```

    "OwnerId": "123456789012",
    "SnapshotId": "snap-01234567890aaaaaa",
    "StorageTier": "archive",
    "Tags": []
  },
  {
    "Description": "Snap B",
    "Encrypted": false,
    "VolumeId": "vol-09876543210bbbbbb",
    "State": "completed",
    "VolumeSize": 10,
    "StartTime": "2021-09-14T21:00:00.000Z",
    "Progress": "100%",
    "OwnerId": "123456789012",
    "SnapshotId": "snap-09876543210bbbbbb",
    "StorageTier": "standard",
    "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
    "Tags": []
  },
  {
    "Description": "Snap C",
    "Encrypted": false,
    "VolumeId": "vol-054321543210cccccc",
    "State": "completed",
    "VolumeSize": 12,
    "StartTime": "2021-08-01T21:00:00.000Z",
    "Progress": "100%",
    "OwnerId": "123456789012",
    "SnapshotId": "snap-054321543210cccccc",
    "StorageTier": "standard",
    "Tags": []
  }
]
}

```

仅查看存储在归档层或标准层中的快照

使用 [describe-snapshot](#) AWS CLI 命令。包括 `--filter` 选项，请指定 `storage-tier` 为筛选条件名称，请指定 `archive` 或 `standard` 为筛选条件值。

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive|standard"
```

例如，以下命令只显示归档快照。

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

## 监控快照归档

Amazon EBS 发出与快照归档操作相关的事件。您可以使用 AWS Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 [Amazon CloudWatch Events 用户指南](#)。

提供的事件如下：

- archiveSnapshot – 当快照归档操作成功或失败时发出。

以下是在快照归档操作成功时发送事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "123456789",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

以下是在快照归档操作失败时发送事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
```

```

"detail-type": "EBS Snapshot Notification",
"source": "aws.ec2",
"account": "123456789012",
"time": "2021-05-25T13:12:22Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
],
"detail": {
  "event": "archiveSnapshot",
  "result": "failed",
  "cause": "Source snapshot ID is not valid",
  "request-id": "1234567890",
  "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
  "startTime": "2021-05-25T13:12:22Z",
  "endTime": "2021-05-45T15:30:00Z",
  "recycleBinExitTime": "2021-10-45T15:30:00Z"
}
}

```

- permanentRestoreSnapshot – 当永久还原操作成功或失败时发出。

以下是在快照还原操作成功时发送事件的示例。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}

```

```
}
```

以下是在永久还原操作失败时发送事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `temporaryRestoreSnapshot` – 当临时还原操作成功或失败时发出。

以下是在快照暂时还原操作成功时发送事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
```

```

    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

下面是在临时还原操作失败时发送事件的示例。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

- `restoreExpiry` – 在临时还原快照的还原期到期时触发。

以下是示例。

```

{
  "version": "0",

```

```
"id": "01234567-0123-0123-0123-012345678901",
"detail-type": "EBS Snapshot Notification",
"source": "aws.ec2",
"account": "123456789012",
"time": "2021-05-25T13:12:22Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
],
"detail": {
  "event": "restoreExpiry",
  "result": "succeeded",
  "cause": "",
  "request-id": "1234567890",
  "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
  "startTime": "2021-05-25T13:12:22Z",
  "endTime": "2021-05-45T15:30:00Z",
  "recycleBinExitTime": "2021-10-45T15:30:00Z"
}
}
```

## 删除 Amazon EBS 快照

当您不再需要卷的 Amazon EBS 快照后，可以将其删除。删除快照对卷没有影响。删除卷对从它生成的快照无任何影响。

### 增量快照删除

如果定期拍摄卷快照，则这些快照为增量快照。这意味着该设备上在您的最新快照之后更改的数据块将保存在新快照中。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以创建卷。

如果数据存在于早期的单个快照或一系列快照中保存的卷上，并且该数据随后从卷中删除，则该数据仍被视为早期快照的唯一数据。只有引用唯一数据的所有快照都被删除，该唯一数据才会从快照序列中删除。

删除快照时，仅删除该快照专门引用的数据。只有在删除引用唯一数据的所有快照时，才会删除该唯一数据。删除卷的之前快照不会影响您使用该卷的之后快照创建卷的能力。

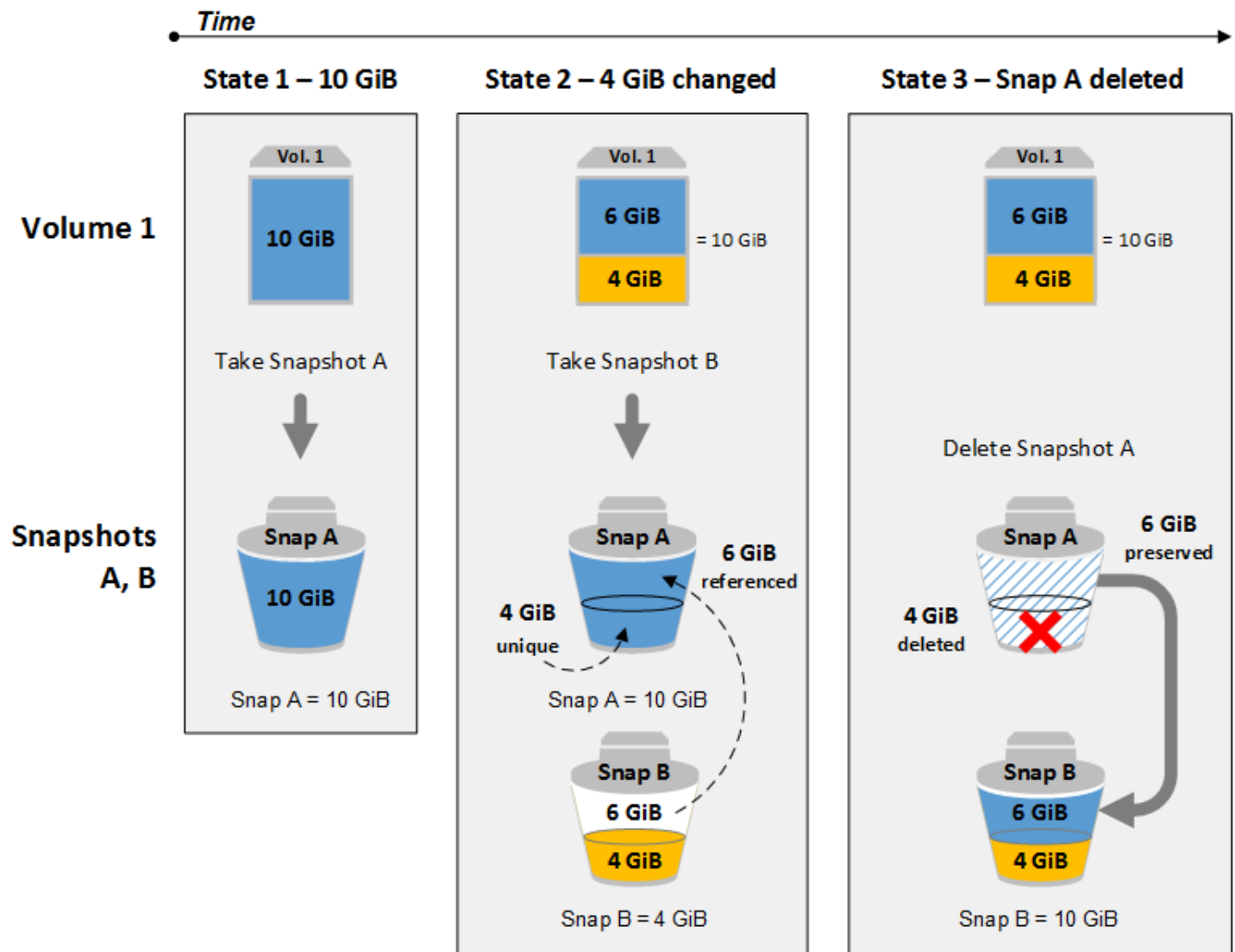
删除快照可能不会降低组织的数据存储成本。其他快照可引用已删除快照的数据，已引用的数据总是会被保留。如果您删除了一个快照，而该快照包含以后的快照使用的数据，那么与所引用数据关联的成本将分配到后来的快照。有关快照如何存储数据的更多信息，请参阅[快照的工作原理](#)和下面的示例。

在下图中，卷 1 在三个时间点上显示。某个快照已捕获前两种状态，在第三种状态中，某个快照已被删除。

- 在状态 1 中，该卷具有 10 GiB 数据。因为快照 A 是为该卷制作的首个快照，因此必须复制所有 10 GiB 数据。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，4 GiB 数据已更改。快照 B 只需复制并存储制作快照 A 后更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已复制并存储在快照 A 中）将由快照 B 引用而不是再次复制。这通过虚线箭头指示。
- 在状态 3 中，卷自状态 2 以来未更改，但快照 A 已被删除。快照 B 引用的存储在快照 A 中的 6 GiB 数据现已移至快照 B，如粗箭头所示。因此，您仍需支付存储 10 GiB 数据的费用；快照 A 中保留的 6 GiB 未更改数据和快照 B 中的 4 GiB 已更改数据。

删除快照及其由其他快照引用的部分数据





## 注意事项

删除快照时需考虑以下事项：

- 您不能删除注册 AMI 使用的 EBS 卷的根设备快照。即使已注册的 AMI 已弃用或禁用，此注意事项依然适用。您必须先注销 AMI，然后才能删除快照。有关更多信息，请参阅[取消注册 AMI](#)。
- 您无法使用 Amazon EC2 删除由该 AWS Backup 服务管理的快照。而是 AWS Backup 使用删除备份保管库中相应的恢复点。有关更多信息，请参阅 AWS Backup 开发人员指南中的[删除备份](#)。
- 您可以手动创建、保留和删除快照，也可以使用 Amazon Data Lifecycle Manager 来管理快照。有关更多信息，请参阅[Amazon Data Lifecycle Manager](#)。
- 尽管您可以删除仍在制作的快照，但该快照必须先完成，删除才能生效。这可能需要较长时间。如果您还具有并发快照限制，而您尝试再制作一个快照，可能会遇到

ConcurrentSnapshotLimitExceeded 错误。有关更多信息，请参阅 Amazon Web Services 一般参考 中 Amazon EBS 的 [服务限额](#)。

- 如果您删除符合回收站保留规则的快照，则该快照将保留在回收站中，而不是立即删除。有关更多信息，请参阅 [回收站](#)。
- 无法删除与已禁用的 EBS 支持的 AMI 关联的快照。有关更多信息，请参阅 [禁用 AMI](#)。
- 您无法删除与您共享的快照。
- 如果您删除自己拥有的共享快照，则与之共享该快照的所有帐户都将失去对该快照的访问权限。

## 删除快照

要删除快照，请使用以下方法之一。

### Console

如需使用控制台删除快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择要删除的快照，然后选择 Actions ( 操作 )、Delete snapshot ( 删除快照 )。
4. 选择删除。

### AWS CLI

要使用删除快照 AWS CLI

使用 [delete-snapshot](#) 命令。

### Tools for Windows PowerShell

使用适用于 Windows 的工具删除快照 PowerShell

使用 [Remove-EC2Snapshot](#) 命令。

#### 故障排除技巧

如果您收到 Failed to delete snapshot 错误，指示 AMI 当前正在使用该快照，则需要先 [取消注册关联的 AMI](#)，然后才能删除该快照。您无法删除与 AMI 关联的快照。

如果您使用控制台且关联的 AMI 已禁用，则必须在 AMI 屏幕上选择已禁用的映像筛选条件才能查看已禁用的 AMI。

## 删除多卷快照

要删除多卷快照，请使用您在创建快照时应用于多卷快照集的标签检索集的所有快照。然后，分别删除这些快照。

系统不会阻止您删除多卷快照集中的各个快照。如果在 pending state 中删除快照，则只删除该快照。多卷快照集中的其他快照仍成功保留。

## 自动化快照生命周期

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除用于备份 Amazon EBS 卷的快照。

有关更多信息，请参阅 [Amazon Data Lifecycle Manager](#)。

## Amazon EBS 快速快照还原

Amazon EBS 快速快照还原 (FSR) 使您能够从创建时已完全初始化的快照创建卷。这会消除首次访问块时对其执行 I/O 操作的延迟。使用快速快照还原创建的卷可以立即交付其所有预置性能。

要开始使用，请在特定可用区中为特定快照启用快速快照还原。每一对快照和可用区指代一个快速快照还原。当您从其中一个已启用该功能的可用区中的快照创建卷时，该卷将使用快速快照还原进行还原。

必须在每个快照的基础上明确启用快照还原。如果从已启用快速快照还原的快照还原卷创建新的快照，则新快照不会自动启用快速快照恢复功能。您必须明确启用新快照的该功能。

您可以使用快速快照还原的全部性能优势还原的卷数是由快照的卷创建积分决定的。有关更多信息，请参阅 [卷创建积分](#)。

您可以为您拥有的快照以及与您共享的公有快照和私有快照启用快速快照还原。

### 内容

- [注意事项](#)
- [卷创建积分](#)
- [管理快速快照还原](#)
- [监控快速快照还原](#)

- [快速快照还原配额](#)
- [定价和计费](#)

## 注意事项

- AWS Outposts Local Zones 和 Wavelength Zone 不支持快速快照还原。
- 可以为大小为 16 TiB 或以下的快照启用快速快照还原。
- 预调配性能高达 64,000 IOPS 和 1,000 MiB/s 吞吐量的卷能够实现快速快照还原的全部性能。对于预调配性能超过 64,000 IOPS 或 1,000 MiB/s 吞吐量的卷，我们建议您[初始化该卷](#)以实现其全部性能。

## 卷创建积分

获得快速快照还原的全部性能优势的卷数是由快照的卷创建积分决定的。每个可用区的每个快照具有一积分存储桶。从快照中创建并启用了快速快照还原的每个卷使用积分存储桶中的一积分。存储桶中必须至少有一积分，您才能从快照创建初始化卷。如果您创建卷但存储桶中的积分少于一个，则创建卷时不能获得快速快照还原的优势。

当您为与您共享的快照启用快速快照还原时，您的账户中的共享快照将获得单独的信用存储桶。如果您从共享快照创建卷，则配额将从您的信用存储桶中消耗；这些配额不会从快照所有者的信用存储桶中消耗。

积分存储桶大小及其重填速率取决于快照的大小，而不是取决于从快照中创建的卷的大小。

当您为快照启用快速快照还原时，积分存储桶从零积分开始，并以设定的速率填满，直到达到最大积分容量。此外，在使用积分时，将随着时间的推移重填积分存储桶，直到其达到最大积分容量。

每积分存储桶的填充率计算如下：

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

积分存储桶的大小计算如下：

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

例如，如果为大小为 128 GiB 的快照启用快速快照还原，则填充率为每分钟 0.1333 积分。

```
MIN (10, (1024 ÷ 128))
```

```
= MIN (10, 8)
= 8 credits per hour
= 0.1333 credits per minute
```

积分存储桶的最大大小为 8 积分。

```
MAX (1, MIN (10, (1024 ÷ 128)))
= MAX (1, MIN (10, 8))
= MAX (1, 8)
= 8 credits
```

在此示例中，启用快速快照还原时，积分存储桶以零积分开始。8 分钟后，积分存储桶有足够的积分来创建一个初始化卷 ( $0.1333 \text{ credits} \times 8 \text{ minutes} = 1.066 \text{ credits}$ )。如果积分存储桶已满，您可以同时创建 8 个初始化卷 (8 积分)。当存储桶低于其最大容量时，它将每分钟重填 0.1333 积分。

您可以使用 CloudWatch 指标来监控积分余额存储桶的大小以及各个存储桶中可用的积分数量。有关更多信息，请参阅[快速快照还原的指标](#)。

从启用了快速快照还原的存储桶创建卷之后，您可以使用 [describe-volumes](#) 来描述卷，并检查输出中的 `fastRestored` 字段以确定是否使用快速快照还原将该卷创建为已初始化卷。

## 管理快速快照还原

### 主题

- [启用或禁用快速快照还原](#)
- [查看快照的快速快照还原状态](#)
- [查看使用快速快照还原功能还原的卷](#)

### 启用或禁用快速快照还原

默认情况下，对于快照禁用快速快照还原。您可以为您拥有的快照以及与您共享的快照启用或禁用快速快照还原。为快照启用或禁用快速快照还原时，所做的更改仅适用于您的账户。

#### Note

当您为快照启用快速快照还原时，您的账户将按特定可用区中启用快速快照还原的每分钟计费。收费按比例计算，最少 1 小时。

当您删除您拥有的快照时，系统会在账户中自动禁用该快照的快速快照还原。如果您为与您共享的快照启用了快速快照还原，并且快照所有者删除或取消共享，则会自动为您账户中的共享快照禁用快速快照还原。

如果为共享的快照启用了快速快照还原，并且使用自定义 CMK 对其进行了加密，则在快照所有者撤消对自定义 CMK 的访问权限时，快速快照还原不会自动为快照禁用。您必须手动为该快照禁用快速快照还原。

使用以下方法之一为您拥有的快照或与您共享的快照启用或禁用快速快照还原。

## Console

### 启用或禁用快速快照还原

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择快照，然后选择 Actions ( 操作 )、Manage fast snapshot restore ( 管理快速快照还原 )。
4. 快速快照还原设置部分会列出所有可用区，您可以在其中为所选快照启用快速快照还原功能。Current status ( 当前状态 ) 卷说明每个区域当前是启用还是禁用快速快照还原。

要在当前禁用快照的区域中启用快速快照还原，选择该区域，然后选择 Enable ( 启用 )，并选择 Enable ( 启用 ) 以确认。

要在当前启用快照还原的区域中禁用快速快照还原，请选择该区域，然后选择 Disable ( 禁用 )。

5. 进行必要的更改后，选择 Close ( 关闭 )。

## AWS CLI

### 使用 AWS CLI 管理快速快照还原

- [enable-fast-snapshot-restores](#)
- [disable-fast-snapshot-restores](#)
- [describe-fast-snapshot-restores](#)

**Note**

为快照启用快速快照还原后，快照将进入 `optimizing` 状态。处于 `optimizing` 状态的快照在使用快照恢复卷时可以提供一些性能优势。只有在进入 `enabled` 状态后，它们才开始发挥快速快照还原的全部性能优势。

## 查看快照的快速快照还原状态

快照的快速快照还原可能处于以下状态之一。

- `enabling` – 发出了启用快速快照还原的请求。
- `optimizing` – 正在启用快速快照还原。对于快照优化，每个 TiB 需要 60 分钟的时间。处于此状态的快照在还原卷时提供了一些性能优势。
- `enabled` – 启用了快速快照还原。处于此状态且具有足够卷创建积分的快照在还原卷时可发挥全部性能优势。
- `disabling` – 发出了禁用快速快照还原的请求，或者启用快速快照还原的请求失败。
- `disabled` – 禁用了快速快照还原。您可以根据需要再次启用快速快照还原。

使用以下方法之一查看所拥有或共享的快照的快速快照还原状态。

### Console

使用控制台查看快速快照还原的状态

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择快照。
4. 在 Details ( 详细信息 ) 选项卡上，查看 Fast Snapshot Restore ( 快速快照还原 )，该选项卡表示快速快照还原的状态。

### AWS CLI

使用 AWS CLI 查看已启用快速快照还原的快照

使用 [describe-fast-snapshot-restores](#) 命令，描述已启用快速快照还原的快照。

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

下面是示例输出。

```
{
  "FastSnapshotRestores": [
    {
      "SnapshotId": "snap-0e946653493cb0447",
      "AvailabilityZone": "us-east-2a",
      "State": "enabled",
      "StateTransitionReason": "Client.UserInitiated - Lifecycle state
transition",
      "OwnerId": "123456789012",
      "EnablingTime": "2020-01-25T23:57:49.596Z",
      "OptimizingTime": "2020-01-25T23:58:25.573Z",
      "EnabledTime": "2020-01-25T23:59:29.852Z"
    },
    {
      "SnapshotId": "snap-0e946653493cb0447",
      "AvailabilityZone": "us-east-2b",
      "State": "enabled",
      "StateTransitionReason": "Client.UserInitiated - Lifecycle state
transition",
      "OwnerId": "123456789012",
      "EnablingTime": "2020-01-25T23:57:49.596Z",
      "OptimizingTime": "2020-01-25T23:58:25.573Z",
      "EnabledTime": "2020-01-25T23:59:29.852Z"
    }
  ]
}
```

## 查看使用快速快照还原功能还原的卷

当您在可用区中，从已启用快速快照还原的快照创建卷时，将使用快速快照还原进行还原。

使用 [describe-volumes](#) 命令，查看从已启用快速快照还原的快照创建的卷。

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

下面是示例输出。



```
{
  "Volumes": [
    {
      "Attachments": [],
      "AvailabilityZone": "us-east-2a",
      "CreateTime": "2020-01-26T00:34:11.093Z",
      "Encrypted": true,
      "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-a87a-5513e232e843",
      "Size": 20,
      "SnapshotId": "snap-0e946653493cb0447",
      "State": "available",
      "VolumeId": "vol-0d371921d4ca797b0",
      "Iops": 100,
      "VolumeType": "gp2",
      "FastRestored": true
    }
  ]
}
```

## 监控快速快照还原

Amazon EBS 会在快照的快速快照还原状态发生变化时发出 Amazon CloudWatch Events。有关更多信息，请参阅[EBS 快速快照还原事件](#)。

## 快速快照还原配额

每个区域最多可启用 5 个快照以用于快速快照还原。配额适用于您拥有的快照以及与您共享的快照。如果为与您共享的快照启用快速快照还原，则它将计入快速快照还原配额。它不计入快照所有者的快速快照还原配额。

## 定价和计费

对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。

例如，假设您在 US-East-1a 中为一个快照启用了一个月（30 天）的快速快照还原，则需要支付 540 美元（1 个快照 x 1 个可用区 x 720 小时 x 每小时 \$0.75）的费用。如果您按照同样的期限在 us-east-1a、us-east-1b 和 us-east-1c 中为两个快照启用了快速快照还原，则需要支付 3240 美元（2 个快照 x 3 个可用区 x 720 小时 x 每小时 \$0.75）的费用。

如果为与您共享的公有快照或私有快照启用快速快照还原，则会对您的账户进行计费；不会对快照所有者进行计费。当快照所有者删除与您共享的快照或取消其共享时，系统会为您账户中的快照禁用快速快照还原，并停止计费。

有关更多信息，请参阅 [Amazon EBS 定价](#)。

## Amazon EBS 快照锁

您可以锁定 Amazon EBS 快照以防止意外或恶意删除，或者以 WORM (write-once-read-many) 格式将其存储在特定时间内。当一个快照处于锁定状态时，任何用户都无法将其删除，无论他们的 IAM 权限如何。您可以像使用任何其他快照一样继续使用锁定的快照。

### Note

快照锁定已由 Cohasset Associates 评估，可在受 SEC 17a-4、CFTC 和 FINRA 法规约束的环境中使用。有关快照锁定如何与这些法规相关的更多信息，请参阅 [Cohasset Associates Compliance Assessment](#)。

可以使用以下两种模式之一锁定快照：合规模式或监管模式，而且可以将快照锁定特定的一段时间或者锁定到某个特定日期。有关更多信息，请参阅 [锁定模式](#) 和 [锁定持续时间](#)。

### 定价

您可以锁定和解锁快照，无需支付额外的费用。您需要为锁定的快照支付标准 Amazon EBS 快照存储费用。

### 主题

- [Amazon EBS 快照锁定的概念](#)
- [Amazon EBS 快照锁定的注意事项](#)
- [Amazon EBS 快照锁定的所需权限](#)
- [使用 Amazon EBS 快照锁定](#)
- [使用监控亚马逊 EBS 快照锁定 AWS CloudTrail](#)
- [使用亚马逊监控亚马逊 EBS 快照锁定 EventBridge](#)

## Amazon EBS 快照锁定的概念

以下是开始使用快照锁定时需要理解的重要概念。

## 目录

- [锁定模式](#)
- [锁定持续时间](#)
- [冷静期](#)
- [锁定状态](#)

## 锁定模式

可以在以下两种模式之一中锁定快照：

### 监管模式

锁定快照之后，拥有适当 IAM 权限的用户可以随时解锁快照，还可以修改锁定模式以及锁定持续时间或到期日期。当在监管模式下锁定快照时，快照会立即被锁定；没有冷静期。要在监管模式下锁定快照之后将其删除，必须首先解锁快照，或者必须等待锁定过期。

通过确保只有某些用户有权解锁快照和修改快照锁定配置，您可以使用监管模式满足组织的数据监管要求。在合规模式下锁定快照之前，还可以利用监管模式测试锁定配置。

### 合规性模式

在合规模式下锁定快照时，可以选择指定在锁定快照之后立即开始的冷静期。在冷静期内，拥有适当权限的用户可以解锁快照、更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间或到期日期。在冷静期过期之后，您将无法解锁快照、更改锁定模式或者缩短锁定持续时间或过期日期；您只能延长锁定持续时间或过期日期。要在合规模式下锁定快照且冷静期过期之后将其删除，必须等待锁定过期。

#### Note

通过在请求中省略冷静期，可以在合规模式下锁定快照而不设冷静期。如果这样做，锁定将立即生效，而且无法解锁快照、更改锁定模式或者缩短锁定持续时间或过期日期；您只能延长锁定持续时间或过期日期。

可以利用合规模式保护出于合规性原因不应在特定的时期内删除的快照。合规模式具有以下优点：

- 它支持对快照使用 WORM (一次写入多次读取) 配置。
- 它提供了一层额外的防御，可保护快照免遭意外删除或恶意删除。
- 它实施了保留期，可防止特权用户提前删除，以满足贵组织的数据保护策略和程序。

**Note**

要删除在锁定到期前锁定在合规模式下的快照，唯一的方法是关闭关联的 AWS 账户。

## 锁定持续时间

锁定持续时间是指快照要保持锁定状态的时期。可以将锁定持续时间指定为以下选项之一，但不能同时指定这两者：

### 天数

将锁定持续时间指定为快照要保持锁定状态的天数。当指定的天数过后，会自动解锁快照。持续时间介于 1 天到 36500 天 ( 100 年 ) 不等。

### 锁定到期日期

锁定持续时间由未来的过期日期决定。快照将保持锁定状态，直到达到锁定过期日期为止。当达到锁定过期日期时，会自动解锁快照。

## 冷静期

冷静期是一个可选的时期，可以在合规模式下锁定快照时指定此时期。在冷静期内，拥有适当权限的用户可以解锁快照、更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间。当冷静期过期之后，无论用户拥有何种权限，都无法解锁快照、更改锁定模式、恢复冷静期或缩短锁定持续时间。

在冷静期内，无法删除快照。

如果指定了冷静期，则冷静期将在您锁定快照之后立即开始。如果省略了冷静期，则会立即在合规模式下锁定快照而不设冷静期。

冷静期介于 1 到 72 小时不等。要在合规模式下立即锁定快照而不设冷静期，请勿在请求中指定冷静期。

## 锁定状态

快照锁定可处于以下几种状态之一：

- `compliance-cooloff` – 已在合规模式下锁定快照，但它仍处于冷静期内。无法删除快照，但可以将它解锁，而且拥有适当权限的用户可以修改锁定设置。

- **governance** – 已在监管模式下锁定快照。无法删除快照，但可以将它解锁，而且拥有适当权限的用户可以修改锁定设置。
- **compliance** – 已在合规模式下锁定快照，且未设冷静期或者冷静期已过期。无法解锁或删除快照。只有拥有适当权限的用户才能延长锁定时间。
- **expired** – 已在合规或监管模式下锁定快照，但锁定已过期。未锁定快照，可以将其删除。

## Amazon EBS 快照锁定的注意事项

- 只有当快照处于 **pending** 或 **completed** 状态时，才能将其锁定。
  - 如果在快照处于 **pending** 状态时将其锁定，并且将其锁定特定的持续时间，将只在快照达到 **completed** 状态时开始计算锁定持续时间。当快照处于 **pending** 状态时无法将其删除。
  - 如果在快照处于 **pending** 状态时将其锁定，但由于任何原因导致创建快照失败，锁定将被取消。
- 如果在冷静期过期之后延长了在合规模式下锁定的快照的锁定持续时间，将无法指定另一个冷静期。如果指定了冷静期，请求将失败。
- 您可以锁定已归档的快照。您可以存档已锁定的快照。
- 您可以锁定与 AMI 相关联的快照。
- 您可以取消注册具有已锁定的关联快照的 AMI。
- 您可以删除用来加密已锁定的快照的 KMS 密钥。
- 我们建议您不要锁定由创建的快照 AWS Backup。AWS Backup 已经确保其快照在保留期到期之前不会被删除。要为由管理的快照添加额外的安全层 AWS Backup，我们建议您使用 AWS Backup 文件库锁定。有关更多信息，请参阅 [AWS Backup Vault Lock](#)。
- 在创建快照期间或 AMI 注册期间，无法锁定快照。
- 您无法在 AWS Outposts 上锁定本地 Amazon EBS 快照。
- 要删除在锁定到期前锁定在合规模式下的快照，唯一的方法是关闭关联的 AWS 账户。

如果您在锁定快照时关闭 AWS 帐户，则会在快照完好无损的情况下 AWS 暂停您的帐户 90 天。如果您未在 90 天内重新打开账户，即使快照已被锁定，也会 AWS 将其删除。

## Amazon EBS 快照锁定的所需权限

默认情况下，用户无权使用快照锁定。要允许用户使用快照锁定，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。有关更多信息，请参阅《IAM 用户指南》中的 [创建 IAM policy](#)。

### 主题

- [所需的权限](#)
- [使用条件键限制访问](#)

## 所需的权限

要使用快照锁定，用户需要以下权限。

- ec2:LockSnapshot – 锁定快照。
- ec2:UnlockSnapshot – 解锁快照。
- ec2:DescribeLockedSnapshots – 查看快照锁定设置。

以下是一个示例 IAM policy，它授权用户锁定和解锁快照以及查看快照锁定设置。其包括控制台用户的 ec2:DescribeSnapshots 权限。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:LockSnapshot",
      "ec2:UnlockSnapshot",
      "ec2:DescribeLockedSnapshots",
      "ec2:DescribeSnapshots"
    ]
  }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

创建权限集合。按照《AWS IAM Identity Center 用户指南》中[创建权限集](#)的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

创建适用于身份联合验证的角色。按照《IAM 用户指南》中[为第三方身份提供商创建角色 \(联合身份验证\)](#)的说明进行操作。

- IAM 用户：

• 创建您的用户可以担任的角色。按照《IAM 用户指南》中[为 IAM 用户创建角色](#)的说明进行操作。

- (不推荐使用) 将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中[向用户添加权限 \(控制台\)](#) 中的说明进行操作。

## 使用条件键限制访问

可以使用条件键限制如何允许用户锁定快照。

### 主题

- [ec2: SnapshotLockDuration](#)
- [ec2: CoolOffPeriod](#)

### ec2: SnapshotLockDuration

当锁定快照时，可以使用 `ec2:SnapshotLockDuration` 条件键将用户限制在特定的锁定持续时间内。

如下示例策略将禁止用户指定一个介于 10 到 50 天之间的锁定持续时间。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan" : {
          "ebs:SnapshotLockDuration" : 10
        }
        "NumericLessThan":{
          "ebs:SnapshotLockDuration": 50
        }
      }
    }
  ]
}
```

### ec2: CoolOffPeriod

可以使用 `ec2:CoolOffPeriod` 条件键防止用户未设冷静期的情况下在合规模式下锁定快照。

如下示例策略将禁止用户在合规模式下锁定快照时指定超过 48 小时的冷静期。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan": {
          "ec2:CoolOffPeriod": 48
        }
      }
    }
  ]
}
```

## 使用 Amazon EBS 快照锁定

按照以下过程使用 Amazon EBS 快照锁定。

### 任务

- [锁定快照](#)
- [解锁快照](#)
- [更新快照锁定设置](#)
- [查看快照锁定设置](#)

### 锁定快照

您可以锁定处于 pending 或 completed 状态的快照。有关更多信息，请参阅 [Amazon EBS 快照锁定的注意事项](#)。

### Console

要锁定一个快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。



3. 选择要锁定的快照，然后选择操作、快照设置、管理快照锁定。
4. 选择锁定快照。
5. 对于锁定模式，选择监管模式或合规模式。有关更多信息，请参阅 [锁定模式](#)。
6. 对于锁定持续时间，执行以下操作之一：
  - 要将快照锁定一个特定的时期，请选择锁定快照，然后以天或年为单位输入此时期。
  - 要将快照锁定到特定的日期和时间，请选择锁定快照直到，然后选择过期日期和时间。

有关更多信息，请参阅 [锁定持续时间](#)。

7. (仅限合规模式) 对于冷静期，请指定一个冷静期，在此期间内可以解锁快照和修改锁定配置。有关更多信息，请参阅 [冷静期](#)。
8. (仅限合规模式) 要确认您希望在合规模式下锁定快照，而且在冷静期过期后将无法解锁快照，请选择确认。
9. 选择保存锁定设置。

## AWS CLI

### 要在监管模式下锁定快照

使用 [lock-snapshot](#) AWS CLI 命令。对于 `--snapshot-id`，请指定要锁定的快照 ID。对于 `--lock-mode`，请指定 `governance`。要将快照锁定一个特定的时期，对于 `--lock-duration`，请指定要将快照锁定的时期。或者，要将快照锁定到特定的日期，对于 `--expiration-date`，请使用 UTC 时区 ( `YYYY-MM-DDThh:mm:ss.sssZ` ) 指定锁定必须过期的日期和时间。

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \  
--lock-mode governance \  
--lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

### 要在合规模式下锁定快照

使用 [lock-snapshot](#) AWS CLI 命令。对于 `--snapshot-id`，请指定要锁定的快照 ID。对于 `--lock-mode`，请指定 `compliance`。对于 `--cool-off-period`，可以选择以小时为单位指定一个冷静期。要将快照锁定一个特定的时期，对于 `--lock-duration`，请指定要将快照锁定的时期。或者，要将快照锁定到特定的日期，对于 `--expiration-date`，请使用 UTC 时区 ( `YYYY-MM-DDThh:mm:ss.sssZ` ) 指定锁定必须过期的日期和时间。

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \  
--lock-mode compliance \  
--cool-off-period 1-300_hours | --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

```
--lock-mode compliance \  
--cool-off-period 1-72_hours \  
--lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

## 解锁快照

只有当在监管模式下锁定了快照，或者在合规模式下锁定了快照且快照仍处于冷静期内时，才能解锁快照。

### Console

#### 要解锁快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择要解锁的快照，然后选择操作、快照设置、管理快照锁定。
4. 选择解锁快照，然后再次选择解锁快照进行确认。

### AWS CLI

#### 要解锁快照

使用 [unlock-snapshot](#) AWS CLI 命令。对于 `--snapshot-id`，请指定要解锁的快照 ID。

```
$ aws ec2 unlock-snapshot --snapshot-id snapshot_id
```

## 更新快照锁定设置

允许的更新取决于锁定状态：

- `governance` – 您可以更改锁定模式以及延长或缩短锁定持续时间或过期日期。
- `compliance-cooloff` – 您可以更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间或过期日期。
- `compliance` – 您只能延长锁定持续时间或过期日期。

## Console

### 要更新快照锁定设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择要为其修改锁定设置的快照，然后选择操作、快照设置、管理快照锁定。
4. 根据需要更新设置，然后选择保存锁定设置。

## AWS CLI

### 要更新快照锁定设置

使用 [lock-snapshot](#) AWS CLI 命令。对于 `--snapshot-id`，请指定要为其更新锁定设置的快照的 ID。然后，仅指定要修改的选项。

## 查看快照锁定设置

使用以下方法之一查看快照的锁定设置。

### Console

#### 要查看快照锁定设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择快照。
3. 选择要查看其锁定设置的快照，然后选择操作、快照设置、管理快照锁定。

### AWS CLI

#### 要查看快照锁定设置

使用 [describe-locked-snapshots](#) 命令。AWS CLI 对于 `--snapshot-ids`，请指定要查看其锁定设置的快照的 ID。

```
$ aws ec2 describe-locked-snapshots --snapshot-ids snapshot_id
```

## 使用监控亚马逊 EBS 快照锁定 AWS CloudTrail

您可以将快照锁定的 API 调用作为事件监控，包括来自控制台的调用和对 API 的代码调用。使用收集到的信息 CloudTrail，您可以确定发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关更多信息，请参阅 [Logging API calls using AWS CloudTrail](#)。

## 使用亚马逊监控亚马逊 EBS 快照锁定 EventBridge

Amazon EBS 发出与快照锁定操作相关的事件。您可以使用 AWS Lambda 和 Amazon EventBridge 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 [Amazon EventBridge 用户指南](#)。

系统将发出以下事件：

- 成功在监管或合规模式下锁定快照。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooloffPeriod": 24,
    "cooloffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

```
}

```

- 当快照处于 pending 状态且被锁定时，锁定事件失败，而且快照无法达到 completed 状态。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "coolOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- 锁定已过期

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
```

```

    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}

```

- 在合规模式下锁定之后，冷静期已过期。

```

{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooloffPeriod": 24,
    "cooloffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}

```

## 阻止公开访问快照

要防止公开共享您的快照，您可以启用阻止公开访问快照。在为一个区域阻止公开访问快照之后，将自动阻止任何尝试在此区域公开共享快照的行为。这可以帮助您提高快照的安全性，并保护您的快照数据免遭未经授权的访问或意外访问。

可以在两种模式之一中阻止公开访问快照：

- **阻止所有共享** – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- **阻止新共享** – 仅阻止对快照进行公开共享的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

### 定价

可以阻止公开访问快照，无需支付额外的费用。

### 目录

- [注意事项](#)
- [IAM 权限](#)
- [启用阻止公开访问快照](#)
  - [配置“阻止公开访问快照”](#)
  - [查看用来阻止公开访问快照的设置](#)
  - [禁用阻止公开访问快照](#)
- [使用 Amazon 监控对快照的封锁公开访问 EventBridge](#)

## 注意事项

- 阻止公开访问快照并不会阻止共享私有快照。
- 如果在阻止所有共享模式下启用阻止公开访问快照，将不会更改对已公开共享的快照的权限。实际上，它会阻止这些快照公开可见和可公开访问。因此，这些快照的属性仍然表明它们是公开共享的，尽管它们不可公开访问。
- 如果在阻止所有共享模式下启用阻止公开访问快照，而且您将此模式更改为阻止新共享或者禁用阻止公开访问，以前公开共享的所有快照将不再被视为私有快照，它们将再次可公开访问。

- 阻止公开访问快照是一个区域性设置。它适用于启用了此功能的区域中的所有快照。您需要在希望阻止公开共享快照的每个区域中启用阻止公开访问快照。
- 阻止公开访问是一个账户级别的设置。它适用于账户中的所有用户，包括管理员用户。您无法在组织级别启用阻止公开访问快照。
- 阻止公开访问快照并不会阻止公开共享由 EBS 支持的 AMI。如果启用阻止公开访问快照，用户仍然可以公开共享由 EBS 支持的 AMI。如果公开共享由 EBS 支持的 AMI，有权访问此 AMI 的用户可以从与它关联的快照创建卷。要防止公开共享您的 AMI，请启用[阻止公开访问 AMI](#)。
- 开启本地快照后，不支持对快照进行公开访问 AWS Outposts。

## IAM 权限

默认情况下，用户无权阻止公开访问快照。要允许用户使用“阻止公开访问快照”，您必须创建 IAM policy，以授权使用特定 API 操作。创建策略后，必须向您的用户、组或角色添加权限。

要阻止公开访问快照，用户需要拥有以下权限。

- `ec2:EnableSnapshotBlockPublicAccess` – 启用阻止公开访问快照以及修改此模式。
- `ec2:DisableSnapshotBlockPublicAccess` – 禁用阻止公开访问快照。
- `ec2:GetSnapshotBlockPublicAccessState` – 查看一个区域的阻止公开访问快照设置。

以下是 IAM policy 示例。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:EnableSnapshotBlockPublicAccess",
      "ec2:DisableSnapshotBlockPublicAccess",
      "ec2:GetSnapshotBlockPublicAccessState"
    ],
    "Resource": "*"
  }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center :



创建权限集合。按照《AWS IAM Identity Center 用户指南》中[创建权限集](#)的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

创建适用于身份联合验证的角色。按照《IAM 用户指南》中[为第三方身份提供商创建角色 \(联合身份验证\)](#)的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中[为 IAM 用户创建角色](#)的说明进行操作。
  - (不推荐使用) 将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中[向用户添加权限 \(控制台\)](#)中的说明进行操作。

## 启用阻止公开访问快照

使用以下过程配置和监控阻止公开访问快照。

### 任务

- [配置“阻止公开访问快照”](#)
- [查看用来阻止公开访问快照的设置](#)
- [禁用阻止公开访问快照](#)

### 配置“阻止公开访问快照”

启用阻止公开访问快照，以防止在此区域中公开共享快照。启用此功能之后，将阻止在此区域中公开共享快照的请求。

#### Important

如果在阻止所有共享模式下启用阻止公开访问快照，而且您将此模式更改为阻止新共享，以前公开共享的所有快照将不再被视为私有快照，它们将再次可公开访问。

### Console

#### 要配置阻止公开访问快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 EC2 控制面板，然后在 ( 右侧的 ) 账户属性中，选择数据保护和安全。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 选择阻止公开访问，然后选择以下选项之一：
  - 阻止所有公开访问 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
  - 阻止新的公开共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。
5. 选择更新。

## AWS CLI

### 要启用或修改阻止公开访问快照

使用 [enable-snapshot-block-public-access](#) 命令。对于 `--state`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing/block-new-sharing
```

## 查看用来阻止公开访问快照的设置

对于您账户中的每个区域，阻止公开访问可能处于以下状态之一。

- 阻止所有共享 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已经公开共享的快照将被视为私有快照，且不可公开访问。
- 阻止新共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。
- 未阻止 – 未阻止公开共享。用户可以公开共享快照。

## Console

要查看用来阻止公开访问快照的设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 EC2 控制面板，然后在 ( 右侧的 ) 账户属性中，选择数据保护和安全。
3. 阻止公开访问 EBS 快照部分会显示当前设置。

## AWS CLI

要查看用来阻止公开访问快照的设置

使用 `get-snapshot-block-public-access-state` 命令。

```
aws ec2 get-snapshot-block-public-access-state
```

## 禁用阻止公开访问快照

禁用阻止公开访问快照，以允许在此区域中公开共享快照。禁用此功能之后，用户可以在此区域公开共享快照。

### Important

如果在阻止所有共享模式下启用阻止公开访问快照，而且您禁用了阻止公开访问，以前公开共享的所有快照将不再被视为私有快照，它们将再次可公开访问。

## Console

要禁用阻止公开访问快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 EC2 控制面板，然后在 ( 右侧的 ) 账户属性中，选择数据保护和安全。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 清除阻止公开访问，然后选择更新。

## AWS CLI

要禁用阻止公开访问快照

使用 [disable-snapshot-block-public-access](#) 命令。

```
aws ec2 disable-snapshot-block-public-access
```

## 使用 Amazon 监控对快照的封锁公开访问 EventBridge

Amazon EBS 将发出与阻止公开访问快照相关的事件。您可以使用 AWS Lambda 和 Amazon EventBridge 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 [Amazon EventBridge 用户指南](#)。

系统将发出以下事件：

- 在“阻止所有共享”模式下，启用阻止公开访问快照

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing' mode"
  }
}
```

- 在“阻止新共享”模式下，启用阻止公开访问快照

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
```

```

"time": "2019-05-31T21:49:54Z",
"region": "us-east-1",
"detail": {
  "SnapshotBlockPublicAccessState": "block-new-sharing",
  "message": "Block Public Access was successfully enabled in 'block-new-sharing'
mode"
}
}

```

- 禁用阻止公开访问快照

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}

```

## 快照回收站

回收站是一项数据恢复功能，支持您还原意外删除的 Amazon EBS 快照和 EBS 支持的 AMI。使用回收站时，如果资源被删除，回收站功能将在您指定的时间段内保留快照，而后永久删除资源。

在资源保留期到期之前，您可以随时从回收站还原资源。从回收站还原资源后，资源将从回收站中删除，您可以像使用账户中任何该类型的其他资源的一样使用此资源。如果保留期过期且资源未还原，则资源将从回收站中永久删除，并且不再可用于恢复。

回收站中快照的计费费率与您账户中的常规快照费率相同。使用回收站和保留规则不会产生额外费用。有关更多信息，请参阅 [Amazon EBS 定价](#)。

有关更多信息，请参阅[回收站](#)。

### 主题

- [使用回收站中的快照的权限](#)

- [在回收站中查看快照](#)
- [从回收站中还原快照](#)

## 使用回收站中的快照的权限

默认情况下，用户无权使用回收站中的快照。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

要查看及恢复回收站中的快照，用户必须具有以下权限：

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

要管理回收站中快照的标签，用户需要以下额外权限。

- `ec2:CreateTags`
- `ec2>DeleteTags`

要使用回收站控制台，用户需要 `ec2:DescribeTags` 权限。

以下是 IAM policy 示例。其中包括控制台用户的 `ec2:DescribeTags` 权限，以及用于管理标签的 `ec2:CreateTags` 和 `ec2>DeleteTags` 权限。如果不需要上述权限，您可以从策略中将其删除。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:RestoreSnapshotFromRecycleBin"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2>DeleteTags",

```

```
        "ec2:DescribeTags"
    ],
    "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
},
]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

创建权限集合。按照《AWS IAM Identity Center 用户指南》中[创建权限集](#)的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

创建适用于身份联合验证的角色。按照《IAM 用户指南》中[为第三方身份提供商创建角色 \(联合身份验证\)](#)的说明进行操作。

- IAM 用户：

- 创建您的用户可以担任的角色。按照《IAM 用户指南》中[为 IAM 用户创建角色](#)的说明进行操作。
- (不推荐使用) 将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中[向用户添加权限 \(控制台\)](#)中的说明进行操作。

有关使用回收站所需权限的更多信息，请参阅[所需的 IAM 权限](#)。

## 在回收站中查看快照

当快照在回收站中时，您可以查看有关该快照的有限信息，包括：

- 快照的 ID。
- 快照描述。
- 从中创建快照的卷的 ID。
- 快照被删除并进入回收站的日期和时间。
- 保留期到期的日期和时间。此时，快照将从回收站中永久删除。

您可以使用以下方法查看回收站中的快照。

## Recycle Bin console

使用控制台查看回收站中的快照

1. 在以下位置打开回收站控制台 <https://console.aws.amazon.com/rbin/home/>
2. 在导航窗格中，选择 Recycle Bin ( 回收站 )。
3. 该网格列出了当前在回收站中的所有快照。要查看特定快照的详细信息，请在网格中选择它，然后选择 Actions ( 操作 )、View details ( 查看详细信息 )。

## AWS CLI

要查看回收站中的快照，请使用 AWS CLI

使用 [list-snapshots-in-recycle-bin](#) AWS CLI 命令。加入 `--snapshot-id` 选项来查看特定快照。或者省略 `--snapshot-id` 选项以查看回收站中的所有快照。

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令提供有关回收站中的快照 `snap-01234567890abcdef` 的信息。

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

输出示例：

```
{
  "SnapshotRecycleBinInfo": [
    {
      "Description": "Monthly data backup snapshot",
      "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
      "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
      "VolumeId": "vol-abcdef09876543210",
      "SnapshotId": "snap-01234567890abcdef"
    }
  ]
}
```



## 从回收站中还原快照

当快照在回收站中时，您不能以任何方式使用它。要使用快照，您必须首先还原它。从回收站还原快照时，该快照立即可供使用，回收站会将其删除。还原快照后，您可以像使用账户中任何其它快照一样使用它。

您可以使用以下方法之一从回收站中还原快照。

### Recycle Bin console

使用控制台从回收站中还原快照

1. 在以下位置打开回收站控制台 <https://console.aws.amazon.com/rbin/home/>
2. 在导航窗格中，选择 Recycle Bin (回收站)。
3. 该网格列出了当前在回收站中的所有快照。选择要还原的快照，然后选择 Recover (还原)。
4. 系统提示时，选择 Recover (还原)。

### AWS CLI

要从回收站中恢复已删除的快照，请使用 AWS CLI

使用 [restore-snapshot-from-recycle-bin](#) AWS CLI 命令。对于 `--snapshot-id`，请指定需还原快照的 ID。

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令将快照 `snap-01234567890abcdef` 从回收站中还原。

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id  
snap-01234567890abcdef
```

输出示例：

```
{  
  "SnapshotId": "snap-01234567890abcdef",  
  "Description": "Monthly data backup snapshot",  
  "Encrypted": false,  
  "OwnerId": "111122223333",  
  "Progress": "100%",
```

```
"StartTime": "2021-12-01T13:00:00.000000+00:00",
"State": "recovering",
"VolumeId": "vol-ffffffff",
"VolumeSize": 30
}
```

## Amazon EBS local snapshots on Outposts

Amazon EBS 快照是 EBS 卷的时间点副本。

默认情况下，Outpost 上 EBS 卷的快照存储在 Amazon S3 中的 Outpost 区域中。您也可以使用 Outposts 上的 Amazon EBS 本地快照在 Outpost 自身的 Amazon S3 中，在本地存储 Outpost 上的卷副本。这可以确保快照数据驻留在您本地的 Outpost 上。此外，您可以使用 AWS Identity and Access Management (IAM) 策略和权限来设置数据驻留执行策略，以确保快照数据不会离开 Outpost。如果您居住在尚未有某个 AWS 区域提供服务且有数据驻留要求的国家或地区，这将特别有用。

此主题提供有关使用 Outposts 上的 Amazon EBS 本地快照的信息。有关 Amazon EBS 快照以及在 AWS 区域中使用快照的更多信息，请参阅 [Amazon EBS 快照](#)。

有关 AWS Outposts 的更多信息，请参阅 [AWS Outposts 功能](#) 和 [AWS Outposts 用户指南](#)。有关定价信息，请参阅 [AWS Outposts 定价](#)。

### 主题

- [常见问题](#)
- [先决条件](#)
- [注意事项](#)
- [使用 IAM 控制访问](#)
- [使用本地快照](#)

## 常见问题

### 1. 什么是本地快照？

默认情况下，Outpost 上卷的 Amazon EBS 快照存储在 Amazon S3 中的 Outpost 区域中。如果 Outpost 预置了 Amazon S3 on Outposts，您可以选择在 Outpost 自身本地存储快照。本地快照采用增量更新，这意味着只保存在最新快照之后更改的卷数据块。您随时可以使用这些快照在快照所在同一 Outpost 上恢复卷。有关 Amazon EBS 快照的更多信息，请参阅 [Amazon EBS 快照](#)。

## 2. 为什么应该使用本地快照？

快照是备份数据的便捷方法。使用本地快照，您的所有快照数据都在 Outpost 上本地存储。这意味着数据不会离开您的本地环境。如果您居住在尚未有某个 AWS 区域提供服务且有数据驻留要求的国家或地区，这将特别有用。

此外，使用本地快照可以在带宽受限环境中帮助减少区域和 Outpost 之间的通信所使用的带宽。

## 3. 如何在 Outpost 上执行快照数据驻留？

您可以使用 AWS Identity and Access Management (IAM) 策略来控制委托人 (AWS 账户、IAM 用户和 IAM 角色) 在使用本地快照时以及在执行数据驻留时拥有的权限。您可以创建一个策略，禁止委托人从 Outpost 卷和实例创建快照并将快照存储在 AWS 区域中。目前，不支持从 Outpost 向区域复制快照和映像。有关更多信息，请参阅[使用 IAM 控制访问](#)。

## 4. 是否支持多卷、崩溃一致性本地快照？

是的，您可以从 Outpost 上的实例创建多卷、崩溃一致性本地快照。

## 5. 我该如何创建本地快照？

您可以使用 (AWS Command Line Interface AWS CLI) 或 Amazon EC2 控制台手动创建快照。有关更多信息，请参阅[使用本地快照](#)。您还可以使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期。有关更多信息，请参阅[在 Outpost 上自动执行快照](#)。

## 6. 如果我的 Outpost 失去了与其区域的连接，我可以创建、使用或删除本地快照吗？

不可以。Outpost 必须与其区域建立连接，因为该区域提供对快照的运行状况至关重要的访问、授权、日志记录和监控服务。如果没有连接，则您无法创建新的本地快照、创建卷或从现有本地快照实例启动实例，也无法删除本地快照。

## 7. 删除本地快照多久后 Amazon S3 存储容量可供使用？

Amazon S3 存储容量在删除引用它们的本地快照和卷后 72 小时内可供使用。

## 8. 我如何确保不会在我的 Outpost 上耗尽 Amazon S3 容量？

我们建议您使用 Amazon CloudWatch 警报来监控 Amazon S3 存储容量，并删除不再需要的快照和卷，以避免存储容量耗尽。如果您在使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期，请确保快照保留策略保留快照的时间不超过所需时长。

## 9. 如果我的 Outposts 上的本地 Amazon S3 容量用尽，会发生什么情况？

如果您的 Outposts 上的本地 Amazon S3 容量不足，Amazon Data Lifecycle Manager 将无法在 Outposts 上成功创建本地快照。Amazon Data Lifecycle Manager 将尝试在 Outposts 上创建本地

快照，但快照会立即过渡到 `error` 状态，最终会被 Amazon Data Lifecycle Manager 删除。建议使用 `SnapshotsCreateFailed` Amazon CloudWatch 指标监控快照生命周期策略，以监控快照创建失败的情况。有关更多信息，请参阅[使用 Amazon 监控您的政策 CloudWatch](#)。

10. 我能否将本地快照以及由本地快照支持的 AMI 与竞价型实例和竞价型实例集一起使用？

不能，您不能使用本地快照以及由本地快照支持的 AMI 启动竞价型实例或竞价型实例集。

11. 我是否可以对本地快照及由本地快照支持的 AMI 使用 Amazon EC2 Auto Scaling？

是的，您可以使用本地快照及由本地快照支持的 AMI，在与快照位于同一个 Outpost 的子网中启动 Auto Scaling 组。Amazon EC2 Auto Scaling 组服务相关角色必须具有使用用于加密快照的 KMS 密钥的权限。

您不能使用本地快照或由本地快照支持的 AMI 在 AWS 区域中启动 Auto Scaling 组。

## 先决条件

要在 Outpost 上存储快照，您必须拥有配置了 Amazon S3 on Outposts 的 Outpost。有关 Amazon S3 on Outposts 的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的[使用 Amazon S3 on Outposts](#)。

## 注意事项

使用本地快照时请记住以下事项。

- Outpost 必须具有与其 AWS 区域的连接才能使用本地快照。
- 快照元数据存储在与 Outpost 关联的 AWS 区域中。其中不包括任何快照数据。
- 存储在 Outpost 上的快照默认处于加密状态。不支持非加密快照。在 Outpost 上创建的快照和复制到 Outpost 的快照，将使用区域的默认 KMS 密钥 或您在请求时指定的其他 KMS 密钥 进行加密。
- 当您从本地快照在 Outpost 上创建卷时，不能使用其他 KMS 密钥 对卷重新加密。从本地快照创建的卷必须使用与源快照相同的 KMS 密钥 进行加密。
- 从 Outpost 中删除本地快照后，删除的快照所使用的 Amazon S3 存储容量将在 72 小时内可供使用。有关更多信息，请参阅[删除本地快照](#)。
- 您不能从 Outpost 导出本地快照。
- 您不能为本地快照启用快速快照还原。
- EBS direct API 不支持本地快照。

- 您不能将本地快照或 AMI 从 Outpost 复制到某个 AWS 区域、在 Outpost 之间或在 Outpost 内复制。但是，您可以将快照从 AWS 区域复制到 Outpost。有关更多信息，请参阅[将快照从 AWS 区域复制到 Outpost](#)。
- 将快照从 AWS 区域复制到 Outpost 时，数据将通过服务链接传输。同时复制多个快照可能会影响在 Outpost 上运行的其他服务。
- 您不能共享本地快照。
- 您必须使用 IAM policy 来确保满足数据驻留要求。有关更多信息，请参阅[使用 IAM 控制访问](#)。
- 本地快照执行增量备份。只保存卷中在最近快照之后发生更改的数据块。每个本地快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的全部信息。有关更多信息，请参阅[快照的工作原理](#)。
- 您不能使用 IAM policy 为 CopySnapshot 和 CopyImage 操作执行数据驻留。

## 使用 IAM 控制访问

您可以使用 AWS Identity and Access Management ( IAM ) 策略来控制委托人 ( AWS 账户、IAM 用户和 IAM 角色 ) 在使用本地快照时拥有的权限。以下示例策略可用于授予或拒绝对本地快照执行特定操作的权限。

### Important

目前不支持将快照和映像从 Outpost 复制到区域。因此，您目前无法使用 IAM policy 为 CopySnapshot 和 CopyImage 操作执行数据驻留。

### 主题

- [为快照执行数据驻留](#)
- [禁止委托人删除本地快照](#)

## 为快照执行数据驻留

以下示例策略禁止所有委托人从 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` 上的卷和实例创建快照并将快照数据存储在 AWS 区域中。委托人仍然可以创建本地快照。此策略可确保所有快照都保留在 Outpost 上。

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

```

    "Statement": [
      {
        "Effect": "Deny",
        "Action": [
          "ec2:CreateSnapshot",
          "ec2:CreateSnapshots"
        ],
        "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
        "Condition": {
          "StringEquals": {
            "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
          },
          "Null": {
            "ec2:OutpostArn": "true"
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:CreateSnapshot",
          "ec2:CreateSnapshots"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

## 禁止委托人删除本地快照

以下示例策略禁止所有委托人删除存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上的本地快照。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2>DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",

```

```
    "Condition": {
      "StringEquals": {
        "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

## 使用本地快照

下面几节介绍如何使用本地快照。

### 主题

- [存储快照的规则](#)
- [从 Outpost 上的卷创建本地快照](#)
- [从 Outpost 上的实例创建多卷本地快照](#)
- [从本地快照创建 AMI](#)
- [将快照从 AWS 区域复制到 Outpost](#)
- [将 AMI 从 AWS 区域复制到 Outpost](#)
- [从本地快照创建卷](#)
- [从由本地快照支持的 AMI 启动实例](#)
- [删除本地快照](#)
- [在 Outpost 上自动执行快照](#)

### 存储快照的规则

以下规则适用于快照存储：

- 如果卷的最新快照存储在某个 Outpost 中，则所有后续快照都必须存储在同一个 Outpost 中。

- 如果卷的最新快照存储在某个 AWS 区域中，则所有后续快照都必须存储在同一区域中。要开始从该卷创建本地快照，请执行以下操作：
  1. 在 AWS 区域中创建卷的快照。
  2. 将快照从 AWS 区域复制到 Outpost。
  3. 从本地快照创建新卷：
  4. 将卷附加到 Outpost 上的实例。

对于 Outpost 上的新卷，下一个快照可以存储在 Outpost 或 AWS 区域中。然后必须将所有后续快照存储在同一位置。

- 本地快照，包括在 Outpost 上创建的快照以及从 AWS 区域复制到 Outpost 的快照，只能用于在同一个 Outpost 上创建卷。
- 如果您从某个区域中的快照在 Outpost 上创建卷，则该新卷的所有后续快照都必须位于同一区域中。
- 如果您从本地快照在 Outpost 上创建卷，则该新卷的所有后续快照都必须位于同一个 Outpost 中。

## 从 Outpost 上的卷创建本地快照

您可以从 Outpost 上的卷创建本地快照。您可以选择将快照存储在源卷所在的同一 Outpost 中，也可以选择将快照存储在 Outpost 的区域中。

本地快照只能用于在同一个 Outpost 上创建卷。

您可以使用以下方法之一从 Outpost 上的卷创建本地快照。

### Console

#### 从 Outpost 上的卷创建本地快照

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择 Volumes。
2. 选择 Outpost 上的卷，依次选择操作和创建快照。
3. (可选) 对于 Description (描述)，输入对快照的简短描述。
4. 对于快照目标，选择 AWS Outpost。快照将在源卷所在的同一 Outpost 上创建。Outpost ARN 字段显示了目标 Outpost 的 Amazon 资源名称 (ARN)。
5. (可选) 选择添加标签以向快照添加标签。对于每个标签，提供标签键和标签值。



## 6. 选择创建快照。

### Command line

从 Outpost 上的卷创建本地快照

使用 `create-snapshot` 命令。指定要从中创建快照的卷的 ID，以及存储快照的目标 Outpost 的 ARN。如果省略 Outpost ARN，则快照将存储在该 Outpost 的 AWS 区域中。

例如，以下命令创建卷 `vol-1234567890abcdef0` 的本地快照，然后将快照存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上。

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --outpost-arn
arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description
"single volume local snapshot"
```

### 从 Outpost 上的实例创建多卷本地快照

您可以从 Outpost 上的实例创建崩溃一致性多卷本地快照。您可以选择将快照存储在源实例所在的同一 Outpost 中，也可以存储在 Outpost 的区域中。

多卷本地快照只能用于在同一个 Outpost 上创建卷。

您可以使用以下方法之一从 Outpost 上的实例创建多卷本地快照。

### Console

从 Outpost 上的实例创建多卷本地快照

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 选择 Create Snapshot (创建快照)。
3. 对于选择资源类型，选择实例。
4. 对于实例 ID，在 Outpost 上选择要从中创建快照的实例。
5. (可选) 对于描述，输入对快照的简短描述。
6. 对于 Snapshot destination (快照目标)，选择 AWS Outpost。快照将在源实例所在的同一 Outpost 上创建。Outpost ARN 显示了目标 Outpost 的 ARN。

7. 若要从多卷快照集中排除实例的根卷，选择 Exclude root volume ( 排除根卷 )。如果这样做，Amazon EBS 将不会创建实例根卷的快照。
8. 若要从多卷快照集中排除特定数据卷，请选择 Exclude specific data volumes ( 排除特定数据卷 )。Attached data volumes ( 附加的数据卷 ) 部分列出了当前附加到所选实例的所有数据卷。

在 Attached data volumes ( 附加的数据卷 ) 部分，取消选择要从多卷快照集中排除的数据卷。只有选中的卷才会包含在多卷快照集中。

9. ( 可选 ) 若要自动将标签从源卷复制到相应快照，请为 Copy tags from source volume ( 从源卷复制标签 ) 选择 Copy tags ( 复制标签 )。这将设置快照元数据 ( 如访问策略、附件信息和成本分配 ) 以匹配源卷。
10. ( 可选 ) 若要为快照分配自定义标签，请在标签部分选择添加标签，然后输入键值对。最多可以添加 50 个标签。
11. 选择 Create Snapshot (创建快照)。

快照创建期间，将一起管理快照。如果卷集中的某个快照失败，则卷集中的其他快照将移至错误状态。

## Command line

从 Outpost 上的实例创建多卷本地快照

使用 [create-snapshots](#) 命令。指定要从中创建快照的实例的 ID，以及存储快照的目标 Outpost 的 ARN。如果省略 Outpost ARN，则快照将存储在 Outpost 的 AWS 区域中。

例如，以下命令创建附加到实例 `i-1234567890abcdef0` 的卷的快照，并将快照存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上。

```
$ aws ec2 create-snapshots --instance-specification InstanceId=i-1234567890abcdef0
--outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
--description "multi-volume local snapshots"
```

## 从本地快照创建 AMI

您可以使用本地快照和存储在 Outpost 区域中的快照组合来创建亚马逊机器映像 (AMI)。例如，如果您在 `us-east-1` 中有一个 Outpost，则可以使用由该 Outpost 上的本地快照支持的数据卷，以及由 `us-east-1` 区域中的快照支持的根卷来创建一个 AMI。

**Note**

- 您不能创建包含存储在多个 Outpost 中的备份快照的 AMI。
- 目前，您无法使用 CreateImage API 或 Amazon EC2 控制台，为通过 Amazon S3 on Outposts 启用的 Outpost，直接从 Outpost 上的实例创建 AMI。
- 由本地快照支持的 AMI 只能用于在同一个 Outpost 上启动实例。

### 从区域中的快照在 Outpost 上创建 AMI

1. 将快照从区域复制到 Outpost。有关更多信息，请参阅[将快照从 AWS 区域复制到 Outpost](#)。
2. 通过 Amazon EC2 控制台或 [register-image](#) 命令使用 Outpost 上的快照副本创建 AMI。有关更多信息，请参阅[从快照创建 AMI](#)。

### 从 Outpost 上的实例在 Outpost 上创建 AMI

1. 从 Outpost 上的实例创建快照并将快照存储在该 Outpost 中。有关更多信息，请参阅[从 Outpost 上的实例创建多卷本地快照](#)。
2. 通过 Amazon EC2 控制台或 [register-image](#) 命令使用本地快照创建 AMI。有关更多信息，请参阅[从快照创建 AMI](#)。

### 从 Outpost 上的实例在区域中创建 AMI

1. 从 Outpost 上的实例创建快照并将快照存储在区域中。有关更多信息，请参阅[从 Outpost 上的卷创建本地快照](#) 或 [从 Outpost 上的实例创建多卷本地快照](#)。
2. 使用 Amazon EC2 控制台或 [寄存器映像](#) 命令使用区域中的快照副本创建 AMI。有关更多信息，请参阅[从快照创建 AMI](#)。

### 将快照从 AWS 区域复制到 Outpost

您可以将快照从 AWS 区域复制到 Outpost。仅当快照位于 Outpost 的区域中时，才能执行此操作。如果快照位于其他区域，则必须先将快照复制到该 Outpost 的区域，再将其从该区域复制到该 Outpost。

**Note**

您不能将本地快照从 Outpost 复制到某个区域、在 Outpost 之间或在 Outpost 内复制。

您可以使用以下方法之一将快照从区域复制到 Outpost。

## Console

### 将快照从 AWS 区域复制到 Outpost

通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

1. 在导航窗格中，选择快照。
2. 在区域中选择快照，然后选择操作和复制。
3. 对于目标区域，选择目标 Outpost 的区域。
4. 对于快照目标，选择 AWS Outpost。

仅当您在所选目标区域中有 Outpost 时，才会显示快照目标字段。如果该字段未显示，则表示选定的目标区域中没有任何 Outpost。

5. 对于目标 Outpost ARN，输入要将快照复制到的 Outpost 的 ARN。
6. （可选）对于描述，输入对复制的快照的简要描述。
7. 默认情况下，快照副本启用加密。无法禁用加密。对于 KMS 密钥，选择要使用的 KMS 密钥。
8. 选择复制。

## Command line

### 将快照从区域复制到 Outpost

使用 `copy-snapshot` 命令。指定要复制的快照的 ID、要从中复制快照的区域以及目标 Outpost 的 ARN。

例如，以下命令将快照 `snap-1234567890abcdef0` 从 `us-east-1` 区域复制到 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`。

```
$ aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-id snap-1234567890abcdef0 --destination-outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description "Local snapshot copy"
```

## 将 AMI 从 AWS 区域复制到 Outpost

您可以将 AMI 从 AWS 区域复制到 Outpost。当您从区域复制 AMI 到 Outpost 时，与该 AMI 关联的所有快照都将从该区域复制到该 Outpost。

仅当与 AMI 关联的快照位于 Outpost 的区域中时，您才能将该 AMI 从该区域复制到该 Outpost。如果快照位于其他区域，则必须先将 AMI 复制到该 Outpost 的区域，再将其从该区域复制到该 Outpost。

### Note

您不能将 AMI 从 Outpost 复制到某个区域、在 Outpost 之间或在 Outpost 内复制。

您只能使用 AWS CLI 将 AMI 从区域复制到 Outpost。

### Command line

将 AMI 从区域复制到 Outpost

使用 [copy-image](#) 命令。指定要复制的 AMI 的 ID、源区域和目标 Outpost 的 ARN。

例如，以下命令将 AMI `ami-1234567890abcdef0` 从 `us-east-1` 区域复制到 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`。

```
$ aws ec2 copy-image --source-region us-east-1 --source-image-id ami-1234567890abcdef0 --name "Local AMI copy" --destination-outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
```

## 从本地快照创建卷

您可以从本地快照在 Outpost 上创建卷。卷必须在源快照所在同一个 Outpost 上创建。您不能使用本地快照在 Outpost 的区域中创建卷。

从本地快照创建卷时，不能使用不同的 KMS 密钥对卷重新加密。从本地快照创建的卷必须使用与源快照相同的 KMS 密钥进行加密。

有关更多信息，请参阅[从快照创建卷](#)。

## 从本地快照支持的 AMI 启动实例

您可以从本地快照支持的 AMI 启动实例。您必须在源 AMI 所在的同一 Outpost 中启动实例。有关更多信息，请参阅 AWS Outposts 用户指南中的[在 Outpost 中启动实例](#)。

## 删除本地快照

您可以从 Outpost 中删除本地快照。从 Outpost 中删除快照后，已删除快照使用的 Amazon S3 存储容量将在删除快照和引用该快照的卷后 72 小时内可用。

由于 Amazon S3 存储容量不会立即可用，我们建议您使用 Amazon CloudWatch 警报来监控 Amazon S3 存储容量。应删除不再需要的快照和卷，以避免存储容量耗尽。

有关删除快照的更多信息，请参阅[删除快照](#)。

## 在 Outpost 上自动执行快照

您可以创建 Amazon Data Lifecycle Manager 快照生命周期策略，使之自动创建、复制、保留和删除 Outpost 上卷和实例的快照。您可以选择是将快照存储在区域中，还是在 Outpost 上本地存储。此外，您还可以将在 AWS 区域中创建和存储的快照自动复制到 Outpost。

下表提供了支持功能的概述。

资源位置	快照目标	跨区域复制		快速快照还原	跨账户共享
		复制到区域	复制到 Outpost		
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

## 注意事项

- 目前仅支持 Amazon EBS 快照生命周期策略。不支持由 EBS 支持的 AMI 策略和跨账户共享事件策略。
- 如果有策略管理某个区域中卷或实例的快照，则快照将在源资源所在同一区域中创建。

- 如果有策略管理 Outpost 上卷或实例的快照，则可以在源 Outpost 或该 Outpost 的区域中创建快照。
- 单个策略无法同时管理区域中的快照和 Outpost 上的快照。如果您需要在区域和 Outpost 中自动执行快照，则必须分别创建策略。
- 在 Outpost 上创建的快照或复制到 Outpost 的快照不支持快照还原。
- 在 Outpost 上创建的快照不支持跨账户共享。

有关创建可管理本地快照的快照生命周期的更多信息，请参阅[自动化快照生命周期](#)。

# Amazon EBS 加密

使用 Amazon EBS 加密 作为与 EC2 实例关联的 EBS 资源的直接加密解决方案。借助 Amazon EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。创建加密卷和快照时，Amazon EBS 加密使用 AWS KMS keys。

加密操作发生在托管 EC2 实例的服务器上，从而确保两者的安全，data-at-rest 以及实例 data-in-transit 与其连接的 EBS 存储之间的安全。

您可以同时将加密卷和未加密卷附加到实例。

## 目录

- [EBS 加密的工作原理](#)
- [Amazon EBS 加密要求](#)
- [使用 Amazon EBS 加密](#)
- [加密 EBS 资源](#)
- [旋转 AWS KMS 钥匙](#)
- [Amazon EBS 加密示例](#)

## EBS 加密的工作原理

您可以加密 EC2 实例的引导卷和数据卷。

在创建加密的 EBS 卷并将其附加到支持的实例类型后，将对以下类型的数据进行加密：

- 卷中的静态数据
- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照
- 从这些快照创建的所有卷

Amazon EBS 通过数据密钥使用行业标准的 AES-256 数据加密来加密您的卷。数据密钥由您的密钥生成，AWS KMS 然后由 AWS KMS 您的 AWS KMS 密钥加密，然后与您的卷信息一起存储。所有快照以及使用相同 AWS KMS 密钥从这些快照创建的任何后续卷共享相同的数据密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的[数据密钥](#)。



Amazon EC2 使用加密和解密您的 EBS 卷的方式略有不同，具体取决于您创建加密卷的快照是加密还是未加密。AWS KMS

## 快照加密时 EBS 加密的工作原理

当您使用自己拥有的加密快照创建加密卷时，Amazon EC2 会按如下方式 AWS KMS 对您的 EBS 卷进行加密和解密：

1. Amazon EC2 向发送[GenerateDataKeyWithoutPlaintext](#)请求 AWS KMS，指定您为批量加密选择的 KMS 密钥。
2. 如果使用与快照相同的 KMS 密钥加密卷，则 AWS KMS 使用与快照相同的数据密钥并使用相同的 KMS 密钥对其进行加密。如果使用不同的 KMS 密钥对卷进行加密，则 AWS KMS 会生成新的数据密钥并使用您指定的 KMS 密钥对其进行加密。加密的数据密钥会发送到 Amazon EBS，并与卷元数据存储在一起。
3. 当您添加加密卷到实例时，Amazon EC2 会向发送[CreateGrant](#)请求，AWS KMS 以便它可以解密数据密钥。
4. AWS KMS 解密加密的数据密钥并将解密后的数据密钥发送到 Amazon EC2。
5. Amazon EC2 使用 Nitro 硬件中的明文数据密钥来加密卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

## 快照未加密时 EBS 加密的工作原理

当您从未加密的快照创建加密卷时，Amazon EC2 和 AWS KMS 结合使用对 EBS 卷进行加密和解密，如下所示：

1. Amazon EC2 向发送[CreateGrant](#)请求 AWS KMS，以便它可以加密根据快照创建的卷。
2. Amazon EC2 向发送[GenerateDataKeyWithoutPlaintext](#)请求 AWS KMS，指定您为批量加密选择的 KMS 密钥。
3. AWS KMS 生成新的数据密钥，使用您为卷加密选择的 KMS 密钥对其进行加密，然后将加密的数据密钥发送到 Amazon EBS，以便与卷元数据一起存储。
4. Amazon EC2 向发送[解密](#)请求 AWS KMS 以解密加密的数据密钥，然后使用该密钥对卷数据进行加密。
5. 当您添加加密卷到实例时，Amazon EC2 会向发送[CreateGrant](#)请求 AWS KMS，以便它可以解密数据密钥。
6. 当您添加加密卷到实例时，Amazon EC2 会向发送[解密](#)请求 AWS KMS，指定加密的数据密钥。

7. AWS KMS 解密加密的数据密钥并将解密后的数据密钥发送到 Amazon EC2。
8. Amazon EC2 使用 Nitro 硬件中的明文数据密钥来加密卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [Amazon Elastic Block Store \( Amazon EBS \) 如何使用 AWS KMS](#) 和 [Amazon EC2 示例 2](#)。

## 不可用的 KMS 密钥如何影响数据密钥

当 KMS 密钥不可用时，您可以立即发现（取决于最终一致性）。KMS 密钥的密钥状态会出现变更，以反映其新情况，并且加密操作中使用 KMS 密钥的所有请求都将失败。

当执行让 KMS 密钥不可用的操作时，不会立即对 EC2 实例或连接的 EBS 卷产生影响。卷附加到实例时，Amazon EC2 使用数据密钥（而不是 KMS 密钥），对所有磁盘 I/O 进行加密。

但是，当加密的 EBS 卷从 EC2 实例分离时，Amazon EBS 将从 Nitro 硬件中删除该数据密钥。下次将加密的 EBS 卷附加到 EC2 实例时，附加会失败，因为 Amazon EBS 无法使用 KMS 密钥来解密卷的加密数据密钥。要再次使用 EBS 卷，您必须使该 KMS 密钥可重新使用。

### Tip

如果不再希望对存储在 EBS 卷中的数据进行访问，该数据使用由 KMS 密钥生成的数据密钥进行加密，但您打算让其无法使用，我们建议您在让 KMS 密钥不可用之前将 EBS 卷与 EC2 实例分离。

有关更多信息，请参见《AWS Key Management Service 开发人员指南》中的 [不可用的 KMS 密钥如何影响数据密钥](#)。

## Amazon EBS 加密要求

在您开始之前，确认您满足以下要求。

### 要求

- [支持的卷类型](#)
- [支持的实例类型](#)

- [用户的权限](#)
- [实例的权限](#)

## 支持的卷类型

所有 EBS 卷类型都支持加密。您可能希望加密卷具有与未加密卷相同的 IOPS 性能，同时对延迟的影响最低。您可以采用与访问未加密卷相同的方式来访问加密卷。加密和解密是以透明方式处理的，并且不需要您或您的应用程序执行额外操作。

## 支持的实例类型

Amazon EBS 加密适用于所有[当前一代](#)和[上一代](#)实例类型。

## 用户的权限

当您使用 KMS 密钥进行 EBS 加密时，KMS 密钥策略允许任何有权访问所需 AWS KMS 操作的用户使用此 KMS 密钥来加密或解密 EBS 资源。您必须授予用户调用以下操作的权限才能使用 EBS 加密：

- kms:CreateGrant
- kms:Decrypt
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlainText
- kms:ReEncrypt

### Tip

为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用 kms:GrantIsForAWSResource 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

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

```

    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": [
        "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
    ],
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": true
        }
    }
}
]
}

```

有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中[“默认密钥策略”](#)部分中的[允许访问 AWS 账户和启用 IAM 策略](#)。

## 实例的权限

当实例尝试与加密的 AMI、卷或快照进行交互时，系统会向该实例的仅限身份角色发放 KMS 密钥授权。仅限身份角色是一个 IAM 角色，实例使用该角色代表您与加密的 AMI、卷或快照进行交互。

仅限身份角色无需手动创建或删除，也没有与之关联的策略。此外，您无法访问仅限身份的角色凭证。

### Note

您的实例上的应用程序不使用仅限身份的角色来访问其他 AWS KMS 加密资源，例如 Amazon S3 对象或 Dynamo DB 表。这些操作是使用 Amazon EC2 实例角色的 AWS 证书或您在实例上配置的其他证书完成的。

仅限身份的角色受[服务控制策略](#) ( SCP ) 和 [KMS 密钥策略](#) 的约束。如果 SCP 或 KMS 密钥拒绝仅限身份的角色访问 KMS 密钥，则您可能无法使用加密卷或使用加密 AMI 或快照启动 EC2 实例。

如果您要使用 `aws:SourceIp`、`aws:VpcSourceIp`、或 `aws:SourceVpce` AWS 全局条件密钥创建基于网络位置拒绝访问的 SCP 或密钥策略，则必须确保这些策略声明不适用于仅限实例的角色。`aws:SourceVpc` 有关示例策略，请参阅[数据外围策略示例](#)。

仅限身份的角色 ARN 使用以下格式：

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

向实例颁发密钥授予时，密钥授予将颁发给特定于该实例的代入角色会话。被授权者主体 ARN 使用以下格式：

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

## 使用 Amazon EBS 加密

按照以下过程使用 Amazon EBS 加密。

### 任务

- [选择 EBS 加密的 KMS 密钥](#)
- [默认启用加密](#)
- [默认使用 API 和 CLI 管理加密](#)

## 选择 EBS 加密的 KMS 密钥

Amazon EBS 会自动 AWS 托管式密钥 在您存储 AWS 资源的每个区域中创建唯一的。此 KMS 密钥具有别名 `alias/aws/ebs`。默认情况下，Amazon EBS 使用此 KMS 密钥 进行加密。您也可以指定一个您创建的对称客户管理加密密钥，以作为 EBS 加密的原定设置 KMS 密钥。使用您自己的 KMS 密钥 可以提高灵活性，包括提供创建、轮换和禁用 KMS 密钥 的能力。

### Important

Amazon EBS 不支持非对称加密 KMS 密钥。有关更多信息，请参阅 [《AWS Key Management Service 开发人员指南》](#) 中的使用对称和非对称加密 KMS 密钥。

## Amazon EC2 console

针对某个区域配置用于 EBS 加密的默认 KMS 密钥

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。

4. 在页面的右上角，选择账户属性，然后选择数据保护和安全。
5. 选择管理。
6. 对于 Default encryption key（原定设置加密密钥），选择对称客户管理加密密钥。
7. 选择更新 EBS 加密。

## 默认启用加密

您可以将您的 AWS 账户配置为强制对您创建的新 EBS 卷和快照副本进行加密。例如，Amazon EBS 加密当您启动实例时创建的 EBS 卷以及您从未加密的快照复制的快照。有关从未加密转换为加密 EBS 资源的示例，请参阅[加密未加密的资源](#)。

默认情况下，加密对现有 EBS 卷或快照没有影响。

### 注意事项

- 默认加密是区域特定的设置。如果您为某个区域启用了它，则无法为该区域中单独的卷或快照禁用。
- Amazon EBS 加密默认支持所有[当前一代](#)和[上一代](#)实例类型。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 使用 AWS Server Migration Service (SMS) 迁移服务器时，请勿默认开启加密。如果默认情况下已启用加密，并且您遇到增量复制失败，请默认关闭加密。改为在创建复制作业时启用 AMI 加密。

### Amazon EC2 console

#### 默认为某个区域启用加密

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择数据保护和安全。
5. 选择管理。
6. 选择启用。您可以保留 AWS 托管式密钥 使用代表您 alias/aws/ebs 创建的别名作为默认加密密钥，或者选择对称的客户托管加密密钥。
7. 选择更新 EBS 加密。

## AWS CLI

### 查看默认设置的加密

- 对于特定区域

```
$ aws ec2 get-efs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do default=$(aws ec2 get-efs-encryption-by-default
--region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}" --
output text); kms_key=$(aws ec2 get-efs-default-kms-key-id --region $region | jq
'.KmsKeyId'); echo "$region --- $default --- $kms_key"; done
```

### 默认启用加密

- 对于特定区域

```
$ aws ec2 enable-efs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do default=$(aws ec2 enable-efs-encryption-by-
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
--output text); kms_key=$(aws ec2 get-efs-default-kms-key-id --region $region |
jq '.KmsKeyId'); echo "$region --- $default --- $kms_key"; done
```

### 默认禁用加密

- 对于特定区域

```
$ aws ec2 disable-efs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do default=$(aws ec2 disable-efs-encryption-by-
```

```
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
--output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region |
jq '.KmsKeyId'); echo "$region --- $default --- $kms_key"; done
```

## PowerShell

### 查看默认设置的加密

- 对于特定区域

```
PS C:\> Get-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
= $_; EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_;
EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

### 默认启用加密

- 对于特定区域

```
PS C:\> Enable-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
= $_; EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_;
EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

### 默认禁用加密

- 对于特定区域

```
PS C:\> Disable-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域



```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
= $_; EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_;
EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

您无法更改与现有快照或加密卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

## 默认使用 API 和 CLI 管理加密

您可以使用以下 API 操作和 CLI 命令默认管理加密和默认 KMS 密钥。

API 操作	CLI 命令	描述
<a href="#">DisableEbsEncryptionByDefault</a>	<a href="#">disable-efs-encryption-by-默认</a>	默认禁用加密。
<a href="#">EnableEbsEncryptionByDefault</a>	<a href="#">enable-efs-encryption-by-默认</a>	默认启用加密。
<a href="#">GetEbsDefaultKmsKeyId</a>	<a href="#">get-efs-default-kms-key-id</a>	描述默认 KMS 密钥。
<a href="#">GetEbsEncryptionByDefault</a>	<a href="#">get-efs-encryption-by-默认</a>	指示是否默认启用了加密。
<a href="#">ModifyEbsDefaultKmsKeyId</a>	<a href="#">modify-efs-default-kms-key-id</a>	更改用于加密 EBS 卷的默认 KMS 密钥。
<a href="#">ResetEbsDefaultKmsKeyId</a>	<a href="#">reset-efs-default-kms-key-id</a>	将重置 AWS 托管式密钥 为用于加密 EBS 卷的默认 KMS 密钥。

## 加密 EBS 资源

您可以通过启用加密来加密 EBS 卷：[使用默认加密](#)，或者在创建要加密的卷时启用加密。

加密卷时，可以指定用于加密该卷的对称加密 KMS 密钥。如果未指定 KMS 密钥，则用于加密的 KMS 密钥 取决于源快照的加密状态及其所有权。有关更多信息，请参阅[加密结果表](#)。

**Note**

如果您正在使用 API 或 AWS CLI 指定 KMS 密钥，请注意这会异步对 KMS 密钥 AWS 进行身份验证。如果您指定了无效的 KMS 密钥 ID、别名或 ARN，则操作可能会显示完成，但最终失败。

您无法更改与现有快照或卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

## 在创建时加密空卷

创建新的空 EBS 卷时，可以通过为特定卷创建操作启用加密来对其进行加密。如果默认情况下启用了 EBS 加密，则会使用 EBS 加密的默认 KMS 密钥 自动加密卷。您也可以为特定的卷创建操作指定不同的对称加密 KMS 密钥。卷从其首次可用时开始加密，因此您的数据始终安全。有关详细步骤，请参阅 [创建 Amazon EBS 卷](#)。

默认情况下，您在创建卷时选择的 KMS 密钥 会对从该卷拍摄的快照加密，并对从这些加密的快照还原的卷加密。您无法从加密卷或快照删除加密，这意味着从加密快照还原的卷或者加密快照的副本始终加密。

加密卷的快照无法公开，但您可以与特定账户共享加密快照。有关详细指导，请参阅 [共享 Amazon EBS 快照](#)。

## 加密未加密的资源

您无法直接加密现有未加密卷或快照。但是，您可以从未加密的卷或快照创建加密卷或快照。如果预设情况下启用加密，Amazon EBS 将使用 EBS 加密的原定设置 KMS 密钥 自动加密新卷和快照。否则，您可以在创建单个卷或快照时启用加密，使用用于 Amazon EBS 加密的原定设置 KMS 密钥 或对称客户管理加密密钥。有关更多信息，请参阅 [创建 Amazon EBS 卷](#) 和 [复制 Amazon EBS 快照](#)。

要将快照副本加密到 客户托管密钥，您必须同时启用加密并指定 KMS 密钥，如 [复制未加密的快照（未启用默认加密）](#) 中所示。

**Important**

Amazon EBS 不支持非对称加密 KMS 密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 [使用对称和非对称加密 KMS 密钥](#)。

在从由 EBS 支持的 AMI 启动实例时，您还可以应用新的加密状态。这是因为 EBS 支持的 AMI 包括可以按照所述进行加密的 EBS 卷的快照。有关更多信息，请参阅[将加密与 EBS 支持的 AMI 结合使用](#)。

## 旋转 AWS KMS 钥匙

加密最佳实践建议不要广泛重复使用加密密钥。

要创建用于 Amazon EBS 加密的新加密材料，您可以创建新的客户托管密钥，然后将应用程序更改为使用新的 KMS 密钥。或者，您可以为现有客户管理的密钥启用自动密钥轮换。

当您为客户托管密钥启用自动密钥轮换时，每年会为 KMS 密钥 AWS KMS 生成新的加密材料。AWS KMS 保存加密材料的所有先前版本，以便您可以继续解密和使用以前使用该 KMS 密钥材料加密的卷和快照。AWS KMS 在您删除 KMS 密钥之前，不会删除任何轮换的密钥材料。

当您使用轮换的客户托管密钥加密新卷或快照时，将 AWS KMS 使用当前（新）密钥材料。当您使用轮换的客户托管密钥解密卷或快照时，将 AWS KMS 使用用于加密卷或快照的加密材料版本。如果使用先前版本的加密材料对卷或快照进行加密，则 AWS KMS 将继续使用先前版本对其进行解密。AWS KMS 不会在密钥轮换后重新加密先前加密的卷或快照以使用新的加密材料。它们仍使用最初加密时使用的加密材料进行加密。您可以安全地在应用程序和 AWS 服务中使用轮换的客户托管密钥，而无需更改代码。

### Note

- 只有具有 AWS KMS 创建密钥材料的对称客户托管密钥才支持自动密钥轮换。
- AWS KMS AWS 托管式密钥 每年自动轮换。您无法启用或禁用 AWS 托管式密钥的密钥轮换。

有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的[轮换 KMS 密钥](#)。

## Amazon EBS 加密示例

创建加密 EBS 资源时，除非您在卷创建参数或 AMI 或实例的块设备映射中指定了不同的 客户托管密钥，否则它将使用您账户的用于 EBS 加密的默认 KMS 密钥 进行加密。有关更多信息，请参阅[选择 EBS 加密的 KMS 密钥](#)。

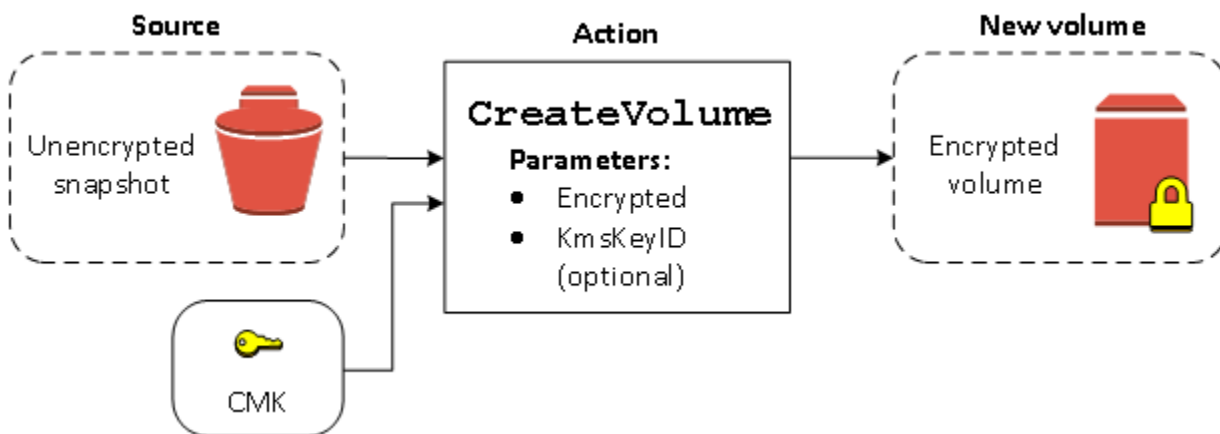
以下示例说明如何管理卷和快照的加密状态。有关加密案例的完整列表，请参阅[加密结果表](#)。

## 示例

- [还原未加密的卷 \(未启用默认加密\)](#)
- [还原未加密的卷 \(启用了默认加密\)](#)
- [复制未加密的快照 \(未启用默认加密\)](#)
- [复制未加密的快照 \(启用了默认加密\)](#)
- [重新加密已加密卷](#)
- [重新加密已加密快照](#)
- [在加密卷与未加密卷之间迁移数据](#)
- [加密结果](#)

## 还原未加密的卷 (未启用默认加密)

未启用默认加密时，从未加密快照还原的卷在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的卷。下图说明了该过程。

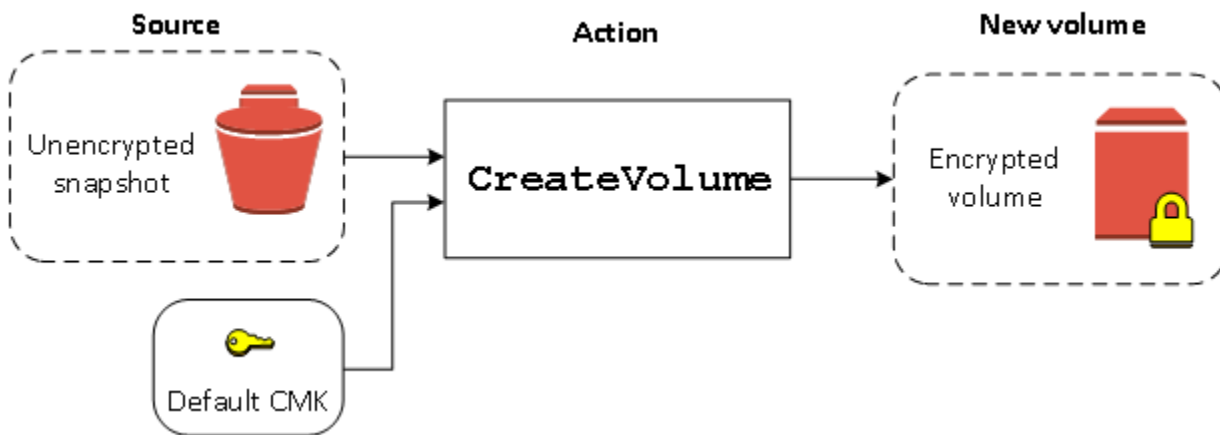


如果您省略 `KmsKeyId` 参数，则将使用您用于 EBS 加密的默认 KMS 密钥加密生成的卷。您必须指定 KMS 密钥 ID 以使用不同的 KMS 密钥加密卷。

有关更多信息，请参阅[从快照创建卷](#)。

## 还原未加密的卷 (启用了默认加密)

在您启用了默认加密时，从未加密快照还原的卷必须加密，无需使用默认 KMS 密钥的加密参数。下图说明了这种简单默认案例：

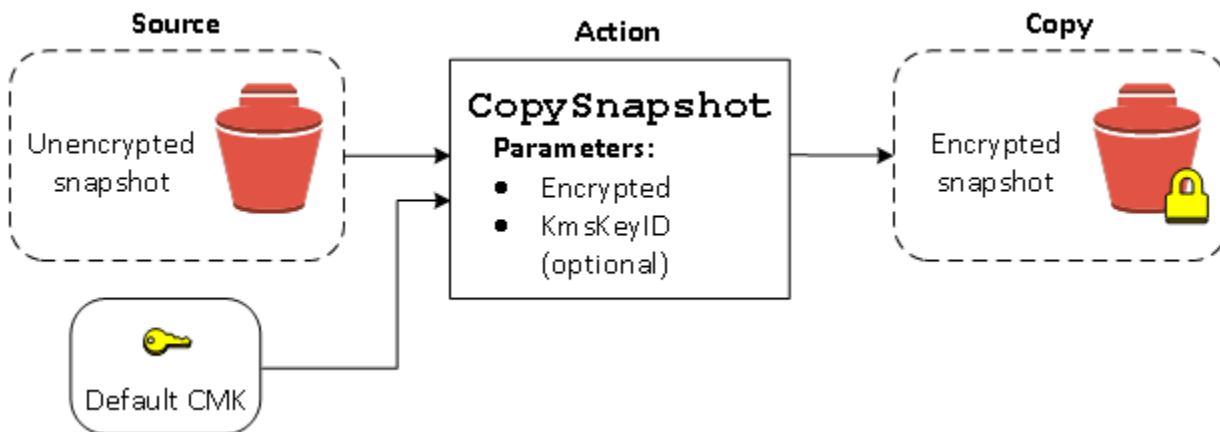


如果您要使用对称客户管理加密密钥来加密还原的卷，则必须提供 `Encrypted` 和 `KmsKeyId` 参数，如 [还原未加密的卷（未启用默认加密）](#) 中所示。

## 复制未加密的快照（未启用默认加密）

未启用默认加密时，未加密快照的副本在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的快照。如果省略 `KmsKeyId`，则使用默认 KMS 密钥加密生成的快照。您必须指定 KMS 密钥 ID 以使用不同的对称加密 KMS 密钥对卷进行加密。

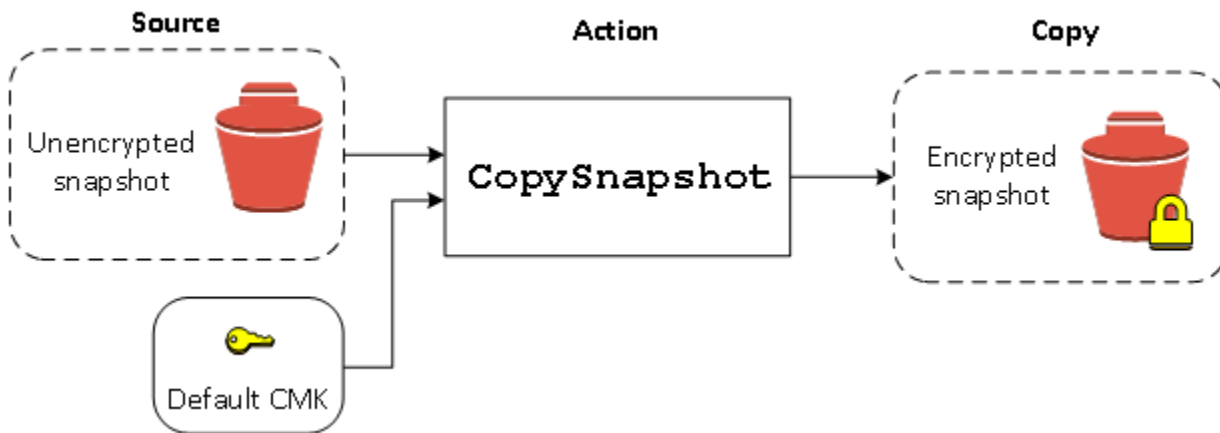
下图说明了该过程。



您可以将未加密的快照复制到加密的快照，然后从加密的快照中创建卷来加密 EBS 卷。有关更多信息，请参阅[复制 Amazon EBS 快照](#)。

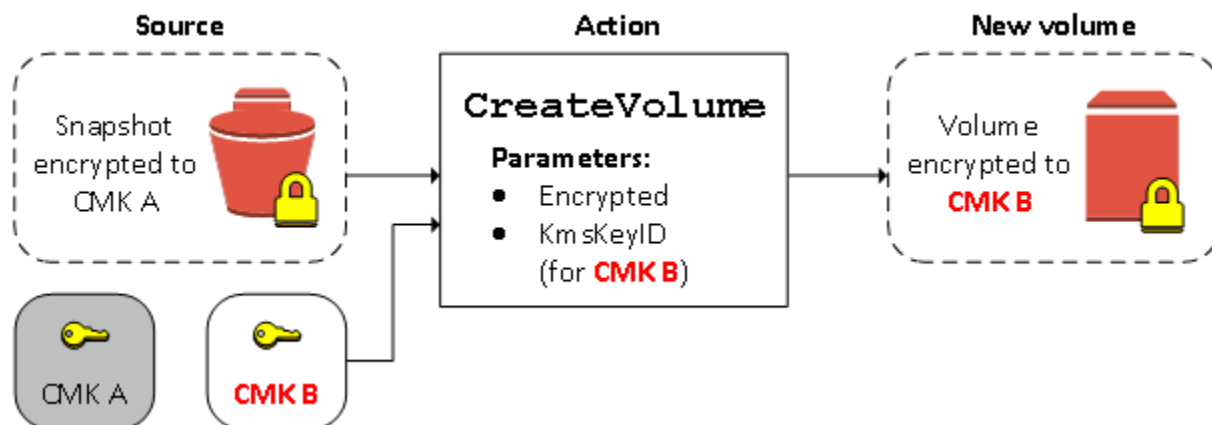
## 复制未加密的快照（启用了默认加密）

在您启用了默认加密时，未加密快照的副本必须加密，无需使用默认 KMS 密钥的加密参数。下图说明了这种默认情况：



## 重新加密已加密卷

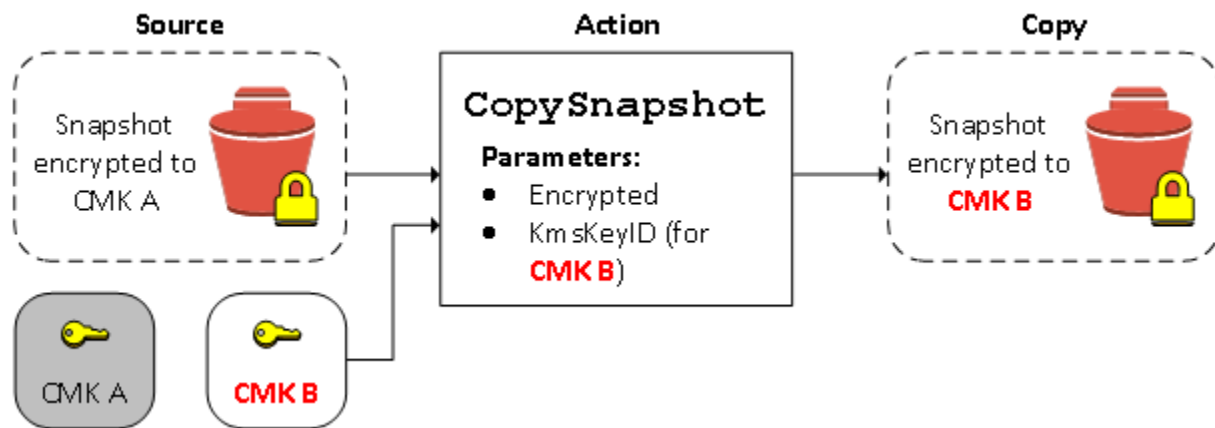
对加密快照执行 CreateVolume 操作时，您可以选择使用不同的 KMS 密钥重新加密它。下图说明了该过程。在本例中，您拥有两个 KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在卷创建期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据被自动解密，然后由 KMS 密钥 B 重新加密。



有关更多信息，请参阅[从快照创建卷](#)。

## 重新加密已加密快照

由于能够在复制过程中加密快照，您可以将新的对称加密 KMS 密钥应用于您拥有的已加密过的快照。从生成的副本还原的卷只能使用新的 KMS 密钥进行访问。下图说明了该过程。在本例中，您拥有两个 KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在复制期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据由 KMS 密钥 B 自动重新加密。



在相关的场景中，您可以选择将新加密参数应用于已与您共享的快照的副本。默认情况下，系统会使用快照拥有者共享的 KMS 密钥 对该副本进行加密。但是，我们建议您使用您控制的其他 KMS 密钥 创建共享快照的副本。这样，即使原始 KMS 密钥 遭到泄露或拥有者出于任何原因撤销了 KMS 密钥，您也不会失去对卷的访问权限。有关更多信息，请参阅[加密和快照复制](#)。

## 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。

### Linux 实例

例如，使用 `rsync` 命令复制数据。在以下命令中，源数据位于 `/mnt/source` 中，目标卷挂载在 `/mnt/destination` 中。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

### Windows 实例

例如，使用 `robocopy` 命令复制数据。在以下命令中，源数据位于 `D:\` 中，目标卷挂载在 `E:\` 中。

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

我们建议使用文件夹而不是复制整个卷，因为这可避免隐藏文件夹的潜在问题。

## 加密结果

下表描述了每种可能的设置组合的加密结果。

是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
否	否	新（空）卷	未加密	不适用
否	否	您拥有的未加密快照	未加密	
否	否	您拥有的加密快照	按相同密钥加密	
否	否	与您共享的未加密快照	未加密	
否	否	与您共享的加密快照	由默认客户托管密钥加密*	
是	否	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密**
是	否	您拥有的未加密快照	由默认客户托管密钥加密	
是	否	您拥有的加密快照	按相同密钥加密	
是	否	与您共享的未加密快照	由默认客户托管密钥加密	
是	否	与您共享的加密快照	由默认客户托管密钥加密	
否	是	新（空）卷	由默认客户托管密钥加密	不适用
否	是	您拥有的未加密快照	由默认客户托管密钥加密	
否	是	您拥有的加密快照	按相同密钥加密	
否	是	与您共享的未加密快照	由默认客户托管密钥加密	



是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
否	是	与您共享的加密快照	由默认客户托管密钥加密	
是	是	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密
是	是	您拥有的未加密快照	由默认客户托管密钥加密	
是	是	您拥有的加密快照	按相同密钥加密	
是	是	与您共享的未加密快照	由默认客户托管密钥加密	
是	是	与您共享的加密快照	由默认客户托管密钥加密	

\* 这是用于 AWS 账户和地区的 EBS 加密的默认客户托管密钥。默认情况下，这是 EBS AWS 托管式密钥的唯一密钥，或者您可以指定客户托管密钥。有关更多信息，请参阅 [选择 EBS 加密的 KMS 密钥](#)。

\*\*这是在启动时为卷指定的客户托管密钥。使用此客户托管密钥代替 AWS 账户和地区的默认客户托管密钥。

# Amazon EBS 卷性能

几个因素（包括 I/O 特性以及实例和卷的配置）会对 Amazon EBS 的性能造成影响。如您按照 Amazon EBS 和 Amazon EC2 产品详细信息页面上的指导操作，通常能获得良好的性能。但是，在某些情况下，您可能需要进行一些调整才能获得峰值性能。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。

AWS 对 EBS 卷类型性能的更新可能不会立即对现有卷生效。要查看较早卷上的全部性能，您需要先在其上执行 ModifyVolume 操作。有关更多信息，请参阅 [使用 Amazon EBS 弹性卷修改卷](#)。

## 内容

- [Amazon EBS 性能提示](#)
- [优化 Amazon EBS 性能](#)
- [Amazon EBS I/O 特性和监控](#)
- [初始化 Amazon EBS 卷](#)
- [Amazon EBS 和 RAID 配置](#)
- [对 EBS 卷进行基准测试](#)

## 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（例如 C3、R3 和 M3）会产生额外成本，另一些实例（例如 M4、C4、C5 和 D2）始终可进行 EBS 优化而不会产生额外成本。有关更多信息，请参阅 [优化 Amazon EBS 性能](#)。

### 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 [Amazon EBS I/O 特性和监控](#)。

## 了解工作负载

EBS 卷的最高性能、I/O 操作的大小和数量，以及完成每个操作所需时间之间存在着某种关系。这些因素（性能、I/O 和延迟）相互影响，不同应用程序对各个因素的敏感程度也不同。有关更多信息，请参阅[对 EBS 卷进行基准测试](#)。

### 请注意，从快照中初始化卷时，性能将会下降

当您首次访问从快照创建的新 EBS 卷上的每个数据块时，延迟会大大增加。您可以使用以下其中一个选项来避免这一性能下降：

- 在将卷部署到生产环境之前访问每个块。此过程称为初始化（以前称为预热）。有关更多信息，请参阅[初始化 Amazon EBS 卷](#)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅[Amazon EBS 快速快照还原](#)。

### 可能导致 HDD 性能下降的因素

如果创建吞吐量优化型 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，在初始化从快照创建的卷时损失性能，以及卷上的小型随机 I/O 过多。有关计算 HDD 卷吞吐量的更多信息，请参阅 [Amazon EBS 卷类型](#)。

如果您的应用程序没有发送足够多的 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 1MiB 的顺序 I/O 时，HDD 卷必须保持 4 或更大的队列长度（四舍五入为最近的整数）。有关确保稳定的卷性能的更多信息，请参阅 [Amazon EBS I/O 特性和监控](#)

### 为 `st1` 和 `sc1` 上的高吞吐量读取密集型工作负载增加预读值（仅限 Linux 实例）

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。此 per-block-device 设置应仅应用于您的 HDD 卷。

要检查您的块储存设备的当前预读数值，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

块储存设备信息采用以下格式返回：

RO	RA	SSZ	BSZ	StartSec	Size	Device
rw	256	512	4096	4096	8587820544	/dev/<device>

以上显示的设备报告预读取值为 256 ( 默认值 )。将此数字乘以扇区大小 ( 512 字节 ) 就可获得预读取缓冲区的大小，在此例中为 128 KiB。要将缓冲区值设置为 1 MiB，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

再次运行第一个命令，验证预读取设置现在显示 2048。

仅当您的工作负载包括大型顺序 I/O 时，才使用此设置。如果它主要包含的是小型随机 I/O，则此设置会降低性能。一般来说，如果工作负载主要包括小型随机 I/O，则应考虑使用通用型 SSD ( gp2 和 gp3 ) 卷，而不是 st1 或 sc1 卷。

## 使用现代 Linux 内核 ( 仅限 Linux 实例 )

借助对间接描述符的支持，使用现代 Linux 内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，以及任何当代 EC2 实例。如果您的平均 I/O 大小达到或接近 44 KiB，则说明您可能是在不支持间接描述符的情况下使用实例或内核。有关从 Amazon CloudWatch 指标得出平均 I/O 大小的信息，请参阅[Amazon EBS I/O 特性和监控](#)。

要在 st1 或 sc1 卷上实现最大吞吐量，建议您将值 256 应用于 xen\_blkfront.max 参数 ( 对于低于 4.6 的 Linux 内核版本 ) 或 xen\_blkfront.max\_indirect\_segments 参数 ( 对于 Linux 内核版本 4.6 及更高版本 )。可在操作系统 boot 命令行中设置相应的参数。

例如，在具有较早内核的 Amazon Linux AMI 中，您可以将它添加到在 /boot/grub/menu.lst 中找到的 GRUB 配置的 kernel 行末尾：

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
xen_blkfront.max=256
```

对于更高版本的内核，该命令将类似于以下内容：

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
xen_blkfront.max_indirect_segments=256
```

重启实例，让此设置生效。

有关更多信息，请参阅[为半虚拟化 AMI 配置 GRUB](#)。对于其他 Linux 发行版（尤其是不使用 GRUB 引导加载程序的版本）可能需要采用不同方法来调整内核参数。

有关 EBS I/O 特征的更多信息，请参阅本主题上的[Amazon EBS：为性能而设计](#) re:Invent 演示文稿。

## 使用 RAID 0 以最大限度利用实例资源

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[Amazon EBS 和 RAID 配置](#)。

## 使用 Amazon 追踪绩效 CloudWatch

Amazon Web Services 为 Amazon EBS 提供性能指标，您可以通过亚马逊进行分析 CloudWatch 和查看，还可以使用状态检查来监控卷的运行状况。有关更多信息，请参阅[监控 Amazon EBS 卷](#)。

## 优化 Amazon EBS 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

EBS 优化的实例将专用带宽提供给 Amazon EBS。当附加到 EBS 优化实例时，通用型 SSD（gp2 和 gp3）卷可在给定年度 99% 的时间内提供至少 90% 的预置 IOPS 性能，而预置 IOPS SSD（io1 和 io2）卷可在给定年度 99.9% 的时间内提供至少 90% 的预置 IOPS 性能。吞吐量优化型 HDD（st1）和 Cold HDD（sc1）在给定年度 99% 的时间内提供至少 90% 的预期吞吐量性能。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](#)。

有关更多信息，请参阅《Amazon EC2 用户指南》中的[Amazon EBS 优化型实例](#)。

## Amazon EBS I/O 特性和监控

在给定卷配置中，某些 I/O 特性会对 EBS 卷的性能表现造成影响。支持 SSD 的卷（即通用型 SSD（gp2 和 gp3）和预置 IOPS SSD（io1 和 io2）能够提供一致的性能，无论 I/O 操作是随机的还是顺序的。支持 HDD 的卷（即吞吐量优化型 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。

### 主题

- [IOPS](#)
- [卷队列长度和延迟](#)
- [I/O 大小和卷吞吐量限制](#)
- [使用监控 I/O 特性 CloudWatch](#)
- [相关资源](#)

## IOPS

IOPS 是表示每秒输入/输出操作数的度量单位。这些操作以 KiB 为单位，而底层驱动程序技术决定了卷类型将作为单个 I/O 计数的最大数据量。由于 SSD 卷处理小型或随机 I/O 比 HDD 卷更有效，因此 SSD 卷的 I/O 大小上限为 256 KiB，而 HDD 卷的 I/O 大小上限为 1,024 KiB。

当小型 I/O 操作在物理上连续进行时，Amazon EBS 会尝试将这些操作合并为单个 I/O 操作，直至最大 I/O 大小。同样，当 I/O 操作大于最大 I/O 大小时，Amazon EBS 会尝试将这些操作分为较小的 I/O 操作。下表显示了一些示例。

卷类型	最大 I/O 大小	来自应用程序的 I/O 操作	IOPS 数量	备注
SSD	256 KiB	1 个 1024 KiB I/O 操作	4 ( $1024 \div 256 = 4$ )	Amazon EBS 将 1,024 个 I/O 操作拆分为四个较小的 256 KiB 操作。
		8 个连续 32 KiB I/O 操作	1 ( $8 \times 32 = 256$ )	Amazon EBS 将 8 个连续 32 KiB I/O 操作合并为一个 256 KiB 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。
HDD	1,024 KiB	1 个 1024 KiB I/O 操作	1	I/O 操作已经等于最大 I/O 大小。它不会被合并或拆分。

卷类型	最大 I/O 大小	来自应用程序的 I/O 操作	IOPS 数量	备注
		8 个连续 128KiB I/O 操作	1 ( 8x128=1024 )	Amazon EBS 将 8 个连续 128 KiB I/O 操作合并为一个 1,024 KiB I/O 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。

这样，当您创建支持 3,000 IOPS ( 通过将 Provisioned IOPS SSD 卷预置为 3000 IOPS 或将 通用型 SSD 卷大小确定为 1000 GiB ) 的 SSD 卷时，您就可以将它挂载到一个 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。延迟是 I/O 操作的真实 end-to-end 客户机时间，换句话说，就是从向 EBS 发送 I/O 到收到来自 EBS 的 I/O 读取或写入已完成的确认之间经过的时间。队列长度必须进行适当调整，以便与 I/O 大小和延迟匹配，避免在访客操作系统上或在到 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 workload 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 IOPS 或吞吐量。

事务密集型应用程序对 I/O 延迟增加很敏感，很适合支持 SSD 的卷。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 支持的卷。您可以在执行大型顺序 I/O 时维持大队列长度，从而对 HDD 卷保持高吞吐量。

## I/O 大小和卷吞吐量限制

对于 SSD 卷，如果 I/O 大小非常大，由于达到卷的吞吐量限制，您的 IOPS 数可能会少于预配置数量。例如，对于具有可用突增积分的 1000GiB 以下的 gp2 卷，IOPS 限制为 3000，卷吞吐量限制为

250 MiB/s。如果您正在使用 256KiB 的 I/O 大小，则您的卷在 IOPS 为 1000 时将达到其吞吐量限制（ $1000 \times 256\text{KiB} = 250\text{MiB}$ ）。当 I/O 大小较小（如 16 KiB）时，这个卷可以支持 3000 IOPS，这是因为吞吐量远低于 250 MiB/s。（这些示例都假设卷的 I/O 不会达到实例的吞吐量限制。）有关每种 EBS 卷类型吞吐量限制的更多信息，请参阅 [Amazon EBS 卷类型](#)。

对于较小的 I/O 操作，您可能会看到从实例内部测量的 higher-than-provisioned IOPS 值。当实例操作系统在将小型 I/O 操作传递到 Amazon EBS 之前将其合并为一个较大的操作时，会发生这种情况。

如果您的工作负载在 HDD 支持的 `st1` 和 `sc1` 卷上使用顺序 I/O，则从实例内部进行度量时，您的 IOPS 值可能会高于预期数量。当实例操作系统将顺序 I/O 进行合并，并以 1024 KiB 大小为单位来对其进行计数时，会发生这种情况。如果您的工作负载使用小型随机 I/O，则吞吐量可能会低于您的预期。这是因为我们会将每个随机的非顺序 I/O 计入总的 IOPS 计数，这可能导致您比预期更快达到卷的 IOPS 限制。

无论您采用何种 EBS 卷类型，如果您的 IOPS 或吞吐量与您在配置中的预期不同，请确保 EC2 实例带宽并不是导致这种结果的限制因素。您应始终使用最新一代的 EBS 优化实例（或包含 10Gb/s 网络连接的实例）以实现最佳性能。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。

## 使用监控 I/O 特性 CloudWatch

您可以使用每个卷的 [CloudWatch 卷指标](#) 来监控这些 I/O 特征。要考虑的重要指标包括以下内容：

- VolumeStalledIOCheck
- BurstBalance
- VolumeReadBytes | VolumeWriteBytes
- VolumeReadOps | VolumeWriteOps
- VolumeQueueLength

VolumeStalledIOCheck 监控 EBS 卷的状态以确定您的卷何时受损。该指标是一个二进制值，将根据 EBS 卷能否完成 I/O 操作返回 0（通过）或 1（失败）状态。此检查可检测 Amazon EBS 基础设施存在的底层问题，如下所示：

- EBS 卷底层的存储子系统的硬件或软件问题
- 物理主机上的硬件问题，该问题会影响来自 EC2 实例的 EBS 卷的可访问性
- 实例和 EBS 卷之间的连接问题



如果该VolumeStalledIOCheck指标失败，您可以等待 AWS 问题得到解决，也可以采取措施，例如更换受影响的卷或停止并重新启动该卷所连接的实例。在大多数情况下，当该指标失败时，EBS 将在几分钟内自动诊断并恢复您的卷。您可以使用中的 [Pause I/O](#) 操作 AWS Fault Injection Service 来运行受控实验，以测试您的架构并基于此指标进行监控，从而提高存储故障恢复能力。

您可以使用 VolumeReadOps、VolumeWriteOps、VolumeTotalReadTime 和 VolumeTotalWriteTime 来测量 Amazon EBS 存储 I/O 延迟。您可以使用以下公式来监控卷的平均 I/O 延迟：

$$\text{Average I/O latency in ms/op} = (\text{VolumeTotalReadTime} + \text{VolumeTotalWriteTime}) / (\text{VolumeReadOps} + \text{VolumeWriteOps})$$

如果您的 I/O 延迟高于您的所需，请检查驱动 IOPS，以确保应用程序不会尝试驱动超过您已预置的 IOPS。您可以使用以下公式来监控卷上的平均驱动 IOPS：

$$\text{Estimated average IOPS in ops/s} = (\text{Sum}(\text{VolumeReadOps}) + \text{Sum}(\text{VolumeWriteOps})) / (\text{Period} - \text{Sum}(\text{VolumeIdleTime}))$$

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，则应考虑使用以下选项之一：

- gp3、io2 或 io1 卷，预置了足够 IOPS 以实现所需延迟
- 更大的 gp2 卷，提供足够的基准 IOPS 性能

HDD 支持的 st1 和 sc1 卷经过特别设计，旨在对使用 1024 KiB 最大 I/O 大小的工作负载提供最佳性能。要确定卷的平均 I/O 大小，请将 VolumeWriteBytes 除以 VolumeWriteOps。同样的计算也适用于读取操作。如果平均 I/O 大小低于 64 KiB，则提高发送到 st1 或 sc1 卷的 I/O 操作的大小应该能够提高性能。

#### Note

如果平均 I/O 大小达到或接近 44 KiB，说明您可能是在不支持间接描述符的情况下使用实例或内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，任何当代实例也具有此支持。

BurstBalance 以剩余余额百分比的形式显示 gp2、st1 和 sc1 卷的突增存储桶余额。当您的突增存储桶耗尽时，卷 I/O（对于 gp2 卷）或卷吞吐量（对于 st1 和 sc1 卷）会限定在基准水平。检查 BurstBalance 值以确定卷是否因为此原因而受限制。有关可用 Amazon EBS 指标的完整列表，请参阅 [亚马逊 EBS 的亚马逊 CloudWatch 指标](#) 和 [基于 Nitro 的实例的 Amazon EBS 指标](#)。

## 相关资源

有关 Amazon EBS I/O 特征的更多信息，请参阅以下 re:Invent 演示文稿：[Amazon EBS：为性能而设计](#)。

## 初始化 Amazon EBS 卷

空的 EBS 卷一经创建便能实现其最高性能，而不需要初始化（以前称为预热）。

对于任何卷类型的卷，必须先从 Amazon S3 下载存储块并将其写入到卷中，然后才能访问这些块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。

### Important

在初始化已从快照创建的 Provisioned IOPS SSD 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 性能状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 Provisioned IOPS SSD 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅[EBS 卷状态检查](#)。

对于大部分应用程序，可将此初始化成本分摊到卷的整个使用期限。为了避免最初在生产环境中出现这种性能下降，您可以使用以下其中一种方案：

- 强制立即初始化整个卷。有关更多信息，请参阅 [Linux 实例](#)（Linux 实例）或 [Windows 实例](#)（Windows 实例）。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅 [Amazon EBS 快速快照还原](#)。

## Linux 实例

在 Linux 上初始化从快照创建的卷

1. 将新还原的卷附加到您的 Linux 实例。
2. 使用 `lsblk` 命令列出实例上的块储存设备。

```
[ec2-user ~]$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
```

```
xvdf 202:80 0 30G 0 disk
xvda1 202:1 0 8G 0 disk /
```

在此处可以看到新卷 `/dev/xvdf` 已附加，但是未挂载（因为 MOUNTPOINT 列下没有列出任何路径）。

3. 使用 `dd` 或 `fio` 实用程序对设备上的所有数据块进行读取。默认情况下，`dd` 命令将安装在 Linux 系统上，但 `fio` 要快得多，因为它允许多线程读取。

#### Note

此步骤可能需要几分钟到几个小时，具体取决于 EC2 实例带宽、为卷配置的 IOPS 和卷的大小。

[`dd`] 应将 `if`（输入文件）参数设置为要初始化的驱动器。应将 `of`（输出文件）参数设置为 Linux 空虚拟设备 `/dev/null`。`bs` 参数设置读取操作的数据块大小；要获得最佳性能，这应设置为 1 MB。

#### Important

不当使用 `dd` 可能容易损坏卷的数据。请务必严格遵循下面的示例命令。只有 `if=/dev/xvdf` 参数将因您要读取的设备的名称而异。

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[`fio`] 如果您在系统上安装了 `fio`，请使用以下命令初始化您的卷。应将 `--filename`（输入文件）参数设置为要初始化的驱动器。

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

要在 Amazon Linux 上安装 `fio`，请使用以下命令：

```
sudo yum install -y fio
```

要在 Ubuntu 上安装 `fio`，请使用以下命令：

```
sudo apt-get install -y fio
```

操作完成时，您会看到读取操作的报告。卷现在已准备就绪，可供使用。有关更多信息，请参阅[使 Amazon EBS 卷可供使用](#)。

## Windows 实例

在使用上述任何一种工具前，请在您的系统上收集有关磁盘的信息，如下所述：

收集有关系统磁盘的信息

1. 使用 wmic 命令列出系统上的可用磁盘：

```
wmic diskdrive get size,deviceid
```

下面是示例输出：

```
DeviceID          Size
\\.\PHYSICALDRIVE2 80517265920
\\.\PHYSICALDRIVE1 80517265920
\\.\PHYSICALDRIVE0 128849011200
\\.\PHYSICALDRIVE3 107372805120
```

2. 使用 dd 或 fio 识别要初始化的磁盘。C: 驱动器位于 \\.\PHYSICALDRIVE0。如果您不确定要使用的盘符，则可以使用 diskmgmt.msc 实用工具将驱动器盘符与磁盘盘符进行比较。

### Use the dd utility

完成以下过程，以安装并使用 dd 来初始化卷。

#### 重要注意事项

- 初始化卷可能需要几分钟到几个小时，取决于 EC2 实例带宽、为卷预置的 IOPS 和卷的大小。
- 不当使用 dd 可能容易损坏卷的数据。一定要准确地遵循此程序。

## 安装适用于 Windows 的 dd

适用于 Windows 程序的 dd 的使用体验类似于 Linux 和 Unix 系统中常用的 dd 程序，通过它您可以初始化已从快照创建的 Amazon EBS 卷。最新的测试版支持 /dev/null 虚拟设备。如果安装早期版本，则可以使用 nul 虚拟设备。完整的文档可在 <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。
2. ( 可选 ) 为命令行实用工具创建易于查找和记住的文件夹，例如 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 ( 例如 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运行该文件夹中的程序。
  - 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。
5. 打开新的命令提示符窗口。上一步不会在您当前的“命令提示符”窗口中更新环境变量。完成上一步后打开的命令提示符窗口将更新。

## 使用适用于 Windows 的 dd 来初始化卷

运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 )。该命令可安全初始化现有数据。

```
dd if=\\.\PHYSICALDRIVE $n$  of=/dev/null bs=1M --progress --size
```

如果 dd 尝试读取卷末尾以外的空间，您可能会收到一个错误。您可以放心地忽略此错误。

如果您使用的是早期版本的 dd 命令，则不支持 /dev/null 设备。相反，您可以按如下方式使用 nul 设备。

```
dd if=\\.\PHYSICALDRIVE $n$  of=nul bs=1M --progress --size
```

## Use the fio utility

完成以下过程，以安装并使用 fio 来初始化卷。

### 安装适用于 Windows 的 fio

适用于 Windows 的 fio 程序的使用体验类似于 Linux 和 Unix 系统中常用的 fio 程序，允许您初始化已从快照创建的 Amazon EBS 卷。有关更多信息，请参阅 <https://github.com/axboe/fio>。

1. 可通过展开最新版本的资产并选择 MSI 安装程序来下载 [fio MSI](#) 安装程序。
2. 安装 fio。

### 使用适用于 Windows 的 fio 初始化卷

1. 运行类似如下的命令来初始化卷：

```
fio --filename=\\.\PHYSICALDRIVE $n$  --rw=read --bs=128k --iodepth=32 --direct=1  
--name=volume-initialize
```

2. 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 卷可供使用](#)。

## Amazon EBS 和 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。

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](#)。

### 内容

- [RAID 配置选项](#)
- [创建 RAID 0 阵列](#)
- [创建 RAID 阵列中卷的快照](#)

## RAID 配置选项

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。如果 I/O 性能至关重要，请使用 RAID 0。I/O 通过 RAID 0 在卷内以条带状分布。如果您添加卷，则会直接增加吞吐量和 IOPS。但是，请记住，条带的性能仅限于集中性能最差的卷，并且集中的单个卷丢失会导致阵列数据完全丢失。

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。例如，预置 IOPS 为 4000 的两个 500 GiB io1 卷将创建可用带宽为 8000 IOPS、吞吐量为 1000 MiB/s 的 1000 GiB RAID 0 阵列。

### 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。

RAID 1 也不建议用于 Amazon EBS。RAID 1 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。此外，RAID 1 不提供任何写入性能改进。

## 创建 RAID 0 阵列

使用以下过程创建 RAID 0 阵列。

### 注意事项

- 在执行此过程之前，您必须确定 RAID 0 阵列的大小以及预调配多少 IOPS。
- 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。
- 您应避免从 RAID 卷启动。如果有一台设备出现故障，您可能无法启动操作系统。

### Linux 实例

在 Linux 上创建 RAID 0 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](#)。
2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅 [将 Amazon EBS 卷挂载到实例](#)。

- 使用 `mdadm` 命令从新附加的 Amazon EBS 卷创建逻辑 RAID 设备。用阵列中的卷数替换 `number_of_volumes`，用阵列中每个卷的设备名称（例如 `/dev/xvdf`）替换 `device_name`。您还可以将 `MY_RAID` 替代为阵列的唯一名称。

**Note**

您可以使用 `lsblk` 命令列出实例上的设备以找到设备名称。

要创建 RAID 0 阵列，请运行以下命令（注意，`--level=0` 选项用于将阵列条带化）：

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

**Tip**

如您遇到 `mdadm: command not found` 错误，请使用以下命令安装 `mdadm`：`sudo yum install mdadm`。

- 给 RAID 阵列一些时间进行初始化和同步。您可以借助下面的命令跟踪这些操作的进度：

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

下面是示例输出：

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

通常，您可以通过下面的命令显示有关 RAID 阵列的详细信息：

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

下面是示例输出：

```
/dev/md0:
```



```

Version : 1.2
Creation Time : Wed May 19 11:12:56 2021
  Raid Level : raid0
  Array Size : 41910272 (39.97 GiB 42.92 GB)
  Raid Devices : 2
  Total Devices : 2
  Persistence : Superblock is persistent

Update Time : Wed May 19 11:12:56 2021
  State : clean
Active Devices : 2
Working Devices : 2
Failed Devices : 0
Spare Devices : 0

Chunk Size : 512K

Consistency Policy : none

Name : MY_RAID
  UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
  Events : 0

Number   Major   Minor   RaidDevice State
  0       202     16       0      active sync  /dev/sdb
  1       202     32       1      active sync  /dev/sdc

```

5. 在您的 RAID 阵列上创建一个文件系统，并为该文件系统分配一个稍后在装载该文件系统时使用的标签。例如，要使用标签 **MY\_RAID** 创建 ext4 文件系统，请运行以下命令：

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

根据应用程序的要求或操作系统的限制，您可以使用其他文件系统类型，如 ext3 或 XFS（请参阅您的文件系统文档以了解相应的文件系统创建命令）。

6. 要确保 RAID 阵列在启动时自动重组，请创建一个包含 RAID 信息的配置文件：

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

**Note**

如果您使用的是 Linux 发行版而非 Amazon Linux，您可能需要修改此命令。例如，您可能需要将文件放在不同的位置，或者添加 `--examine` 参数。有关更多信息，请在 Linux 实例上运行 `man mdadm.conf`。

7. 创建新的 Ramdisk Image 以为新的 RAID 配置正确地预加载块储存设备模块：

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. 为 RAID 阵列创建装载点。

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. 最后，在已创建的装载点上安装 RAID 设备：

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

RAID 设备现已准备就绪，可供使用。

10. (可选) 要在每次系统重启时装载此 Amazon EBS 卷，可在 `/etc/fstab` 文件中为该设备添加一个条目。
  - a. 创建 `/etc/fstab` 文件的备份，当您进行编辑时意外损坏或删除了此文件的情况下，可以使用该备份。


```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

- b. 使用您常用的文本编辑器 (如 `/etc/fstab` 或 `nano`) 打开 `vim` 文件。
- c. 注释掉任何以“`UUID=`”开头的行，然后，在文件末尾，使用以下格式为您的 RAID 卷添加新行：

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

此行的最后三个字段分别是文件系统装载选项、文件系统转储频率和启动时的文件系统检查顺序。如果您不知道这些值应该是什么，请使用以下示例中的值 (`defaults,nofail 0 2`)。有关 `/etc/fstab` 条目的更多信息，请参阅 `fstab` 手册页面 (方法：在命令行输入

man fstab )。例如，要在设备上的装载点 `/mnt/raid` 装载带 `MY_RAID` 标签的 `ext4` 文件系统，请将以下条目添加到 `/etc/fstab`。

 Note


如果您要在未附加该卷的情况下启动实例（例如，以便该卷可以在不同实例之间向后和向前移动），则应添加 `nofail` 装载选项，该选项允许实例即使在卷安装过程中出现错误时也可启动。Debian 衍生物（例如 Ubuntu）还必须添加 `nobootwait` 装载选项。

```
LABEL=MY_RAID    /mnt/raid    ext4    defaults,nofail    0    2
```

- d. 在您将新条目添加到 `/etc/fstab` 后，需要检查您的条目是否有效。运行 `sudo mount -a` 命令以在 `/etc/fstab` 中装载所有文件系统。

```
[ec2-user ~]$ sudo mount -a
```

如果上述命令未产生错误，说明您的 `/etc/fstab` 文件正常，您的文件系统会在下次启动时自动装载。如果该命令产生了任何错误，请检查这些错误并尝试更正 `/etc/fstab`。

 Warning

`/etc/fstab` 文件中的错误可能显示系统无法启动。请勿关闭 `/etc/fstab` 文件中有错误的系统。

- e. （可选）如果您无法确定如何更正 `/etc/fstab` 错误，则始终可以使用以下命令还原您的备份 `/etc/fstab` 文件。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

## Windows 实例

### 在 Windows 上创建 RAID 0 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](#)。

2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅[将 Amazon EBS 卷挂载到实例](#)。
3. 连接到您的 Windows 实例。有关更多信息，请参阅[连接到 Windows 实例](#)。
4. 打开命令提示符并键入 diskpart 命令。

**diskpart**

```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51C0
```

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		

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 命令使它联机。
- c. 如果所选磁盘在前面的 Dyn 命令输出的 list disk 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
```

```
XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type    : SCSI
Status  : Online
Path    : 0
Target  : 1
LUN ID  : 0
Location Path : PCIR00T(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。在该示例中，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](#)。

7. 验证您要使用的磁盘现在是否为动态。在这种情况下，我们将磁盘 1 和磁盘 2 用于 RAID 卷。

```
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	*	

8. 创建 RAID 阵列。在 Windows 上，RAID 0 卷指条带卷。

要在磁盘 1 和 2 上创建条带卷阵列，请使用以下命令（注意，stripe 选项用于将阵列条带化）：

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

9. 验证您的新卷。

```
DISKPART> list volume
```

```
DISKPART> list volume
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 0	C		NTFS	Partition	29 GB	Healthy	System
Volume 1			RAW	Stripe	15 GB	Healthy	

请注意，Type 列现在表示卷 1 是 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。

## 创建 RAID 阵列中卷的快照

如果要使用快照备份 RAID 阵列中 EBS 卷上的数据，则必须确保快照的一致性。原因在于这些卷的快照是独立创建的。从不同步的快照恢复 RAID 阵列中的 EBS 卷会降低阵列的完整性。

要为 RAID 阵列创建一组一致的快照，请使用 [EBS 多卷快照](#)。多卷快照允许您跨连接到 point-in-time EC2 实例的多个 EBS 卷进行数据协调和崩溃一致的快照。您不需要停止实例以在多个卷之间协调来确保一致性，因为快照将跨多个 EBS 卷自动拍摄。有关更多信息，请参阅 [创建 Amazon EBS 快照](#) 下的有关创建多卷快照的步骤。

## 对 EBS 卷进行基准测试

您可以通过模拟 I/O 工作负载来测试 Amazon EBS 卷的性能。过程如下所述：

1. 启动 EBS 优化实例。
2. 创建新的 EBS 卷。
3. 将这些卷附加到您的 EBS 优化实例。
4. 配置并挂载块储存设备。
5. 安装工具以便测试 I/O 性能。
6. 测试卷的 I/O 性能。
7. 删除卷并终止实例，确保不会继续引发更改。

### Important

某些过程可能会对您进行基准测试的 EBS 卷上的现有数据造成破坏。基准测试程序适用于出于测试目的而特别创建的卷，并不适用于生产卷。

## 设置实例

为了获得最佳的 EBS 卷性能，我们建议您使用 EBS 优化实例。EBS 优化实例可在 Amazon EC2 和 Amazon EBS 之间提供实例专用吞吐量。EBS 优化的实例在 Amazon EC2 与 Amazon EBS 之间提供了专用带宽，其规格取决于实例类型。

要创建 EBS 优化实例，可在使用 Amazon EC2 控制台启动实例时选择作为 EBS 优化实例启动，或在使用命令行时指定 `--ebs-optimized`。请确保选择的实例类型支持该选项。

## 设置 Provisioned IOPS SSD 或 通用型 SSD 卷

要使用 Amazon EC2 控制台创建预调配 IOPS SSD ( `io1` 和 `io2` ) 或通用型 SSD ( `gp2` 和 `gp3` ) 卷，对于卷类型，选择预调配 IOPS SSD ( `io1` )、预调配 IOPS SSD ( `io2` )、通用型 SSD ( `gp2` ) 或通用型 SSD ( `gp3` )。在命令行中，为 `io1` 参数指定 `io2`、`gp2`、`gp3` 或 `--volume-type`。对于 `io1`、`io2` 和 `gp3` 卷，请指定 `--iops` 参数的每秒 I/O 操作数 ( IOPS )。有关更多信息，请参阅[Amazon EBS 卷类型](#)和[创建 Amazon EBS 卷](#)。

( 仅限 Linux 实例 ) 要了解这些示例测试，我们建议您创建一个包含 6 个卷的高性能 RAID 0 阵列。因为您是按照预配置的 GB 数量 ( 以及为 `io1`、`io2` 和 `gp3` 卷预配置的 IOPS 数量，而不是卷的数量 ) 付



费，因此创建多个较小卷并使用它们来创建条带集不会产生额外费用。如果您是使用 Oracle Orion 来测试卷的性能，则它可以模拟 Oracle ASM 的条带化操作，因此我们建议您让 Orion 执行条带化分区。如果您使用的是其他基准测试工具，则需要自己对卷执行条带化分区。

有关如何创建 RAID 0 阵列的更多信息，请参阅[创建 RAID 0 阵列](#)。

## 设置吞吐量优化型 HDD ( **st1** ) 卷或 Cold HDD ( **sc1** ) 卷

要创建 **st1** 卷，可在使用 Amazon EC2 控制台创建卷时选择吞吐量优化型 HDD，或在使用命令行时指定 `--type st1`。要创建 **sc1** 卷，可在使用 Amazon EC2 控制台创建卷时选择 Cold HDD，或在使用命令行时指定 `--type sc1`。有关创建 EBS 卷的信息，请参阅[创建 Amazon EBS 卷](#)。有关将这些卷附加到您的实例的信息，请参阅[将 Amazon EBS 卷挂载到实例](#)。

( 仅限 Linux 实例 ) AWS 提供了一个用于的 JSON 模板 AWS CloudFormation ，可简化此设置过程。访问[模板](#)并将其另存为 JSON 文件。AWS CloudFormation 允许您配置自己的 SSH 密钥，并提供了一种更简单的方法来设置性能测试环境来评估容 **st1** 量。此模板会创建一个最新一代的实例以及一个 2 TiB 的 **st1** 卷，然后将该卷附加到 `/dev/xvdf` 处的实例。

( 仅限 Linux 实例 ) 使用模板创建 HDD 卷

1. 打开 AWS CloudFormation 控制台，[网址为 https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation)。
2. 选择 Create Stack。
3. 选择 Upload a Template to Amazon S3，然后选择之前获得的 JSON 模板。
4. 为您的堆栈提供名称（例如“ebs-perf-testing”），然后选择实例类型（默认为 `r3.8xlarge`）和 SSH 密钥。
5. 选择 Next 两次，然后选择 Create Stack。
6. 新堆栈的状态从 `CREATE_IN_PROGRESS` 变为 `COMPLETE` 后，选择 Outputs（输出）以获取新实例的公有 DNS 条目，新实例将附加一个 2TiB 的 **st1** 卷。
7. 以用户 `ec2-user` 的身份使用 SSH 连接到您的新堆栈（使用从上一步的 DNS 条目中获得的主机名）。
8. 继续执行[安装基准测试工具](#)。

## 安装基准测试工具

下表列出了您可用于对 EBS 卷的性能进行基准测试的部分可用工具。

## Linux 实例

工具	描述
fio	<p>用于测试 I/O 性能。( 请注意, fio 依赖于 libaio-devel 。 )</p> <p>要在 Amazon Linux 上安装 fio, 请运行以下命令 :</p> <pre>[ec2-user ~]\$ sudo yum install -y fio</pre> <p>要在 Ubuntu 上安装 fio, 请执行以下命令 :</p> <pre>sudo apt-get install -y fio</pre>
<a href="#">Oracle Orion 校准工具</a>	用于校准要与 Oracle 数据库搭配使用的存储系统的 I/O 性能。

## Windows 实例

工具	描述
<a href="#">DiskSpd</a>	<p>DiskSpd 是微软 Windows、Windows Server 和云服务器基础架构工程团队推出的存储性能工具。可以在 <a href="https://github.com/Microsoft/diskspd/releases">https://github.com/Microsoft/diskspd/releases</a> 下载它。</p> <p>下载 diskspd.exe 可执行文件后, 以管理权限打开命令提示符 ( 通过选择“以管理员身份运行” ), 然后导航到复制 diskspd.exe 文件的目录。</p> <p>将所需的 diskspd.exe 可执行文件从相应的可执行文件的文件夹 ( amd64fre、armfre 或 x86fre ) 复制到简短的路径, 如 C:\DiskSpd。在大多数情况下, 您需要 DiskSpd 从该amd64fre文件夹中获得 64 位版本的。</p> <p>的源代码托管 DiskSpd GitHub 在 : <a href="https://github.com/Microsoft/diskspd">https://github.com/Microsoft/diskspd</a>。</p>
CrystalDiskMark	CrystalDiskMark 是一款简单的磁盘基准测试软件。可以在 <a href="https://crystalmark.info/en/software/crystaldiskmark/">https://crystalmark.info/en/software/crystaldiskmark/</a> 下载它。

这些基准测试工具可支持各种测试参数。您应该使用命令来测试您的卷支持的工作负载。下面提供的命令示例可帮助您入门。

## 选择卷队列长度

基于工作负载和卷类型选择最佳卷队列长度。

### SSD 支持的卷的队列长度

要确定支持 SSD 的卷上工作负载的最佳队列长度，建议您将每 1000 IOPS (通用型 SSD 卷的基准量，Provisioned IOPS SSD 卷的预置量) 对应 1 个队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。

在达到预配置 IOPS、吞吐量或最佳系统队列长度值之前，增加队列长度有好处，当前队列长度设置为 32。举例来说，预配置 3,000 IOPS 的卷应该将队列长度设置为 3。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

### HDD 支持的卷的队列长度

要确定 HDD 卷上工作负载的最佳队列长度，建议您在执行 1MiB 顺序 I/O 时以至少为 4 的队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。例如，突发吞吐量为 500 MiB/s、IOPS 为 500 的 2 TiB st1 卷在执行 1024 KiB、512 KiB 或 256 KiB 的顺序 I/O 时，分别应该将队列长度 4、8 或 16 作为目标。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

## 禁用 C 状态

在运行基准测试之前，您应禁用处理器 C 状态。支持此功能的 CPU 中的核心在暂时空闲时，会进入 C 状态以节省功耗。在调用核心以恢复处理时，将经过一段特定的时间，核心才能再次全速运行。此延迟可能会干扰处理器基准测试例程。有关 C 状态以及哪些 EC2 实例类型支持此状态的更多信息，请参阅 [EC2 实例的处理器状态控制](#)。

### Linux 实例

您可在 Amazon Linux、RHEL 和 CentOS 上按以下所示禁用 C 状态：

1. 获取 C 状态数。

```
$ C:\> cpubower idle-info | grep "Number of idle states:"
```

2. 从 c1 到 cN 禁用 C 状态。理想情况下，核心应处于状态 c0。

```
$ C:\> for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

## Windows 实例

在 Windows 上，您可以按以下所示禁用 C 状态：

1. 在 PowerShell，获取当前的有功功率方案。

```
$current_scheme = powercfg /getactivescheme
```

2. 获取电源方案 GUID。

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter "ElementName='High performance']").InstanceID
```

3. 获取电源设置 GUID。

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter "ElementName='Processor idle disable']").InstanceID
```

4. 获取电源设置子组 GUID。

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -Filter "ElementName='Processor power management']").InstanceID
```

5. 通过将索引的值设置为 1 来禁用 C 状态。值为 0 表示已禁用 C 状态。

```
powercfg /  
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>  
1
```

6. 设置活动方案以确保设置已保存。

```
powercfg /setactive <power_scheme_guid>
```

## 执行基准测试

以下步骤介绍各种 EBS 卷类型的基准测试命令。

对附加了 EBS 卷的 EBS 优化实例运行以下命令。如果已从快照创建 EBS 卷，在执行基准测试之前，请确保初始化这些卷。有关更多信息，请参阅 [初始化 Amazon EBS 卷](#)。

完成对卷的测试后，可参阅以下主题来帮助清除卷：[删除 Amazon EBS 卷](#)和[终止实例](#)。

## 基准 Provisioned IOPS SSD 和 通用型 SSD 卷

### Linux 实例

在您创建的 RAID 0 阵列上运行 fio。

以下命令可执行 16 KB 随机写入操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --  
name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --  
time_based --runtime=180 --group_reporting --norandommap
```

以下命令可执行 16 KB 随机读取操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1  
--rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --  
group_reporting --norandommap
```

有关解析结果的更多信息，请参阅以下教程：[使用 fio 检查磁盘 IO 性能](#)。

### Windows 实例

在您创建的卷上运行 DiskSpd。

以下命令将使用位于 C: 驱动器上的 20GB 测试文件运行 30 秒随机 I/O 测试（25% 的写入比率和 75% 的读取比率以及 8K 块大小）。它将使用八个工作线程，每个线程具有四个未完成的 I/O 和一个 1GB 的写入熵值种子。测试结果将保存到名为 DiskSpeedResults.txt 的文本文件中。这些参数模拟 SQL Server OLTP 工作负载。

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

有关解析结果的更多信息，请参阅以下教程：[使用 DiskSPd 检查磁盘 IO 性能](#)。

## st1 和 sc1 卷 ( Linux 实例 ) 基准测试

在 fio 或 st1 卷上运行 sc1。

**Note**

在执行这些测试之前，请按为 [st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值 \(仅限 Linux 实例\)](#) 所述在实例上设置缓冲 I/O。

以下命令针对附加的 st1 块设备 (例如 /dev/xvdf) 执行 1MiB 的顺序读取操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

以下命令针对附加的 st1 块储存设备执行 1 MiB 的顺序写入操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

有些工作负载可对块储存设备的不同部分混合执行顺序读取和顺序写入操作。要对此类工作负载进行基准测试，我们建议您为读取和写入操作单独、同时使用 fio 作业，并为每个作业使用 fio `offset_increment` 选项将块储存设备的不同位置作为目标。

运行此类工作负载比顺序写入或顺序读取工作负载要复杂一些。使用文本编辑器创建一个 fio 作业文件，在此示例中名为 `fio_rw_mix.cfg`，包含以下内容：

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100
```

```
[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

然后运行以下命令：

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

有关解析结果的更多信息，请参阅以下教程：[使用 fio 检查磁盘 IO 性能](#)。

对于 fio 和 st1 卷而言，通过多个 sc1 作业来执行直接 I/O（即使使用顺序读入或写入操作）可能会导致吞吐量小于预期数值。建议您使用一个直接 I/O 作业并使用 iodepth 参数来控制并发 I/O 操作的数量。

# Amazon Data Lifecycle Manager

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除 EBS 快照和 EBS 支持的 AMI。当您执行自动快照和 AMI 管理时，它可以帮助您：

- 通过实施定期备份计划来保护重要数据。
- 创建可定期刷新的标准化 AMI。
- 按照审核员的要求或内部合规性保留备份。
- 通过删除过时的备份来降低存储成本。
- 创建将数据备份到隔离区域或账户的灾难恢复备份策略。

与 Amazon EventBridge 和的监控功能相结合 AWS CloudTrail，Amazon Data Lifecycle Manager 可为亚马逊 EC2 实例和单个 EBS 卷提供完整的备份解决方案，无需支付额外费用。

## Important

- Amazon Data Lifecycle Manager 不能管理由任何其他方式创建的快照或 AMI。
- Amazon Data Lifecycle Manager 不能自动创建、保留和删除实例存储支持的 AMI。

## 内容

- [配额](#)
- [Amazon Data Lifecycle Manager 的工作原理](#)
- [默认策略与自定义策略](#)
- [默认策略](#)
- [自定义策略](#)
- [查看、修改和删除生命周期策略](#)
- [AWS Identity and Access Management](#)
- [监控快照和 AMI 的生命周期](#)
- [故障排除](#)



## 配额

您的 AWS 账户具有以下与 Amazon Data Lifecycle Manager 相关的配额：

描述	限额
每个区域的自定义生命周期策略	100
每个区域的 EBS 快照的默认策略	1
每个区域的启用 EBS 的 AMI 的默认策略	1
每个资源的标签	45

## Amazon Data Lifecycle Manager 的工作原理

以下是 Amazon Data Lifecycle Manager 的关键要素。

### 元素

- [策略](#)
- [策略计划 \( 仅限自定义策略 \)](#)
- [目标资源标签 \( 仅限自定义策略 \)](#)
- [快照](#)
- [EBS 支持的 AMI](#)
- [Amazon Data Lifecycle Manager 标签](#)

## 策略

借助 Amazon Data Lifecycle Manager，您可以创建策略来定义备份创建和保留要求。这些策略通常会指定以下内容：

- 策略类型 – 定义策略管理的备份资源类型 ( 快照或 EBS 支持的 AMI )。
- 目标资源 – 定义策略的目标资源类型 ( 实例或 EBS 卷 )。

- 创建频率 – 定义策略运行和创建快照或 AMI 的频率。
- 保留阈值 – 定义策略在创建快照或 AMI 后保留的时长。
- 其他操作 – 定义策略应执行的其他操作，例如跨区域复制、存档或资源标记。

Amazon Data Lifecycle Manager 提供默认策略和自定义策略。

### 默认策略

默认策略会备份某个区域中最近没有备份的所有卷和实例。您可以选择通过指定排除参数来排除卷和实例。

Amazon Data Lifecycle Manager 支持以下默认策略：

- EBS 快照的默认策略 – 以卷为目标，自动创建、保留和删除快照。
- EBS 支持的 AMI 的默认策略 – 以实例为目标，自动创建、保留和取消注册 EBS 支持的 AMI。

每个账户和 AWS 区域中的每个资源类型只能有一个默认策略。

### 自定义策略

自定义策略根据分配的标签将特定资源作为目标，并支持高级功能，例如快速快照还原、快照存档、跨账户复制以及前置和后置脚本。自定义策略最多可以包含 4 个计划，其中每个计划可以有自己的创建频率、保留阈值和高级功能配置。

Amazon Data Lifecycle Manager 支持以下自定义策略：

- EBS 快照策略 – 以卷或实例为目标，自动创建、保留和删除 EBS 快照。
- EBS 支持的 AMI 策略 – 以实例为目标，自动创建、保留和取消注册 EBS 支持的 AMI。
- 跨账户复制事件策略 – 为与您共享的快照自动执行跨区域复制操作。

有关更多信息，请参阅 [默认策略与自定义策略](#)。

## 策略计划 ( 仅限自定义策略 )

策略计划定义策略创建快照或 AMI 的时间。策略最多可以有四个计划 – 一个强制要求的计划和最多三个可选计划。

在单个策略中添加多个计划，可让您使用同一策略按不同频率创建快照或 AMI。例如，您可以创建一个策略来按每日、每周、每月和每年的频率创建快照。这样就无需管理多个策略。

对于每个计划，您可以定义频率、快速快照还原设置（仅限快照生命周期策略）、跨区域复制规则和标签。分配给计划的标签将自动分配给启动计划时创建的快照或 AMI。此外，Amazon Data Lifecycle Manager 还会根据计划的频率自动为每个快照或 AMI 分配系统生成的标签。

每个计划都会根据其频率单独启动。如果同时启动多个计划，Amazon Data Lifecycle Manager 只会创建一个快照或 AMI，并采用保留期限最长的计划保留设置。启动的所有计划的标签都会应用于该快照或 AMI。

- （仅限快照生命周期策略）如果为启动的多个计划启用了快速快照还原，则会在所有启动的计划中指定的所有可用区内为该快照启用快速快照还原。为每个可用区使用所启动计划的最长保留期限设置。
- 如果为启动的多个计划启用了跨区域复制，则该快照或 AMI 会被复制到启动的所有计划中指定的所有区域。应用所启动计划的最长保留期限。

## 目标资源标签（仅限自定义策略）

Amazon Data Lifecycle Manager 自定义策略使用资源标签来标识要备份的资源。在创建快照或 EBS 支持的 AMI 策略时，可以指定多个目标资源标签。至少具有指定目标资源标签之一的指定类型（实例或卷）的所有资源都将根据策略被设为目标。例如，如果您创建以卷为目标的快照策略并指定 `purpose=prod`、`costcenter=prod` 和 `environment=live` 作为目标资源标签，则该策略将以具有上述任意标签键值对的所有卷为目标。

如果要在资源上运行多个策略，可以为目标资源分配多个标签，然后创建单独的策略，每个策略都以特定的资源标签为目标。

您不能在标签键中使用 \ 或 = 字符。目标资源标签区分大小写。有关更多信息，请参阅[标记资源](#)。

## 快照

快照是备份 EBS 卷中的数据的主要方式。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。在您删除卷的一系列快照中的一个快照时，只删除该快照独有的数据。将保留卷的其余捕获历史记录。有关更多信息，请参阅[Amazon EBS 快照](#)。

## EBS 支持的 AMI

亚马逊机器映像（AMI）提供启动实例所需的信息。在需要具有相同配置的多个实例时，您可以从单个 AMI 启动多个实例。Amazon Data Lifecycle Manager 仅支持 EBS 支持的 AMI。EBS 支持的 AMI 包括挂载到源实例的每个 EBS 卷的快照。有关更多信息，请参阅[亚马逊机器映像（AMI）](#)。

## Amazon Data Lifecycle Manager 标签

Amazon Data Lifecycle Manager 对通过策略创建的所有快照和 AMI 应用以下系统标签，以便与通过任何其他方法创建的快照和 AMI 区分开来：

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` – 适用于根据基于期限的计划创建的快照。指示何时从标准层中删除快照。
- `dlm:managed`
- `aws:dlm:archived` – 适用于按计划存档的快照。
- `aws:dlm:pre-script` – 用于使用前置脚本创建的快照。
- `aws:dlm:post-script` – 用于使用后置脚本创建的快照。

还可以在创建时指定要应用于快照和 AMI 的自定义标签。您不能在标签键中使用 \ 或 = 字符。

Amazon Data Lifecycle Manager 用于将卷与快照策略关联的目标标签可以选择性地应用于策略创建的快照。同样，用于将实例与 AMI 策略关联的目标标签也可以选择性地应用于策略创建的 AMI。

## 默认策略与自定义策略

本节比较了默认策略和自定义策略，并重点介绍了其相似之处和不同之处。

主题

- [EBS 快照策略比较](#)
- [EBS 支持的 AMI 策略比较](#)

## EBS 快照策略比较

下表重点介绍了 EBS 快照的默认策略和自定义 EBS 快照策略之间的区别。

功能	EBS 快照的默认策略	自定义 EBS 快照策略
托管备份资源	EBS 快照	EBS 快照
目标资源类型	卷	卷或实例

功能	EBS 快照的默认策略	自定义 EBS 快照策略
资源目标定位	将该区域中所有没有近期快照的卷作为目标。您可以指定排除参数来排除特定卷。	仅将具有特定标签的卷或实例作为目标。
排除参数	是，可以排除启动卷、特定卷类型和带有特定标签的卷。	是，在以实例作为目标时可以排除启动卷和带有特定标签的卷。
Support AWS Outposts	否	是
支持多个计划	否	是，每份策略最多 4 个计划
支持的保留类型	仅限基于期限的保留	基于期限和基于计数的保留
快照创建频率	每 1 到 7 天一次。	使用 cron 表达式的每日、每周、每月、每年或自定义频率。
快照保留	2 到 14 天。	最多 1000 张快照（基于计数）或最多 100 年（基于期限）。
支持应用程序一致性快照	否	是，使用前置和后置脚本
支持快照存档	否	是
支持快速快照还原	否	是
支持跨区域复制	是，使用默认设置 <sup>1</sup>	是，使用自定义设置
支持跨账户共享	否	是
支持扩展删除 <sup>2</sup>	是	不支持

<sup>1</sup> 对于默认策略：

- 您无法将标签复制到跨区域副本。
- 副本使用的保留期与源快照相同。

- 副本的加密状态与源快照相同。如果目标区域在默认情况下启用了加密功能，则即使源快照未加密，副本也始终处于加密状态。副本始终使用目标区域的默认 KMS 密钥进行加密。

<sup>2</sup> 对于默认策略和自定义策略：

- 如果删除了目标实例或卷，Amazon Data Lifecycle Manager 会根据保留期继续删除快照，直至（但不包括）最后一个快照。对于默认策略，您可以扩展删除以包括最后一个快照。
- 如果策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止删除快照。对于默认策略，您可以扩展删除以继续删除快照，包括最后一个快照。

## EBS 支持的 AMI 策略比较

下表重点介绍了 EBS 支持的 AMI 的默认策略与 EBS 支持的自定义 AMI 策略之间的区别。

功能	EBS 支持的 AMI 的默认策略	EBS 支持的自定义 AMI 策略
托管备份资源	EBS 支持的 AMI	EBS 支持的 AMI
目标资源类型	实例	实例
资源目标定位	将该区域所有最近没有 AMI 的实例作为目标。您可以指定排除参数来排除特定实例。	仅将具有特定标签的实例作为目标。
创建 AMI 之前重启实例	否	是
排除参数	是，可以排除带有特定标签的实例。	否
支持多个计划	否	是，每份策略最多 4 个计划。
AMI 创建频率	每 1 到 7 天一次。	使用 cron 表达式的每日、每周、每月、每年或自定义频率。
支持的保留类型	仅限基于期限的保留。	基于期限和基于计数的保留。
AMI 保留	2 到 14 天。	最多 1000 个 AMI（基于计数）或最长 100 年（基于期限）。

功能	EBS 支持的 AMI 的默认策略	EBS 支持的自定义 AMI 策略
支持 AMI 弃用	否	是
支持跨区域复制	是，使用默认设置 <sup>1</sup>	是，使用自定义设置
支持扩展删除 <sup>2</sup>	是	不支持

<sup>1</sup> 对于默认策略：

- 您无法将标签复制到跨区域副本。
- 副本使用的保留期与源 AMI 相同。
- 副本的加密状态与源 AMI 相同。如果目标区域在默认情况下启用了加密功能，则即使源 AMI 未加密，副本也始终处于加密状态。副本始终使用目标区域的默认 KMS 密钥进行加密。

<sup>2</sup> 对于默认策略和自定义策略：

- 如果目标实例终止，Amazon Data Lifecycle Manager 会根据保留期继续取消注册 AMI，直至（但不包括）最后一个 AMI。对于默认策略，您可以扩展取消注册以包括最后一个 AMI。
- 如果策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止取消注册 AMI。对于默认策略，您可以扩展删除以继续取消注册 AMI，包括最后一个 AMI。

## 默认策略

要从实例中创建 EBS 支持的定期 AMI，请使用 EBS 支持的 AMI 的默认策略。要创建所有卷的快照（无论其附加状态如何）或者如果您想要排除特定卷，请使用 EBS 快照的默认策略。

本节介绍如何创建默认策略。

### 主题

- [注意事项](#)
- [EBS 快照的默认策略](#)
- [EBS 支持的 AMI 的默认策略](#)
- [启用跨账户和地区的默认政策](#)

## 注意事项

使用默认策略时请记住以下事项：

- 默认策略不备份具有最近备份（快照或 AMI）的目标资源（实例或卷）。创建频率决定备份哪些资源。只有当卷或实例的最后一个快照或 AMI 的时间超过策略的创建频率时，才会对其进行备份。例如，如果您将创建频率指定为 3 天，则 EBS 快照的默认策略仅在上次卷的快照超过 3 天时才会创建该卷的快照。
- 默认情况下，除非指定了排除参数，否则默认策略会将该区域的所有实例或卷作为目标。
- 默认策略将创建最少的唯一快照集。例如，如果您启用 EBS 支持的 AMI 策略和 EBS 快照策略，则该快照策略将不会复制已由 EBS 支持的 AMI 策略备份的卷的快照。
- 默认策略将仅开始以至少已有 24 小时历史的资源作为目标。
- 如果您删除卷或终止默认策略作为目标的实例，则 Amazon Data Lifecycle Manager 将根据保留期继续删除其之前创建的备份（快照或 AMI），直至（但不包括）最后一个备份。如果不需要此备份，您必须手动将其删除。

如果您希望 Amazon Data Lifecycle Manager 删除最后一个备份，则可以启用扩展删除。

- 如果默认策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止删除之前创建的备份（快照或 AMI）。如果您希望 Amazon Data Lifecycle Manager 继续删除备份（包括最后一个备份），则必须在删除策略之前或策略的状态更改为已禁用或已删除之前启用扩展删除。
- 当您创建并启用默认策略时，Amazon Data Lifecycle Manager 会将目标资源随机分配到四小时的时间窗口期。目标资源在其分配的窗口期间以指定的创建频率进行备份。例如，如果策略的创建频率为 3 天，并且目标资源分配给 12:00 - 16:00 的窗口期间，则该资源将每 3 天在 12:00 - 16:00 期间备份一次。

## EBS 快照的默认策略

以下过程演示了如何创建 EBS 快照的默认策略。

### Console

#### 创建 EBS 快照的默认策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择生命周期管理器，然后选择创建生命周期策略。
3. 对于策略类型，请选择默认策略，然后选择 EBS 快照策略。




4. 对于描述，输入策略的简短描述。
5. 对于 IAM 角色，请选择有权管理快照的 IAM 角色。

我们建议您选择默认值以使用 Amazon Data Lifecycle Manager 提供的默认 IAM 角色。但是，您还可以使用之前创建的自定义 IAM 角色。

6. 对于创建频率，请指定您希望策略运行的频率并创建卷的快照。


您指定的频率还决定了备份哪些卷。该策略将仅备份在指定频率内未通过任何其他方式备份的卷。例如，如果您将创建频率指定为 3 天，则该策略将仅为过去 3 天内未备份的卷创建快照。

7. 对于保留期，请指定您希望策略将其创建的快照保留的时长。当快照达到保留阈值时，将被自动删除。保留期必须大于或等于创建频率。
8. ( 可选 ) 配置排除参数，以从计划备份中排除特定卷。策略运行时，将不会备份已排除的卷。
  - a. 要排除启动卷，请选择排除启动卷。如果您排除启动卷，则该策略将仅备份数据 ( 非启动 ) 卷。换句话说，其不会创建作为启动卷附加到实例的卷的快照。
  - b. 要排除特定的卷类型，请选择排除特定卷类型，然后选择要排除的卷类型。该策略将仅备份其余类型的卷。
  - c. 要排除具有特定标签的卷，请选择添加标签，然后指定标签键和值。该策略不会创建具有任何指定标签的卷的快照。
9. ( 可选 ) 在高级设置中，请指定策略应执行的其他操作。
  - a. 要将分配的标签从源卷复制到其快照，请选择从卷复制标签。
  - b. 禁用扩展删除后：
    - 如果删除了源卷，Amazon Data Lifecycle Manager 会根据保留期继续删除之前创建的快照，直至 ( 但不包括 ) 最后一个快照。如果您希望 Amazon Data Lifecycle Manager 删除所有快照，包括最后一个快照，请选择扩展删除。
    - 如果策略被删除或进入 error 或 disabled 状态，Amazon Data Lifecycle Manager 将停止删除快照。如果您希望 Amazon Data Lifecycle Manager 继续删除快照，包括最后一个快照，请选择扩展删除。

 Note

如果启用“扩展删除”，则可以同时覆盖上述两种行为。

- c. 要将该策略创建的快照复制到其他区域，请选择创建跨区域副本，然后选择最多 3 个目标区域。
  - 如果源快照已加密或默认情况下启用了目标区域的加密功能，则会在目标区域中使用 EBS 加密的默认 KMS 密钥对复制的快照进行加密。
  - 如果源快照未加密且默认情况下禁用目标区域的加密功能，则复制的快照为未加密快照。
10. (可选) 要向策略添加标签，请选择添加标签，然后指定标签键和值。
11. 选择创建默认策略。

 Note

如果发生 Role with name AWSDatalifecycleManagerDefaultRole already exists 错误，请参阅 [故障排除](#) 来了解更多信息。

## AWS CLI

### 创建 EBS 快照的默认策略

使用 [create-lifecycle-policy](#) 命令。您可以通过以下两种方法之一来指定请求参数，具体取决于您的用例或偏好：

- 方法 1：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
gp3 | io1 | io2 | st1 | sc1"
```

例如，要创建 EBS 快照的默认策略，该策略以该地区所有卷为目标、使用默认 IAM 角色、每天运行（默认）并将快照保留 7 天（默认），您需要指定以下参数：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- 方法 2：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

其中 `policyDetails.json` 包含以下内容：

```
{
  "PolicyLanguage": "SIMPLIFIED",
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceType": "VOLUME",
  "CopyTags": true | false,
  "CreateInterval": creation_frequency_in_days (1-7),
  "RetainInterval": retention_period_in_days (2-14),
  "ExtendDeletion": true | false,
  "CrossRegionCopyTargets": [{"TargetRegion": "destination_region_code"}],
  "Exclusions": {
    "ExcludeBootVolume": true | false,
    "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
    "ExcludeTags": [{
      "Key": "exclusion_tag_key",
      "Value": "exclusion_tag_value"
    }]
  }
}
```

## EBS 支持的 AMI 的默认策略

以下过程演示了如何创建 EBS 支持的 AMI 的默认策略。

### Console

#### 创建 EBS 支持的 AMI 的默认策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Lifecycle Manager，然后选择创建生命周期策略。
3. 对于策略类型，请选择默认策略，然后选择由 EBS 支持的 AMI 策略。
4. 对于描述，输入策略的简短描述。
5. 对于 IAM 角色，请选择有权管理 AMI 的 IAM 角色。


我们建议您选择默认值以使用 Amazon Data Lifecycle Manager 提供的默认 IAM 角色。但是，您还可以使用之前创建的自定义 IAM 角色。

6. 对于创建频率，请指定您希望策略运行的频率，并从实例创建 AMI。

您指定的频率还决定了备份哪些实例。该策略将仅备份在指定频率内未通过任何其他方式备份的实例。例如，如果您将创建频率指定为 3 天，则该策略将仅会从过去 3 天内未备份的实例创建 AMI。


7. 对于保留期，请指定您希望策略将其创建的 AMI 保留的时长。当 AMI 达到保留阈值时，将会被自动取消注册并删除其关联的快照。保留期必须大于或等于创建频率。
8. ( 可选 ) 配置排除参数，以从计划备份中排除特定实例。策略运行时，将不会备份已排除的实例。
  - 要排除具有特定标签的实例，请选择添加标签，然后指定标签键和值。该策略不会从具有任何指定标签的实例创建 AMI。
9. ( 可选 ) 在高级设置中，请指定策略应执行的其他操作。
  - a. 要将分配的标签从源实例复制到其 AMI，请选择从实例复制标签。
  - b. 禁用扩展删除后：
    - 如果源实例终止，Amazon Data Lifecycle Manager 将根据保留期继续取消注册之前创建的 AMI，直至 ( 但不包括 ) 最后一个 AMI。如果您希望 Amazon Data Lifecycle Manager 取消注册所有 AMI，包括最后一个 AMI，请选择扩展删除。

- 如果策略被删除或进入 `error` 或 `disabled` 状态，Amazon Data Lifecycle Manager 将停止取消注册 AMI。如果您希望 Amazon Data Lifecycle Manager 继续取消注册 AMI，包括最后一个 AMI，请选择扩展删除。

 Note

如果启用“扩展删除”，则可以同时覆盖上述两种行为。

- c. 要将该策略创建的 AMI 复制到其他区域，请选择创建跨区域副本，然后选择最多 3 个目标区域。
  - 如果源 AMI 已加密或默认情况下启用了目标区域的加密功能，则会在目标区域中使用 EBS 加密的默认 KMS 密钥对复制的 AMI 进行加密。
  - 如果源 AMI 未加密且默认情况下禁用目标区域的加密功能，则复制的 AMI 为未加密 AMI。
10. (可选) 要向策略添加标签，请选择添加标签，然后指定标签键和值。
11. 选择创建默认策略。

 Note

如果发生 `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` 错误，请参阅 [故障排除](#) 来了解更多信息。

## AWS CLI

### 创建 EBS 支持的 AMI 的默认策略

使用 [create-lifecycle-policy](#) 命令。您可以通过以下两种方法之一来指定请求参数，具体取决于您的用例或偏好：

- 方法 1：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
```

```
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

例如，要创建 EBS 支持的 AMI 的默认策略 [该策略以该地区所有实例为目标、使用默认 IAM 角色、每天运行（默认）并将 AMI 保留 7 天（默认）]，您需要指定以下参数：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- 方法 2：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

其中 policyDetails.json 包含以下内容：

```
{
  "PolicyLanguage": "SIMPLIFIED",
  "PolicyType": "IMAGE_MANAGEMENT",
  "ResourceType": "INSTANCE",
  "CopyTags": true | false,
  "CreateInterval": creation_frequency_in_days (1-7),
  "RetainInterval": retention_period_in_days (2-14),
  "ExtendDeletion": true | false,
  "CrossRegionCopyTargets": [{"TargetRegion": "destination_region_code"}],
  "Exclusions": {
    "ExcludeTags": [{
      "Key": "exclusion_tag_key",
      "Value": "exclusion_tag_value"
    }
  ]
}
```

```
    }  
  }  
}
```

## 启用跨账户和地区的默认策略

使用 AWS CloudFormation StackSets，您只需一次操作即可在多个账户和 AWS 地区启用亚马逊数据生命周期管理器默认策略。

您可以通过以下方式之一使用堆栈集来启用默认策略：

- 在整个 AWS 组织中-确保在整个 AWS 组织或组织中的特定组织单位中统一启用和配置默认策略。这是使用服务管理权限完成的。AWS CloudFormation StackSets 代表您创建所需的 IAM 角色。
- 跨特定 AWS 账户-确保在特定目标账户中一致启用和配置默认策略。这需要自我管理的权限。您可以创建在堆栈集管理员账户和目标账户之间建立信任关系所需的 IAM 角色。

有关更多信息，请参阅《AWS CloudFormation 用户指南》中的[堆栈集权限模型](#)。

使用以下过程在整个 AWS 组织、特定 OU 或特定目标账户中启用 Amazon Data Lifecycle Manager 的默认策略。

### 先决条件

根据您的启用默认策略的方式，执行以下任一操作：


- (跨 AWS 组织) 您必须[启用组织中的所有功能](#)并使用[激活可信访问权限 AWS Organizations](#)。您还必须使用组织的管理账户或[委派的管理员账户](#)。
- (跨特定目标账户) 您必须通过创建在堆栈集管理员帐户和目标账户之间建立信任关系所需的角色来[授予自我管理权限](#)。

### Console

#### 跨 AWS 组织或跨特定目标账户启用默认策略

1. 打开 AWS CloudFormation 控制台，[网址为 https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation)。
2. 在导航窗格中，选择 StackSets，然后选择创建 StackSet。
3. 对于权限，根据启用默认策略的方式，执行以下任一操作：

- (在整个 AWS 组织中) 选择服务管理权限。
  - (跨特定目标账户) 选择自助服务权限。然后, 对于 IAM 管理员角色 ARN, 选择您为管理员账户创建的 IAM 服务角色, 对于 IAM 执行角色名称, 输入您在目标账户中创建的 IAM 服务角色的名称。
4. 在“准备模板”中, 选择“使用示例模板”。
  5. 对于示例模板, 请执行以下任一操作:
    - (EBS 快照的默认策略) 选择“为 EBS 快照创建 Amazon Data Lifecycle Manager 默认策略”。
    - (EBS 支持的 AMI 的默认策略) 选择“为 EBS 支持的 AMI 创建 Amazon Data Lifecycle Manager 默认策略”。
  6. 选择下一步。
  7. 在 StackSet 名称和 StackSet 描述中, 输入描述性名称和简短描述。
  8. 在“参数”部分, 根据需要配置默认策略设置。

 Note

对于关键工作负载, 我们建议 CreateInterval = 1 天和 RetainInterval = 7 天。

9. 选择下一步。
10. (可选) 在“标签”中, 指定标签以帮助您识别 StackSet 和堆栈资源。
11. 对于托管执行, 请选择活动。
12. 选择下一步。
13. 对于 Add stacks to stack set (将堆栈添加到堆栈集), 选择 Deploy new stacks (部署新堆栈)。
14. 根据您的启用默认策略的方式, 执行以下任一操作:
  - (跨 AWS 组织) 对于部署目标, 请选择以下选项之一:
    - 要在整个 AWS 组织中部署, 请选择部署到组织。
    - 要部署到特定的组织单位 (OU), 请选择“部署到组织单位”, 然后在 OU ID 中输入 OU ID。要添加其他 OU, 请选择添加另一个 OU。
  - (跨特定目标账户) 对于帐户, 请执行以下任一操作:
    - 要部署到特定的目标账户, 请选择在帐户中部署堆栈, 然后在帐户号中输入目标账户的 ID。



- 要部署到特定 OU 中的所有帐户，请选择将堆栈部署到组织单位中的所有帐户，然后在组织编号中输入目标 OU 的 ID。
15. 对于自动部署，请选择已激活。
  16. 对于账户删除行为，请选择保留堆栈。
  17. 在“指定区域”中，选择要在其中启用默认策略的特定区域，或者选择添加所有区域以在所有区域中启用默认策略。
  18. 选择下一步。
  19. 查看堆栈集设置，选择我确认 AWS CloudFormation 可能会创建 IAM 资源，然后选择提交。

## AWS CLI

### 在整个 AWS 组织中启用默认策略

1. 创建堆栈集。使用 `create-stack-set` 命令。

对于 `--permission-model`，请指定 `SERVICE_MANAGED`。

对于 `--template-url`，请指定以下模板 URL 之一：

- (EBS 支持的 AMI 的默认策略) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
- (EBS 快照的默认策略) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

对于 `--parameters`，请指定默认策略的设置。有关支持的参数、参数描述和有效值，请使用 URL 下载模板，然后使用文本编辑器查看模板。

对于 `--auto-deployment`，请指定 `Enabled=true`，`RetainStacksOnAccountRemoval=true`。

```
$ aws cloudformation create-stack-set \  
--stack-set-name stackset_name \  
--permission-model SERVICE_MANAGED \  
--template-url template_url \  

```

```
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
"ParameterKey=param_name_2,ParameterValue=param_value_2" \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

## 2. 部署堆栈集。使用 [create-stack-instances](#) 命令。

对于 `--stack-set-name`，请指定您在上一步中创建的堆栈集的名称。

对于 `--deployment-targets OrganizationalUnitIds`，指定要部署到整个组织的根 OU 的 ID，或者指定要部署到组织中特定 OU 的 OU ID。

对于 `--regions`，请指定要在其中启用默认策略的 AWS 区域。

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | ["ou_id_1",
"ou_id_2"] \
--regions ["region_1", "region_2"]'
```

为特定目标账户启用默认策略

### 1. 创建堆栈集。使用 [create-stack-set](#) 命令。

对于 `--template-url`，请指定以下模板 URL 之一：

- (EBS 支持的 AMI 的默认策略) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml>
- (EBS 快照的默认策略) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml>

对于 `--administration-role-arn`，请指定您之前为堆栈集管理员创建的 IAM 服务角色的 ARN。

对于 `--execution-role-name`，请指定您在目标账户中创建的 IAM 服务角色的名称。

对于 `--parameters`，请指定默认策略的设置。有关支持的参数、参数描述和有效值，请使用 URL 下载模板，然后使用文本编辑器查看模板。

对于 `--auto-deployment`，请指定 `Enabled=true`，`RetainStacksOnAccountRemoval=true`。

```
$ aws cloudformation create-stack-set \  
--stack-set-name stackset_name \  
--template-url template_url \  
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1" \  
"ParameterKey=param_name_2,ParameterValue=param_value_2" \  
--administration-role-arn administrator_role_arn \  
--execution-role-name target_account_role \  
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

## 2. 部署堆栈集。使用 [create-stack-instances](#) 命令。

对于 `--stack-set-name`，请指定您在上一步中创建的堆栈集的名称。

对于 `--accounts`，请指定目标 AWS 帐户的 ID。

对于 `--regions`，请指定要在其中启用默认策略的 AWS 区域。

```
$ aws cloudformation create-stack-instances \  
--stack-set-name stackset_name \  
--accounts '["account_ID_1","account_ID_2"]' \  
--regions '["region_1", "region_2"]'
```

## 自定义策略

本节介绍如何创建自定义 EBS 快照、EBS 支持的 AMI 和跨账户复制事件策略。

### 主题

- [自动化快照生命周期](#)
- [自动化 AMI 生命周期](#)
- [自动执行跨账户快照副本](#)

## 自动化快照生命周期

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 Amazon EBS 快照生命周期。

## 主题

- [创建快照生命周期策略](#)
- [快照生命周期策略的注意事项](#)
- [其他资源](#)
- [使用前置和后置脚本的要求](#)
- [使用前置和后置脚本自动生成应用程序一致性快照](#)
- [前置和后置脚本的其他用例](#)
- [前置和后置脚本的工作方式](#)
- [识别使用前置和后置脚本创建的快照](#)
- [监控前置和后置脚本的执行情况](#)

## 创建快照生命周期策略

使用以下过程之一创建快照生命周期策略。

### Console

#### 要创建快照策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：
  - a. 对于目标资源类型，选择要备份的资源的类型。选择 Volume 创建各个卷的快照，或选择 Instance 从挂载到实例的卷创建多卷快照。
  - b. (仅AWS限 Outpost 客户) 指定目标资源的位置。

对于目标资源位置，请指定目标资源的位置。

- 如果目标资源位于某个 AWS 区域，请选择AWS 区域。Amazon Data Lifecycle Manager 仅备份当前区域中所有具有匹配目标标签的指定类型资源。如果资源位于某个区域中，则由策略创建的快照将存储在同一区域中。
- 如果目标资源位于您账户中的 Outpost 上，请选择 AWS Outpost。Amazon Data Lifecycle Manager 将备份您的账户中所有 Outpost 上具有匹配目标标签的全部指定类

型资源。如果资源位于 Outpost 上，则策略创建的快照可以存储在资源所在同一区域或 Outpost 上。


- 如果您的账户中没有任何 Outposts，则会隐藏此选项并为您选择“AWS 区域”。
- c. 对于目标资源标签，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。
5. 对于 Description (描述)，输入策略的简短描述。
  6. 对于 IAM 角色，选择一个有权管理快照以及描述卷和实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择默认角色。或者，要使用您之前创建的自定义 IAM 角色，请选择选择其他角色，然后选择要使用的角色。
  7. 对于策略标签，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
  8. 对于 Policy status (策略状态)，选择 Enable (启用)，以在下次计划时间开启策略运行，或者选择 Disable policy (禁用策略) 以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始创建快照。
  9. (仅限以实例为目标的策略) 从多卷快照集中排除卷。

默认情况下，Amazon Data Lifecycle Manager 将创建附加到目标实例的所有卷的快照。不过，您可以选择创建附加卷子集的快照。在 Parameters (参数) 部分，执行以下操作：

- 如果您不想创建附加到目标实例的根卷的快照，请选择 Exclude root volume (排除根卷)。如果选择此选项，则只有附加到目标实例的数据 (非根) 卷才会包含在多卷快照集中。
- 如果要创建附加到目标实例的数据 (非根) 卷子集的快照，请选择排除特定的数据卷，然后指定用于标识不应创建快照的数据卷的标签。Amazon Data Lifecycle Manager 不会为具有任何指定标签的数据卷创建快照。Amazon Data Lifecycle Manager 仅为不具有任何指定标签的数据卷创建快照。

10. 选择下一步。
11. 在配置计划屏幕上，配置策略计划。一个策略最多可以有 4 个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：
  - a. 在计划详细信息部分中，执行以下操作：
    - i. 对于计划名称，请指定计划的描述性名称。
    - ii. 在频率和相关字段中配置策略运行之间的间隔。

您可以按每日、每周、每月或每年计划配置策略运行。或者，选择自定义 cron 表达式以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon Ev CloudWatch ents 用户指南中的 [Cron 表达式](#)。

 Note

如果您需要为此计划启用 snapshot archiving (快照存档)，则必须选择 monthly (每月) 或 yearly (每年) 频率，或者指定一个创建频率至少为 28 天的 cron 表达式。

如果指定一个将在特定周次的特定日期 (例如，当月第二周星期四) 创建快照的每月频率，则对于基于计数的计划，存档层的保留计数必须为 4 或以上。

- iii. 对于开始时间，请指定计划开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。时间必须输入 hh:mm UTC 格式。
- iv. 对于保留类型，请指定计划创建的快照的保留策略。


您可以根据其总计数或存在时间保留快照。

- 基于计数的保留

- 禁用快照归档后，范围为 1 到 1000。当达到保留阈值时，最早的快照将永久删除。
- 启用快照归档后，范围为 0 (创建后立即归档) 到 1000。达到保留阈值时，最早的快照将转换为完整快照，然后移动到存档层。

- 基于时长的保留

- 禁用快照归档后，范围为 1 天到 100 年。当达到保留阈值时，最早的快照将永久删除。
- 启用快照归档后，范围为 0 天 (创建后立即归档) 到 100 年。达到保留阈值时，最早的快照将转换为完整快照，然后移动到存档层。

 Note

- 所有计划必须具有相同的保留类型 (基于期限或基于计数)。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。

- 如果您启用了快速快照还原、跨区域复制或快照共享，则必须指定 1 或更大的保留计数，或者 1 天或更长的保留期。

v. (仅限AWS Outposts 客户) 指定快照目标。

对于快照目标 – 请指定策略创建的快照目标。

- 如果该政策针对的是某个区域中的资源，则必须在同一区域创建快照。AWS 已选定您的区域。
- 如果策略的目标是 Outpost 上的资源，您可以选择在源资源所在同一 Outpost 上创建快照，或者在与 Outpost 关联的区域中创建快照。
- 如果您的账户中没有任何 Outposts，则会隐藏此选项并为您选择“AWS 区域”。

b. 配置快照标签。

在标记部分中，请执行以下操作：


- i. 要将所有用户定义的标签从源卷复制到计划创建的快照，请选择从源中复制标签。
- ii. 要指定分配给由该计划创建的快照的其他标签，请选择添加标签。

c. 配置应用程序一致性快照的前置和后置脚本。

有关更多信息，请参阅 [使用前置和后置脚本自动生成应用程序一致性快照](#)。


d. (仅限以卷为目标的策略) 配置快照存档。

在快照存档部分，请执行以下操作：

 Note

您在一个策略中只能为一个计划启用快照存档。


- i. 要为此计划启用快照存档，请选择 Archive snapshots created by this schedule (将此计划创建的快照存档)。

 Note

只有在快照创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

ii. 为存档层中的快照指定保留规则。

- 对于基于计数的计划，指定要在存档层中保留的快照数量。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 3，则计划将在存档层中最多保留 3 个快照。存档第四个快照时，系统将会删除存档层中三个现有快照中最老的一个。
- 对于基于期限的计划，指定要在存档层中保留快照的期限。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 120 天，则计划将在该期限届满时自动从存档层中删除快照。


 Important

存档快照的最短保留期为 90 天。必须指定一个会将快照保留至少 90 天的保留规则。

e. 启用快速快照还原。

要为计划创建的快照启用快速快照还原，请在快速快照还原部分中选择启用快速快照还原。如果您启用快速快照还原，则必须选择要在其中启用该功能的可用区。如果计划使用基于时间的保留计划，则必须指定为每个快照启用快速快照还原的时间段。如果计划使用基于计数的保留，您必须指定要启用快速快照还原的最大快照数。

如果计划在 Outpost 上创建快照，则无法启用快速快照还原。存储在 Outpost 上的本地快照不支持快速快照还原。

 Note

对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。


f. 配置跨区域复制。

要将计划创建的快照复制到 Outpost 或其他区域，请在跨区域复制部分中选择启用跨区域复制。

如果计划在区域中创建快照，则您可以将快照复制到账户中最多三个其他区域 或 Outpost。您必须为每个目标区域或 Outpost 指定单独的跨区域复制规则。



对于每个区域或 Outpost，您可以选择不同的保留策略，还可以选择复制所有标签还是不复制任何标签。如果源快照已加密或默认启用加密，则会加密已复制的快照。如果源快照未加密，您可以启用加密。如果未指定 KMS 密钥，则会在每个目标区域中使用 EBS 加密的默认 KMS 密钥对快照进行加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥的访问权限。

 Note

您必须确保没有超过每个区域的并发快照副本数。


如果策略在 Outpost 上创建快照，则无法将快照复制到区域或另一个 Outpost，并且跨区域复制设置不可用。

g. 配置跨账户共享。

在跨账户共享中，将策略配置为自动与其他 AWS 账户共享按计划创建的快照。执行以下操作：

- i. 要启用与其他 AWS 账户共享，请选择启用跨账户共享。
- ii. 要添加要与之共享快照的账户，请选择添加账户，输入 12 位 AWS 账户 ID，然后选择添加。
- iii. 要在特定时间段后自动取消共享所共享的快照，请选择 Unshare automatically (自动取消共享)。如果您选择自动将共享快照取消共享，则自动取消快照共享前的持续时间不能超过策略保留其快照的期限。例如，如果策略的保留配置可将快照保留 5 天，则您可以将策略配置为在最多 4 天的时间后自动取消快照共享。这适用于采用基于存在时间和基于计数的快照保留配置的策略。

如果不启用自动取消共享，快照将一直共享直至删除。

 Note

您只能共享未加密的快照或使用客户托管密钥加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的[允许其他账户中的用户使用 KMS 密钥](#)。

- h. 要添加其他计划，请选择位于页面顶部的添加其他计划。每个其他计划请按照本主题之前所述填写字段。
  - i. 添加所需计划之后，请选择查看策略。
12. 查看策略摘要，然后选择创建策略。

**Note**

如果发生 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 错误，请参阅 [故障排除](#) 来了解更多信息。

## Command line

可使用 [create-lifecycle-policy](#) 命令创建快照生命周期策略。对于 `PolicyType`，请指定 `EBS_SNAPSHOT_MANAGEMENT`。

**Note**

为简化语法，以下示例使用包含策略详细信息的 JSON 文件 `policyDetails.json`。

### 示例 1 – 具有两个计划的快照生命周期策略

此示例创建的快照生命周期策略可创建标签键 `costcenter` 的值为 115 的所有卷的快照。该策略包含两个计划。第一个计划在每天 3:00 UTC 创建快照。第二个计划在每周五 17:00 UTC 创建一个周快照。

```
aws dlm create-lifecycle-policy \  
  --description "My volume policy" \  
  --state ENABLED \  
  --execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \  
  --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{  
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
  "ResourceTypes": [  

```

```

    "VOLUME"
  ],
  "TargetTags": [{
    "Key": "costcenter",
    "Value": "115"
  }],
  "Schedules": [{
    "Name": "DailySnapshots",
    "TagsToAdd": [{
      "Key": "type",
      "Value": "myDailySnapshot"
    }],
    "CreateRule": {
      "Interval": 24,
      "IntervalUnit": "HOURS",
      "Times": [
        "03:00"
      ]
    },
    "RetainRule": {
      "Count": 5
    },
    "CopyTags": false
  },
  {
    "Name": "WeeklySnapshots",
    "TagsToAdd": [{
      "Key": "type",
      "Value": "myWeeklySnapshot"
    }],
    "CreateRule": {
      "CronExpression": "cron(0 17 ? * FRI *)"
    },
    "RetainRule": {
      "Count": 5
    },
    "CopyTags": false
  }
]}

```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
```

```
"PolicyId": "policy-0123456789abcdef0"
}
```

## 示例 2 - 以实例为目标并创建数据（非根）卷子集快照的快照生命周期策略

此示例创建的快照生命周期策略可从标记为 `code=production` 的实例创建多卷快照集。该策略仅包含一个计划。该计划不会创建标记为 `code=temp` 的数据卷的快照。

```
aws dlm create-lifecycle-policy \
  --description "My volume policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "code",
    "Value": "production"
  }],
  "Parameters": {
    "ExcludeDataVolumeTags": [{
      "Key": "code",
      "Value": "temp"
    }]
  },
  "Schedules": [{
    "Name": "DailySnapshots",
    "TagsToAdd": [{
      "Key": "type",
      "Value": "myDailySnapshot"
    }]
  },
  "CreateRule": {
    "Interval": 24,
    "IntervalUnit": "HOURS",
    "Times": [
      "03:00"
    ]
  }
}
```

```

    ]
  },
  "RetainRule": {
    "Count": 5
  },
  "CopyTags": false
}
]]

```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```

{
  "PolicyId": "policy-0123456789abcdef0"
}

```

### 示例 3 - 自动执行 Outpost 资源本地快照的快照生命周期策略

此示例创建一个快照生命周期策略，该策略创建所有 Outpost 中带有 team=dev 标记的卷的快照。该策略在源卷所在的同一 Outpost 上创建快照。该策略从 12 UTC 开始每 00:00 小时创建一次快照。

```

aws dlm create-lifecycle-policy \
  --description "My local snapshot policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json

```

以下是 policyDetails.json 文件的示例。

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": "VOLUME",
  "ResourceLocations": "OUTPOST",
  "TargetTags": [{
    "Key": "team",
    "Value": "dev"
  }],
  "Schedules": [{
    "Name": "on-site backup",
    "CreateRule": {

```

```

        "Interval": 12,
        "IntervalUnit": "HOURS",
        "Times": [
            "00:00"
        ],
    "Location": [
        "OUTPOST_LOCAL"
    ]
    },
    "RetainRule": {
        "Count": 1
    },
    "CopyTags": false
}
]]}

```

#### 示例 4 - 在区域中创建快照并将其复制到 Outpost 的快照生命周期策略

以下示例策略创建带 `team=dev` 标记的卷的快照。快照在源卷所在的同一区域中创建。从 12 UTC 开始，每 `00:00` 小时创建一次快照，并保留最多 1 个快照。该策略还会将快照复制到 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`，使用默认加密 KMS 密钥对复制的快照进行加密，并将副本保留 1 个月。

```

aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json

```

以下是 `policyDetails.json` 文件的示例。

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": "VOLUME",
  "ResourceLocations": "CLOUD",
  "TargetTags": [{
    "Key": "team",
    "Value": "dev"
  }],
  "Schedules": [{
    "Name": "on-site backup",

```

```

    "CopyTags": false,
    "CreateRule": {
      "Interval": 12,
      "IntervalUnit": "HOURS",
      "Times": [
        "00:00"
      ],
      "Location": "CLOUD"
    },
    "RetainRule": {
      "Count": 1
    },
    "CrossRegionCopyRules" : [
      {
        "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
        "Encrypted": true,
        "CopyTags": true,
        "RetainRule": {
          "Interval": 1,
          "IntervalUnit": "MONTHS"
        }
      }
    ]
  }
}

```

### 示例 5 – 快照生命周期策略，具有已启用归档并基于期限的计划

此示例将创建一个以带有 Name=Prod 标签的卷为目标的快照生命周期策略。此策略采用基于期限的计划，该计划会在每月第一天 09:00 创建快照。此计划会在标准层中将每个快照保留一天，之后将其转移到至存档层。快照在存档层中存储 90 天后将被删除。

```

aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json

```

以下是 policyDetails.json 文件的示例。

```
{
```

```

"ResourceTypes": [ "VOLUME"],
"PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
"Schedules" : [
  {
    "Name": "sched1",
    "TagsToAdd": [
      {"Key":"createdby","Value":"dlm"}
    ],
    "CreateRule": {
      "CronExpression": "cron(0 9 1 * ? *)"
    },
    "CopyTags": true,
    "RetainRule":{
      "Interval": 1,
      "IntervalUnit": "DAYS"
    },
    "ArchiveRule": {
      "RetainRule":{
        "RetentionArchiveTier": {
          "Interval": 90,
          "IntervalUnit": "DAYS"
        }
      }
    }
  }
],
"TargetTags": [
  {
    "Key": "Name",
    "Value": "Prod"
  }
]
}

```

### 示例 6 – 快照生命周期策略，具有已启用归档并基于计数的计划

此示例将创建一个以带有 Purpose=Test 标签的卷为目标的快照生命周期策略。此策略采用基于计数的计划，该计划会在每月第一天 09:00 创建快照。此计划将在快照创建后立即将其存档，并在存档层中最多保留三个快照。

```

aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \

```



```
--execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
--policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
  "ResourceTypes": [ "VOLUME" ],
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "Schedules" : [
    {
      "Name": "sched1",
      "TagsToAdd": [
        {"Key": "createdby", "Value": "dlm"}
      ],
      "CreateRule": {
        "CronExpression": "cron(0 9 1 * ? *)"
      },
      "CopyTags": true,
      "RetainRule": {
        "Count": 0
      },
      "ArchiveRule": {
        "RetainRule": {
          "RetentionArchiveTier": {
            "Count": 3
          }
        }
      }
    }
  ],
  "TargetTags": [
    {
      "Key": "Purpose",
      "Value": "Test"
    }
  ]
}
```

## 快照生命周期策略的注意事项

以下一般注意事项适用于快照生命周期策略：

- 快照生命周期策略仅针对与策略位于同一区域的实例或卷。
- 第一个快照创建操作将在指定的开始时间后一小时内开始。后续快照创建操作将在计划时间的一小时内开始。
- 您可以创建多个策略来备份卷或实例。例如，假设一个卷有两个标签，其中标签 A 是每 12 小时创建一次快照的策略 A 的目标，标签 B 是每 24 小时创建一次快照的策略 B 的目标，则 Amazon Data Lifecycle Manager 将根据这两个策略的计划创建快照。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 目标资源标签区分大小写。
- 如果从策略所针对的资源中删除目标标签，则 Amazon Data Lifecycle Manager 不再管理标准层和存档层中的现有快照；如不再需要，您必须手动将其删除。
- 如果您创建了以实例为目标的策略，并且在创建策略后将新卷挂载到目标实例，则在下次运行策略时，新添加的卷将包含在备份中。策略运行时挂载到实例的所有卷都包括在内。
- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个快照，则该策略不会在达到保留阈值时自动删除该快照。如果不再需要快照，则必须手动删除该快照。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一张快照，直到创建下一张快照。例如，如果基于存在时间的策略每月创建一个快照，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个快照保留一个月，即使保留期为七天。

#### [共享快照](#)时需考虑以下事项：

- 您只能为将卷作为目标的快照策略启用快照存档。
- 对于每个策略，您只能为一个计划指定一个存档规则。
- 如果您使用控制台，则只有在创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

如果您使用的是 AWS CLI、AWS API 或 AWS SDK，则只有在计划中包含创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

- 存档层中的最短保留期为 90 天。
- 快照存档时，快照将在移动到存档层时转换为完整快照。这可能会导致快照存储成本增加。有关更多信息，请参阅 [定价和计费](#)。
- 快照存档时将会禁用快速快照还原和快照共享。
- 如果在某个闰年中，您的保留规则导致存档保留期少于 90 天，则 Amazon Data Lifecycle Manager 会确保快照至少保留 90 天。

- 如果您手动将 Amazon Data Lifecycle Manager 创建的快照存档，并且该快照在达到计划的保留阈值时仍在存档，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前将快照还原到标准层，则该计划将继续按照保留规则管理快照。
- 如果您将 Amazon Data Lifecycle Manager 创建的快照永久或临时还原到标准层，并且该快照在达到计划的保留阈值时仍处于标准层中，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前重新将快照存档，则计划将在达到保留阈值时删除快照。
- Amazon Data Lifecycle Manager 存档的快照会使用您的 `Archived snapshots per volume` 和 `In-progress snapshot archives per account` 限额。
- 如果计划在重试 24 小时后仍无法将快照存档，则该快照将保留在标准层中，并按照本应从存档层中删除的时间来计划删除时间。例如，假设计划将快照存档 120 天，则在存档失败后，快照会保留在标准层中 120 天，然后才会被永久删除。对于基于计数的计划，快照不会计入计划的保留计数。
- 快照存档的区域必须与创建快照的区域相同。如果您启用了跨区域复制和快照存档，Amazon Data Lifecycle Manager 不会将快照副本存档。
- Amazon Data Lifecycle Manager 存档的快照将会使用 `aws:dlm:archived=true` 系统标签进行标记。此外，如果创建快照的计划已启用存档并且基于期限，则将会使用 `aws:dlm:expirationTime` 系统标签标记所创建的快照，以注明计划将快照存档的日期和时间。

以下注意事项适用于排除根卷和数据（非根）卷：

- 如果您选择排除启动卷，并且指定的标签因此排除所有附加到实例的额外数据卷，那么 Amazon Data Lifecycle Manager 将不会为受影响的实例创建任何快照，而是会发布一个 `SnapshotsCreateFailedCloudWatch` 指标。有关更多信息，请参阅 [使用监控您的政策 CloudWatch](#)。

删除或终止快照生命周期策略用作目标的卷或实例时应注意以下事项：

- 对于具有基于计数的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则 Amazon Data Lifecycle Manager 将不再管理标准层和存档层中之前从已删除的卷或已终止的实例创建的快照。如果不再需要较早版本的快照，您必须手动将其删除。
- 对于具有基于期限的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则该策略将继续按照既定计划从标准层和存档层中删除从已删除的卷或实例创建的快照，直到但不包括最后一个快照。如果不再需要最后一个快照，则必须手动删除该快照。

快照生命周期策略和 [快速快照还原](#) 应注意以下事项：

- Amazon Data Lifecycle Manager 只能为大小为 16 TiB 或以下的快照启用快速快照还原。有关更多信息，请参阅 [Amazon EBS 快速快照还原](#)。
- 即使您删除或禁用了策略，为该策略禁用了快速快照还原，或者为该可用区禁用了快速快照还原，已启用快速快照还原的快照仍会保持启用状态。您必须手动为这些快照禁用快速快照还原。
- 如果您为策略启用了快速快照还原，并且超出了可启用快速快照还原的最大快照数，Amazon Data Lifecycle Manager 将按计划创建快照，但不会为其启用快速快照还原。在删除启用了快速快照还原的快照后，将为 Amazon Data Lifecycle Manager 创建的下一个快照启用快速快照还原。
- 快照启用快速快照还原后，每 TiB 需要 60 分钟来优化快照。我们建议您配置相应的计划，以确保在 Amazon Data Lifecycle Manager 创建下一个快照之前对每个快照进行完全优化。
- 如果您为以实例为目标的策略启用快速快照还原，Amazon Data Lifecycle Manager 会为多卷快照集中的各个快照单独启用快速快照还原。如果 Amazon Data Lifecycle Manager 无法为多卷快照集中的其中一个快照启用快速快照还原，它仍会尝试为快照集中的其余快照启用快速快照还原。
- 对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。有关更多信息，请参阅 [定价和计费](#)。

#### Note

根据生命周期策略的配置，您可以在多个可用区同时为多个快照启用快速快照还原。

快照生命周期策略和启用 [多重挂载](#) 的卷应注意以下事项：

- 如果创建的生命周期策略以启用了多重挂载的卷为目标实例，则 Amazon Data Lifecycle Manager 将为每个挂载的实例启动卷的快照。使用时间戳标签来标识从附加实例创建的时间一致的快照集。

跨账户共享快照时需注意以下事项：

- 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。
- 您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。
- 如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [允许其他账户中的用户使用 KMS 密钥](#)。

快照策略和 [快照归档](#) 应注意以下事项：

- 如果您手动归档由策略创建的快照，并且该快照在达到策略的保留阈值时位于归档层中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在归档层中时，Amazon Data Lifecycle Manager 不管理快照。如果您不再需要存储在归档层中的快照，则必须手动将其删除。

以下注意事项适用于快照策略和[回收站](#)：

- 如果 Amazon Data Lifecycle Manager 删除快照并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原快照，则必须在不再需要该快照时手动删除它。Amazon Data Lifecycle Manager 将不再管理该快照。
- 如果您手动删除由策略创建的快照，并且该快照在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在回收站中时，Amazon Data Lifecycle Manager 不管理快照。

如果在达到策略的保留阈值之前从回收站还原了快照，那么当达到策略的保留阈值时，Amazon Data Lifecycle Manager 将删除快照。

如果在达到策略的保留阈值之前从回收站还原了快照，则 Amazon Data Lifecycle Manager 将不再删除快照。如果不再需要快照，则必须手动删除该快照。

以下注意事项适用于处于 error ( 错误 ) 状态的快照生命周期策略：

- 对于具有基于存在时间的保留计划的策略，则设置为在策略处于 error 状态时过期的快照将无限期保留。您必须手动删除快照。重新启用该策略时，Amazon Data Lifecycle Manager 会在其保留期到期时恢复删除快照。
- 对于具有基于计数的保留计划的策略，策略会在其处于 error 状态时停止创建和删除快照。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建快照，并在达到保留阈值时恢复删除快照。

快照策略和[快照锁定](#)应注意以下事项：

- 如果您手动锁定由 Amazon Data Lifecycle Manager 创建的快照，并且在达到计划的保留阈值时该快照仍处于锁定状态，则 Amazon Data Lifecycle Manager 将不再管理该快照。如果不再需要快照，则必须手动删除该快照。
- 如果您手动锁定由 Amazon Data Lifecycle Manager 创建并启用了“快速快照还原”功能的快照，并且在达到保留阈值时该快照仍处于锁定状态，则 Amazon Data Lifecycle Manager 将不会禁用“快速快照还原”功能或删除该快照。如果不再需要快照，则必须手动禁用“快速快照还原”功能并删除该快照。

- 如果您手动将 Amazon Data Lifecycle Manager 创建的快照注册到 AMI，然后锁定该快照，并且在达到保留阈值时该快照仍处于锁定状态并与 AMI 关联，则 Amazon Data Lifecycle Manager 将继续尝试删除该快照。当 AMI 取消注册并解锁快照时，Amazon Data Lifecycle Manager 将自动删除该快照。

## 其他资源

有关更多信息，请参阅[使用 Amazon Data Lifecycle Manager AWS 存储自动化 Amazon EBS 快照和 AMI 管理](#)博客。

## 使用前置和后置脚本的要求

下表概述了将前置和后置脚本与 Amazon Data Lifecycle Manager 一起使用的要求。

要求	应用程序一致性快照		
	VSS 备份	自定义 SSM 文档	其他用例
SSM 代理已安装并在目标实例上运行	✓	✓	✓
目标实例已满足 VSS 系统要求	✓		
与目标实例关联的启用 VSS 的实例配置文件	✓		
安装在目标实例上的 VSS 组件	✓		
使用脚本前和后置脚本命令准备 SSM 文档		✓	✓
准备 Amazon Data Lifecycle Manager IAM 角色运行前脚本和后脚本	✓	✓	✓

## 应用程序一致性快照

创建以实例为目标的快照策略，并针对前脚本和后脚本进行配置	✓	✓	✓
------------------------------	---	---	---

### 使用前置和后置脚本自动生成应用程序一致性快照

您可以通过在以实例为目标的快照生命周期策略中启用前置和后置脚本，使用 Amazon Data Lifecycle Manager 自动生成应用程序一致性快照。

Amazon Data Lifecycle Manager 与 AWS Systems Manager ( Systems Manager ) 集成，以支持应用程序一致性快照。Amazon Data Lifecycle Manager 使用 Systems Manager ( SSM ) 命令文档 ( 包括前置和后置脚本 ) 来自动执行完成应用程序一致性快照所需的操作。在 Amazon Data Lifecycle Manager 启动快照创建之前，其会运行前置脚本中的命令来冻结和刷新 I/O。在 Amazon Data Lifecycle Manager 启动快照创建后，其会运行后置脚本中的命令来解冻 I/O。

使用 Amazon Data Lifecycle Manager，您可以自动生成以下内容的应用程序一致性快照：

- 使用卷影复制服务 ( VSS ) 的 Windows 应用程序
- SAP HANA 使用 AWS 托管 SSDM 文档。有关更多信息，请参阅 [Amazon EBS snapshots for SAP HANA](#)。
- 使用 SSM 文档模板自行管理的数据库，例如 MySQL、PostgreSQL InterSystems 或 IRIS

### 主题

- [应用程序一致性快照入门](#)
- [使用 Amazon Data Lifecycle Manager 进行 VSS 备份的注意事项](#)
- [应用程序一致性快照的共同责任](#)

### 应用程序一致性快照入门

本节介绍使用 Amazon Data Lifecycle Manager 自动生成应用程序一致性快照所需遵循的步骤。

## 步骤 1：准备目标实例

您需要使用 Amazon Data Lifecycle Manager 为应用程序一致性快照准备目标实例。根据您的用例执行以下操作之一。

### Prepare for VSS Backups

为 VSS 备份准备目标实例

1. 在目标实例上安装 SSM Agent ( 如果尚未安装 )。如果目标实例上已安装 SSM Agent，请跳过此步骤。

有关更多信息，请参阅[在适用于 Windows 的 Amazon EC2 实例上手动安装 SSM Agent](#)。

2. 确保 SSM Agent 正在运行。有关更多信息，请参阅[正在检查 SSM Agent 状态并启动代理](#)。
3. 为 Amazon EC2 实例设置 Systems Manager。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的[为 Amazon EC2 实例设置 Systems Manager](#)。
4. [确保满足 VSS 备份的系统要求](#)。
5. [将启用 VSS 的实例配置文件附加到目标实例](#)。
6. [安装 VSS 组件](#)。

### Prepare for SAP HANA backups

为 SAP HANA 备份准备目标实例

1. 在目标实例上准备 SAP HANA 环境。
  - a. 使用 SAP HANA 设置实例。如果您还没有现成的 SAP HANA 环境，则可以参考[SAP HANA Environment Setup on AWS](#)。
  - b. 以合适的管理员用户身份登录 SystemDB。
  - c. 创建要与 Amazon Data Lifecycle Manager 一起使用的数据库备份用户。

```
CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

例如，以下命令创建了一个名为 `d1m_user` 并且密码为 `password` 的用户。

```
CREATE USER d1m_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

- d. 将 BACKUP OPERATOR 角色分配给您在上一步中创建的数据库备份用户。



```
GRANT BACKUP OPERATOR TO username
```

例如，以下命令将角色分配给名为 `d1m_user` 的用户。

```
GRANT BACKUP OPERATOR TO d1m_user
```

- e. 以管理员身份登录操作系统，例如 `sidadm`。
- f. 创建一个 `hdbuserstore` 条目来存储连接信息，这样 SAP HANA SSM 文档就可以连接到 SAP HANA，而无需用户输入信息。

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER  
localhost:3hana_instance_number13 username password
```

例如：

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 d1m_user password
```

- g. 测试连接。

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. 在目标实例上安装 SSM Agent ( 如果尚未安装 )。如果目标实例上已安装 SSM Agent，请跳过此步骤。

有关更多信息，请参阅[在适用于 Linux 的 Amazon EC2 实例上手动安装 SSM Agent](#)。

3. 确保 SSM Agent 正在运行。有关更多信息，请参阅[正在检查 SSM Agent 状态并启动代理](#)。
4. 为 Amazon EC2 实例设置 Systems Manager。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的[为 Amazon EC2 实例设置 Systems Manager](#)。

## Prepare for custom SSM documents

为 SSM 文档准备目标实例

1. 在目标实例上安装 SSM Agent ( 如果尚未安装 )。如果目标实例上已安装 SSM Agent，请跳过此步骤。
  - ( Linux 实例 ) [在适用于 Linux 的 Amazon EC2 实例上手动安装 SSM Agent](#)

- ( Windows 实例 ) [在适用于 Windows 的 Amazon EC2 实例上手动安装 SSM Agent](#)
- 2. 确保 SSM Agent 正在运行。有关更多信息，请参阅[正在检查 SSM Agent 状态并启动代理](#)。
- 3. 为 Amazon EC2 实例设置 Systems Manager。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的[为 Amazon EC2 实例设置 Systems Manager](#)。

## 步骤 2：准备 SSM 文档

### Note

只有自定义 SSM 文档才需要执行此步骤。VSS 备份或 SAP HANA 不需要执行此步骤。对于 VSS 备份和 SAP HANA，Amazon Data Lifecycle Manager 使用 AWS 托管 SSM 文档。

如果要为自管理的数据库（例如 MySQL、PostgreSQL 或 InterSystems IRIS）自动生成应用程序一致性快照，则必须创建一个 SSM 命令文档，其中包含用于在启动快照创建之前冻结和刷新 I/O 的预脚本，以及用于在启动快照创建后解冻 I/O 的后置脚本。

如果您的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库使用标准配置，则可以使用下面的示例 SSM 文档内容创建 SSM 命令文档。如果您的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库使用非标准配置，则可以使用以下示例内容作为 SSM 命令文档的起点，然后对其进行自定义以满足您的要求。或者，如果想要从头开始创建新的 SSM 文档，则可以使用下面的 SSM 文档空白模板，并在相应的文档部分中添加前置和后置命令。

### ⚠ 请注意以下几点：

- 您负责确保 SSM 文档为数据库配置执行正确且必需的操作。
- 只有当 SSM 文档中的前置和后置脚本能够成功冻结、刷新和解冻 I/O 时，才能保证快照具有应用程序一致性。
- SSM 文档必须包含 allowedValues 的必填字段，包括 pre-script、post-script 和 dry-run。Amazon Data Lifecycle Manager 将根据这些部分的内容在您的实例上执行命令。如果您的 SSM 文档没有这些部分，则 Amazon Data Lifecycle Manager 会将其视为执行失败。

## MySQL sample document content

```
###=====###
```

```

# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
# this
# software and associated documentation files (the "Software"), to deal in the
# Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions
during policy execution.
    # 'dry-run' option is intended for validating the document execution without
triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager
to successfully
    # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
be executed.
    allowedValues:
      - pre-script
      - post-script
      - dry-run

```

```

mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
      - platformType
      - Linux
  inputs:
    runCommand:
      - |
        #!/bin/bash

###=====###
    ### Error Codes

###=====###
    # The following Error codes will inform Data Lifecycle Manager of the type of
error
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206

###=====###
    ### Global variables
###=====###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}
    FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
    FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
    FS_BUSY_ERROR='mount point is busy'

    # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the

```

```
# duration specified in the global variable below. Choose the duration based
on your
# database application's tolerance to freeze.
export AUTO_THAW_DURATION_SECS="60"

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
    # Check if filesystem is already frozen. No error code indicates that
filesystem
# is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
    check_fs_freeze
    # Execute the DB commands to flush the DB in preparation for snapshot
snap_db
    # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
    freeze_fs

    echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
    $(nohup bash -c execute_schedule_auto_thaw >/dev/null 2>&1 &)
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
    # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
    unfreeze_fs
    thaw_db
}

# Execute Auto Thaw to automatically unfreeze the application after the
duration configured
# in the AUTO_THAW_DURATION_SECS global variable.
execute_schedule_auto_thaw() {
    sleep ${AUTO_THAW_DURATION_SECS}
    execute_post_script
}

# Disable Auto Thaw if it is still enabled
execute_disable_auto_thaw() {
    echo "INFO: Attempting to disable auto thaw if enabled"
```

```

        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == */boot* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"

                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201

```

```

        echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
        exit 201
    fi
done
}

# Iterate over all the mountpoints and freeze the filesystem.
freeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
        # operations for root and boot mountpoints.
        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi
        echo "INFO: Freezing $target"
        error_message=$(sudo fsfreeze -f $target 2>&1)
        if [ $? -ne 0 ];then
            # If the filesystem is already in frozen, return error code 204
            if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"

                sudo mysql -e 'UNLOCK TABLES;'
                exit 204
            fi
            # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
            echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"

            thaw_db
            exit 201
        fi
        echo "INFO: Freezing complete on $target"
    done
}

# Iterate over all the mountpoints and unfreeze the filesystem.
unfreeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.

```

```

# Hence, will skip the root and boot mountpoints during unfreeze as
well.
if [ $target == '/' ]; then continue; fi
if [[ "$target" == */boot* ]]; then continue; fi
echo "INFO: Thawing $target"
error_message=$(sudo fsfreeze -u $target 2>&1)
# Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
if [ $? -ne 0 ]; then
    if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
        echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
        exit 205
    fi
    # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
    echo "ERROR: Failed to unfreeze mountpoint $target due due to error
- $error_message"
    exit 202
fi
echo "INFO: Thaw complete on $target"
done
}

snap_db() {
# Run the flush command only when MySQL DB service is up and running
sudo systemctl is-active --quiet mysqld.service
if [ $? -eq 0 ]; then
    echo "INFO: Execute MySQL Flush and Lock command."
    sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
    # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
    if [ $? -ne 0 ]; then
        echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
        exit 201
    fi
    sync
else
    echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
fi
}

thaw_db() {

```



```
# Run the unlock command only when MySQL DB service is up and running
sudo systemctl is-active --quiet mysqld.service
if [ $? -eq 0 ]; then
    echo "INFO: Execute MySQL Unlock"
    sudo mysql -e 'UNLOCK TABLES;'
else
    echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Unlock command."
fi
}

export -f execute_schedule_auto_thaw
export -f execute_post_script
export -f unfreeze_fs
export -f thaw_db

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        execute_disable_auto_thaw
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
```

```
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
```

## PostgreSQL sample document content

```
###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
# this
# software and associated documentation files (the "Software"), to deal in the
# Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions
during policy execution.
    # 'dry-run' option is intended for validating the document execution without
triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager
to successfully
    # trigger pre and post script actions.
    type: String
```

```

    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

```

mainSteps:

```

- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

```

```
###=====###
```

```
### Error Codes
```

```
###=====###
```

```

# The following Error codes will inform Data Lifecycle Manager of the type of
error

```

```

# and help guide handling of the error.

```

```

# The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.

```

```

# 1 Pre-script failed during execution - 201

```

```

# 2 Post-script failed during execution - 202

```

```

# 3 Auto thaw occurred before post-script was initiated - 203

```

```

# 4 Pre-script initiated while post-script was expected - 204

```

```

# 5 Post-script initiated while pre-script was expected - 205

```

```

# 6 Application not ready for pre or post-script initiation - 206

```

```
###=====###
```

```
### Global variables
```

```
###=====###
```

```
START=$(date +%s)
```

```
OPERATION={{ command }}
FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
FS_BUSY_ERROR='mount point is busy'

# Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
# duration specified in the global variable below. Choose the duration based
on your
# database application's tolerance to freeze.
export AUTO_THAW_DURATION_SECS="60"

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
    # Check if filesystem is already frozen. No error code indicates that
filesystem
# is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
    check_fs_freeze
    # Execute the DB commands to flush the DB in preparation for snapshot
snap_db
    # Freeze the filesystem. No error code indicates that filesystem was
succesfully frozen
    freeze_fs

    echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
    $(nohup bash -c execute_schedule_auto_thaw >/dev/null 2>&1 &)
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
    # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
    unfreeze_fs
}

# Execute Auto Thaw to automatically unfreeze the application after the
duration configured
# in the AUTO_THAW_DURATION_SECS global variable.
execute_schedule_auto_thaw() {
    sleep ${AUTO_THAW_DURATION_SECS}
```

```

    execute_post_script
}

# Disable Auto Thaw if it is still enabled
execute_disable_auto_thaw() {
    echo "INFO: Attempting to disable auto thaw if enabled"
    auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
    if [ -n "${auto_thaw_pgid}" ]; then
        echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
        sudo pkill -g ${auto_thaw_pgid}
        rc=$?
        if [ ${rc} != 0 ]; then
            echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
        else
            echo "INFO: Auto Thaw has been disabled"
        fi
    fi
}

# Iterate over all the mountpoints and check if filesystem is already in
freeze state.
# Return error code 204 if any of the mount points are already frozen.
check_fs_freeze() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
        # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi

        error_message=$(sudo mount -o remount,noatime $target 2>&1)
        # Remount will be a no-op without a error message if the filesystem is
unfrozen.
        # However, if filesystem is already frozen, remount will fail with
busy error message.
        if [ $? -ne 0 ];then
            # If the filesystem is already in frozen, return error code 204
            if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then

```

```

        echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
        exit 204
    fi
    # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
    echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
    exit 201
fi
done
}

# Iterate over all the mountpoints and freeze the filesystem.
freeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
        # operations for root and boot mountpoints.
        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi
        echo "INFO: Freezing $target"
        error_message=$(sudo fsfreeze -f $target 2>&1)
        if [ $? -ne 0 ];then
            # If the filesystem is already in frozen, return error code 204
            if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                exit 204
            fi
            # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
            echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
            exit 201
        fi
        echo "INFO: Freezing complete on $target"
    done
}

# Iterate over all the mountpoints and unfreeze the filesystem.
unfreeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)

```

```

do
    # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
    # Hence, will skip the root and boot mountpoints during unfreeze as
well.
    if [ $target == '/' ]; then continue; fi
    if [[ "$target" == */boot* ]]; then continue; fi
    echo "INFO: Thawing $target"
    error_message=$(sudo fsfreeze -u $target 2>&1)
    # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
    if [ $? -ne 0 ]; then
        if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
            echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
            exit 205
        fi
        # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
        echo "ERROR: Failed to unfreeze mountpoint $target due to error
- $error_message"
        exit 202
    fi
    echo "INFO: Thaw complete on $target"
done
}

snap_db() {
    # Run the flush command only when PostgreSQL DB service is up and running
sudo systemctl is-active --quiet postgresql
    if [ $? -eq 0 ]; then
        echo "INFO: Execute Postgres CHECKPOINT"
        # PostgreSQL command to flush the transactions in memory to disk
sudo -u postgres psql -c 'CHECKPOINT;'
        # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
        if [ $? -ne 0 ]; then
            echo "ERROR: Postgres CHECKPOINT command failed."
            exit 201
        fi
        sync
    else
        echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
    fi
}

```

```

    fi
}

export -f execute_schedule_auto_thaw
export -f execute_post_script
export -f unfreeze_fs

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        execute_disable_auto_thaw
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."

```

## InterSystems IRIS sample document content

```

###=====###
# MIT License
#
# Copyright (c) 2024 InterSystems
#

```



```

# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
  feature for InterSystems IRIS.
parameters:
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
  execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
    You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
  be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
  trigger pre and post script actions.
    allowedValues:
      - pre-script
      - post-script
      - dry-run

mainSteps:

```

```

- action: aws:runShellScript
description: Run InterSystems IRIS Database freeze/thaw commands
name: run_pre_post_scripts
precondition:
  StringEquals:
    - platformType
    - Linux
inputs:
  runCommand:
    - |
      #!/bin/bash

###=====###
  ### Global variables

###=====###
  DOCKER_NAME=iris
  LOGDIR=./
  EXIT_CODE=0
  OPERATION={{ command }}
  START=$(date +%s)

  # Check if Docker is installed
  # By default if Docker is present, script assumes that InterSystems IRIS is
running in Docker
  # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
non-containerised (and Docker is present).
  # Script assumes irissys user has OS auth enabled, change the OS user or
supply login/password depending on your configuration.
  if command -v docker &> /dev/null
  then
    DOCKER_EXEC="docker exec $DOCKER_NAME"
  else
    DOCKER_EXEC="sudo -i -u irissys"
  fi

  # Add all pre-script actions to be performed within the function below
execute_pre_script() {
  echo "INFO: Start execution of pre-script"

  # find all iris running instances
  iris_instances=$(($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5- | awk '{print $1}')
```

```

echo "`date`: Running iris instances $iris_instances"

# Only for running instances
for INST in $iris_instances; do

    echo "`date`: Attempting to freeze $INST"

    # Detailed instances specific log
    LOGFILE=$LOGDIR/$INST-pre_post.log

    #check Freeze status before starting
    $DOCKER_EXEC irissession $INST -U '%SYS'
    "##Class(Backup.General).IsWDSuspendedExt()"
    freeze_status=$?
    if [ $freeze_status -eq 5 ]; then
        echo "`date`: ERROR: $INST IS already FROZEN"
        EXIT_CODE=204
    else
        echo "`date`: $INST is not frozen"
        # Freeze
        # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
        \$DOCKER\_EXEC irissession \$INST -U '%SYS'
        "##Class\(Backup.General\).ExternalFreeze\(\"\$LOGFILE\",,,,,,600,,,300\)"
        status=\$?

        case \$status in
            5\) echo "`date`: \$INST IS FROZEN"
                ;;
            3\) echo "`date`: \$INST FREEZE FAILED"
                EXIT\_CODE=201
                ;;
            \*\) echo "`date`: ERROR: Unknown status code: \$status"
                EXIT\_CODE=201
                ;;
        esac
        echo "`date`: Completed freeze of \$INST"
    fi
done
echo "`date`: Pre freeze script finished"
}

# Add all post-script actions to be performed within the function below
execute\_post\_script\(\) {

```

```

echo "INFO: Start execution of post-script"

# find all iris running instances
iris_instances=$(($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5- | awk '{print $1}'))
echo "`date`: Running iris instances $iris_instances"

# Only for running instances
for INST in $iris_instances; do

    echo "`date`: Attempting to thaw $INST"

    # Detailed instances specific log
    LOGFILE=$LOGDIR/$INST-pre_post.log

    #check Freeze status befor starting
    $DOCKER_EXEC irissession $INST -U '%SYS'
    "##Class(Backup.General).IsWDSuspendedExt()"
    freeze_status=$?
    if [ $freeze_status -eq 5 ]; then
        echo "`date`: $INST is in frozen state"
        # Thaw
        # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
        %25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
        $DOCKER_EXEC irissession $INST -U%SYS
        "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
        status=$?

        case $status in
            5) echo "`date`: $INST IS THAWED"
                $DOCKER_EXEC irissession $INST -U%SYS
                "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
            3) echo "`date`: $INST THAW FAILED"
                EXIT_CODE=202
                ;;
            *) echo "`date`: ERROR: Unknown status code: $status"
                EXIT_CODE=202
                ;;
        esac
        echo "`date`: Completed thaw of $INST"
    else
        echo "`date`: ERROR: $INST IS already THAWED"
        EXIT_CODE=205
    fi
done

```

```

        fi
    done
    echo "`date`: Post thaw script finished"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        # return failure
        EXIT_CODE=1
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: ((${END} -
${START})) seconds."
exit $EXIT_CODE

```

有关更多信息，请参阅[GitHub 存储库](#)。

### Empty document template

```

###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
this

```

```

# software and associated documentation files (the "Software"), to deal in the
Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
    command:
      # Data Lifecycle Manager will trigger the pre-script and post-script actions
during policy execution.
      # 'dry-run' option is intended for validating the document execution without
triggering any commands
      # on the instance. The following allowedValues will allow Data Lifecycle Manager
to successfully
      # trigger pre and post script actions.
      type: String
      default: 'dry-run'
      description: (Required) Specifies whether pre-script and/or post-script should
be executed.
      allowedValues:
        - pre-script
        - post-script
        - dry-run

mainSteps:
- action: aws:runShellScript

```

```

description: Run Database freeze/thaw commands
name: run_pre_post_scripts
precondition:
  StringEquals:
    - platformType
    - Linux
inputs:
  runCommand:
    - |
      #!/bin/bash

```

```

###=====###
### Error Codes

###=====###
# The following Error codes will inform Data Lifecycle Manager of the type of
error
# and help guide handling of the error.
# The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
# 1 Pre-script failed during execution - 201
# 2 Post-script failed during execution - 202
# 3 Auto thaw occurred before post-script was initiated - 203
# 4 Pre-script initiated while post-script was expected - 204
# 5 Post-script initiated while pre-script was expected - 205
# 6 Application not ready for pre or post-script initiation - 206

###=====###
### Global variables

###=====###
START=$(date +%s)
# For testing this script locally, replace the below with OPERATION=$1.
OPERATION={{ command }}

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
}

# Add all post-script actions to be performed within the function below
execute_post_script() {

```

```
    echo "INFO: Start execution of post-script"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
```

获得 SSM 文档内容后，请参照以下过程之一创建自定义 SSM 文档。

## Console

### 创建 SSM 命令文档

1. 打开 AWS Systems Manager 控制台，[网址为 https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/)。
2. 在导航窗格中，选择文档，然后选择创建文档、命令或会话。
3. 对于名称，为文档输入一个描述性名称。



4. 对于目标类型，选择/AWS::EC2::Instance。
5. 对于文档类型，请选择命令。
6. 在内容字段中，选择 YAML，然后粘贴文档内容。
7. 在文档标签部分，添加标签键为 DLMScriptsAccess、标签值为 true 的标签。

 Important

该DLMScriptsAccess:true标签是步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色中使用的AWSDataLifecycleManagerSSMFullAccess AWS 托管策略所必需的。该策略使用 aws:ResourceTag 条件键来限制对带有此标签的 SSM 文档的访问权限。

8. 选择创建文档。


## AWS CLI

### 创建 SSM 命令文档

使用 [create-document](#) 命令。对于 --name，请为文档指定一个描述性名称。对于 --document-type，请指定 Command。对于 --content，请指定包含 SSM 文档内容的.yaml 文件的路径。对于 --tags，请指定 "Key=DLMScriptsAccess,Value=true"。

```
$ aws ssm create-document \  
--content file://path/to/file/documentContent.yaml \  
--name "document_name" \  
--document-type "Command" \  
--document-format YAML \  
--tags "Key=DLMScriptsAccess,Value=true"
```

### 步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色

 Note

如果出现以下情况，则需要执行此步骤：

- 创建或更新使用自定义 IAM 角色的启用前置/后置脚本的快照策略。
- 使用命令行创建或更新使用默认值的启用前置/后置脚本的快照策略。

如果您使用控制台创建或更新启用脚本前/后脚本的快照策略，该策略使用默认角色管理快照 ( `AWSDataLifecycleManagerDefaultRole` )，请跳过此步骤。在这种情况下，我们会自动将 `AWSDataLifecycleManagerSSMFullAccess` 策略附加到该角色。

您必须确保您用于策略的 IAM 角色授予 Amazon Data Lifecycle Manager 权限，以执行在策略作为目标的实例上运行前置和后置脚本所需的 SSM 操作。

Amazon Data Lifecycle Manager 提供了包含所需权限的托管策略 (`AWSDataLifecycleManagerSSMFullAccess`)。您可以将此策略附加到您的 IAM 角色以管理快照，从而确保其包含这些权限。

#### Important

使用前脚本和后置脚本时，`AWSDataLifecycleManagerSSMFullAccess` 托管策略使用 `aws:ResourceTag` 条件键来限制对特定 SSM 文档的访问。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

或者，您可以手动创建自定义策略或将所需权限直接分配给您使用的 IAM 角色。您可以使用 `AWSDataLifecycleManagerSSMFullAccess` 托管策略中定义的同权限，但是，`aws:ResourceTag` 条件密钥是可选的。如果您决定不包含该条件键，则无需用 `DLMScriptsAccess:true` 标记您的 SSM 文档。

使用以下方法之一将 `AWSDataLifecycleManagerSSMFullAccess` 策略添加到您的 IAM 角色。

#### Console

将托管策略附加到您的自定义角色

1. 通过 <https://console.aws.amazon.com/iam/> 打开 IAM 控制台。
2. 在导航面板中，选择 Roles ( 角色 )。
3. 搜索并选择用于管理快照的自定义角色。
4. 在权限选项卡上，选择添加权限、附加策略。
5. 搜索并选择 `AWSDataLifecycleManagerSSMFullAccess` 托管策略，然后选择添加权限。

## AWS CLI

将托管策略附加到您的自定义角色

使用 [attach-role-policy](#) 命令。对于 `---role-name`，请指定您自定义角色的名称。对于 `--policy-arn`，请指定 `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`。

```
$ aws iam attach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \  
--role-name your_role_name
```

### 步骤 4：创建快照生命周期策略

要自动生成应用程序一致性快照，您必须创建以实例为目标的快照生命周期策略，并为该策略配置前置和后置脚本。

### Console

#### 创建快照生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：
  - a. 对于目标资源类型，请选择 Instance。
  - b. 对于目标资源标签，请指定识别要备份的实例的资源标签。仅备份具有指定标签的资源。
5. 对于 IAM 角色，可以选择 AWSDataLifecycleManagerDefaultRole (用于管理快照的默认角色)，也可以选择您创建并准备使用前脚本和发布脚本的自定义角色。
6. 根据需要配置计划和其他选项。我们建议您将快照创建时间计划在与您工作负载相匹配的时间段，例如在维护窗口期间。

对于 SAP HANA，我们建议您启用“快速快照还原”。

**Note**

如果您为 VSS 备份启用计划，则无法启用排除特定数据卷或从源中复制标签。

7. 在前置和后置脚本部分中，选择启用前置和后置脚本，然后根据您的工作负载执行以下操作：
  - 要创建 Windows 应用程序的应用程序一致性快照，请选择 VSS 备份。
  - 要创建您的 SAP HANA 工作负载的应用程序一致性快照，请选择 SAP HANA。
  - 要使用自定义 SSM 文档为所有其他数据库和工作负载（包括自行管理的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库）创建应用程序一致的快照，请选择自定义 SSM 文档。
    1. 对于自动化选项，请选择前置和后置脚本。
    2. 对于 SSM 文档，请选择您准备的 SSM 文档。
8. 根据您所选的选项，配置以下其他选项：
  - 脚本超时 –（仅限自定义 SSM 文档）如果脚本运行尝试尚未完成，则在此超时期间后，Amazon Data Lifecycle Manager 的尝试失败。如果脚本未在其超时期间内完成，Amazon Data Lifecycle Manager 的尝试失败。超时期间分别适用于前置和后置脚本。最小的默认超时期间为 10 秒。最长超时期间为 120 秒。
  - 重试失败的脚本 – 选择此选项可重试未在其超时期间内完成的脚本。如果前置脚本失败，则 Amazon Data Lifecycle Manager 会重试整个快照创建过程，包括运行前置和后置脚本。如果后置脚本失败，则 Amazon Data Lifecycle Manager 将仅重试后置脚本；在这种情况下，前置脚本将完成并且可能已创建快照。
  - 默认创建崩溃一致性快照 – 如果前置脚本运行失败，则选择此选项以默认创建崩溃一致性快照。如果未启用前置和后置脚本，则这是 Amazon Data Lifecycle Manager 的默认快照创建行为。如果您启用了重试，则只有在所有重试尝试都用尽之后，Amazon Data Lifecycle Manager 才会默认创建崩溃一致性快照。如果前置脚本失败并且您没有默认创建崩溃一致性快照，则 Amazon Data Lifecycle Manager 将不会在该计划运行期间为实例创建快照。

**Note**

如果您要为 SAP HANA 创建快照，则可能需要禁用此选项。无法以相同的方式还原 SAP HANA 工作负载的崩溃一致性快照。

9. 选择创建默认策略。

**Note**

如果发生 Role with name AWSDataLifecycleManagerDefaultRole already exists 错误，请参阅 [故障排除](#) 来了解更多信息。

## AWS CLI

## 创建快照生命周期策略

使用 [create-lifecycle-policy](#) 命令，并将 Scripts 参数包含在 CreateRule 中。有关参数的更多信息，请参阅 [Amazon Data Lifecycle Manager API Reference](#)。

```
$ aws dlm create-lifecycle-policy \  
--description "policy_description" \  
--state ENABLED \  
--execution-role-arn iam_role_arn \  
--policy-details file://policyDetails.json
```

其中 policyDetails.json 包含以下内容之一，具体取决于您的用例：

## • VSS 备份

```
{  
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
  "ResourceTypes": [  
    "INSTANCE"  
  ],  
  "TargetTags": [{  
    "Key": "tag_key",  
    "Value": "tag_value"  
  }],  
  "Schedules": [{  
    "Name": "schedule_name",  
    "CreateRule": {  
      "CronExpression": "cron_for_creation_frequency",  
      "Scripts": [{  
        "ExecutionHandler": "AWS_VSS_BACKUP",  
        "ExecuteOperationOnScriptFailure": true/false,  
        "MaximumRetryCount": retries (0-3)  
      }]  
    }  
  }]  
}
```

```

    },
    "RetainRule": {
      "Count": retention_count
    }
  ]
}

```

- SAP HANA 备份

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE", "POST"],
        "ExecutionHandlerService": "AWS_SYSTEMS_MANAGER",
        "ExecutionHandler": "AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA",
        "ExecuteOperationOnScriptFailure": true/false,
        "ExecutionTimeout": timeout_in_seconds (10-120),
        "MaximumRetryCount": retries (0-3)
      }
    ]
  },
  "RetainRule": {
    "Count": retention_count
  }
}
]
}

```

- 自定义 SSM 文档

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [

```

```

    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE","POST"],
        "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
        "ExecutionHandler":"ssm_document_name|arn",
        "ExecuteOperationOnScriptFailure":true/false,
        "ExecutionTimeout":timeout_in_seconds (10-120),
        "MaximumRetryCount":retries (0-3)
      }]
    },
    "RetainRule": {
      "Count": retention_count
    }
  }]
}

```

## 使用 Amazon Data Lifecycle Manager 进行 VSS 备份的注意事项

借助 Amazon Data Lifecycle Manager，您可以备份和还原在 Amazon EC2 实例上运行的启用 VSS（卷影复制服务）的 Windows 应用程序。如果应用程序已在 Windows VSS 中注册了 VSS 写入器，则 Amazon Data Lifecycle Manager 会为该应用程序创建具有应用程序一致性的快照。

### Note

Amazon Data Lifecycle Manager 目前仅支持在 Amazon EC2 上运行的资源的应用程序一致性快照，特别适用于可以通过将现有实例替换为从备份创建的新实例来还原应用程序数据的备份场景。并非所有实例类型或应用程序都支持 VSS 备份。有关更多信息，请参阅[什么是 AWS VSS？](#) 在 Amazon EC2 用户指南中。

## 不支持的实例类型

以下 Amazon EC2 实例类型不支持 VSS 备份。如果您的策略以这些实例类型之一为目标，则 Amazon Data Lifecycle Manager 可能仍会创建 VSS 备份，但快照可能不会使用所需的系统标签进行标记。没有这些标签，快照在创建后将无法由 Amazon Data Lifecycle Manager 进行管理。您可能需要手动删除这些快照。

- T3 : t3.nano | t3.micro
- T3a : t3a.nano | t3a.micro
- T2 : t2.nano | t2.micro

### 应用程序一致性快照的共同责任

您必须确保：

- SSM 代理已安装并在您的目标实例上运行 up-to-date
- Systems Manager 有权在目标实例上执行所需操作
- Amazon Data Lifecycle Manager 有权执行在目标实例上运行前置和后置脚本所需的 Systems Manager 操作。
- 对于自定义工作负载，例如自行管理的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库，您使用的 SSM 文档包含用于冻结、刷新和解冻 I/O 的正确和必需的操作。
- 快照创建时间与您的工作负载计划保持一致。例如，请尝试在计划的维护窗口期内安排快照创建。

Amazon Data Lifecycle Manager 应确保：

- 快照创建将在计划快照创建时间的 60 分钟内启动。
- 在启动快照创建之前运行前置脚本。
- 在前置脚本成功且快照创建已启动后运行前置脚本。只有在前置脚本成功的情况下，Amazon Data Lifecycle Manager 才会运行后置脚本。如果前置脚本失败，Amazon Data Lifecycle Manager 将不会运行后置脚本。
- 快照在创建时会用相应的标签进行标记。
- CloudWatch 当脚本启动时，以及脚本失败或成功时，都会发出指标和事件。

### 前置和后置脚本的其他用例

除了使用前置和后置脚本自动生成应用程序一致性快照外，您还可以同时或单独使用前置和后置脚本，在创建快照之前或之后自动执行其他管理任务。例如：



- 创建快照之前使用前置脚本来应用补丁。这可以帮助您在应用每周或每月定期软件更新后创建快照。

#### Note

如果您选择仅运行前置脚本，则默认情况下会启用默认创建崩溃一致性快照。

- 创建快照后使用后置脚本应用补丁。这可以帮助您在应用每周或每月定期软件更新之前创建快照。

## 其他用例入门

本节介绍将前置和/或后置脚本用于应用程序一致性快照以外的用例中时需要执行的步骤。

### 步骤 1：准备目标实例

为前置和/或后置脚本准备目标实例

1. 在目标实例上安装 SSM Agent ( 如果尚未安装 )。如果目标实例上已安装 SSM Agent，请跳过此步骤。
  - ( Linux 实例 ) [在适用于 Linux 的 Amazon EC2 实例上手动安装 SSM Agent](#)
  - ( Windows 实例 ) [在适用于 Windows 的 Amazon EC2 实例上手动安装 SSM Agent](#)
2. 确保 SSM Agent 正在运行。有关更多信息，请参阅[正在检查 SSM Agent 状态并启动代理](#)。
3. 为 Amazon EC2 实例设置 Systems Manager。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的[为 Amazon EC2 实例设置 Systems Manager](#)。

### 步骤 2：准备 SSM 文档

您必须创建一个 SSM 命令文档，其中包含要运行的命令的前置和/或后置脚本。

您可以使用下面的 SSM 文档空白模板创建 SSM 文档，并在相应的文档部分中添加前置和后置脚本命令。

#### 请注意以下几点：

- 您负责确保 SSM 文档为工作负载执行正确和必需的操作。
- SSM 文档必须包含 allowedValues 的必填字段，包括 pre-script、post-script 和 dry-run。Amazon Data Lifecycle Manager 将根据这些部分的内容在您的实例上执行命

令。如果您的 SSM 文档没有这些部分，则 Amazon Data Lifecycle Manager 会将其视为执行失败。

```
###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
  feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
    command:
      # Data Lifecycle Manager will trigger the pre-script and post-script actions during
policy execution.
      # 'dry-run' option is intended for validating the document execution without
triggering any commands
      # on the instance. The following allowedValues will allow Data Lifecycle Manager to
successfully
      # trigger pre and post script actions.
      type: String
      default: 'dry-run'
      description: (Required) Specifies whether pre-script and/or post-script should be
executed.
```

```

    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

###=====###
    ### Error Codes

###=====###
    # The following Error codes will inform Data Lifecycle Manager of the type of
error
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206

###=====###
    ### Global variables

###=====###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}

```

```
# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
```

### 步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色

#### Note

如果出现以下情况，则需要执行此步骤：

- 创建或更新使用自定义 IAM 角色的启用前置/后置脚本的快照策略。
- 使用命令行创建或更新使用默认值的启用前置/后置脚本的快照策略。

如果您使用控制台创建或更新启用脚本前/后脚本的快照策略，该策略使用默认角色管理快照 ( `AWSDataLifecycleManagerDefaultRole` )，请跳过此步骤。在这种情况下，我们会自动将 `AWSDataLifecycleManagerSSMFullAccess` 策略附加到该角色。

您必须确保用于策略的 IAM 角色授予 Amazon Data Lifecycle Manager 权限，以执行在策略作为目标的实例上运行前置和后置脚本所需的 SSM 操作的权限。

Amazon Data Lifecycle Manager 提供了包含所需权限的托管策略 (`AWSDataLifecycleManagerSSMFullAccess`)。您可以将此策略附加到您的 IAM 角色以管理快照，从而确保其包含这些权限。

#### Important

使用前脚本和后置脚本时，`AWSDataLifecycleManagerSSMFullAccess` 托管策略使用 `aws:ResourceTag` 条件键来限制对特定 SSM 文档的访问。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

或者，您可以手动创建自定义策略或将所需权限直接分配给您使用的 IAM 角色。您可以使用 `AWSDataLifecycleManagerSSMFullAccess` 托管策略中定义的同权限，但是，`aws:ResourceTag` 条件密钥是可选的。如果您决定不使用该条件键，则无需使用 `DLMScriptsAccess:true` 标记您的 SSM 文档。

使用以下方法之一将 `AWSDataLifecycleManagerSSMFullAccess` 策略添加到您的 IAM 角色。

#### Console

将托管策略附加到您的自定义角色

1. 通过 <https://console.aws.amazon.com/iam/> 打开 IAM 控制台。
2. 在导航面板中，选择 Roles ( 角色 )。
3. 搜索并选择用于管理快照的自定义角色。

4. 在权限选项卡上，选择添加权限、附加策略。
5. 搜索并选择AWSDataLifecycleManagerSSMFullAccess托管策略，然后选择添加权限。

## AWS CLI

将托管策略附加到您的自定义角色

使用 [attach-role-policy](#) 命令。对于 `---role-name`，请指定您自定义角色的名称。对于 `--policy-arn`，请指定 `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`。

```
$ aws iam attach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \  
--role-name your_role_name
```


## 创建快照生命周期策略

### Console

#### 创建快照生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：
  - a. 对于目标资源类型，请选择 Instance。
  - b. 对于目标资源标签，请指定识别要备份的实例的资源标签。仅备份具有指定标签的资源。
5. 对于 IAM 角色，可以选择 AWSDataLifecycleManagerDefaultRole (用于管理快照的默认角色)，也可以选择您创建并准备使用前脚本和发布脚本的自定义角色。
6. 根据需要配置计划和其他选项。我们建议您将快照创建时间计划在与您工作负载相匹配的时间段，例如在维护窗口期间。
7. 在前置和后置脚本部分中，选择启用前置和后置脚本，然后执行以下操作：
  - a. 选择自定义 SSM 文档。

- b. 对于自动化选项，请选择与要运行的脚本相匹配的选项。
  - c. 对于 SSM 文档，请选择您准备的 SSM 文档。
8. 如果需要，请配置以下其他选项：
- 脚本超时 – 如果脚本运行尝试尚未完成，则在此超时期间后，Amazon Data Lifecycle Manager 的尝试失败。如果脚本未在其超时期间内完成，Amazon Data Lifecycle Manager 的尝试失败。超时期间分别适用于前置和后置脚本。最小的默认超时期间为 10 秒。最长超时期间为 120 秒。
  - 重试失败的脚本 – 选择此选项可重试未在其超时期间内完成的脚本。如果前置脚本失败，则 Amazon Data Lifecycle Manager 会重试整个快照创建过程，包括运行前置和后置脚本。如果后置脚本失败，则 Amazon Data Lifecycle Manager 将仅重试后置脚本；在这种情况下，前置脚本将完成并且可能已创建快照。
  - 默认创建崩溃一致性快照 – 如果前置脚本运行失败，则选择此选项以默认创建崩溃一致性快照。如果未启用前置和后置脚本，则这是 Amazon Data Lifecycle Manager 的默认快照创建行为。如果您启用了重试，则只有在所有重试尝试都用尽之后，Amazon Data Lifecycle Manager 才会默认创建崩溃一致性快照。如果前置脚本失败并且您没有默认创建崩溃一致性快照，则 Amazon Data Lifecycle Manager 将不会在该计划运行期间为实例创建快照。
9. 选择创建默认策略。

 Note

如果发生 Role with name AWSDataLifecycleManagerDefaultRole already exists 错误，请参阅 [故障排除](#) 来了解更多信息。

## AWS CLI

### 创建快照生命周期策略

使用 [create-lifecycle-policy](#) 命令，并将 Scripts 参数包含在 CreateRule 中。有关参数的更多信息，请参阅 [Amazon Data Lifecycle Manager API Reference](#)。

```
$ aws dlm create-lifecycle-policy \  
--description "policy_description" \  
--state ENABLED \  
--execution-role-arn iam_role_arn \  
--policy-details file://policyDetails.json
```

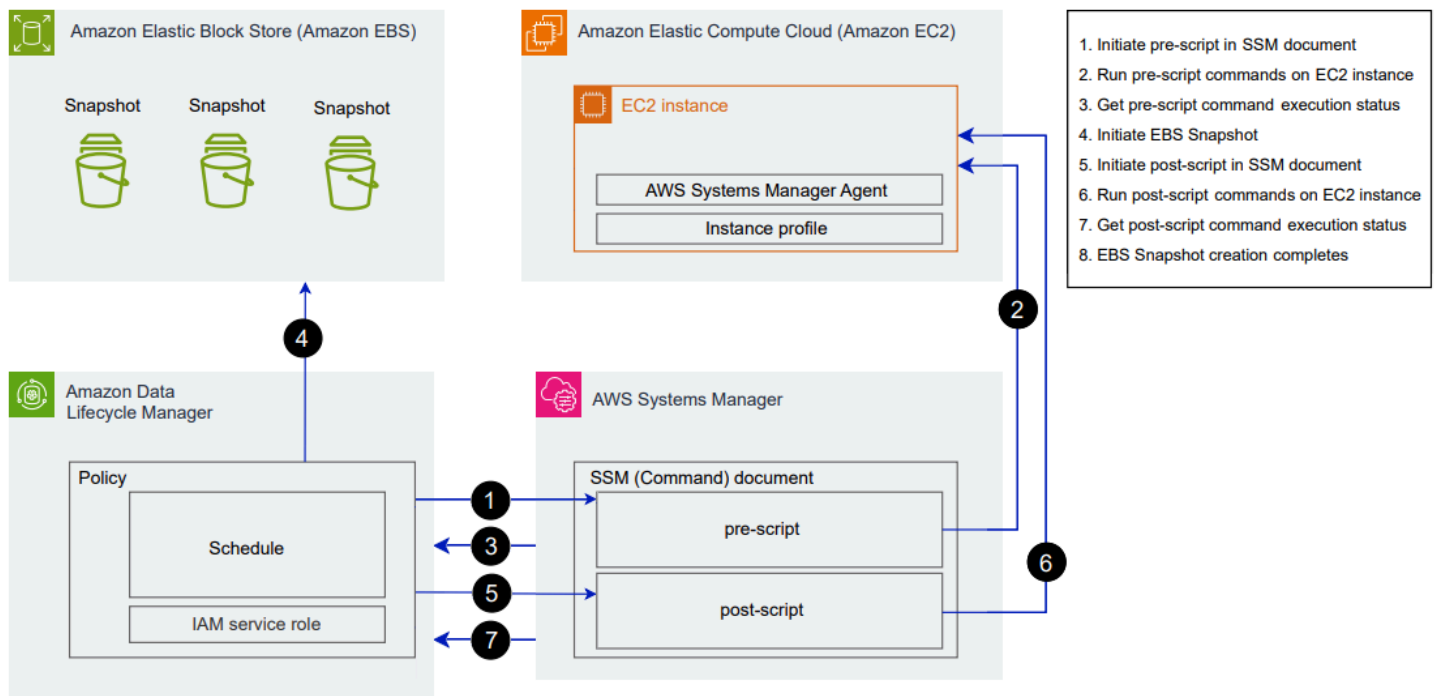
其中 `policyDetails.json` 包含以下内容。

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE" | "POST" | "PRE", "POST"],
        "ExecutionHandlerService": "AWS_SYSTEMS_MANAGER",
        "ExecutionHandler": "ssm_document_name|arn",
        "ExecuteOperationOnScriptFailure": true/false,
        "ExecutionTimeout": timeout_in_seconds (10-120),
        "MaximumRetryCount": retries (0-3)
      }]
    },
    "RetainRule": {
      "Count": retention_count
    }
  }]
}
```

## 前置和后置脚本的工作方式

下图显示了使用自定义 SSM 文档时前置和后置脚本的流程。这不适用于 VSS 备份。





在计划创建快照时，会发生以下操作和跨服务交互。

1. Amazon Data Lifecycle Manager 通过调用 SSM 文档并传递 pre-script 参数来启动前置脚本操作。

#### Note

只有在运行前置脚本时才会执行步骤 1 到 3。如果您仅运行后置脚本，则会跳过步骤 1 到 3。


2. Systems Manager 向在目标实例上运行的 SSM Agent 发送前置脚本命令。SSM Agent 在实例上运行命令，并将状态信息发送回 Systems Manager。

例如，如果使用 SSM 文档创建应用程序一致性快照，则前置脚本可能会冻结并刷新 I/O，以确保在拍摄快照之前将所有缓冲的数据写入卷。

3. Systems Manager 向 Amazon Data Lifecycle Manager 发送前置脚本命令状态更新。如果前置脚本失败，则 Amazon Data Lifecycle Manager 将执行以下操作之一，具体取决于您配置前置和后置脚本选项的方式：

重试	默认创建崩溃一致性快照	操作
已启用，剩余重试次数	已启用	重试脚本，直到脚本成功或重试次数用尽
次数用尽但未成功完成	已启用	创建崩溃一致性快照，且不运行后置脚本。
已启用，剩余重试次数	已禁用	重试脚本，直到脚本成功或重试次数用尽
次数用尽但未成功完成	已禁用	跳过为目标实例创建快照，且不运行后置脚本。
已禁用	已启用	创建崩溃一致性快照，且不运行后置脚本。
已禁用	已禁用	跳过为目标实例创建快照，且不运行后置脚本。

- Amazon Data Lifecycle Manager 启动快照创建。
- Amazon Data Lifecycle Manager 通过调用 SSM 文档并传递 `post-script` 参数来启动后置脚本操作。

 Note

只有在运行前置脚本时才会执行步骤 5 到 7。如果您仅运行后置脚本，则会跳过步骤 1 到 3。

- Systems Manager 向在目标实例上运行的 SSM Agent 发送后置脚本命令。SSM Agent 在实例上运行命令，并将状态信息发送回 Systems Manager。

例如，如果 SSM 文档启用了应用程序一致性快照，则此后置脚本可能会解冻 I/O，以确保您的数据库在拍摄快照后恢复正常 I/O 操作。

- 如果您运行后置脚本且 Systems Manager 指示该脚本已成功完成，则该过程完成。

如果后置脚本失败，则 Amazon Data Lifecycle Manager 将执行以下操作之一，具体取决于您配置前置和后置脚本选项的方式：

重试	操作
已启用，剩余重试次数	重试后置脚本，直到脚本成功或重试次数用尽
次数用尽，但未成功	跳过后置脚本
已禁用	跳过后置脚本

请记住，如果后置脚本失败，则前置脚本（如已启用）将成功完成，并且可能已创建快照。您可能需要对实例采取进一步操作以确保其按预期运行。例如，如果前置脚本暂停并刷新了 I/O，但后置脚本未能解冻 I/O，则可能需要将数据库配置为自动解冻 I/O，或者需要手动解冻 I/O。

8. 后置脚本完成后，快照创建过程可能会完成。完成快照所需的时间取决于快照的大小。

## 识别使用前置和后置脚本创建的快照

Amazon Data Lifecycle Manager 会自动为使用前置和后置脚本创建的快照分配以下系统标签。

- 密钥：aws:dlm:pre-script；值：SUCCESS|FAILED

标签值为 SUCCESS 表示前置脚本已成功执行。标签值为 FAILED 表示前置脚本未成功执行。

- 密钥：aws:dlm:post-script；值：SUCCESS|FAILED

标签值为 SUCCESS 表示后置脚本已成功执行。标签值为 FAILED 表示后置脚本未成功执行。

对于自定义 SSM 文档和 SAP HANA 备份，如果快照同时用 aws:dlm:pre-script:SUCCESS 和 aws:dlm:post-script:SUCCESS 标记，则可以推断成功创建了应用程序一致性快照。

此外，使用 VSS 备份创建的应用程序一致性快照会自动标记：

- 密钥：AppConsistent tag；值：true|false

标签值为 true 表示 VSS 备份成功且快照具有应用程序一致性。标签值为 false 表示 VSS 备份未成功，并且快照不符合应用程序一致性。

## 监控前置和后置脚本的执行情况

亚马逊 CloudWatch 指标

Amazon Data Lifecycle Manager 会在前脚本和后脚本失败和成功以及 VSS 备份失败和成功时发布以下 CloudWatch 指标。

- PreScriptStarted
- PreScriptCompleted
- PreScriptFailed
- PostScriptStarted
- PostScriptCompleted
- PostScriptFailed
- VSSBackupStarted
- VSSBackupCompleted
- VSSBackupFailed

有关更多信息，请参阅 [使用 Amazon 监控您的政策 CloudWatch](#)。

## 亚马逊 EventBridge

当前脚本或后脚本启动、成功或失败时，Amazon Data Lifecycle Manager 会发出以下亚马逊 EventBridge 事件

- DLM Pre Post Script Notification

有关更多信息，请参阅 [使用“CloudWatch 事件”监控您的政策](#)。

## 自动化 AMI 生命周期

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 EBS 支持的 AMI 生命周期。

### 主题

- [创建 AMI 生命周期策略](#)
- [AMI 生命周期策略的注意事项](#)
- [其他资源](#)

## 创建 AMI 生命周期策略

使用以下程序之一创建 AMI 生命周期策略。

## Console

### 创建 AMI 策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面，选择 EBS 支持的 AMI 策略，然后选择下一步。
4. 在目标资源部分，对于目标资源标签，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。
5. 对于 Description (描述)，输入策略的简短描述。
6. 对于 IAM 角色，选择一个有权管理 AMI 和快照以及描述实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色，请选择默认角色。或者，要使用您之前创建的自定义 IAM 角色，请选择选择其他角色，然后选择要使用的角色。
7. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
8. 对于创建后的策略状态，选择启用策略，以在下次计划时间启动策略运行，或者选择禁用策略，以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始创建 AMI。
9. 在实例重启部分中，指明是否在创建 AMI 之前重启实例。为了防止目标实例重启，请选择否。选择否可能会导致数据一致性问题。要在创建 AMI 之前重启实例，请选择是。选择此选项可确保数据一致性，但可能导致多个目标实例同时重新启动。
10. 选择下一步。
11. 在 Configure schedule (配置计划) 页面配置策略计划。一个策略最多可以有四个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：
  - a. 在计划详细信息部分中，执行以下操作：
    - i. 对于计划名称，请指定计划的描述性名称。
    - ii. 在频率和相关字段中配置策略运行之间的间隔。


您可以按每日、每周、每月或每年计划配置策略运行。或者，选择自定义 cron 表达式以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon Ev CloudWatch ents 用户指南中的 [Cron 表达式](#)。

- iii. 对于开始时间，请指定策略开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。您必须输入 hh:mm UTC 格式的时间。
- iv. 对于保留类型，请指定计划创建的 AMI 的保留策略。

您可以根据其总计数或存在时间保留 AMI。

对于基于计数的保留，范围为 1 到 1000。在达到最大计数后，将在创建新 AMI 时注销最早 AMI。

对于基于存在时间的保留，范围是 1 天到 100 年。在每个 AMI 的保留期限过期后，会将其注销。

 Note

所有计划必须具有相同的保留类型。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。

b. 配置 AMI 标签。

请在 Tagging (标记) 部分执行以下操作：

- i. 要将所有用户定义的标签从源实例复制到计划创建的 AMI，请选择从源中复制标签。
- ii. 默认情况下，计划创建的 AMI 会自动标记为源实例的 ID。要防止发生此自动标记，请在变量标签中，删除 `instance-id:$(instance-id)` 平铺。
- iii. 要指定分配给由该计划创建的 AMI 的其他标签，请选择添加标签。

c. 配置 AMI 弃用。

要在不应再使用 AMI 时将其弃用，请在 AMI deprecation (AMI 弃用) 部分选择 Enable AMI deprecation for this schedule (为此计划启用 AMI 弃用)，然后指定 AMI 弃用规则。AMI 弃用规则指定何时弃用 AMI。

如果计划使用基于计数的 AMI 保留，您必须指定要弃用的最早 AMI 的数量。弃用计数必须小于或等于计划的 AMI 保留计数，并且不能大于 1000。例如，如果计划配置为最多保留 5 个 AMI，则可以将计划配置为弃用最多 5 个最早的 AMI。

如果计划使用基于存在时间的 AMI 保留，则必须指定弃用 AMI 的期限。弃用计数必须小于或等于计划的 AMI 保留期限，并且不能超过 10 年 (120 个月、520 周或 3650 天)。


例如，如果计划配置为将 AMI 保留 10 天，则可以将计划配置为在创建后最多 10 天的期限后弃用 AMI。

d. 配置跨区域复制。

要将计划创建的 AMI 复制到其他区域，请在跨区域复制部分中选择启用跨区域复制。您可以将 AMI 复制到账户中最多三个其他区域。您必须为每个目标区域指定单独的跨区域复制规则。

对于每个目标地区，您可以指定以下内容：

- AMI 副本的保留策略。保留期限过期后，将自动取消注册目标区域中的副本。
- AMI 副本的加密状态。如果源 AMI 已加密或预设情况下启用加密，则会始终加密复制的 AMI。如果源 AMI 未加密，并且预设情况下禁用加密，则您可以选择启用加密。如果未指定 KMS 密钥，则会在每个目标区域中使用 EBS 加密的默认 KMS 密钥对 AMI 进行加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥的访问权限。
- AMI 副本的弃用规则。当弃用期限过期时，将自动弃用 AMI 副本。弃用期限必须小于或等于副本保留期限，并且不能超过 10 年。
- 是从源 AMI 复制所有标签还是不复制标签。


 Note

请勿超过每个区域的并发 AMI 副本数。

e. 要添加其他计划，请选择位于页面顶部的 Add another schedule (添加其他计划)。每个其他计划请按照本主题之前所述填写字段。

f. 添加所需计划之后，请选择查看策略。

12. 查看策略摘要，然后选择创建策略。

 Note

如果发生 Role with name  
AWSDataLifecycleManagerDefaultRoleForAMIManagement already  
exists 错误，请参阅 [故障排除](#) 来了解更多信息。

## Command line

可使用 [create-lifecycle-policy](#) 命令创建 AMI 生命周期策略。对于 PolicyType，请指定 IMAGE\_MANAGEMENT。

### Note

为简化语法，以下示例使用包含策略详细信息的 JSON 文件 `policyDetails.json`。

### 示例 1：基于存在时间的保留和 AMI 弃用

此示例创建的 AMI 生命周期策略可在不重新启动目标实例的情况下创建标签键 `purpose` 的值为 `production` 的所有实例的 AMI。该策略包括一个每天可在 UTC 01:00 创建 AMI 的计划。该策略保留 AMI 2 天，并在 1 天后弃用。还会将标签从源实例复制到其创建的 AMI。

```
aws dlm create-lifecycle-policy \  
  --description "My AMI policy" \  
  --state ENABLED \  
  --execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \  
  --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{  
  "PolicyType": "IMAGE_MANAGEMENT",  
  "ResourceTypes": [  
    "INSTANCE"  
  ],  
  "TargetTags": [{  
    "Key": "purpose",  
    "Value": "production"  
  }],  
  "Schedules": [{  
    "Name": "DailyAMIs",  
    "TagsToAdd": [{  
      "Key": "type",  
      "Value": "myDailyAMI"  
    }],  
    "CreateRule": {
```



```

        "Interval": 24,
        "IntervalUnit": "HOURS",
        "Times": [
            "01:00"
        ]
    },
    "RetainRule":{
        "Interval" : 2,
        "IntervalUnit" : "DAYS"
    },
    "DeprecateRule": {
        "Interval" : 1,
        "IntervalUnit" : "DAYS"
    },
    "CopyTags": true
}
],
"Parameters" : {
    "NoReboot":true
}
}

```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```

{
  "PolicyId": "policy-9876543210abcdef0"
}

```

## 示例 2：基于计数的保留和使用跨区域复制的 AMI 弃用

此示例创建的 AMI 生命周期策略可创建标签键 `purpose` 的值为 `production` 的所有实例的 AMI，并重新启动目标实例。该策略包括一个可在 UTC 17:30 起每 6 小时创建 AMI 的计划。该策略保留 3 AMI 并自动弃用 2 最早的 AMI。它具有跨区域复制规则，该规则会将 AMI 复制到 `us-east-1`，保留 2 AMI 副本，并自动弃用最早的 AMI。

```

aws dlm create-lifecycle-policy \
  --description "My AMI policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
  --policy-details file://policyDetails.json

```

以下是 policyDetails.json 文件的示例。

```
{
  "PolicyType": "IMAGE_MANAGEMENT",
  "ResourceTypes" : [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key":"purpose",
    "Value":"production"
  }],
  "Parameters" : {
    "NoReboot": true
  },
  "Schedules" : [{
    "Name" : "Schedule1",
    "CopyTags": true,
    "CreateRule" : {
      "Interval": 6,
      "IntervalUnit": "HOURS",
      "Times" : ["17:30"]
    },
    "RetainRule":{
      "Count" : 3
    },
    "DeprecateRule":{
      "Count" : 2
    },
    "CrossRegionCopyRules": [{
      "TargetRegion": "us-east-1",
      "Encrypted": true,
      "RetainRule":{
        "IntervalUnit": "DAYS",
        "Interval": 2
      },
      "DeprecateRule":{
        "IntervalUnit": "DAYS",
        "Interval": 1
      },
      "CopyTags": true
    }
  ]
}]
}
```

## AMI 生命周期策略的注意事项

创建 AMI 生命周期策略时应注意以下一般注意事项：

- AMI 生命周期策略仅针对与策略位于同一区域的实例。
- 第一个 AMI 创建操作将在指定开始时间之后的一小时内启动。后续 AMI 创建操作将在计划时间的一小时内开始。
- 当 Amazon Data Lifecycle Manager 注销 AMI 时，它会自动删除其支持的快照。
- 目标资源标签区分大小写。
- 如果从策略所针对的实例中删除目标标签，则 Amazon Data Lifecycle Manager 不再管理标准中的现有 AMI；如不再需要，您必须手动将其删除。
- 您可以创建多个策略来备份实例。例如，假设一个实例有两个标签，其中标签 A 是每 12 小时创建一个 AMI 的策略 A 的目标，标签 B 是每 24 小时创建一个 AMI 的策略 B 的目标，则 Amazon Data Lifecycle Manager 将根据这两个策略的计划创建 AMI。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 在下次运行策略时，备份中将自动包含在创建策略后挂载到目标实例的新卷。策略运行时挂载到实例的所有卷都包括在内。
- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个 AMI，则该策略不会在达到保留阈值时自动注销该 AMI。如果不再需要该 AMI，则必须手动将其注销。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一个 AMI，直到创建下一个 AMI。例如，如果基于存在时间的策略每月创建一个 AMI，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个 AMI 保留一个月，即使保留期为七天。
- 对于基于计数的策略，Amazon Data Lifecycle Manager 在尝试根据保留策略取消注册最旧的 AMI 之前，始终根据创建频率创建 AMI。
- 成功取消注册 AMI 并删除其关联的备份快照可能需要几小时。如果 Amazon Data Lifecycle Manager 在之前创建的 AMI 成功取消注册之前创建了下一个 AMI，则您可以临时保留一些大于保留次数的 AMI。

终止策略针对的实例时应注意以下注意事项：

- 如果您终止某个策略按照基于计数的保留计划针对的实例，则该策略将不再管理以前从已终止的实例创建的 AMI。如果不再需要较早版本的 AMI，您必须手动将其注销。

- 如果您终止某个策略按照基于存在时间的保留计划针对的实例，则该策略将继续按照原定计划取消注册之前从已终止的实例创建的 AMI，直至（但不包括）最后一个 AMI。如果不再需要最后一个 AMI，则必须手动将其注销。

AMI 策略和 AMI 弃用应注意以下事项：

- 如果您针对具有基于计数的保留的计划增加 AMI 弃用计数，则更改将应用于该计划创建的所有 AMI（现有 AMI 和新 AMI）。
- 如果您针对具有基于存在时间的保留的计划增加 AMI 弃用期限，则更改仅应用于新 AMI。现有 AMI 不受影响。
- 如果您从计划中删除 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将不会取消该计划之前弃用的 AMI 弃用。
- 如果您要减少计划的 AMI 弃用计数或期限，则 Amazon Data Lifecycle Manager 将不会取消该计划之前弃用的 AMI 弃用。
- 如果您手动弃用由 AMI 策略创建的 AMI，则 Amazon Data Lifecycle Manager 将不会覆盖弃用操作。
- 如果您手动取消之前已被 AMI 策略弃用的 AMI 的弃用，则 Amazon Data Lifecycle Manager 将不会覆盖取消操作。
- 如果 AMI 由多个冲突的计划创建，并且其中一个或多个计划没有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将不会弃用该 AMI。
- 如果 AMI 由多个相互冲突的计划创建，并且其中所有计划都有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将会使用导致最新弃用日期的弃用规则。

以下注意事项适用于 AMI 策略和[回收站](#)：

- 如果 Amazon Data Lifecycle Manager 注销 AMI 并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原 AMI，则必须在不再需要该 AMI 时手动注销 AMI。Amazon Data Lifecycle Manager 将不再管理该 AMI。
- 如果您手动注销由策略创建的 AMI，并且该 AMI 在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会注销该 AMI。当 AMI 在回收站中时，Amazon Data Lifecycle Manager 不管理 AMI。

如果在达到策略的保留阈值之前从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将在达到策略的保留阈值时注销 AMI。

如果在达到策略的保留阈值之后从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将不再注销 AMI。如果不再需要 AMI，则必须手动将其删除。

以下注意事项适用于处于错误状态的 AMI 策略：

- 对于具有基于存在时间的保留计划的策略，则设置为在策略处于 error 状态时过期的 AMI 将无限期保留。您必须手动取消注册 AMI。重新启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时恢复取消注册 AMI。
- 对于具有基于计数的保留计划的策略，策略会在其处于 error 状态时停止创建和取消注册 AMI。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建 AMI，并在达到保留阈值时恢复取消注册 AMI。

以下注意事项适用于 AMI 策略和[禁用 AMI](#)：

- 如果您禁用了 Amazon Data Lifecycle Manager 创建的 AMI，并且在达到其保留阈值时该 AMI 被禁用，则 Amazon Data Lifecycle Manager 将注销该 AMI 并删除其关联的快照。
- 如果您禁用了 Amazon Data Lifecycle Manager 创建的 AMI，并手动归档了其关联的快照，并且这些快照在达到保留阈值时处于已归档状态，则 Amazon Data Lifecycle Manager 将不会删除这些快照，也不会再对其进行管理。

以下注意事项适用于 AMI 策略和[AMI 注销注册保护](#)：

- 如果您为由亚马逊数据生命周期管理器创建的 AMI 手动启用注销保护，并且在达到 AMI 保留阈值时该保护仍处于启用状态，则亚马逊数据生命周期管理器将不再管理该 AMI。如果不再需要，则必须手动注销 AMI 并删除其底层快照。

## 其他资源

有关更多信息，请参阅[使用 Amazon Data Lifecycle Manager AWS 存储自动化 Amazon EBS 快照和 AMI 管理](#)博客。

## 自动执行跨账户快照副本

通过自动执行跨账户快照副本，您可以将 Amazon EBS 快照复制到隔离账户中的特定区域，并使用加密密钥对这些快照进行加密。这样，您能够在账户遭到泄露时防止自己的数据丢失。

自动执行跨账户快照副本涉及两个账户：

- 源账户 – 源账户是创建快照并与目标账户共享快照的账户。在此账户中，您必须创建一个 EBS 快照策略，该策略以设定的时间间隔创建快照，然后与其他 AWS 账户共享。
- 目标账户 – 目标账户是与之共享快照的目标账户，它也是创建共享快照副本的账户。在此账户中，您必须创建跨账户复制事件策略，以自动复制由一个或多个指定源账户共享的快照。

主题

- [创建跨账户快照复制策略](#)
- [指定快照描述筛选条件](#)
- [跨账户快照复制策略的注意事项](#)
- [其他资源](#)

## 创建跨账户快照复制策略

要为跨账户快照复制准备源账户和目标账户，您需要执行以下步骤：

步骤 1：创建 EBS 快照策略（源账户）

在源账户中，创建一个 EBS 快照策略，该策略将创建快照并与所需的目标账户共享。

创建策略时，请确保启用跨账户共享，并指定要与之共享快照的目标 AWS 账户。这些是您要与之共享快照的账户。如果您要共享加密快照，则必须授予所选目标账户使用用于加密源卷的 KMS 密钥的权限。有关更多信息，请参阅 [步骤 2：共享客户托管密钥（源账户）](#)。

### Note

您只能共享未加密的快照或使用客户托管密钥加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [允许其他账户中的用户使用 KMS 密钥](#)。

有关手动创建 EBS 快照策略的更多信息，请参阅 [自动化快照生命周期](#)。

使用以下方法之一创建 EBS 快照策略。

## 步骤 2：共享客户托管密钥（源账户）

如果您要共享加密快照，则必须授予 IAM 角色和（您在上一步中选择的）目标 AWS 账户使用用于加密源卷的客户托管密钥的权限。

### Note

仅在共享加密快照时执行此步骤。如果您正在共享的是未加密快照，请跳过此步骤。

## Console

1. 打开 AWS KMS 控制台，[网址为 https://console.aws.amazon.com/kms](https://console.aws.amazon.com/kms)。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥，然后选择您需要与目标账户共享的 KMS 密钥。

记下 KMS 密钥 ARN，稍后您将用到它。

4. 在密钥策略选项卡上，向下滚动到密钥用户部分。选择添加，输入您在上一步中选择的 IAM 角色的名称，然后选择添加。
5. 在密钥策略选项卡上，向下滚动到其他 AWS 账户部分。选择“添加其他 AWS 帐户”，然后添加您在上一步中选择与之共享快照的所有目标 AWS 帐户。
6. 选择保存更改。

## Command line

使用 `get-key-policy` 命令检索当前附加到 KMS 密钥的密钥策略。

例如，以下命令检索 ID 为 `9d5e2b3d-e410-4a27-a958-19e220d83a1e` 的 KMS 密钥的密钥策略，并将其写入名为 `snapshotKey.json` 的文件。

```
$ aws kms get-key-policy \
  --policy-name default \
  --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
  --query Policy \
  --output text > snapshotKey.json
```

使用首选文本编辑器打开密钥策略。添加您在创建快照策略时指定的 IAM 角色的 ARN 以及要与之共享 KMS 密钥的目标账户的 ARN。

例如，在以下策略中，我们添加了默认 IAM 角色的 ARN 以及目标账户 222222222222. 的根账户的 ARN

 Tip

为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用 kms:GrantIsForAWSResource 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
  "Sid" : "Allow use of the key",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : [
      "arn:aws:iam::111111111111:role/service-role/AWSDataLifecycleManagerDefaultRole",
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action" : [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Allow attachment of persistent resources",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : [
      "arn:aws:iam::111111111111:role/service-role/AWSDataLifecycleManagerDefaultRole",
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action" : [
    "kms:CreateGrant",
    "kms:ListGrants",
```



```

    "kms:RevokeGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
}

```

保存并关闭 文件。然后使用 `put-key-policy` 命令将更新后的密钥策略附加到 KMS 密钥。

```

$ aws kms put-key-policy \
  --policy-name default \
  --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
  --policy file://snapshotKey.json

```

### 第 3 步：创建跨账户复制事件策略（目标账户）

在目标账户中，您必须创建跨账户复制事件策略，该策略将自动复制由所需源账户共享的快照。

只有当指定的源账户之一与该账户共享快照时，此策略才会在目标账户中运行。

使用以下方法之一创建跨账户复制事件策略。

#### Console

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager，然后选择创建生命周期策略。
3. 在选择策略类型屏幕上，选择跨账户复制事件策略，然后选择下一步。
4. 对于策略描述，输入策略的简短描述。
5. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
6. 在事件设置部分中，定义将导致策略运行的快照共享事件。执行以下操作：
  - a. 对于共享帐户，请指定要从中复制共享快照的源 AWS 帐户。选择“添加账户”，输入 12 位数的 AWS 帐户 ID，然后选择“添加”。

- b. 对于按描述筛选，请使用正则表达式输入所需的快照描述。该策略仅复制由指定源账户共享且其描述与指定筛选条件匹配的快照。有关更多信息，请参阅[指定快照描述筛选条件](#)。
7. 对于 IAM 角色，请选择有权执行快照复制操作的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择 Default role (默认角色)。或者，要使用您之前创建的自定义 IAM 角色，请选择 Choose another role (选择其他角色)，然后选择要使用的角色。

如果您要复制加密快照，您必须授予所选 IAM 角色使用用于加密源卷的加密 KMS 密钥 的权限。同样，如果您使用不同的 KMS 密钥 对目标区域中的快照进行加密，则必须授予 IAM 角色使用目标 KMS 密钥 的权限。有关更多信息，请参阅[步骤 4：允许 IAM 角色使用所需的 KMS 密钥 \(目标账户\)](#)。

8. 在复制操作部分中，定义激活策略时应执行的快照复制操作。该策略最多可以将快照复制到三个区域。您必须为每个目标区域指定单独的复制规则。对要添加的每个规则执行以下操作：
  - a. 对于名称，为复制操作输入一个描述性名称。
  - b. 对于目标区域，选择要将快照复制到的区域。
  - c. 对于过期，请指定快照副本创建之后在目标区域中保留多长时间。
  - d. 要加密快照副本，请在加密中选择启用加密。如果源快照已加密，或者预设情况下为您的账户启用了加密，则快照副本将始终加密，即使您在此处没有启用加密也一样。如果源快照未加密，并且默认情况下未为您的账户启用加密，则您可以选择启用或禁用加密。如果启用了加密但未指定 KMS 密钥，则快照在每个目标区域中都将使用默认加密 KMS 密钥 进行加密。如果您为目标区域指定 KMS 密钥，则您必须具有对 KMS 密钥 的访问权限。
9. 要添加其他快照复制操作，请选择添加新区域。
10. 对于创建后的策略状态，选择启用策略，以在下次计划时间启动策略运行，或者选择禁用策略，以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始复制快照。
11. 选择 Create policy。

## Command line

使用 [create-lifecycle-policy](#) 命令创建策略。要创建跨账户复制事件策略，请为 PolicyType 指定 EVENT\_BASED\_POLICY。

例如，以下命令可在目标账户 222222222222 中创建跨账户复制事件策略。该策略会复制由源账户 111111111111 共享的快照。该策略将快照复制到 sa-east-1 和 eu-west-2。复制到 sa-east-1 的快照未加密，它们将保留 3 天。复制到 eu-west-2 的快照使用 KMS 密钥

8af79514-350d-4c52-bac8-8985e84171c7 进行加密，它们将保留 1 个月。该策略使用默认 IAM 角色。

```
$ aws dlm create-lifecycle-policy \  
  --description "Copy policy" \  
  --state ENABLED \  
  --execution-role-arn arn:aws:iam::222222222222:role/service-role/  
AWSDataLifecycleManagerDefaultRole \  
  --policy-details file://policyDetails.json
```

下面显示的是 policyDetails.json 文件的内容。

```
{  
  "PolicyType" : "EVENT_BASED_POLICY",  
  "EventSource" : {  
    "Type" : "MANAGED_CWE",  
    "Parameters": {  
      "EventType" : "shareSnapshot",  
      "SnapshotOwner": ["111111111111"]  
    }  
  },  
  "Actions" : [{  
    "Name" : "Copy Snapshot to Sao Paulo and London",  
    "CrossRegionCopy" : [{  
      "Target" : "sa-east-1",  
      "EncryptionConfiguration" : {  
        "Encrypted" : false  
      },  
      "RetainRule" : {  
        "Interval" : 3,  
        "IntervalUnit" : "DAYS"  
      }  
    },  
    {  
      "Target" : "eu-west-2",  
      "EncryptionConfiguration" : {  
        "Encrypted" : true,  
        "CmkArn" : "arn:aws:kms:eu-west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"  
      },  
      "RetainRule" : {  
        "Interval" : 1,  
        "IntervalUnit" : "MONTHS"  
      }  
    }  
  ]  
}
```

```
    }  
  }]  
}]  
}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{  
  "PolicyId": "policy-9876543210abcdef0"  
}
```

#### 步骤 4：允许 IAM 角色使用所需的 KMS 密钥（目标账户）

如果您要复制加密快照，则必须授予（您在上一步中选择的）IAM 角色使用用于加密源卷的 客户托管密钥 的权限。

#### Note

仅在复制加密快照时执行此步骤。如果您要复制的是未加密快照，请跳过此步骤。

使用以下方法之一将所需策略添加到 IAM 角色。

#### Console

1. 通过 <https://console.aws.amazon.com/iam/> 打开 IAM 控制台。
2. 在导航窗格中，选择角色。搜索并选择您在在上一步中创建跨账户复制事件策略时选择的 IAM 角色。如果您选择使用默认角色，则该角色的名称为 `AWSDataLifecycleManagerDefaultRole`。
3. 选择添加内联策略，然后选择 JSON 选项卡。
4. 将现有策略替换为以下内容，然后指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

#### Note

如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

 Tip

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。相反，使用 `kms:GrantIsForAWSResource` 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
      ]
    }
  ]
}
```

```

        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
      ]
    }
  ]
}

```

5. 选择查看策略
6. 对于名称，为策略输入描述性名称，然后选择创建策略。

## Command line

使用首选文本编辑器，创建一个名为 `policyDetails.json` 的新 JSON 文件。添加以下策略并指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

### Note

如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

### Tip

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。相反，使用 `kms:GrantIsForAWSResource` 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```

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

```

```

    "Effect": "Allow",
    "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
    ],
    "Resource": [
        "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ],
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ]
}
]
}

```

保存并关闭文件。然后使用 `put-role-policy` 命令将策略添加到 IAM 角色。

例如

```

$ aws iam put-role-policy \
  --role-name AWSDataLifecycleManagerDefaultRole \
  --policy-name CopyPolicy \

```

```
--policy-document file://AdminPolicy.json
```

## 指定快照描述筛选条件

在目标账户中创建快照复制策略时，必须指定快照描述筛选条件。通过快照描述筛选条件，您可指定额外的筛选级别，从而控制策略应复制哪些快照。这意味着只有当快照由指定源账户之一共享，并且其快照描述与指定筛选条件匹配时，策略才会复制该快照。换句话说，如果快照由指定源账户之一共享，但其描述不符合指定的筛选条件，则策略不会复制该快照。

必须使用正则表达式指定快照描述筛选条件。使用控制台和命令行创建跨账户复制事件策略时，它是必填字段。下面是可以使用的示例正则表达式：

- `.*` – 此筛选条件匹配所有快照描述。如果使用此表达式，该策略将复制由指定源账户之一共享的所有快照。
- `Created for policy: policy-0123456789abcdef0.*` – 此筛选条件仅匹配由 ID 为 `policy-0123456789abcdef0` 的策略创建的快照。`policy-0123456789abcdef0` 如果您使用类似这样的表达式，则该策略仅复制由指定源账户之一与您的账户共享以及由具有指定 ID 的策略创建的快照。
- `.*production.*` – 此筛选条件匹配描述中任意位置包含词语 `production` 的任何快照。如果使用此表达式，该策略将复制由指定源账户之一共享且描述中包含指定文本的所有快照。

## 跨账户快照复制策略的注意事项

跨账户复制事件策略时需考虑以下事项：

- 您只能复制未加密的快照或使用 客户托管密钥 加密的快照。
- 您可以创建跨账户复制事件策略，用于复制在 Amazon Data Lifecycle Manager 外部共享的快照。
- 如果要加密目标账户中的快照，则为跨账户复制事件策略选择的 IAM 角色必须拥有使用所需 KMS 密钥 的权限。

## 其他资源

有关更多信息，请参阅[跨 AWS 账户 AWS 存储自动复制加密的 Amazon EBS 快照](#)博客。

## 查看、修改和删除生命周期策略

使用以下程序查看、修改和删除现有生命周期策略。



## 主题

- [查看生命周期策略](#)
- [修改生命周期策略](#)
- [删除生命周期策略](#)

## 查看生命周期策略

使用以下程序之一查看生命周期策略。

### Console

#### 查看生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略的 ID。

### Command line

获取有关生命周期策略的摘要信息

使用 [get-lifecycle-policies](#) 命令。

```
aws dlm get-lifecycle-policies
```

显示有关特定生命周期策略的信息

使用 [get-lifecycle-policy](#) 命令。对于 `--policy-id`，请指定要查看的策略的 ID。

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

## 修改生命周期策略

### 修改策略的注意事项

- 如果您通过删除其目标标签来修改了 AMI 或快照策略，则具有这些标签的卷或实例将不再受此策略管理。

- 如果您修改了计划的名称，则使用旧计划名称创建的快照或 AMI 将不再由此策略管理。
- 如果您修改了基于存在时间的保留计划以使用新的时间间隔，则新间隔仅适用于在更改之后创建的新快照或 AMI。新计划不影响更改之前创建的快照或 AMI 的保留计划。
- 创建后，您无法将策略的保留计划从基于计数更改为基于存在时间。要进行该更改，您必须创建新的策略。
- 如果您禁用了其保留计划基于存在时间的策略，则设置为在禁用策略期间过期的快照或 AMI 将无限期地保留。您必须删除快照或手动注销 AMI。再次启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时继续删除快照或取消注册 AMI。
- 如果您禁用了具有基于计数的保留计划的策略，则该策略将停止创建和删除快照或 AMI。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建快照和 AMI，并在达到保留阈值时恢复删除快照或 AMI。
- 如果您禁用了某个具有已启用快照存档策略的策略，则禁用该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您按某个基于计数的计划启用了快照存档，则存档规则适用于由该计划创建和存档的所有新快照，也适用于之前由该计划创建和存档的现有快照。
- 如果您按某个基于期限的计划启用了快照存档，则存档规则仅适用于启用快照存档后创建的新快照。对于在启用快照存档之前创建的现有快照，将继续根据最初创建和存档快照时设定的计划，从各自的存储层中删除。
- 如果您为某个基于计数的计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。
- 如果您为某个基于期限的计划禁用了快照存档，则由该策略创建并计划存档的快照将在 `aws:dLM:expirationTime` 系统标签注明发原定存档日期和时间永久删除。
- 如果您为某个计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。
- 如果您为基于计数的计划修改了存档保留计数，则新的保留计数将包括之前由该计划存档的现有快照。
- 如果您为基于期限的计划修改了存档保留期，则新的保留期仅适用于修改保留规则后存档的快照。

使用以下程序之一修改生命周期策略。

## Console

### 修改生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择操作，然后选择修改生命周期策略。
5. 根据需要，修改策略设置。例如，您可以修改计划，添加或删除标签，或者启用或禁用策略。
6. 选择修改策略。

## Command line

可使用 [update-lifecycle-policy](#) 命令来修改生命周期策略中的信息。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetailsUpdated.json`。

```
aws dlm update-lifecycle-policy \  
  --state DISABLED \  
  --execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \  
  --policy-details file://policyDetailsUpdated.json
```

以下是 `policyDetailsUpdated.json` 文件的示例。

```
{  
  "ResourceTypes": [  
    "VOLUME"  
  ],  
  "TargetTags": [  
    {  
      "Key": "costcenter",  
      "Value": "120"  
    }  
  ],  
  "Schedules": [  
    {  
      "Name": "DailySnapshots",  
      "TagsToAdd": [  
        {  
          "Key": "type",  
          "Value": "myDailySnapshot"  
        }  
      ],  
      "CreateRule": {  
        "Interval": 12,
```

```
        "IntervalUnit": "HOURS",
        "Times": [
            "15:00"
        ]
    },
    "RetainRule": {
        "Count" :5
    },
    "CopyTags": false
}
]
```

要查看更新后的策略，请使用 `get-lifecycle-policy` 命令。您可以看到更改了状态、标签的值、快照时间间隔和快照开始时间。

## 删除生命周期策略

### 修改策略的注意事项

- 如果您删除了某个策略，则该策略创建的快照或 AMI 不会自动删除。如果您不再需要快照或 AMI，则必须手动将其删除。
- 如果您删除了某个具有已启用快照存档策略的策略，则删除该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您删除了某个策略，并且该策略具有已启用存档并且基于期限的计划，则由该策略创建并计划存档的快照将在 `aws:dlm:expirationtime` 系统标签注明发原定存档日期和时间永久删除。

使用以下程序之一删除生命周期策略。

### Console

#### 删除生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择操作，然后选择删除生命周期策略。
5. 在提示确认时，选择删除策略。

## Command line

可使用 [delete-lifecycle-policy](#) 命令来删除生命周期策略并释放策略中指定的目标标签以供重复使用。

### Note

您可以仅删除由 Amazon Data Lifecycle Manager 创建的快照。

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

[Amazon Data Lifecycle Manager API 参考](#)提供了 Amazon Data Lifecycle Manager 查询 API 的各种操作和数据类型的描述和语法。

或者，您可以使用其中一个 AWS SDK 以针对您正在使用的编程语言或平台量身定制的方式访问 API。有关更多信息，请参阅 [AWS 软件开发工具包](#)。

## AWS Identity and Access Management

Amazon Data Lifecycle Manager 的访问需要凭据。这些凭证必须拥有权限访问 AWS 资源，如实例、卷、快照和 AMI。以下各节详细介绍了如何使用 AWS Identity and Access Management (IAM)，并有助于保护对资源的访问。

### 主题

- [AWS 托管策略](#)
- [IAM 服务角色](#)
- [用户的权限](#)
- [加密权限](#)

## AWS 托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管策略旨在为许多常见用例提供权限。AWS 与必须自己编写策略相比，托管策略可以更为有效地为用户、组和角色分配适当的权限。

但是，您无法更改 AWS 托管策略中定义的权限。AWS 偶尔会更新 AWS 托管策略中定义的权限。当发生此情况时，更新会影响策略附加到的所有委托人实体（用户、组和角色）。

Amazon Data Lifecycle Manager 为常见用例提供 AWS 托管策略。通过这些策略可以更高效地定义适当的权限，并控制对资源的访问。Amazon Data Lifecycle Manager 提供的 AWS 托管策略旨在附加到您传递给亚马逊数据生命周期管理器的角色。

## 主题

- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWS 托管策略更新](#)

## AWSDataLifecycleManagerServiceRole

该AWSDataLifecycleManagerServiceRole政策为 Amazon Data Lifecycle Manager 提供了创建和管理亚马逊 EBS 快照策略和跨账户复制事件策略的相应权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "events:PutRule",
      "events>DeleteRule",
      "events:DescribeRule",
      "events:EnableRule",
      "events:DisableRule",
      "events:ListTargetsByRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*::rule/AwsDataLifecycleRule.managed-cwe.*"
  }
]
}

```

## AWSDatalifecycleManagerServiceRoleForAMIManagement

该AWSDatalifecycleManagerServiceRoleForAMIManagement政策为亚马逊 Data Lifecycle Manager 提供了创建和管理由亚马逊 EBS 支持的 AMI 策略的相应权限。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",

```

```

        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
    ],
    "Resource": "arn:aws:ec2:*::image/*"
}
]
}

```

## AWSDatalifecycleManagerSSMFullAccess

提供 Amazon Data Lifecycle Manager 权限，允许其执行在所有 Amazon EC2 实例上运行前置和后置脚本所需的 Systems Manager 操作。



**⚠ Important**

使用前置和后置脚本时，该策略使用 `aws:ResourceTag` 条件键来限制对特定 SSM 文档的访问权限。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSMReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowTaggedSSMDocumentsOnly",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/DLMScriptsAccess": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAWSOwnedSSMDocuments",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
```

```

        "ssm:DescribeDocument",
        "ssm:GetDocument"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
    ]
},
{
    "Sid": "AllowAllEC2Instances",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}
}

```

## AWS 托管策略更新

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

下表详细介绍了 Amazon Data Lifecycle Manager AWS 托管策略自该服务开始跟踪这些更改以来该服务所做的更新。要获得有关此页面更改的自动提示，请订阅 [《Amazon EBS 用户指南》的文档历史记录](#) 上的 RSS 源。

更改	描述	日期
AWSDataLifecycleManagerSSMFullAccess— 更新了策略权限。	使用 AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA SSM 文档	2023 年 11 月 17 日

更改	描述	日期
	更新了政策，以支持 SAP HANA 的应用程序一致性快照。	
AWSDataLifecycleManagerSSMFullAccess— 添加了新的 AWS 托管策略。	Amazon Data Lifecycle Manager 添加了 AWSDataLifecycleManagerSSMFullAccess AWS 托管策略。	2023 年 11 月 7 日
AWSDataLifecycleManagerServiceRole— 增加了支持快照存档的权限。	Amazon Data Lifecycle Manager 添加了 ec2:ModifySnapshotTier 和 ec2:DescribeSnapshotTierStatus 操作，以授予快照策略存档快照和检查快照存档状态的权限。	2022 年 9 月 30 日

更改	描述	日期
AWSDataLifecycleManagerServiceRoleForAMIManagement—增加了支持 AMI 弃用的权限。	Amazon Data Lifecycle Manager 添加了 ec2:EnableImageDeprecation 和 ec2:DisableImageDeprecation 操作以授予 EBS 支持的 AMI 策略权限，从而启用和禁用 AMI 弃用。	2021 年 8 月 23 日
Amazon Data Lifecycle Manager 已开启跟踪更改	Amazon Data Lifecycle Manager 开始跟踪其 AWS 托管策略的变更。	2021 年 8 月 23 日

## IAM 服务角色

AWS Identity and Access Management (IAM) 角色与用户类似，因为它是一个具有权限策略的 AWS 身份，该策略决定了该身份可以做什么和不能做什么 AWS。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。服务角色是 AWS 服务代替您执行操作的角色。作为代表您执行备份操作的服务，Amazon Data Lifecycle Manager 要求您在该服务代表您执行策略操作时将其传递给要代入的角色。有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 [IAM 角色](#)。

您传递到 Amazon Data Lifecycle Manager 的角色必须拥有一个 IAM policy，该策略具有的权限可让 Amazon Data Lifecycle Manager 执行策略操作关联的操作，如创建快照和 AMI、复制快照和 AMI、删除快照以及取消注册 AMI。每种 Amazon Data Lifecycle Manager 策略类型需要不同的权限。该角色还必须将 Amazon Data Lifecycle Manager 列为可信实体，这使得 Amazon Data Lifecycle Manager 能够代入该角色。

## 主题

- [Amazon Data Lifecycle Manager 的原定设置服务角色](#)
- [Amazon Data Lifecycle Manager 的自定义服务角色](#)

## Amazon Data Lifecycle Manager 的原定设置服务角色

Amazon Data Lifecycle Manager 使用以下原定设置的服务角色：

- `AWSDataLifecycleManagerDefaultRole`—管理快照的默认角色。它只信任 `d1m.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行快照和跨账户快照复制策略所需的操作。此角色使用 `AWSDataLifecycleManagerServiceRole` AWS 托管策略。

### Note

角色的 ARN 格式会有所不同，具体取决于使用控制台还是 AWS CLI 创建角色。如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果角色是使用创建的 AWS CLI，则 ARN 格式为 `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`

- `AWSDataLifecycleManagerDefaultRoleForAMIManagement`—管理 AMI 的默认角色。它只信任 `d1m.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行由 EBS 支持的 AMI 策略所需的操作。此角色使用 `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS 托管策略。

如果您使用的是 Amazon Data Lifecycle Manager 控制台，则在您首次创建快照或跨账户快照复制策略时，Amazon Data Lifecycle Manager 会自动创建 `AWSDataLifecycleManagerDefaultRoleForAMIManagement` 服务角色，并在您首次创建由 EBS 支持的 AMI 策略时自动创建服务角色 `AWSDataLifecycleManagerDefaultRole`

如果您不使用控制台，可以使用 [create-default-role](#) 命令手动创建服务角色。对于 `--resource-type`，请 `snapshot` 指定“创建 `AWSDataLifecycleManagerDefaultRole`”或 `image` “创建” `AWSDataLifecycleManagerDefaultRoleForAMIManagement`。

```
$ aws dlm create-default-role --resource-type snapshot/image
```

如果您删除了原定设置服务角色，然后需要再次创建，则可以使用相同的流程在您的账户中重新创建它们。

## Amazon Data Lifecycle Manager 的自定义服务角色

作为使用原定设置服务角色的替代方案，您可以在创建生命周期策略时创建具有所需权限的自定义 IAM 角色，然后选择它们。

### 创建自定义 IAM 角色

1. 创建具有以下权限的角色。
  - 管理快照生命周期策略所需的权限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    }
  ]
}
```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/DLMScriptsAccess": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [

```

```

        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
    ],
    "Resource": [
        "arn:aws:ssm:*::document/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringNotLike": {
            "aws:ResourceTag/DLMScriptsAccess": "false"
        }
    }
}
]
}

```

- 管理 AMI 生命周期策略所需的权限

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
            ]
        }
    ]
}

```



```

        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:ResetImageAttribute",
      "ec2:DeregisterImage",
      "ec2:CreateImage",
      "ec2:CopyImage",
      "ec2:ModifyImageAttribute"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:EnableImageDeprecation",
      "ec2:DisableImageDeprecation"
    ],
    "Resource": "arn:aws:ec2:*::image/*"
  }
]
}

```

有关更多信息，请参阅IAM 用户指南中的[创建角色](#)。

## 2. 向角色添加信任关系。

- a. 在 IAM 控制台中，选择角色。
- b. 选择您创建的角色，然后选择信任关系。
- c. 选择编辑信任关系，添加以下策略，然后选择更新信任策略。

```

{
  "Version": "2012-10-17",

```

```

"Statement": [{
  "Effect": "Allow",
  "Principal": {
    "Service": "dlm.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}]
}

```

建议您使用 `aws:SourceAccount` 和 `aws:SourceArn` 条件键来防止出现[混淆代理人问题](#)。例如，您可以将以下条件块添加到以前的信任策略。`aws:SourceAccount` 是生命周期策略的所有者，`aws:SourceArn` 是生命周期策略的 ARN。如果您不知道生命周期策略的 ID，可以用通配符 ( \* ) 替换 ARN 的该部分，然后在创建生命周期策略后更新信任策略。

```

"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
  }
}

```

## 用户的权限

用户必须具有以下权限才能使用 Amazon Data Lifecycle Manager。

### Note

- 仅控制台用户需要 `ec2:DescribeAvailabilityZones`、`ec2:DescribeRegions`、`kms:ListAliases` 和 `kms:DescribeKey` 权限。如果不需要访问控制台，则可以删除权限。
- `AWSDataLifecycleManagerDefaultRole` 角色的 ARN 格式会有所不同，具体取决于它是使用控制台还是使用控制台创建的。AWS CLI 如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果角色是使用创建的 AWS CLI，则

ARN 格式为。以下策略假定该角色是使用创建的。arn:aws:iam::*account\_id*:role/AWSDataLifecycleManagerDefaultRole AWS CLI

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "dlm:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole",
        "arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRoleForAMIManagement"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的[更改用户权限](#)。

## 加密权限

使用 Amazon Data Lifecycle Manager 和加密资源时，请考虑以下情况。

- 如果源卷已加密，请确保 Amazon Data Lifecycle Manager 的默认角色 ( [AWSDataLifecycleManagerDefaultRole](#) 和 [AWSDataLifecycleManagerDefaultRoleForAMIManagement](#) ) 有权使用用于加密卷的 KMS 密钥。
- 如果您为未加密快照或未加密快照支持的 AMI 启用跨区域复制，并选择在目标区域中启用加密，请确保默认角色有权使用在目标区域中执行加密所需的 KMS 密钥。
- 如果您为加密快照或加密快照支持的 AMI 启用跨区域复制，请确保默认角色有权同时使用源和目标 KMS 密钥。
- 如果您为加密快照启用快照存档，请确保 Amazon Data Lifecycle Manager 的默认角色 ( [AWSDataLifecycleManagerDefaultRole](#) ) 有权使用用于加密快照的 KMS 密钥。

有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 [允许其他账户中的用户使用 KMS 密钥](#)。

## 监控快照和 AMI 的生命周期

您可以使用以下功能来监控快照和 AMI 的生命周期。

### 功能

- [控制台和 AWS CLI](#)
- [AWS CloudTrail](#)
- [使用“CloudWatch 事件”监控您的策略](#)
- [使用 Amazon 监控您的策略 CloudWatch](#)

## 控制台和 AWS CLI

您可以使用 Amazon EC2 控制台或 AWS CLI 来查看生命周期策略。策略创建的每个快照和 AMI 均具有时间戳以及与策略相关的标签。您可以使用这些标签来筛选快照和 AMI 以验证是否按您的预期创建备份。有关使用控制台查看生命周期策略的信息，请参阅 [查看生命周期策略](#)。

## AWS CloudTrail

借 AWS CloudTrail 助，您可以跟踪用户活动和 API 使用情况，以证明其符合内部政策和监管标准。有关更多信息，请参阅 [《AWS CloudTrail 用户指南》](#)。

### 使用“CloudWatch 事件”监控您的政策

Amazon EBS 和 Amazon Data Lifecycle Manager 发出与生命周期策略操作相关的事件。您可以使用 AWS Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 [Amazon Ev CloudWatch ents 用户指南](#)。

提供的事件如下：

#### Note

AMI 生命周期策略操作不会触发任何事件。

- createSnapshot – 当 CreateSnapshot 操作成功或失败时发出的 Amazon EBS 事件。有关更多信息，请参阅 [Amazon f EventBridge or Amazon EBS](#)。
- DLM Policy State Change – 当生命周期策略进入错误状态时发出的 Amazon Data Lifecycle Manager 事件。此事件包含有关导致错误的问题的描述。

下面是在 IAM 角色授予的权限不足时发出的事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "DLM Policy State Change",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2018-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  ],
  "detail": {
    "state": "ERROR",
    "cause": "Role provided does not have sufficient permissions",
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  }
}
```

```
}
}
```

下面是在超过限制时发出的事件的示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "DLM Policy State Change",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2018-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  ],
  "detail":{
    "state": "ERROR",
    "cause": "Maximum allowed active snapshot limit exceeded",
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
  }
}
```

- DLM Pre Post Script Notification – 前置或后置脚本启动、成功或失败时发出的事件。

以下是 VSS 备份成功时的示例事件。

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-123456789012",
  "detail-type": "DLM Pre Post Script Notification",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2023-10-27T22:04:52Z",
  "region": "us-east-1",
  "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
  "detail": {
    "script_stage": "",
    "result": "success",
    "cause": "",

```

```
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
    "execution_handler": "AWS_VSS_BACKUP",
    "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
    "resource_type": "EBS_SNAPSHOT",
    "resources": [{
        "status": "pending",
        "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
        "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
    }],
    "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
    "start_time": "2023-10-27T22:03:29.370Z",
    "end_time": "2023-10-27T22:04:51.370Z",
    "timeout_time": ""
}
}
```

## 使用 Amazon 监控您的政策 CloudWatch

您可以使用监控您的 Amazon Data Lifecycle Manager 生命周期策略 CloudWatch，该策略收集原始数据并将其处理为可读的近乎实时的指标。您可以使用这些指标来准确查看您的策略随着时间的推移创建、删除和复制了多少 Amazon EBS 快照和 EBS 支持的 AMI。还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。

指标的保留期限为 15 个月，以便您可以访问历史信息，并更好地了解生命周期策略在较长时间内的表现。

有关亚马逊的更多信息 CloudWatch，请参阅[亚马逊 CloudWatch 用户指南](#)。

### 主题

- [受支持的指标](#)
- [查看您的政策 CloudWatch 指标](#)
- [绘制策略的指标图表](#)
- [为策略创建 CloudWatch 警报](#)
- [使用案例示例](#)
- [管理报告失败操作的策略](#)

## 受支持的指标

Data Lifecycle Manager 命名空间包括 Amazon Data Lifecycle Manager 生命周期策略的以下指标。支持的指标因策略类型而异。

所有指标都可以在 DLMPolicyId 维度上衡量。最有用的统计工具为 sum 和 average，并且度量单位为 count。

选择选项卡以查看该策略类型支持的指标。

### EBS snapshot policies

指标	描述
Resources Targeted	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。
Snapshots CreateStarted	快照策略启动的快照创建操作数。即使有多次后续重试，每个操作也只记录一次。  如果快照创建操作失败，Amazon Data Lifecycle Manager 会发送 SnapshotsCreateFailed 指标。
Snapshots CreateCompleted	快照策略创建的快照数量。这包括在计划时间后 60 分钟内的成功重试。
Snapshots CreateFailed	不能由快照策略创建的快照数量。这包括在计划时间后 60 分钟内的不成功重试。
Snapshots SharedCompleted	快照策略跨账户共享的快照数量。
Snapshots DeleteCompleted	快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。  此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。
Snapshots DeleteFailed	不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。



指标	描述
	此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。
Snapshots CopiedRegionStarted	快照策略启动的跨区域快照复制操作数。
Snapshots CopiedRegionCompleted	快照策略创建的跨区域快照副本数量。这包括在计划时间的 24 小时内的成功重试。
Snapshots CopiedRegionFailed	不能由快照策略创建的跨区域快照副本的数量。这包括在计划时间后 24 小时内的不成功重试。
Snapshots CopiedRegionDeleteCompleted	快照策略删除的跨区域快照副本的数量，由保留规则指定。
Snapshots CopiedRegionDeleteFailed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
snapshots ArchiveDeletionFailed	不能由快照策略从存档层中删除的存档快照数量。
snapshots ArchiveScheduled	计划由快照策略存档的快照数量。
snapshots ArchiveCompleted	成功由快照策略存档的快照数量。

指标	描述
snapshots ArchiveFailed	不能由快照策略存档的快照数量。
snapshots ArchiveDeletionCompleted	成功由快照策略从存档层中删除的存档快照数量。
PreScript Started	前置脚本成功启动的实例数。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PreScript Completed	前置脚本成功完成的实例数。即使前置脚本在指定的超时期间之外完成，也会发出该指标。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PreScript Failed	前置脚本未能成功完成的实例数。即使前置脚本在指定的超时期间之外完成，也会发出该指标。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScript Started	后置脚本成功启动的实例数。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScript已完成	后置脚本成功完成的实例数。即使后置脚本在指定的超时期间之外完成，也会发出该指标。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScript失败	后置脚本未能成功完成的实例数。即使后置脚本在指定的超时期间之外完成，也会发出该指标。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
VSSBackup Started	VSS 备份成功启动的实例数。  如果启用了脚本重试，则每次策略运行时可以多次发出此指标。

指标	描述
VSSBackup Completed	<p>VSS 备份成功完成的实例数。即使 VSS 备份在超时期间之外完成，也会发出该指标。</p> <p>如果启用了脚本重试，则每次策略运行时可以多次发出此指标。</p>
VSSBackup Failed	<p>VSS 备份未能成功完成的实例数。即使 VSS 备份在超时期间之外完成，也会发出该指标。</p> <p>如果启用了脚本重试，则每次策略运行时可以多次发出此指标。</p>

## EBS-backed AMI policies

以下指标可与 EBS 支持的 AMI 策略一起使用：

指标	描述
Resources Targeted	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。
Snapshots DeleteCompleted	<p>快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。</p> <p>此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。</p>
Snapshots DeleteFailed	<p>不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。</p> <p>此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。</p>
Snapshots CopiedRegionDeleteCompleted	快照策略删除的跨区域快照副本的数量，由保留规则指定。

指标	描述
Snapshots CopiedRegionDeleteFailed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
ImagesCreateStarted	由 EBS 支持的 AMI 策略启动的CreateImage操作数量。
ImagesCreateCompleted	由 EBS 支持的 AMI 策略创建的 AMI 数量。
ImagesCreateFailed	不能由 EBS 支持的 AMI 策略创建的 AMI 数量。
ImagesDeregisterCompleted	由 EBS 支持的 AMI 策略取消注册的 AMI 数量。
ImagesDeregisterFailed	不能由 EBS 支持的 AMI 策略取消注册的 AMI 数量。
ImagesCopiedRegionStarted	由 EBS 支持的 AMI 策略启动的跨区域复制操作的数量。
ImagesCopiedRegionCompleted	由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。

指标	描述
ImagesCopiedRegionFailed	不能由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。
ImagesCopiedRegionDeregisterCompleted	由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。
ImagesCopiedRegionDeregisteredFailed	不能由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。
EnableImageDeprecationCompleted	由 EBS 支持的 AMI 策略标记为弃用的 AMI 数量。
EnableImageDeprecationFailed	EBS 支持的 AMI 策略无法标记为弃用的 AMI 数。
EnableCopiedImageDeprecationCompleted	由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。
EnableCopiedImageDeprecationFailed	不能由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。

## Cross-account copy event policies

跨账户复制事件策略可以使用以下指标：

指标	描述
Snapshots CopiedAccountStarted	跨账户复制事件策略启动的跨账户快照复制操作的数量。
Snapshots CopiedAccountCompleted	跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的成功重试。
Snapshots CopiedAccountFailed	不能由跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的不成功重试。
Snapshots CopiedAccountDeleteCompleted	跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。
Snapshots CopiedAccountDeleteFailed	不能由跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。

### 查看您的政策 CloudWatch 指标

您可以使用 [AWS Management Console](#) 或 [命令行工具](#) 列出 Amazon Data Lifecycle Manager 发送给亚马逊的指标 CloudWatch。

## Amazon EC2 console

使用 Amazon EC2 控制台查看指标

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Lifecycle Manager ( 生命周期管理器 )。
3. 在网格中选择一个策略，然后选择 Monitoring ( 监控 ) 选项卡。

## CloudWatch console

使用 Amazon CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 在导航窗格中，选择指标。
3. 选择 EBS 命名空间，然后选择 Data Lifecycle Manager metrics ( 数据生命周期管理器指标 )。

## AWS CLI

列出 Amazon Data Lifecycle Manager 的所有可用指标

使用 [list-metrics](#) 命令。

```
$ C:\> aws cloudwatch list-metrics \  
    --namespace AWS/EBS
```

列出特定策略的所有指标

使用 [list-metrics](#) 命令并指定 DLMPolicyId 维度。

```
$ C:\> aws cloudwatch list-metrics \  
    --namespace AWS/EBS \  
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

列出所有策略的单个指标

使用 [list-metrics](#) 命令并指定 --metric-name 选项。

```
$ C:\> aws cloudwatch list-metrics \  
    --metric-name
```

```
--namespace AWS/EBS \  
--metric-name SnapshotsCreateCompleted
```

## 绘制策略的指标图表

在您创建策略后，可以打开 Amazon EC2 控制台并在 Monitoring ( 监控 ) 选项卡上查看策略的监控图表。每个图表以一个可用的 Amazon EC2 指标为基础。

可供使用图表指标如下：

- 资源目标已确定 ( 基于 ResourcesTargeted )
- 快照创建已启动 ( 基于 SnapshotsCreateStarted )
- 快照创建已完成 ( 基于 SnapshotsCreateCompleted )
- 快照创建已失败 ( 基于 SnapshotsCreateFailed )
- 快照共享已完成 ( 基于 SnapshotsSharedCompleted )
- 快照删除已完成 ( 基于 SnapshotsDeleteCompleted )
- 快照删除已失败 ( 基于 SnapshotsDeleteFailed )
- 快照跨区域复制已启动 ( 基于 SnapshotsCopiedRegionStarted )
- 快照跨区域复制已完成 ( 基于 SnapshotsCopiedRegionCompleted )
- 快照跨区域复制已失败 ( 基于 SnapshotsCopiedRegionFailed )
- 快照跨区域复制删除已完成 ( 基于 SnapshotsCopiedRegionDeleteCompleted )
- 快照跨区域复制删除已失败 ( 基于 SnapshotsCopiedRegionDeleteFailed )
- 快照跨账户复制已启动 ( 基于 SnapshotsCopiedAccountStarted )
- 快照跨账户复制已完成 ( 基于 SnapshotsCopiedAccountCompleted )
- 快照跨账户复制已失败 ( 基于 SnapshotsCopiedAccountFailed )
- 快照跨账户复制删除已完成 ( 基于 SnapshotsCopiedAccountDeleteCompleted )
- 快照跨账户复制删除已失败 ( 基于 SnapshotsCopiedAccountDeleteFailed )
- AMI 创建已开始 ( 基于 ImagesCreateStarted )
- AMI 创建已完成 ( 基于 ImagesCreateCompleted )
- AMI 创建已失败 ( 基于 ImagesCreateFailed )
- AMI 取消注册已完成 ( 基于 ImagesDeregisterCompleted )
- AMI 取消注册已失败 ( 基于 ImagesDeregisterFailed )



- AMI 跨区域复制已启动 ( 基于 ImagesCopiedRegionStarted )
- AMI 跨区域复制已完成 ( 基于 ImagesCopiedRegionCompleted )
- AMI 跨区域复制已失败 ( 基于 ImagesCopiedRegionFailed )
- AMI 跨区域取消注册已完成 ( 基于 ImagesCopiedRegionDeregisterCompleted )
- AMI 跨区域复制取消注册已失败 ( 基于 ImagesCopiedRegionDeregisteredFailed )
- AMI 启用弃用已完成 ( 基于 EnableImageDeprecationCompleted )
- AMI 启用弃用已失败 ( 基于 EnableImageDeprecationFailed )
- AMI 跨区域复制启用弃用已完成 ( 基于 EnableCopiedImageDeprecationCompleted )
- AMI 跨区域复制启用弃用已失败 ( 基于 EnableCopiedImageDeprecationFailed )

## 为策略创建 CloudWatch 警报

您可以创建用于监控策略 CloudWatch 指标的 CloudWatch 警报。CloudWatch 当指标达到您指定的阈值时，将自动向您发送通知。您可以使用 CloudWatch 控制台创建 CloudWatch 警报。

有关使用 CloudWatch 控制台创建警报的更多信息，请参阅 Amazon CloudWatch 用户指南中的以下主题。

- [基于静态阈值创建 CloudWatch 警报](#)
- [基于异常检测创建 CloudWatch 警报](#)

## 使用案例示例

以下是使用案例示例：

### 主题

- [示例 1：ResourcesTargeted 指标](#)
- [示例 2：SnapshotDeleteFailed 指标](#)
- [示例 3：SnapshotsCopiedRegionFailed 指标](#)

### 示例 1：ResourcesTargeted 指标

您可以使用 ResourcesTargeted 指标来监控特定策略每次运行时所针对的资源总数。这使您能够在目标资源的数量低于或高于预期阈值时触发告警。

例如，如果您希望每日策略创建不超过 50 卷的备份，可以创建告警，该告警会在 ResourcesTargeted 的 sum 大于 50 超过 1 小时时发送电子邮件通知。通过这种方式，您可以确保没有从已错误标记的卷意外创建任何快照。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name resource-targeted-monitor \  
  --alarm-description "Alarm when policy targets more than 50 resources" \  
  --metric-name ResourcesTargeted \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 50 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

## 示例 2：SnapshotDeleteFailed 指标

您可以使用 SnapshotDeleteFailed 指标，以根据策略的快照保留规则来监控删除快照的故障情况。

例如，如果您已创建应每 12 小时自动删除一次快照的策略，则可以创建一个告警，该告警会在 SnapshotDeletionFailed 的 sum 大于 0 超过 1 小时通知您的工程团队。这有助于调查不正确的快照保留，并确保您的存储成本不会因不必要的快照而增加。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name snapshot-deletion-failed-monitor \  
  --alarm-description "Alarm when snapshot deletions fail" \  
  --metric-name SnapshotsDeleteFailed \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 0 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

### 示例 3：SnapshotsCopiedRegionFailed 指标

使用 SnapshotsCopiedRegionFailed 指标以确定您的策略何时无法将快照复制到其他区域。

例如，如果您的策略每天跨区域复制快照，则可以创建告警，该告警会在 SnapshotCrossRegionCopyFailed 的 sum 大于 0 超过 1 小时时向您的工程团队发送 SMS。这对于验证策略是否成功复制了谱系中的后续快照非常有用。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name snapshot-copy-region-failed-monitor \  
  --alarm-description "Alarm when snapshot copy fails" \  
  --metric-name SnapshotsCopiedRegionFailed \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 0 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

### 管理报告失败操作的策略

有关当您的某项政策报告操作失败指标出现意外非零值时该怎么办的更多信息，请参阅[如果 Amazon Data Lifecycle Manager 报告 CloudWatch 指标中的失败操作该怎么办？](#) AWS 知识中心文章。

## 故障排除

以下文档可以帮助排查可能遇到的问题。

### 主题

- [错误：Role with name already exists](#)

## 错误：Role with name already exists

### 描述

您在尝试使用控制台创建策略时收到了 Role with name `AWSDataLifecycleManagerDefaultRole` already exists 或 Role with name `AWSDataLifecycleManagerDefaultRoleForAMIManagement` already exists 错误。

## 原因

默认角色的 ARN 格式会有所不同，具体取决于使用控制台还是 AWS CLI 创建角色。虽然 ARN 不同，但角色使用相同的角色名称，这会导致控制台和 AWS CLI 之间出现角色命名冲突。

## 解决方案

要解决此问题，请执行以下操作：

1. （仅适用于为预处理和发布脚本启用的快照策略）手动将 `AWSDataLifecycleManagerSSMFullAccess` AWS 托管策略附加到 `AWSDataLifecycleManagerDefaultRoleIAM` 角色。有关更多信息，请参阅[添加 IAM 身份权限](#)。
2. 在创建 Amazon Data Lifecycle Manager 策略时，对于 IAM 角色，选择选择其他角色，然后选择 `AWSDataLifecycleManagerDefaultRole`（对于快照策略）或 `AWSDataLifecycleManagerDefaultRoleForAMIManagement`（对于 AMI 策略）。
3. 像往常一样继续创建策略。

## 使用 EBS direct API 访问 EBS 快照的内容

您可以使用 Amazon Elastic Block Store ( Amazon EBS ) 直接 API 创建 EBS 快照，将数据直接写入快照，读取快照上的数据，并标识两个快照之间的差异或发生的更改。如果您是为 Amazon EBS 提供备份服务的独立软件供应商 ( ISV )，则利用 EBS direct API，可以更高效、更具成本效益地通过快照跟踪 EBS 卷上的增量更改。无需从快照创建新卷，然后使用 Amazon Elastic Compute Cloud ( Amazon EC2 ) 实例来比较差异，即可完成此操作。

您可以从本地数据直接创建增量快照到 EBS 卷和云中，以用于快速灾难恢复。通过写入和读取快照的功能，您可以在发生灾难时将本地数据写入 EBS 快照。然后，恢复后，您可以将其恢复到快照 AWS 或从快照恢复到本地。您不再需要构建和维护复杂的机制来将数据复制到 Amazon EBS 或从中复制数据。

本用户指南概述了构成 EBS direct API 的元素，并提供了如何有效使用这些元素的示例。有关 API 的操作、数据类型、参数和错误的更多信息，请参阅 [EBS direct API 参考](#)。有关 EBS 直接 API 支持的 AWS 区域、终端节点和服务配额的更多信息，请参阅中的 [Amazon EBS 终端节点和配额](#)。AWS 一般参考

### 内容

- [了解 EBS direct API](#)
- [EBS 直接 API 的 IAM 权限](#)
- [使用 EBS 直接 API](#)
- [EBS 直接 API 的定价](#)
- [将接口 VPC 终端节点与 EBS 直接 API 结合使用](#)
- [使用 EBS 直接 API 记录 API 的 API 调用 AWS CloudTrail](#)
- [常见问题](#)

## 了解 EBS direct API

下面是您在开始使用 EBS direct API 前应了解的关键元素。

### 快照

快照是备份 EBS 卷中的数据的主要方式。使用 EBS direct API，您还可以将数据从本地磁盘备份到快照。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。有关更多信息，请参阅 [Amazon EBS 快照](#)。

**Note**

EBS 直接 API 不支持 Outposts 上的公有快照和本地快照。

## 数据块

数据块是快照中的数据片段。每个快照可以包含数千个数据块。快照中的所有数据块都具有固定大小。

## 数据块索引

数据块索引是以 512 KiB 数据块为单位的逻辑索引。若要确定数据块索引，请用逻辑卷中数据的逻辑偏移量除以数据块大小（数据的逻辑偏移量/524288）。数据的逻辑偏移量必须与 512 KiB 一致。

## 数据块令牌

数据块令牌是快照中的数据块的标识哈希，它用于查找数据块数据。EBS direct API 返回的数据块令牌是临时的。它们会在为其指定的到期时间戳时发生变化，或者如果您运行另一个快照 ListSnapshotBlocks 或 ListChangedBlocks 请求相同的快照。

## 校验和

校验和是从数据块中派生的大小很小的基准值，用于检测其传输或存储过程中引入的错误。EBS direct API 使用校验和验证数据完整性。从 EBS 快照读取数据时，该服务会为传输的每个数据块提供 Base64 编码的 SHA256 校验和，您可以使用这些校验和进行验证。向 EBS 快照写入数据时，您必须为传输的每个数据块提供一个 Base64 编码的 SHA256 校验和。服务使用提供的校验和验证接收的数据。有关更多信息，请参阅本指南下文中的[使用校验和](#)。

## 加密

通过加密，您的数据将转换为无法读取的代码，只能由有权访问加密数据所用 KMS 密钥的人员破译这些代码，从而为数据提供保护。您可以使用 EBS direct API 读取和写入加密快照，但存在一些限制。有关更多信息，请参阅本指南下文中的[使用加密](#)。

## API 操作

EBS direct API 由六个操作组成。包含三个读取操作和三个写入操作。读取操作包括：

- ListSnapshotBlocks — 返回指定快照中区块的区块索引和区块标记
- ListChangedBlocks — 返回同一卷和快照谱系的两个指定快照之间存在差异的区块索引和区块标记。

- GetSnapshotBlock — 返回区块中指定快照 ID、区块索引和区块令牌的数据。

写入操作包括：

- StartSnapshot— 启动快照，可以是现有快照的增量快照，也可以是新快照。在使用 CompleteSnapshot 操作完成之前，已启动的快照将保持待处理状态。
- PutSnapshotBlock — 以单个块的形式向已启动的快照添加数据。您必须为传输的数据块指定一个 Base64 编码的 SHA256 校验和。该服务会在传输完成以后验证校验和。若该服务计算的校验和与您指定值的不匹配，请求将会失败。
- CompleteSnapshot— 完成处于待处理状态的已启动快照。然后，该快照的状态会更改为“已完成”。

## EBS 直接 API 的 IAM 权限

用户必须具有以下策略才能使用 EBS direct API。有关更多信息，请参阅[更改用户权限](#)。

有关 EBS 直接 API 资源、操作和用于 IAM 权限策略中的条件上下文键的更多信息，请参阅服务授权参考中的 [Amazon Elastic Block Store 的操作、资源和条件键](#)。

### Important

向用户分配以下策略时请小心谨慎。通过分配这些策略，您可以向被拒绝通过 Amazon EC2 API 访问相同资源的用户授予访问权限，例如 CopySnapshot 或 CreateVolume 操作。

## 读取快照的权限

以下策略允许在特定 AWS 区域的所有快照上使用读取 EBS 直接 API。在该策略中，将 *<Region>* 替换为快照的区域。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:ec2:<Region>::snapshot/*"
  }
]
}

```

以下策略允许在对具有特定键/值标记的快照使用读取 EBS 直接 API。在策略中，将 *<Key>* 替换为标签的键值，并将 *<Value>* 替换为标签的值。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "aws:ResourceTag/<Key>": "<Value>"
        }
      }
    }
  ]
}

```

以下策略允许仅对账户中特定时间范围内的所有快照使用读取 EBS 直接 API。此策略授权基于 `aws:CurrentTime` 全局条件键使用 EBS 直接 API。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ]
    }
  ]
}

```



```

    ],
    "Resource": "arn:aws:ec2:*::snapshot/*",
    "Condition": {
      "DateGreaterThan": {
        "aws:CurrentTime": "2018-05-29T00:00:00Z"
      },
      "DateLessThan": {
        "aws:CurrentTime": "2020-05-29T23:59:59Z"
      }
    }
  }
]
}

```

有关更多信息，请参阅《IAM 用户指南》中的[更改用户权限](#)。

## 写入快照的权限

以下策略允许在特定 AWS 区域的所有快照上使用写入 EBS 直接 API。在该策略中，将 *<Region>* 替换为快照的区域。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock",
        "ebs:CompleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:<Region>::snapshot/*"
    }
  ]
}

```

以下策略允许在对具有特定键/值标记的快照使用写入 EBS 直接 API。在策略中，将 *<Key>* 替换为标签的键值，并将 *<Value>* 替换为标签的值。

```

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

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock",
        "ebs:CompleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "aws:ResourceTag/<Key>": "<Value>"
        }
      }
    }
  ]
}

```

以下策略允许使用所有 EBS direct API。只有在指定了父快照 ID 时，它才允许执行 StartSnapshot 操作。因此，此策略会阻止在不使用父快照的情况下开始新快照的功能。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
        }
      }
    }
  ]
}

```

以下策略允许使用所有 EBS direct API。它还允许只为新快照创建 user 标签键。此策略还确保用户有权创建标签。StartSnapshot 操作是唯一可以指定标签的操作。

```

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

```

```

    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "user"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "*"
    }
  ]
}

```

以下策略允许仅对账户中特定时间范围内的所有快照使用写入 EBS 直接 API。此策略授权基于 `aws:CurrentTime` 全局条件键使用 EBS 直接 API。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock",
        "ebs:CompleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "DateGreaterThan": {
          "aws:CurrentTime": "2018-05-29T00:00:00Z"
        },
        "DateLessThan": {
          "aws:CurrentTime": "2020-05-29T23:59:59Z"
        }
      }
    }
  ]
}

```

```
}
```

有关更多信息，请参阅《IAM 用户指南》中的[更改用户权限](#)。

## 使用权限 AWS KMS keys

以下策略授予使用特定 KMS 密钥解密已加密快照的权限。该策略还授予使用 EBS 加密的默认 KMS 密钥来加密新快照的权限。在策略中，用 <Region>KMS 密钥的区域替换，< *AccountId* > 替换为 KMS 密钥的 AWS 账户 ID，将 < *KeyId* > 替换为 KMS 密钥的 ID。

### Note

默认情况下，账户中的所有委托人都可以访问用于 Amazon EBS 加密的默认 AWS 托管 KMS 密钥，并且可以将其用于 EBS 加密和解密操作。如果您使用的是客户托管式密钥，则必须创建新的密钥策略或修改客户托管式密钥的现有密钥策略，以便授予主体对客户托管式密钥的访问权限。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的[在 AWS KMS 中使用密钥策略](#)。

### Tip

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。相反，使用 `kms:GrantIsForAWSResource` 条件密钥允许用户仅在 AWS 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:CreateTags",
```

```
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": true
        }
    }
}
]
```

有关更多信息，请参阅《IAM 用户指南》中的[更改用户权限](#)。

## 使用 EBS 直接 API

以下主题介绍如何使用 EBS 直接 API 读取和写入快照。您只能使用 AWS CLI、AWS API 和 AWS 软件开发工具包读取和写入快照。有关更多信息，请参阅：

- [安装 AWS CLI 并配置 AWS CLI](#)
- [EBS 直接 API 参考](#)
- [AWS 开发工具包](#)

### Important

EBS 直接 API 需要 AWS 签名版本 4 签名。有关更多信息，请参阅 [使用签名版本 4 签名](#)。

### 主题

- [使用 EBS 直接 API 读取快照](#)
- [使用 EBS 直接 API 写入快照](#)
- [使用加密](#)
- [使用签名版本 4 签名](#)
- [使用校验和](#)
- [API 的等性 StartSnapshot](#)
- [错误重试](#)
- [优化性能](#)

- [EBS 直接 API 服务端点](#)

## 使用 EBS 直接 API 读取快照

以下步骤介绍了如何使用 EBS direct API 读取快照：

1. 使用 ListSnapshotBlocks 操作可查看快照中区块的所有区块索引和区块标记。或者使用该 ListChangedBlocks 操作仅查看同一卷的两个快照和快照谱系之间不同的区块索引和区块令牌。这些操作可帮助您标识可能希望获取其数据的数据块的数据块令牌和数据块索引。
2. 使用 GetSnapshotBlock 操作，并指定要获取其数据的区块的区块索引和区块标记。

以下示例显示如何使用 EBS 直接 API 读取快照。

### 主题

- [列出快照中的数据块](#)
- [列出两个快照之间存在不同的数据块](#)
- [从快照获取数据块数据](#)

## 列出快照中的数据块

### AWS CLI

以下 [list-snapshot-blocks](#) 示例命令返回快照 snap-0987654321 中数据块的数据块索引和数据块令牌。--starting-block-index 参数将结果限制为索引大于 1000 的数据块，并且 --max-results 参数将结果限制为前 100 个数据块。

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --max-results 100
```

以下为上一个命令的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
  "Blocks": [
    {
      "BlockIndex": 1001,
```

```

        "BlockToken": "AAABAV3/
PNhX0ynVdMYHUpPsetaSvjLB1dtIGfbJv50J0sX855EzGTWos4a4"
    },
    {
        "BlockIndex": 1002,
        "BlockToken": "AAABATGQIgwI0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
    },
    {
        "BlockIndex": 1007,
        "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07e0gTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
    },
    {
        "BlockIndex": 1012,
        "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
    },
    {
        "BlockIndex": 1030,
        "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
    },
    {
        "BlockIndex": 1031,
        "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBC1kw6spzCxJVqDVaTskJ"
    },
    ...
],
"ExpiryTime": 1576287332.806,
"VolumeSize": 32212254720,
"BlockSize": 524288
}

```

## AWS API

以下 BI [ListSnapshotocks](#) 示例请求返回快照中区块的区块索引和区块标记snap-0acEXAMPLEcf41648。startingBlockIndex 参数将结果限制为索引大于 1000 的数据块，并且 maxResults 参数将结果限制为前 100 个数据块。

```

GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
HTTP/1.1

```

```
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T231953Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 `GetSnapshotBlock` 操作并指定要获取其数据的区块的区块索引和区块标记。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
Content-Type: application/json
Content-Length: 2472
Date: Wed, 17 Jun 2020 23:19:56 GMT
Connection: keep-alive

{
  "BlockSize": 524288,
  "Blocks": [
    {
      "BlockIndex": 0,
      "BlockToken": "AAUBAcuWq0CnDNuK1e11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
    },
    {
      "BlockIndex": 1536,
      "BlockToken": "AAUBAWudwfmofcrQhGVlLwuRkm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
    },
    {
      "BlockIndex": 3072,
      "BlockToken": "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
    },
    {
      "BlockIndex": 3073,
      "BlockToken": "AAUBAbqt9zpqBUEvt02HINAFaWTo0w1PjbIsQ01x6JUN/0+iMQ10NtNbnX4"
    },
    ...
  ],
  "ExpiryTime": 1.59298379649E9,
```



```

    "VolumeSize": 3
  }

```

## 列出两个快照之间存在不同的数据块

在发出分页请求以列出两个快照之间发生更改的块时应注意以下几点：

- 响应可能包含一个或多个空的 ChangedBlocks 数组。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 0 – 999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 999 的增量快照。

使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照发生更改的块时，将返回一个空的 ChangedBlocks 数组。您必须使用 nextToken 请求剩余的结果，直到第十个结果集（其中包括块索引为 900 - 999 的块）返回发生更改的块为止。

- 响应可能回跳过快照中未写入的块。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 2000 – 2999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 2000 的增量快照。

使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照中发生更改的块时，响应将跳过块索引 0 - 1999 并将包含块索引 2000。响应不会包含空的 ChangedBlocks 数组。

## AWS CLI

以下 [list-changed-blocks](#) 示例命令返回快照 snap-1234567890 与 snap-0987654321 之间存在不同的数据块的数据块索引和数据块令牌。--starting-block-index 参数将结果限制为索引大于 0 的数据块，并且 --max-results 参数将结果限制为前 500 个数据块。

```

aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-id snap-0987654321 --starting-block-index 0 --max-results 500

```

以下为上一个命令的示例响应，其中显示了两个快照的数据块索引 0、6000、6001、6002 和 6003 存在不同。此外，数据块索引 6001、6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```

{
  "ChangedBlocks": [
    {
      "BlockIndex": 0,
      "FirstBlockToken": "AAABAVahm9S060Dyi00RySzn2ZjGjW/
KN3uygG1S0Q0YweszBbDnX2dGpmC",
      "SecondBlockToken":
      "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9T1vtCQxxoKV8qrUPQP7vcM6iWGSr"
    },
    {
      "BlockIndex": 6000,
      "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecljN4kkazK8inFXVintPkdaVFLfCMQsKe",
      "SecondBlockToken":
      "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777e1D9oVR"
    },
    {
      "BlockIndex": 6001,
      "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
    },
    {
      "BlockIndex": 6002,
      "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
    },
    {
      "BlockIndex": 6003,
      "FirstBlockToken":
      "AAABASmJ005JxA0ce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBR0uICb2A"
    },
    ...
  ],
  "ExpiryTime": 1576308931.973,
  "VolumeSize": 32212254720,
  "BlockSize": 524288,
  "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVa00zsPH/QM3Bi3zF//
06Mdi/BbJarBnp8h"
}

```

## AWS API

以下 BI [ListChangedblocks](#) 示例请求返回快照和之间不同区块的区块索引 `snap-0acEXAMPLEcf41648` 和区块标识 `snap-0c9EXAMPLE1b30e2f`。 `startingBlockIndex` 参数将结果限制为索引大于 0 的数据块，并且 `maxResults` 参数将结果限制为前 500 个数据块。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232546Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了两个快照的数据块索引 0、3072、6002 和 6003 存在不同。此外，数据块索引 6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 `GetSnapshotBlock` 操作，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
Content-Type: application/json
Content-Length: 1456
Date: Wed, 17 Jun 2020 23:25:47 GMT
Connection: keep-alive

{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "BlockIndex": 0,
      "FirstBlockToken": "AAUBAVaWq0CnDNuK1e11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+0JkL",
      "SecondBlockToken": "AAUBASxzy0Y0b33JVRL0Ym3N0resCxn5R0+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
    },
    {
      "BlockIndex": 3072,
```

```

        "FirstBlockToken":
        "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZ0LEmeXLmHBf2R/Yb24MaS",
        "SecondBlockToken":
        "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid"
    },
    {
        "BlockIndex": 6002,
        "FirstBlockToken": "AAABASqX4/
NWjvNceoyMULjcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
    },
    {
        "BlockIndex": 6003,
        "FirstBlockToken":
        "AAABASmJ005JxA0ce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBR0uICb2A"
    },
    ...
],
"ExpiryTime": 1.592976647009E9,
"VolumeSize": 3
}

```

## 从快照获取数据块数据

### AWS CLI

以下 [get-snapshot-block](#) 示例命令返回快照 6001 中，数据块令牌为 AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR 的数据块索引 snap-1234567890 中的数据。在 Windows 计算机上，二进制数据将输出到 data 目录中的 C:\Temp 文件。如果您在 Linux 或 Unix 计算机上运行该命令，请将输出路径替换为 /tmp/data 以将数据输出到 data 目录中的 /tmp 文件。

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

以下为上一个命令的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及校验和的算法。二进制数据会自动保存到您在请求命令中指定的目录和文件中。

```

{
    "DataLength": "524288",
    "Checksum": "cf0Y6/Fn0oFa4VyjQP0a/iD0zhTf1PTKzxGv20KowXc=",
    "ChecksumAlgorithm": "SHA256"
}

```

}

## AWS API

以下 [GetSnapshotBlock](#) 示例请求以快照形式返回区块索引中3072带有区块令牌AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid的数据snap-0c9EXAMPLE1b30e2f。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232838Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及用于生成校验和的算法。二进制数据在响应正文中传输，如下例所*BlockData*示。

```
HTTP/1.1 200 OK
x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
x-amz-Data-Length: 524288
x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/octet-stream
Content-Length: 524288
Date: Wed, 17 Jun 2020 23:28:38 GMT
Connection: keep-alive
```

*BlockData*

## 使用 EBS 直接 API 写入快照

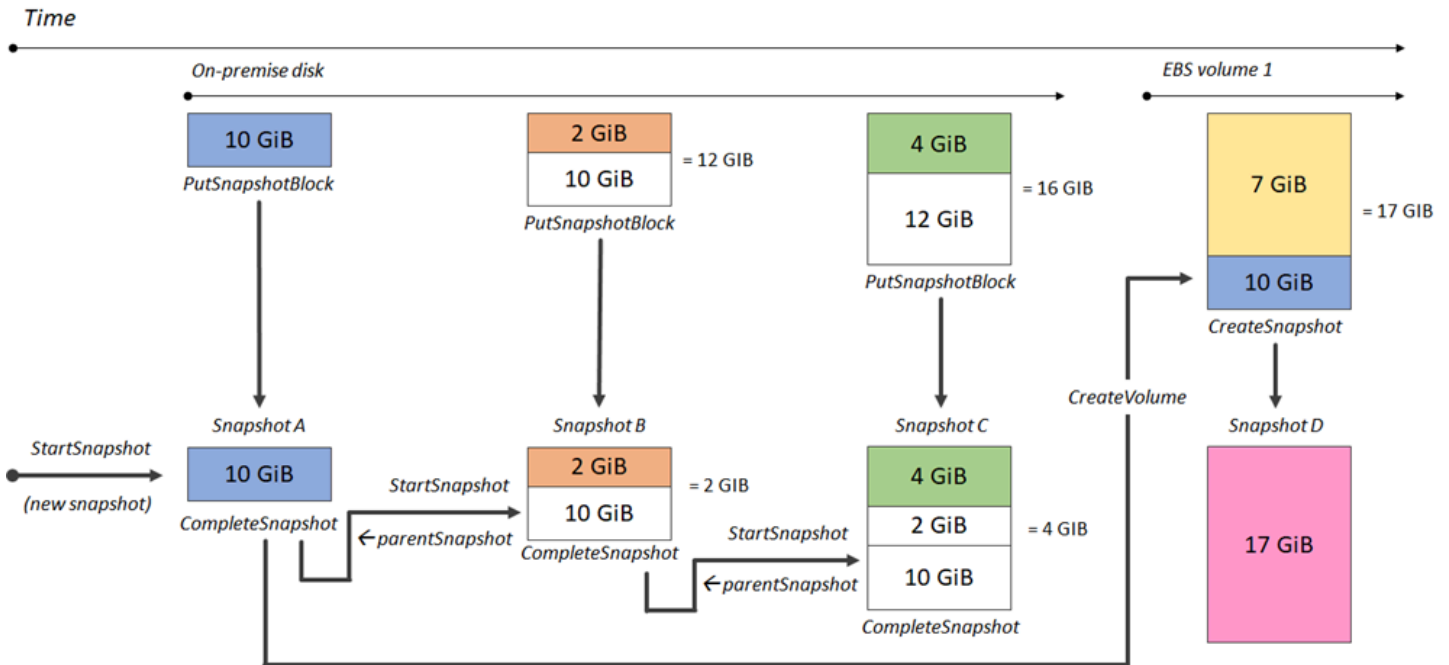
以下步骤介绍了如何使用 EBS direct API 写入增量快照：

1. 使用 StartSnapshot 操作并指定父快照 ID 将快照作为现有快照的增量快照启动，或者省略父快照 ID 以启动新快照。此操作返回处于“待处理”状态的新快照 ID。
2. 使用 PutSnapshotBlock 操作并指定待处理快照的 ID，以单个块的形式向其中添加数据。您必须为传输的数据块指定一个 Base64 编码的 SHA256 校验和。服务将计算接收到的数据的校验和，并使用您指定的校验和对其进行验证。如果校验和不匹配，则操作失败。

3. 向待处理的快照添加完数据后，使用 CompleteSnapshot操作启动异步工作流程，该工作流程将快照封存起来并将其移至已完成状态。

重复这些步骤，使用之前创建的快照作为父级创建新的增量快照。

例如，在下图中，快照 A 是启动的第一个新快照。快照 A 用作父快照来启动快照 B。快照 B 用作父快照来启动和创建快照 C。快照 A、B 和 C 均为增量快照。快照 A 用于创建 EBS 卷 1。快照 D 创建自 EBS 卷 1。快照 D 是 A 的增量快照；它不是 B 或 C 的增量快照。



以下示例显示如何使用 EBS 直接 API 写入快照。

## 主题

- [启动快照](#)
- [将数据放入快照](#)
- [完成快照](#)

## 启动快照

### AWS CLI

以下 `start-snapshot` 示例命令启动 8 GiB 快照，使用快照 `snap-123EXAMPLE1234567` 作为父快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或完成请求，则快照将转为错误状态。550e8400-e29b-41d4-a716-446655440000 客户端令牌

确保请求的幂等性。如果省略了客户端令牌，AWS SDK 会自动为您生成一个。有关幂等性的更多信息，请参阅 [API 的等性 StartSnapshot](#)。

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

以下为上一个命令的示例响应，其中显示了快照 ID、AWS 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以 pending 状态启动。在后续 put-snapshot-block 命令中指定快照 ID 以将数据写入快照，然后使用 complete-snapshot 命令完成快照并将其状态更改为 completed。

```
{
  "SnapshotId": "snap-0aaEXAMPLEe306d62",
  "OwnerId": "111122223333",
  "Status": "pending",
  "VolumeSize": 8,
  "BlockSize": 524288
}
```

## AWS API

以下 [StartSnapshot](#) 示例请求使用快照 `snap-123EXAMPLE1234567` 作为父快照启动 8 GiB 快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或完成请求，则快照将转为错误状态。`550e8400-e29b-41d4-a716-446655440000` 客户端令牌确保请求的幂等性。如果省略了客户端令牌，AWS SDK 会自动为您生成一个。有关幂等性的更多信息，请参阅 [API 的等性 StartSnapshot](#)。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
  "VolumeSize": 8,
  "ParentSnapshot": snap-123EXAMPLE1234567,
  "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
  "Timeout": 60
}
```

以下为上一个请求的示例响应，其中显示了快照 ID、AWS 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以“待处理”状态开始。在后续 PutSnapshotBlocks 请求中指定快照 ID，以将数据写入快照。

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
  "BlockSize": 524288,
  "Description": null,
  "OwnerId": "138695307491",
  "Progress": null,
  "SnapshotId": "snap-052EXAMPLEc85d8dd",
  "StartTime": null,
  "Status": "pending",
  "Tags": null,
  "VolumeSize": 8
}
```

## 将数据放入快照

### AWS CLI

以下 [put-snapshot](#) 示例命令将 524288 字节的数据写入快照 1000 上的数据块索引 snap-0aaEXAMPLEe306d62。Base64 编码的 Q0D3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= 校验和使用 SHA256 算法生成。传输的数据位于 /tmp/data 文件中。

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
--block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum Q0D3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= --checksum-algorithm SHA256
```

以下为上一个命令的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```
{
  "DataLength": "524288",
```



```

    "Checksum": "Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=",
    "ChecksumAlgorithm": "SHA256"
  }

```

## AWS API

以下[PutSnapshot](#)示例请求将524288字节的数据写入快照1000上的块索引snap-052EXAMPLEc85d8dd。Base64 编码的 Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= 校验和使用 SHA256 算法生成。数据在请求的正文中传输，如*BlockData*以下示例所示。

```

PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

```

*BlockData*

以下为上一个请求的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```

HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

```

```
{}
```

## 完成快照

### AWS CLI

以下 [complete-snapshot](#) 示例命令完成快照 `snap-0aaEXAMPLEe306d62`。该命令指定将 5 数据块写入快照。`6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacd0cA3KCM3c=` 校验和表示写入快照的完整数据集的校验和。有关校验和的更多信息，请参阅本指南前文中的[使用校验和](#)。

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacd0cA3KCM3c= --checksum-algorithm SHA256 --checksum-aggregation-method LINEAR
```

以下为上一个命令的示例响应。

```
{
  "Status": "pending"
}
```

### AWS API

以下 [CompleteSnapshot](#) 示例请求完成快照 `snap-052EXAMPLEc85d8dd`。该命令指定将 5 数据块写入快照。`6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacd0cA3KCM3c=` 校验和表示写入快照的完整数据集的校验和。

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacd0cA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应。

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
```

```
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

## 使用加密

使用启动新快照时 [StartSnapshot](#)，加密状态取决于您为“已加密”、“KmsKeyArn”和“ParentSnapshotID”指定的值，以及您的 AWS 账户是否在[默认情况下启用了加密功能](#)。

### Note

- 您可能需要其他 IAM 权限才能对 EBS direct API 使用加密。有关更多信息，请参阅 [使用权限 AWS KMS keys](#)。
- 如果您的 AWS 账户默认启用 Amazon EBS 加密，则无法创建未加密的快照。
- 如果您的 AWS 账户默认启用 Amazon EBS 加密，则无法使用未加密的父快照启动新快照。您必须首先通过复制父快照来对其进行加密。有关更多信息，请参阅 [复制 Amazon EBS 快照](#)。

### 主题

- [加密结果：未加密父快照](#)
- [加密结果：已加密父快照](#)
- [加密结果：无父快照](#)

### 加密结果：未加密父快照

下表描述了指定未加密父快照时每种可能的设置组合的加密结果。

ParentSnapshot我是	已加密	KmsKeyArn	默认加密	结果
未加密	已忽略	已忽略	已启用	请求失败并显示 ValidationException 。
			已禁用	快照未加密。

ParentSnapshot我是	已加密	KmsKeyArn	默认加密	结果
未加密	True	指定	已启用	请求失败并显示 ValidationException 。
			已禁用	
		已忽略	已启用	
			已禁用	
		指定	已启用	
			已禁用	
未加密	False	已忽略	已启用	请求失败并显示 ValidationException 。
			已禁用	
		指定	已启用	
			已禁用	

## 加密结果：已加密父快照

下表描述了指定已加密父快照时每种可能的设置组合的加密结果。

ParentSnapshot我是	已加密	KmsKeyArn	默认加密	结果
已加密	已忽略	已忽略	已启用	已使用与父快照相同的 KMS 密钥对快照进行加密。
			已禁用	
		指定	已启用	请求失败并显示 ValidationException 。
			已禁用	
已加密	True	已忽略	已启用	请求失败并显示 ValidationException 。

ParentSnapshot	已加密	KmsKeyArn	默认加密	结果
已加密	True	指定	已禁用	
			已启用	
			已禁用	
已加密	False	已忽略	已启用	请求失败并显示 ValidationException 。
			已禁用	
		指定	已启用	
			已禁用	

## 加密结果：无父快照

下表描述了未使用父快照时每种可能的设置组合的加密结果。

ParentSnapshot	已加密	KmsKeyArn	默认加密	结果
已忽略	True	已忽略	已启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	
		指定	已启用	使用为 KmsKeyArn 指定的 KMS 密钥对快照进行加密。
			已禁用	
已忽略	False	已忽略	已启用	请求失败并显示 ValidationException 。
			已禁用	快照未加密。
		指定	已启用	请求失败并显示 ValidationException 。
			已禁用	

ParentSnapshot	已加密	KmsKeyArn	默认加密	结果
已忽略	已忽略	已忽略	已启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	快照未加密。
		指定	已启用	使用为 KmsKeyArn 指定的 KMS 密钥对快照进行加密。
			已禁用	

\* 此默认 KMS 密钥可以是客户托管密钥，也可以是用于 Amazon EBS 加密的默认 AWS 托管 KMS 密钥。

## 使用签名版本 4 签名

签名版本 4 是向 HTTP 发送的 AWS 请求添加身份验证信息的过程。为了安全起见，对的大多数请求都 AWS 必须使用访问密钥进行签名，访问密钥由访问密钥 ID 和私有访问密钥组成。这两个密钥通常称为您的安全凭证。有关如何获取账户凭证的信息，请参阅 [AWS 安全凭证](#)。

如果您打算手动创建 HTTP 请求，则必须了解如何对其签名。当您使用 AWS Command Line Interface (AWS CLI) 或其中一个 AWS 软件开发工具包向发出请求时 AWS，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。当您使用这些工具时，您不必了解如何亲自签署这些请求。

有关更多信息，请参阅 IAM 用户指南中的 [签署 AWS API 请求](#)。

## 使用校验和

该 GetSnapshotBlock 操作返回快照块中的数据，该 PutSnapshotBlock 操作将数据添加到快照中的区块中。传输的数据块数据不在签名版本 4 签名流程中进行签名。因此，使用校验和来验证数据的完整性，如下所示：

- 当您使用 GetSnapshotBlock 操作时，响应会使用 x-amz-checkSum 标头为区块数据提供 Base64 编码的 SHA256 校验和，并使用 x-amz-checksum 算法标头为校验和算法提供校验和算法。使用返回的校验和验证数据的完整性。如果生成的校验和与 Amazon EBS 提供的校验和不匹配，您应将数据视为无效，然后重试请求。

- 使用 PutSnapshotBlock 操作时，您的请求必须使用 x-amz-checkSum 标头为区块数据提供 Base64 编码的 SHA256 校验和，并使用 x-amz-checksum 算法标头提供校验和算法。您提供的校验和将根据 Amazon EBS 生成的校验和进行验证，以验证数据的完整性。如果校验和不相符，请求将失败。
- 使用该 CompleteSnapshot 操作时，您的请求可以选择为添加到快照中的完整数据集提供一个 Base64 编码的 SHA256 汇总校验和。使用 x-amz-Checksum 标头提供校验和，使用 x-amz-Checksum-Algorithm 标头提供校验和算法，并使用 x-amz-Checksum-Aggregation-Method 标头提供校验和聚合方法。要使用线性聚合方法生成聚合校验和，请按照数据块索引的升序排列各个写入数据块的校验和，将它们连接成单个字符串，然后使用 SHA256 算法生成整个字符串的校验和。

这些操作中的校验和是签名版本 4 签名流程的一部分。

## API 的等性 StartSnapshot

幂等性确保 API 请求仅完成一次。对于幂等请求，如果原始请求成功完成，则后续重试将返回原始成功请求的结果，它们不会有额外的影响。

[StartSnapshot](#) API 使用客户端令牌支持等性。客户端令牌是您在发出 API 请求时指定的唯一字符串。如果在某个 API 请求成功完成后，您使用相同的客户端令牌和相同的请求参数重试该请求，则返回原始请求的结果。如果使用相同的客户端令牌重试请求，但更改了一个或多个请求参数，则返回 ConflictException 错误。

如果您未指定自己的客户端令牌，AWS SDK 会自动为请求生成客户端令牌，以确保其是等效的。

客户端令牌可以是包含最多 64 个 ASCII 字符的任意字符串。您不应为不同的请求重复使用相同的客户端令牌。

使用 API 使用您自己的客户端令牌发出等效 StartSnapshot 请求

指定 ClientToken 请求参数。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
  "VolumeSize": 8,
  "ParentSnapshot": snap-123EXAMPLE1234567,
  "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
```

```
"Timeout": 60
}
```

要使用您自己的客户端令牌发出等效 StartSnapshot 请求，请使用 AWS CLI

指定 `client-token` 请求参数。

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

## 错误重试

AWS SDK 对返回错误响应的请求实施自动重试逻辑。您可以为 AWS SDK 配置重试设置。有关更多信息，请参阅 SDK 文档。

AWS CLI 可以配置为自动重试部分失败的请求。有关为配置重试次数的更多信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》中的[AWS CLI 重试次数](#)。

AWS 查询 API 不支持失败的请求的重试逻辑。如果您使用的是 HTTP 或 HTTPS 请求，则必须在客户端应用程序中实现重试逻辑。

下表显示了可能的 API 错误响应。部分 API 错误是可重试的。客户端应用程序始终可以重试收到可重试错误的失败请求。

错误	响应代码	描述	由以下对象引发	可重试？
InternalServerErrorException	500	由于网络或 AWS 服务器端问题，请求失败。	所有 API	是
ThrottlingException	400	API 请求的数量已超过账户允许的最大 API 请求节流限制。	所有 API	是
RequestThrottlingException	400	API 请求的数量已超过快照允许的最大 API 请求节流限制。	GetSnapshotBlock   PutSnapshotBlock	是



错误	响应代码	描述	由以下对象引发	可重试？
显示消息“Failed to read block data”的 ValidationException	400	提供的数据块不可读。	PutSnapshot屏蔽	是
显示任何其他消息的 ValidationException	400	请求语法格式错误，或输入不满足 AWS 服务规定的约束。	所有 API	否
ResourceNotFoundException	404	指定的快照 ID 不存在。	所有 API	否
ConflictException	409	指定的客户端令牌曾在具有不同请求参数的类似请求中使用过。有关更多信息，请参阅 <a href="#">API 的等性 StartSnapshot</a> 。	StartSnapshot	否
AccessDeniedException	403	您无权执行请求的操作。	所有 API	否
ServiceQuotaExceededException	402	请求失败，因为执行请求将超出您账户的一项或多项相关服务限额。	所有 API	否

错误	响应代码	描述	由以下对象引发	可重试？
InvalidSignatureException	403	请求授权签名已过期。必须刷新授权签名才能重试请求。	所有 API	否

## 优化性能

您可以并发运行 API 请求。假设 PutSnapshotBlock 延迟为 100 毫秒，则一个线程可以在一秒钟内处理 10 个请求。此外，假设您的客户端应用程序创建多个线程和连接（例如 100 个连接），那么它每秒可以发出 1000（10 \* 100）个请求。这对应于大约每秒 500 MB 的吞吐量。

以下列表包含在您应用程序中需要了解的几点：

- 每个线程是否使用单独的连接？如果应用程序上的连接受限制，则多线程将等待可用连接，而您会发现吞吐量较低。
- 应用程序的两个放置请求之间是否有任何等待时间？这将降低线程的有效吞吐量。
- 实例的带宽限制-如果实例上的带宽由其他应用程序共享，则可能会限制 PutSnapshotBlock 请求的可用吞吐量。

请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应将重试机制内置到 EBS direct API 工作流程中，以处理限制、超时和服务不可用性。

查看 EBS direct API 服务配额以确定您每秒可运行的最大 API 请求数。有关更多信息，请参阅 AWS 一般参考中的 [Amazon Elastic Block Store 终端节点和配额](#)。

## EBS 直接 API 服务端点

端点是用作 AWS Web 服务入口点的 URL。EBS 直接 API 支持以下端点类型：

- IPv4 端点
- 同时支持 IPv4 和 IPv6 的双堆栈端点
- FIPS 端点

当您发出请求时，您可以指定要使用的端点和区域。如果不指定端点，则默认使用 IPv4 端点。要使用不同的端点类型，您必须在请求中指定。有关如何执行此操作的示例，请参阅[指定端点](#)。

有关区域的更多信息，请参阅 Amazon EC2 用户指南中的 [区域和可用区](#)。有关 EBS 直接 API 的端点列表，请参阅 Amazon Web Services 一般参考 中的 [EBS 直接 API 的端点](#)。

## 主题

- [IPv4 端点](#)
- [双栈 \( IPv4 和 IPv6 \) 端点](#)
- [FIPS 端点](#)
- [指定端点](#)

## IPv4 端点

IPv4 端点仅支持 IPv4 流量。IPv4 端点适用于所有区域。

EBS 直接 API 仅支持可用于发出请求的区域 IPv4 终端节点。您必须在终端节点名称中指定区域。端点名称使用以下命名约定：

- `ebs.region.amazonaws.com`

例如，要将请求定向到 us-east-2 IPv4 终端节点，必须指定 `ebs.us-east-2.amazonaws.com` 为终端节点。有关 EBS 直接 API 的端点列表，请参阅 Amazon Web Services 一般参考 中的 [EBS 直接 API 的端点](#)。

## 定价

在相同区域使用 IPv4 端点时，EBS 直接 API 和 Amazon EC2 实例之间直接传输数据是免费的。但是，如果有中间服务，例如 AWS PrivateLink 终端节点、NAT 网关或 Amazon VPC 传输网关，则需要向您收取相关费用。

## 双栈 ( IPv4 和 IPv6 ) 端点

同时支持 IPv4 和 IPv6 流量的双堆栈端点。双堆栈端点适用于所有区域。

要使用 IPv6，您必须使用双堆栈端点。当您向双堆栈端点发出请求时，端点 URL 解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

EBS 直接 API 只支持区域双堆栈端点，这意味着，您必须将区域指定为端点名称的一部分。双堆栈端点名称使用以下命名约定：

- `ebs.region.api.aws`

例如，eu-west-1 区域的双堆栈端点名称是 ebs.eu-west-1.api.aws。有关 EBS 直接 API 的端点列表，请参阅 Amazon Web Services 一般参考 中的 [EBS 直接 API 的端点](#)。

## 定价

在相同区域使用双堆栈端点时，EBS 直接 API 和 Amazon EC2 实例之间直接传输数据是免费的。但是，如果有中间服务，例如 AWS PrivateLink 终端节点、NAT 网关或 Amazon VPC 传输网关，则需要向您收取相关费用。

## FIPS 端点

EBS 直接 API 为以下区域提供经过 FIPS 验证的 IPv4 和双堆栈 ( IPv4 和 IPv6 ) 端点：

- us-east-1 – 美国东部 ( 弗吉尼亚州北部 )
- us-east-2 – 美国东部 ( 俄亥俄州 )
- us-west-1 – 美国西部 ( 北加利福尼亚 )
- us-west-2 – 美国西部 ( 俄勒冈州 )
- ca-central-1 – 加拿大 ( 中部 )

FIPS IPv4 端点使用以下命名约定：ebs-fips.*region*.amazonaws.com。例如，us-east-1 的 FIPS IPv4 端点是 ebs-fips.us-east-1.amazonaws.com。

FIPS 双堆栈端点使用以下命名约定：ebs-fips.*region*.api.aws。例如，us-east-1 的 FIPS 双堆栈端点是 ebs-fips.us-east-1.api.aws。

有关 FIPS 端点的更多信息，请参阅 Amazon Web Services 一般参考 中的 [FIPS 端点](#)。

## 指定端点

本节提供了一些在发出请求时如何指定端点的示例。

### AWS CLI

以下示例显示如何使用 AWS CLI 为 us-east-2 区域指定端点。

- 双堆栈

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

## AWS SDK for Java 2.x

以下示例显示如何使用 AWS SDK for Java 2.x 为 `us-east-2` 区域指定端点。

- 双堆栈

```
AwsClientBuilder.EndpointConfiguration config = new  
    AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-east-2");  
AmazonEBS ebs = AmazonEBSClientBuilder.standard()  
    .withEndpointConfiguration(config)  
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new  
    AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com", "us-east-2");  
AmazonEBS ebs = AmazonEBSClientBuilder.standard()  
    .withEndpointConfiguration(config)  
    .build();
```

## AWS SDK for Go

以下示例显示如何使用 AWS SDK for Go 为 `us-east-2` 区域指定端点。

- 双堆栈

```
sess := session.Must(session.NewSession())  
svc := ebs.New(sess, &aws.Config{  
    Region: aws.String(endpoints.UsEast1RegionID),  
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")  
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

## EBS 直接 API 的定价

### 主题

- [API 的定价](#)
- [联网成本](#)

## API 的定价

您为使用 EBS direct API 支付的费用取决于您发出的请求数。有关更多信息，请参阅 [Amazon EBS 定价](#)。

- ListChanged区块和 ListSnapshotBlocks API 按请求收费。例如，如果您在某个地区发出 100,000 ListSnapshotBlocks 个 API 请求，且该地区每 1,000 个请求收费 0.0006 美元，则将向您收取 0.06 美元的费用（每 1,000 个请求 0.0006 美元 x 100）。
- GetSnapshot按返回的@@ 区块收取区块费用。例如，如果您在某个地区发出 100,000 GetSnapshotBlock 个 API 请求，且每返回 1,000 个区块收费 0.003 美元，则将支付 0.30 美元（每返回 1,000 个区块 0.003 美元 x 100）。
- PutSnapshot区块按写入的区块收费。例如，如果您在某个地区发出 100,000 PutSnapshotBlock 个 API 请求，且每写入 1,000 个区块收费 0.006 美元，则将支付 0.60 美元的费用（每写入 1,000 个区块 0.006 美元 x 100）。

## 联网成本

### 数据传输成本

使用[非 FIP S](#) 终端节点时，直接在 EBS 直接 API 和同一 AWS 区域的 Amazon EC2 实例之间传输的数据是免费的。有关更多信息，请参阅[AWS 服务端点](#)。如果您的数据传输途中还有其他 AWS 服务，则将向您收取相关的数据处理费用。这些服务包括但不限于 PrivateLink 终端节点、NAT 网关和 Transit Gateway。

## VPC 接口终端节点

如果您使用来自 Amazon EC2 实例的 EBS 直接 API 或私有子网中的 AWS Lambda 函数，则可以使用 VPC 接口终端节点，而不使用 NAT 网关，以降低网络数据传输成本。有关更多信息，请参阅 [将接口 VPC 终端节点与 EBS 直接 API 结合使用](#)。

## 将接口 VPC 终端节点与 EBS 直接 API 结合使用

您可以通过创建由 [AWS PrivateLink](#) 提供支持的接口 VPC 终端节点在 VPC 和 EBS 直接 API 之间建立私有连接。您可以访问 EBS 直接 API，就像它在您的 VPC 中一样，而无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例即使没有公有 IP 地址也可与 EBS direct API 进行通信。

我们将在您为接口终端节点启用的每个子网中创建一个终端节点网络接口。

有关更多信息，请参阅 [AWS PrivateLink 指南](#) 中的 [AWS PrivateLink 中的 AWS 服务 直通访问](#)。

## 关于 EBS direct API VPC 终端节点的注意事项

在为 EBS 直接 API 设置接口 VPC 终端节点之前，请查看 [AWS PrivateLink 指南](#) 中的 [注意事项](#)。

默认情况下，允许通过终端节点对 EBS direct API 进行完全访问。您可以使用 VPC 终端节点策略控制对接口终端节点的访问。您可以将终端节点策略附加到控制对 EBS 直接 API 的访问权限的 VPC 终端节点。该策略指定以下信息：

- 可以执行操作的委托人。
- 可以执行的操作。
- 可以对其执行操作的资源。

有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [使用 VPC 终端节点控制对服务的访问](#)。

以下是 EBS 直接 API 的终端节点策略示例。当连接到终端节点时，此策略授予对所有资源的所有 EBS 直接 API 操作的访问权限，但标有密钥 `Environment` 和值 `Test` 的快照除外。

```
{
  "Statement": [
    {
      "Effect": "Deny",
```

```
    "Action": "ebs:*",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    },
    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

## 为 EBS direct API 创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface ( AWS CLI ) 为 EBS 直接 API 创建 VPC 端点。有关更多信息，请参阅 AWS PrivateLink 指南中的[创建 VPC 终端节点](#)。

使用以下服务名称为 EBS direct API 创建 VPC 终端节点：

- `com.amazonaws.region.ebs`

如果为终端节点启用私有 DNS，则可以使用其默认 DNS 名称作为区域，向 EBS direct API 发送 API 请求，例如 `ebs.us-east-1.amazonaws.com`。

## 使用 EBS 直接 API 记录 API 的 API 调用 AWS CloudTrail

EBS 直接 API 服务已与集成。AWS CloudTrail CloudTrail 是一项提供用户、角色或服务所执行操作记录的 AWS 服务。CloudTrail 将在 EBS 直接 API 中执行的所有 API 调用捕获为事件。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到亚马逊简单存储服务 (Amazon S3) 存储桶。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的管理事件。事件历史记录中不会捕获数据事件。您可以使用收集的信息 CloudTrail 来确定向 EBS direct API 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关的更多信息 CloudTrail，请参阅 [《AWS CloudTrail 用户指南》](#)。



## EBS 直接 API 中的信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 EBS direct API 中出现支持的事件活动时，该活动将与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅[使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您的 AWS 账户中的事件，包括 EBS 直接 API 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传送到 S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- [创建跟踪概述](#)
- [CloudTrail 支持的服务和集成](#)
- [配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)和[接收来自多个账户的 CloudTrail 日志文件](#)

### 支持的 API 操作

对于 EBS 直接 API CloudTrail，您可以使用记录两种类型的事件：

- 管理事件 — 管理事件提供对 AWS 账户快照执行的管理操作的可见性。以下 API 操作预设情况下将作为管理事件记录在跟踪记录中：
  - [StartSnapshot](#)
  - [CompleteSnapshot](#)

有关记录管理事件的更多信息，请参阅《CloudTrail 用户指南》中的[记录跟踪的管理事件](#)。

- 数据事件 – 通过这些事件，可以了解对快照执行的或在快照内执行的快照操作。以下 API 操作可以选择作为跟踪中的数据事件记录：
  - [ListSnapshot](#)方块
  - [ListChanged](#)方块
  - [GetSnapshotBlock](#)
  - [PutSnapshot](#)屏蔽

预设情况下，在您创建跟踪记录时，未记录数据事件。您只能使用 advanced event selectors ( 高级事件选择器 ) 来记录 EBS 直接 API 调用上的数据事件。有关更多信息，请参阅 CloudTrail 用户指南中的 [记录跟踪的数据事件](#)。

#### Note

如果您对与您共享的快照执行操作，则不会将数据事件发送到拥有该快照的 AWS 账户。

## 身份信息

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail 用户 IdentityElement](#)。

## 了解 EBS direct API 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下是示例 CloudTrail 日志条目。

### StartSnapshot

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  }
}
```

```

},
"eventTime": "2020-07-03T23:27:26Z",
"eventSource": "ebs.amazonaws.com",
"eventName": "StartSnapshot",
"awsRegion": "eu-west-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "PostmanRuntime/7.25.0",
"requestParameters": {
  "volumeSize": 8,
  "clientToken": "token",
  "encrypted": true
},
"responseElements": {
  "snapshotId": "snap-123456789012",
  "ownerId": "123456789012",
  "status": "pending",
  "startTime": "Jul 3, 2020 11:27:26 PM",
  "volumeSize": 8,
  "blockSize": 524288,
  "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
"eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}

```

## CompleteSnapshot

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2020-07-03T23:28:24Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "CompleteSnapshot",
  "awsRegion": "eu-west-1",

```

```

"sourceIPAddress": "192.0.2.0",
"userAgent": "PostmanRuntime/7.25.0",
"requestParameters": {
  "snapshotId": "snap-123456789012",
  "changedBlocksCount": 5
},
"responseElements": {
  "status": "completed"
},
"requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
"eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}

```

## ListSnapshotBlocks

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-03T00:32:46Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "ListSnapshotBlocks",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "111.111.111.111",
  "userAgent": "PostmanRuntime/7.28.0",
  "requestParameters": {
    "snapshotId": "snap-abcdef01234567890",
    "maxResults": 100,
    "startingBlockIndex": 0
  },
  "responseElements": null,
  "requestID": "example6-0e12-4aa9-b923-1555eexample",
  "eventID": "example4-218b-4f69-a9e0-2357dexample",
  "readOnly": true,
  "resources": [

```

```

    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Snapshot",
      "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012",
  "eventCategory": "Data",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-SHA",
    "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
  }
}

```

## ListChangedBlocks

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-02T21:11:46Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "ListChangedBlocks",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "111.111.111.111",
  "userAgent": "PostmanRuntime/7.28.0",
  "requestParameters": {
    "firstSnapshotId": "snap-abcdef01234567890",
    "secondSnapshotId": "snap-9876543210abcdef0",
    "maxResults": 100,
    "startingBlockIndex": 0
  },
  "responseElements": null,
  "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
}

```

```

"eventID": "example3-fac4-4a78-8ebb-3e9d3example",
"readOnly": true,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-SHA",
  "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}

```

## GetSnapshotBlock

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-02T20:43:05Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "GetSnapshotBlock",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "111.111.111.111",
  "userAgent": "PostmanRuntime/7.28.0",

```

```

"requestParameters": {
  "snapshotId": "snap-abcdef01234567890",
  "blockIndex": 1,
  "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
},
"responseElements": null,
"requestID": "examplea-6eca-4964-abfd-fd9f0example",
"eventID": "example6-4048-4365-a275-42e94example",
"readOnly": true,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-SHA",
  "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}

```

## PutSnapshotBlock

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-02T21:09:17Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "PutSnapshotBlock",
  "awsRegion": "us-east-1",

```

```
"sourceIPAddress": "111.111.111.111",
"userAgent": "PostmanRuntime/7.28.0",
"requestParameters": {
  "snapshotId": "snap-abcdef01234567890",
  "blockIndex": 1,
  "dataLength": 524288,
  "checksum": "exampleodSGvFSb1e3kxWUgb0Q4TbzPurnsfVexample",
  "checksumAlgorithm": "SHA256"
},
"responseElements": {
  "checksum": "exampleodSGvFSb1e3kxWUgb0Q4TbzPurnsfVexample",
  "checksumAlgorithm": "SHA256"
},
"requestID": "example3-d5e0-4167-8ee8-50845example",
"eventID": "example8-4d9a-4aad-b71d-bb31fexample",
"readOnly": false,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-SHA",
  "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}
```

## 常见问题

如果快照具有挂起状态，是否可以使用 EBS direct API 访问该快照？

不可以。仅当快照具有已完成状态时，才能访问该快照。

EBS direct API 是否按数字顺序返回数据块索引？

是。返回的数据块索引是唯一的，并按数字顺序排列。



我能否提交 MaxResults 参数值低于 100 的请求？

不是。您可以使用的最小 MaxResult 参数值为 100。如果您提交的请求 MaxResult 参数值低于 100，并且快照中有超过 100 个区块，则 API 将返回至少 100 个结果。

我是否可以并发运行 API 请求？

您可以并发运行 API 请求。请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应将重试机制内置到 EBS direct API 工作流程中，以处理限制、超时和服务不可用性。有关更多信息，请参阅[优化性能](#)。

查看 EBS direct API 服务配额以确定您每秒可运行的 API 请求数。有关更多信息，请参阅 AWS General Reference 中的 [Amazon Elastic Block Store 终端节点和配额](#)。

运行 ListChangedBlocks 操作时，即使快照中有块，是否也可能得到空响应？

是。如果快照中几乎没有更改的数据块，则响应可能为空，但 API 将返回下一页令牌值。使用下一页令牌值来继续转到下一页结果。当 API 返回的下一页令牌值为 null 时，您可以确认已到达最后一页结果。

如果 NextToken 参数与参数一起指定，则使用两者中的哪一个 StartingBlockIndex ？

使用 NextToken 了，而忽略 StartingBlockIndex 了。

数据块令牌和下一个令牌的有效期是多久？

数据块令牌的有效期为七天，下一个令牌的有效期为 60 分钟。

是否支持已加密快照？

是。可以使用 EBS direct API 访问加密快照。

要访问加密快照，用户必须有权访问用于加密快照的 KMS 密钥和 AWS KMS 解密操作。有关分配给用户的 AWS KMS 策略，请参阅本指南前[EBS 直接 API 的 IAM 权限](#)面的部分。

是否支持公有快照？

不支持公有快照。

是否支持 Outposts 上的 Amazon EBS 本地快照？

不支持 Outposts 上的 Amazon EBS 本地快照。

list snapshot block 是返回快照中的所有数据块索引和数据块令牌，还是仅返回那些写入数据的数据块索引和数据块令牌？

它只返回写入数据的数据块索引和令牌。

我能否获得 EBS direct API 在我的账户上发起的所有 API 调用的历史记录，以便用于安全分析和运营方面的故障排除？

是。要获取您账户上的 EBS direct API 的 API 调用的历史记录，请在 AWS Management Console 中打开 AWS CloudTrail。有关更多信息，请参阅 [使用 EBS 直接 API 记录 API 的 API 调用 AWS CloudTrail](#)。

# Amazon Elastic Block Store 中的安全性

AWS 的云安全性的优先级最高。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 的客户，您也可以从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。[责任共担模式](#)将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 [AWS Compliance Programs](#) 的一部分。要了解适用于 Amazon Elastic Block Store 的合规性计划，请参阅[按合规性计划提供的范围内 AWS 服务](#)。
- 云中的安全性：您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon EBS 时应用责任共担模式。以下主题说明如何配置 Amazon EBS 以实现安全性和合规性目标。您还会了解如何使用其他 AWS 服务来帮助自己监控和保护 Amazon EBS 资源。

## 主题

- [Amazon Elastic Block Store 中的数据保护](#)
- [适用于 Amazon Elastic Block Store 的 Identity and Access Management](#)
- [Amazon Elastic Block Store 的合规性验证](#)
- [Amazon Elastic Block Store 中的恢复功能](#)

# Amazon Elastic Block Store 中的数据保护

AWS [责任共担模式](#)应用于 Amazon Elastic Block Store 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题解答](#)。有关欧洲数据保护的信息，请参阅 AWS 安全性博客上的 [AWS 责任共担模式和 GDPR](#) 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅 [《美国联邦信息处理标准 \( FIPS \) 第 140-2 版》](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。将控制台、API、AWS CLI 或 AWS SDK 与 Amazon EBS 或其他 AWS 服务结合使用时，也是如此。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

## 主题

- [Amazon EBS 数据安全](#)
- [静态和动态加密](#)
- [KMS 密钥管理](#)

## Amazon EBS 数据安全

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说明了的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

## 静态和动态加密

Amazon EBS 加密是一种加密解决方案，使您能够使用 AWS Key Management Service 加密密钥对 Amazon EBS 卷和 Amazon EBS 快照进行加密。EBS 加密操作在托管 Amazon EC2 实例的服务器上进行，用于确保静态数据的安全性，以及在实例和其挂载的卷与任何后续快照之间的传输中数据的安全性。有关更多信息，请参阅 [Amazon EBS 加密](#)。

## KMS 密钥管理

创建加密的 Amazon EBS 卷或快照时，您可以指定 AWS Key Management Service 密钥。默认情况下，Amazon EBS 将在您的账户和区域 (aws/ebs) 中将 AWS 托管 KMS 密钥用于 Amazon EBS。不过，您可以指定自己创建和管理的客户托管的 KMS 密钥。使用客户托管的 KMS 密钥可以提高灵活性，包括提供创建、轮换和禁用 KMS 密钥的能力。

要使用客户托管的 KMS 密钥，您必须向用户授予使用 KMS 密钥的权限。有关更多信息，请参阅[用户的权限](#)。

### Important

Amazon EBS 仅支持[对称 KMS 密钥](#)。不能使用[非对称 KMS 密钥](#)来加密 Amazon EBS 卷和快照。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅[识别非对称 KMS 密钥](#)。

对于每个卷，Amazon EBS 要求 AWS KMS 生成一个使用您指定的 KMS 密钥进行加密的唯一数据密钥。Amazon EBS 使用该卷存储加密数据密钥。然后，当您为卷附加到 Amazon EC2 实例时，Amazon EBS 会调用 AWS KMS 来解密数据密钥。Amazon EBS 使用管理程序内存中的明文数据密钥来加密卷的所有 I/O。有关更多信息，请参阅[EBS 加密的工作原理](#)。

## 适用于 Amazon Elastic Block Store 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证 (登录) 和获得授权 (具有权限) 来使用 Amazon EBS 资源。IAM 是一项无需额外费用即可使用的 AWS 服务。

### 主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [Amazon Elastic Block Store 如何与 IAM 配合使用](#)
- [适用于 Amazon Elastic Block Store 的基于身份的策略示例](#)
- [Amazon EBS 身份和访问疑难解答](#)

## 受众

如何使用 AWS Identity and Access Management ( IAM ) 因您在 Amazon EBS 中执行的操作而异。

**服务用户** – 如果使用 Amazon EBS 服务来完成任务，管理员会为您提供所需的凭证和权限。随着用来完成工作的 Amazon EBS 功能增多，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果无法访问 Amazon EBS 中的功能，请参阅[Amazon EBS 身份和访问疑难解答](#)。

**服务管理员** – 如果您在公司负责管理 Amazon EBS 资源，您可能对 Amazon EBS 具有完全访问权限。您有义务为服务用户确定可访问的 Amazon EBS 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon EBS 搭配使用的更多信息，请参阅[Amazon Elastic Block Store 如何与 IAM 配合使用](#)。

**IAM 管理员** – 如果您是 IAM 管理员，您可能需要详细了解如何编写策略以管理对 Amazon EBS 的访问。要查看您可在 IAM 中使用的 Amazon EBS 基于身份的策略示例，请参阅[适用于 Amazon Elastic Block Store 的基于身份的策略示例](#)。

## 使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过担任 IAM 角色进行身份验证 ( 登录到 AWS )。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center ( IAM Identity Center ) 用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接代入角色。

根据用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的[如何登录到您的 AWS 账户](#)。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证以加密方式签署您的请求。如果不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的[签署 AWS API 请求](#)。

无论使用何种身份验证方法，您可能需要提供其它安全信息。例如，AWS 建议您使用多重身份验证 ( MFA ) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[多重身份验证](#)和《IAM 用户指南》中的[在 AWS 中使用多重身份验证 \( MFA \)](#)。

## AWS 账户根用户

创建AWS 账户时，最初使用的是一个对账户中所有AWS 服务和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

## 联合身份

作为最佳实操，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份来源提供的凭证来访问 AWS 服务的用户。当联合身份访问 AWS 账户时，他们担任角色，而角色提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到自己的身份源中的一组用户和组以跨所有 AWS 账户 和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的[什么是 IAM Identity Center ?](#)

## IAM 用户和组

[IAM 用户](#)是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是一个用于指定一组 IAM 用户的身份。您不能使用组的身份登录。可以使用群组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，可能具有一个名为 IAMAdmins 的群组，并为该群组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人担任。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的[何时创建 IAM 用户（而不是角色）](#)。

## IAM 角色

[IAM 角色](#)是 AWS 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 AWS Management Console 中暂时担任 IAM 角色。您可以调用 AWS CLI 或 AWS

API 操作或使用自定义网址以担任角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的[使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。如果使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。
- 临时 IAM 用户权限 – IAM 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 AWS 服务，可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户存取的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问：某些 AWS 服务使用其它 AWS 服务中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用主体调用 AWS 服务的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。
- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的[创建向 AWS 服务委派权限的角色](#)。
- 服务相关角色：服务相关角色是与 AWS 服务关联的一种服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序：您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的[使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。



要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的[何时创建 IAM 角色（而不是用户）](#)。

## 使用策略管理访问

将创建策略并将其附加到AWS身份或资源，以控制AWS中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评测这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在AWS中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的[JSON 策略概览](#)。

管理员可以使用AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 iam:GetRole 操作的策略。具有该策略的用户可以从AWS Management Console、AWS CLI或AWS API 获取角色信息。

### 基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到AWS账户中的多个用户、组和角色的独立策略。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的[在托管式策略与内联策略之间进行选择](#)。

### 基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管策略。

## 访问控制列表 ( ACL )

访问控制列表 ( ACL ) 控制哪些主体 ( 账户成员、用户或角色 ) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的[访问控制列表 \(ACL\) 概览](#)。

## 其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型所授予的最大权限。

- **权限边界**：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体 ( IAM 用户或角色 ) 授予的最大权限。可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 字段中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的[IAM 实体的权限边界](#)。
- **服务控制策略 ( SCP )**：SCP 是 JSON 策略，指定了组织或组织单位 ( OU ) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 ( SCP )。SCP 限制成员账户中实体 ( 包括每个 AWS 账户根用户 ) 的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的[SCP 的工作原理](#)。
- **会话策略** – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的[会话策略](#)。

## 多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅《IAM 用户指南》中的[策略评估逻辑](#)。

## Amazon Elastic Block Store 如何与 IAM 配合使用

在使用 IAM 管理对 Amazon EBS 的访问权限之前，您应该了解哪些 IAM 功能可用于 Amazon EBS。

## 可与 Amazon Elastic Block Store 配合使用的 IAM 功能

IAM 功能	Amazon EBS 支持
<a href="#">基于身份的策略</a>	是
<a href="#">基于资源的策略</a>	否
<a href="#">策略操作</a>	是
<a href="#">策略资源</a>	是
<a href="#">策略条件键</a>	是
<a href="#">ACL</a>	否
<a href="#">ABAC (策略中的标签)</a>	部分
<a href="#">临时凭证</a>	是
<a href="#">主体权限</a>	是
<a href="#">服务角色</a>	是
<a href="#">服务相关角色</a>	否

要大致了解 Amazon EBS 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅《IAM 用户指南》中的[使用 IAM 的 AWS 服务](#)。

### Amazon EBS 基于身份的策略

支持基于身份的策略 是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素引用](#)。

## Amazon EBS 基于身份的策略示例

要查看 Amazon EBS 基于身份的策略示例，请参阅[适用于 Amazon Elastic Block Store 的基于身份的策略示例](#)。

## Amazon EBS 内基于资源的策略

支持基于资源的策略	否
-----------	---

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 AWS 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的 [IAM 角色与基于资源的策略有何不同](#)。

## Amazon EBS 的策略操作

支持策略操作	是
--------	---

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Amazon EBS 操作的列表，请参阅《服务授权参考》中的[操作、资源和条件键](#)。

Amazon EBS 中的策略操作在操作前面使用以下前缀：

```
ec2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"  
]
```

要查看 Amazon EBS 基于身份的策略示例，请参阅[适用于 Amazon Elastic Block Store 的基于身份的策略示例](#)。

## Amazon EBS 的策略资源

支持策略资源

是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实操，请使用 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (\*) 指示语句应用于所有资源。

```
"Resource": "*"
```

有关 Amazon EBS 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 [Amazon Elastic Block Store 定义的资源](#)。要了解您可以使用哪些操作指定每个资源的 ARN，请参阅 [Amazon Elastic Block Store 定义的操作](#)。

某些 Amazon EBS API 操作支持多个资源。要在单个语句中指定多个资源，请使用逗号分隔 ARN。例如，DescribeVolumes 访问 vol-01234567890abcdef 和 vol-09876543210fedcba，因此主体必须具有访问这两个资源的权限。

```
"Resource": [  
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",  
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"  
]
```

## Amazon EBS 的策略条件键

支持特定于服务的策略条件键 **是**

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素 ( 或 Condition 块 ) 中，可以指定语句生效的条件。Condition 元素是可选的。可以创建使用[条件运算符](#) ( 例如，等于或小于 ) 的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评测它们。如果您要为单个条件键指定多个值，则 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM policy 元素：变量和标签](#)。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文键](#)。

例如，以下条件允许主体仅在卷类型为 gp2 时才对卷执行操作。

```
"Condition":{  
  "StringLikeIfExists":{  
    "ec2:VolumeType":"gp2"  
  }  
}
```

要查看 Amazon EBS 条件键的列表，请参阅《服务授权参考》中的[操作、资源和条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅[Amazon Elastic Block Store 定义的操作](#)。

## Amazon EBS 中的 ACL

支持 ACL	否
--------	---

访问控制列表 (ACL) 控制哪些主体 ( 账户成员、用户或角色 ) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

## ABAC 与 Amazon EBS

支持 ABAC ( 策略中的标签 )	部分
--------------------	----

基于属性的访问权限控制 ( ABAC ) 是一种授权策略，该策略基于属性来定义权限。在 AWS 中，这些属性称为标签。您可以将标签附加到 IAM 实体 ( 用户或角色 ) 以及 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的 [什么是 ABAC ?](#) 要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的 [使用基于属性的访问权限控制 \( ABAC \)](#)。

## 将临时凭证用于 Amazon EBS

支持临时凭证	是
--------	---

某些 AWS 服务 在使用临时凭证登录时无法正常工作。有关更多信息，包括 AWS 服务与临时凭证配合使用，请参阅《IAM 用户指南》中的 [使用 IAM 的 AWS 服务](#)。

如果您不使用用户名和密码而用其他方法登录到 AWS Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录 ( SSO ) 链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户

身份登录控制台，然后切换角色时，还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的[切换到角色 \(控制台\)](#)。

您可以使用 AWS CLI 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅[IAM 中的临时安全凭证](#)。

## Amazon EBS 的跨服务主体权限

支持转发访问会话 (FAS)	是
----------------	---

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

## Amazon EBS 的服务角色

支持服务角色	是
--------	---

服务角色是由一项服务代入、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的[创建向 AWS 服务委派权限的角色](#)。

### Warning

更改服务角色的权限可能会破坏 Amazon EBS 的功能。仅当 Amazon EBS 提供相关指导时才编辑服务角色。

## Amazon EBS 的服务相关角色

支持服务相关角色	否
----------	---



服务相关角色是一种与 AWS 服务相关的服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅[能够与 IAM 搭配使用的 AWS 服务](#)。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

## 适用于 Amazon Elastic Block Store 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Amazon EBS 资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface ( AWS CLI ) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

有关 Amazon EBS 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的[Amazon Elastic Block Store 的操作、资源和条件键](#)。

### 主题

- [策略最佳实践](#)
- [使用 Amazon EBS 控制台](#)
- [允许用户查看他们自己的权限](#)
- [使用卷](#)
- [使用快照](#)

## 策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon EBS 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 托管策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。建议通过定义特定于您的应用场景的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#) 或 [工作职能的 AWS 托管策略](#)。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的[IAM 中的策略和权限](#)。

- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证 IAM policy，确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，确保策略符合 IAM policy 语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM Access Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA) – 如果您所处的场景要求您的 AWS 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》中的 [配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

## 使用 Amazon EBS 控制台

要访问 Amazon Elastic Block Store 控制台，您必须具有一组最低权限。这些权限必须允许您列出和查看有关 AWS 账户中的 Amazon EBS 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或 AWS API 的用户，您无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

要确保用户和角色仍可使用 Amazon EBS 控制台，请将 Amazon EBS *ConsoleAccess* 或者 *ReadOnly* AWS 托管策略也挂载到实体。有关更多信息，请参阅《IAM 用户指南》中的 [为用户添加权限](#)。

## 允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
```

```

        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

## 使用卷

### 示例

- [示例：附加和分离卷](#)
- [示例：创建卷](#)
- [示例：创建带有标签的卷](#)
- [示例：通过 Amazon EC2 控制台使用卷](#)

### 示例：附加和分离卷

在 API 操作需要发起人指定多种资源时，您必须创建一个策略语句，允许用户访问所需的所有资源。如果使用 Condition 元素时需要其中一种或多种资源，则必须创建多个语句，如本示例所示。

以下策略允许用户将带有“volume\_user=iam-user-name”标签的卷与带有“department=dev”标签的实例关联起来，以及将这些卷与这些实例取消关联。如果您将此策略添加到 IAM

组，`aws:username` 策略变量将授权组中的每位用户向具有 `volume_user` 标签 ( 将用户的用户名作为值 ) 的实例挂载卷，或从那些实例分离这些卷。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
    }
  ]
}
```

### 示例：创建卷

以下策略允许用户使用 [CreateVolume](#) API 操作。系统只允许用户创建加密且大小不足 20 GiB 的卷。

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

```

    "Effect": "Allow",
    "Action": [
      "ec2:CreateVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
    "Condition":{
      "NumericLessThan": {
        "ec2:VolumeSize" : "20"
      },
      "Bool":{
        "ec2:Encrypted" : "true"
      }
    }
  }
]
}

```

### 示例：创建带有标签的卷

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求用户标记其使用标签 `costcenter=115` 和 `stack=prod` 创建的任何卷。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，用户还必须具有使用 `CreateTags` 操作的权限。第二个语句使用 `ec2:CreateAction` 条件键使用户只能在 `CreateVolume` 上下文中创建标签。用户无法标记现有卷或任何其他资源。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {

```

```

    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction" : "CreateVolume"
      }
    }
  }
]
}

```

下面的策略允许用户创建卷而无需指定标签。仅当用户在 CreateTags 请求中指定了标签时，系统才会评估 CreateVolume 操作。如果用户指定了标签，则标签必须为 purpose=test。请求中不允许使用任何其他标签。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "test",
          "ec2:CreateAction" : "CreateVolume"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "purpose"
        }
      }
    }
  ]
}

```

```
}
```

### 示例：通过 Amazon EC2 控制台使用卷

以下策略为用户授予通过 Amazon EC2 控制台查看和创建卷以及将卷挂载到特定实例和与之分离的权限。

用户可以将任何卷附加到具有标签“purpose=test”的实例，也可以从这些实例分离卷。要使用 Amazon EC2 控制台连接卷，用户有权使用 `ec2:DescribeInstances` 操作会很有帮助，因为这可以让他们从 Attach Volume (连接卷) 对话框的预填充列表中选择实例。但是，这也会允许用户在控制台的 Instances 页面上查看所有实例，因此，您可以省略此操作。

在第一条语句中，需要 `ec2:DescribeAvailabilityZones` 操作以确保用户可以在创建卷时选择可用区。

用户无法标记其创建的卷 (卷创建期间或之后)。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVolumes",
      "ec2:DescribeAvailabilityZones",
      "ec2:CreateVolume",
      "ec2:DescribeInstances"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:region:111122223333:instance/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/purpose": "test"
      }
    }
  }
],
```

```

{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource": "arn:aws:ec2:region:111122223333:volume/*"
}
]
}

```

## 使用快照

以下是 `CreateSnapshot` ( EBS 卷的时间点快照 ) 和 `CreateSnapshots` ( 多卷快照 ) 的示例策略。

### 示例

- [示例：创建快照](#)
- [示例：创建快照](#)
- [示例：创建具有标签的快照](#)
- [示例：创建带有标签的多卷快照](#)
- [示例：复制快照](#)
- [示例：修改快照的权限设置](#)

### 示例：创建快照

以下策略允许客户使用 [CreateSnapshot](#) API 操作。仅当卷已加密并且卷大小不超过 20 GiB 时，客户才能创建快照。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
    },
    {

```



```

    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
    "Condition": {
      "NumericLessThan": {
        "ec2:VolumeSize": "20"
      },
      "Bool": {
        "ec2:Encrypted": "true"
      }
    }
  }
]
}

```

### 示例：创建快照

以下策略允许客户使用 [CreateSnapshots](#) API 操作。仅当实例上的所有卷均为类型 GP2 时，客户才能创建快照。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": [
        "arn:aws:ec2:us-east-1::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1:*:volume/*",
      "Condition": {
        "StringLikeIfExists": {
          "ec2:VolumeType": "gp2"
        }
      }
    }
  ]
}

```

```
}
```

### 示例：创建具有标签的快照

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求客户将标签 `costcenter=115` 和 `stack=prod` 应用于任何新快照。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，客户还必须具有使用 `CreateTags` 操作的权限。第三个语句使用 `ec2:CreateAction` 条件键使客户只能在 `CreateSnapshot` 上下文中创建标签。客户无法标记现有卷或任何其他资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*"
    },
    {
      "Sid": "AllowCreateTaggedSnapshots",
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateSnapshot"
        }
      }
    }
  ]
}
```

```
}

```

### 示例：创建带有标签的多卷快照

下面的策略包含 `aws:RequestTag` 条件键，该条件键要求客户在创建多卷快照集时应用标签 `costcenter=115` 和 `stack=prod`。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": [
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "AllowCreateTaggedSnapshots",
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateSnapshots"
        }
      }
    }
  ]
}
```

```
]
}
```

下面的策略允许客户创建快照而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "test",
          "ec2:CreateAction": "CreateSnapshot"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "purpose"
        }
      }
    }
  ]
}
```

下面的策略允许客户创建多卷快照集而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
```

```

    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/purpose": "test",
        "ec2:CreateAction": "CreateSnapshots"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": "purpose"
      }
    }
  }
]
}

```

以下策略仅允许在以下情况下创建快照：源卷已使用客户的 `User:username` 进行标记，并且快照本身已使用 `Environment:Dev` 和 `User:username` 进行标记。客户可向快照添加其他标签。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/User": "${aws:username}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Environment": "Dev",
          "aws:RequestTag/User": "${aws:username}"
        }
      }
    }
  ]
}

```

```

    }
  }
},
{
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
}
]
}

```

CreateSnapshots 的以下策略仅允许在以下情况下创建快照：源卷已使用客户的 `User:username` 进行标记，并且快照本身已使用 `Environment:Dev` 和 `User:username` 进行标记。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1:*:instance/*",
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/User": "${aws:username}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Environment": "Dev",
          "aws:RequestTag/User": "${aws:username}"
        }
      }
    }
  ],
}

```

```

    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
    }
  ]
}

```

以下策略仅允许在以下情况下删除快照：快照已使用客户的 User:username 进行标记。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/User": "${aws:username}"
        }
      }
    }
  ]
}

```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",

```

```

        "Condition":{
            "ForAnyValue:StringEquals":{
                "aws:TagKeys":"stack"
            }
        }
    ]
}

```

以下策略允许客户创建快照，但在要创建的快照具有标签键 `value=stack` 时拒绝操作。

```

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateSnapshots",
        "ec2:CreateTags"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Deny",
      "Action":"ec2:CreateSnapshots",
      "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
      "Condition":{
        "ForAnyValue:StringEquals":{
          "aws:TagKeys":"stack"
        }
      }
    }
  ]
}

```

以下策略允许您将多个操作整合到单个策略中。您只能在快照在区域 `us-east-1` 中创建时创建快照（在 `CreateSnapshots` 的上下文稿中）。您只能在快照正在区域 `CreateSnapshots` 中创建时且实例类型为 `us-east-1` 时创建快照（在 `t2*` 的上下文中）。

```

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

```



```

    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshots",
        "ec2:CreateSnapshot",
        "ec2:CreateTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:volume*"
      ],
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ec2:Region": "us-east-1"
        },
        "StringLikeIfExists": {
          "ec2:InstanceType": ["t2.*"]
        }
      }
    }
  ]
}

```

### 示例：复制快照

为 CopySnapshot 操作指定的资源级权限仅适用于新快照。无法为源快照指定资源级权限。

只有在使用标签键 purpose 和标签值 production (purpose=production) 创建新快照时，以下示例策略才允许委托人复制快照。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCopySnapshotWithTags",
      "Effect": "Allow",
      "Action": "ec2:CopySnapshot",
      "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "production"
        }
      }
    }
  ]
}

```

```
    }  
  }  
]  
}
```

### 示例：修改快照的权限设置

以下策略仅允许在以下情况下修改快照：快照已使用 `User:username` 标记，其中 `username` 是客户的 AWS 账户用户名。如果未满足此条件，则请求将失败。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:ModifySnapshotAttribute",  
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
      "Condition": {  
        "StringEquals": {  
          "aws:ResourceTag/user-name": "${aws:username}"  
        }  
      }  
    }  
  ]  
}
```

## Amazon EBS 身份和访问疑难解答

使用以下信息可帮助您诊断和修复在使用 Amazon EBS 和 IAM 时可能遇到的常见问题。

### 问题

- [我无权在 Amazon EBS 中执行操作](#)
- [我无权执行 iam:PassRole](#)
- [我希望允许我的 AWS 账户以外的人访问我的 Amazon EBS 资源](#)

## 我无权在 Amazon EBS 中执行操作

如果 AWS Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。管理员是向您提供登录凭证的人。

当不具有 `ec2:DescribeVolumes` 权限的 `mateojackson` IAM 用户尝试使用控制台查看有关卷的详细信息时，就会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:DescribeVolumes on resource: volume-id
```

在这种情况下，Mateo 请求其 AWS 管理员允许自己描述卷。

## 我无权执行 `iam:PassRole`

如果您收到一个错误，指明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Amazon EBS。

有些 AWS 服务 允许将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon EBS 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

## 我希望允许我的 AWS 账户 以外的人访问我的 Amazon EBS 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon EBS 是否支持这些功能，请参阅[Amazon Elastic Block Store 如何与 IAM 配合使用](#)。
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅《IAM 用户指南》中的[为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方 AWS 账户 提供您的资源的访问权限，请参阅《IAM 用户指南》中的[为第三方拥有的 AWS 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的[为经过外部身份验证的用户 \( 联合身份验证 \) 提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。

## Amazon Elastic Block Store 的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务“[按合规计划划分的范围](#)”，然后选择您感兴趣的合规计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的“[下载报告](#)”中的“[AWS Artifact](#)”。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#) — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 [Amazon Web Services 上构建 HIPAA 安全与合规架构](#) — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

### Note

并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅[符合 HIPAA 要求的服务参考](#)。

- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [AWS 客户合规指南](#) — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践，AWS 服务 并将指南映射到跨多个框架 ( 包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO) ) 的安全控制。

- [使用AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- [AWS Security Hub](#)— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 [Security Hub 控件参考](#)。
- [Amazon GuardDuty](#) — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- [AWS Audit Manager](#)— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

## Amazon Elastic Block Store 中的恢复功能

AWS 全球基础设施围绕 AWS 区域和可用区构建。AWS 区域提供多个在物理上独立且隔离的可用区，这些可用区与延迟率低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 [AWS 全球基础设施](#)。

除了 AWS 全球基础设施之外，Amazon EBS 还提供多种功能，帮助支持您的数据恢复能力和备份需求。

- 使用 Amazon Data Lifecycle Manager 自动处理 EBS 快照
- 跨区域复制 EBS 快照

# 监控 Amazon Elastic Block Store

监控是维护 Amazon Elastic Block Store 和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供以下监控工具，用于监视 Amazon EBS，在出现问题时进行报告，并在适当时自动采取措施：

- AWS CloudTrail 捕获由您或代表您发起的 API 调用和相关事件，AWS 账户 并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和账户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 [《AWS CloudTrail 用户指南》](#)。
- Amazon 会实时 CloudWatch 监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及 设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。
- Amazon EventBridge 可用于实现 AWS 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 [Amazon EventBridge 用户指南](#)。

## 主题

- [适用于 Amazon EBS 的 AWS CloudTrail](#)
- [亚马逊 EBS 的亚马逊 CloudWatch 指标](#)
- [Amazon f EventBridge or Amazon EBS](#)
- [Amazon f GuardDuty or Amazon EBS](#)

## 适用于 Amazon EBS 的 AWS CloudTrail

Amazon Elastic Block Store ( Amazon EBS ) 与 AWS CloudTrail 集成，后者是在 Amazon EBS 中提供由用户、角色或 AWS 服务所采取操作的记录的服务。CloudTrail 将 Amazon EBS 的所有 API 调用作为事件捕获。捕获调用中包括通过 Amazon EBS 控制台的调用和对 Amazon EBS API 操作的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶 ( 包括 Amazon EBS 的事件 )。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 事件历史记录 中查看最新事件。使用通过 CloudTrail 收集的信息，您可以确定向 Amazon EBS 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 [AWS CloudTrail 用户指南](#)。

## CloudTrail 中的 Amazon EBS 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon EBS 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一起保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅[使用 CloudTrail 事件历史记录查看事件](#)。

要持续记录 AWS 账户中的事件（包括 Amazon EBS 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送到 Simple Storage Service (Amazon S3) 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送到您指定的 Simple Storage Service (Amazon S3) 桶。此外，您可以配置其它 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- [创建跟踪记录概览](#)
- [CloudTrail supported services and integrations](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)
- [从多个区域接收 CloudTrail 日志文件](#)和[从多个账户接收 CloudTrail 日志文件](#)

所有 [Amazon EBS API 操作](#)均由 CloudTrail 记录。例如，对 CreateVolume、DeleteVolume 和 CreateSnapshot 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

## 了解 Amazon EBS 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日记账条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例是演示 CreateVolume 操作的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Root",
    "principalId": "AROAJABCHBVMHREXAMPLE:root",
    "arn": "123456789012",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2024-02-08T08:02:21Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CreateVolume",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "12.12.123.123",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
  "requestParameters": {
    "size": "100",
    "zone": "us-east-1a",
    "volumeType": "gp3",
    "iops": "3000",
    "encrypted": true,
    "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
    "throughput": "125",
    "clientToken": "12345678-2427-4336-a555-e8607example"
  },
  "responseElements": {
    "requestId": "12345678-4229-4cfd-9cb1-0b094example",
    "volumeId": "vol-01234567890abcdef",
    "size": "100",
    "zone": "us-east-1a",
    "status": "creating",
    "createTime": 1707379341000,
    "volumeType": "gp3",
    "iops": 3000,
    "encrypted": true,
    "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
    "tagSet": {},
    "multiAttachEnabled": false,
    "throughput": 125
  },
  "requestID": "12345678-4229-4cfd-9cb1-0b094example",
```



```
"eventID": "12345678-4b33-4c18-90a1-76d4bexample",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}
```

## 亚马逊 EBS 的亚马逊 CloudWatch 指标

Amazon CloudWatch 指标是统计数据，可用于查看、分析卷的运行行为并设置警报。

数据在 1 分钟期间内自动可用，无需收费。

当您从中获取数据时 CloudWatch，可以包含一个 `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（1 分钟时间）。我们建议您在请求中指定的时间大于等于收集时间，从而确保返回数据有效。

您可以使用 CloudWatch API 或 Amazon EC2 控制台获取数据。控制台从 CloudWatch API 中获取原始数据，并根据这些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。

### 主题

- [Amazon EBS 卷的指标](#)
- [Nitro 实例的指标](#)
- [快速快照还原的指标](#)
- [Amazon EC2 控制台图表](#)

## Amazon EBS 卷的指标

AWS/EBS 命名空间包括连接到所有实例类型的 EBS 卷的以下指标。所有 Amazon EBS 卷类型都会自动向其发送 1 分钟指标 CloudWatch，但前提是该卷已连接到实例。

要从实例上的操作系统获取有关可用磁盘空间的信息，请参阅[查看可用磁盘空间](#)。


**Note**

某些指标在基于 Nitro 系统构建的实例上存在差异。有关这些实例类型的列表，请参阅在 [Nitro 系统上构建的实例](#)。

指标	描述	单位	尺寸	有意义的统计数据
VolumeReadBytes	<p>提供有关指定时间段内的读取操作的信息。</p> <ul style="list-style-type: none"> <li>Sum 统计数据将报告该时间段内传输的总字节数。</li> <li>附加到 Nitro 实例的卷除外，Average 统计数据报告该时间段内每个读取操作的平均大小，其中的平均值表示指定时间段的平均值。</li> <li>附加到基于 Nitro 实例的卷除外，SampleCount 统计数据报告该时间段内的读取操作总数，其中的样本数表示在统计计算中使用的数据点数。</li> </ul>	字节	VolumeId	<ul style="list-style-type: none"> <li>Average</li> <li>Sum</li> <li>SampleCount</li> <li>Minimum   Maximum：仅适用于附加到基于 Nitro 实例的卷</li> </ul>

**Note**

对于 Xen 实例，只有在卷上有读取活动时才报告数据。

指标	描述	单位	尺寸	有意义的统计数据
VolumeWriteBytes	<p>提供有关指定时间段内的写入操作的信息</p> <ul style="list-style-type: none"> <li>Sum 统计数据将报告该时间段内传输的总字节数。</li> <li>Average 统计数据报告该时间段内的每个写入操作的平均大小，附加到基于 Nitro 的实例的卷除外，其中的平均值表示指定时间段的平均值。</li> <li>SampleCount 统计数据报告该时间段内的写入操作总数，但附加到基于 Nitro 的实例的卷除外，其中的样本数表示在统计计算中使用的数据点数。</li> </ul> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>对于 Xen 实例，只有在卷上有写入活动时才报告数据。</p> </div>	字节	VolumeId	<ul style="list-style-type: none"> <li>Average</li> <li>Sum</li> <li>SampleCount</li> <li>Minimum   Maximum : 仅适用于附加到基于 Nitro 实例的卷</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
VolumeReadOps	<p>在指定时间的读取操作总数。读取操作在完成时计在内。</p> <p>要计算该时间段的平均每秒读取操作数（读取 IOPS），请将该时间段的总读取操作数除以秒数。</p>	计数	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Sum</li> <li>• Minimum</li> <li> </li> <li>Maximum :</li> </ul> <p>仅适用于附加到基于 Nitro 实例的卷</p>
VolumeWriteOps	<p>在指定时间的写入操作总数。写入操作在完成时计在内。</p> <p>要计算该时间段的平均每秒写入操作数（写入 IOPS），请将该时间段的总写入操作数除以秒数。</p>	计数	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Sum</li> <li>• Minimum</li> <li> </li> <li>Maximum :</li> </ul> <p>仅适用于附加到基于 Nitro 实例的卷</p>

指标	描述	单位	尺寸	有意义的统计数据
VolumeTotalReadTime	<div data-bbox="349 310 657 640"> <p> <b>Note</b></p> <p>启用多重挂载的卷不支持此指标。对于 Xen 实例，只有在卷上有读取活动时才报告数据。</p> </div> <p>指定时间段中所有读取操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 1 分钟（60 秒）的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。</p>	秒	VolumeId	<ul style="list-style-type: none"> <li>• Average : 与附加到基于 Nitro 实例的卷无关</li> <li>• Sum</li> <li>• Minimum   Maximum : 仅适用于附加到基于 Nitro 实例的卷</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
VolumeTotalWriteTime	<p><b>Note</b></p> <p>启用多重挂载的卷不支持此指标。对于 Xen 实例，只有在卷上有写入活动时才报告数据。</p> <p>指定时间段中所有写入操作耗费的总秒数。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 1 分钟（60 秒）的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。</p>	秒	VolumeId	<ul style="list-style-type: none"> <li>Average : 与附加到基于 Nitro 实例的卷无关</li> <li>Sum</li> <li>Minimum   Maximum : 仅适用于附加到基于 Nitro 实例的卷</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
VolumeIdleTime	<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b> 启用多重挂载的卷不支持此指标。</p> </div> <p>未提交读取或写入操作的指定时间段中的总秒数。</p>	秒	VolumeId	<ul style="list-style-type: none"> <li>• Average : 与附加到基于 Nitro 实例的卷无关</li> <li>• Sum</li> <li>• Minimum   Maximum : 仅适用于附加到基于 Nitro 实例的卷</li> </ul>
VolumeQueueLength	指定时间段中等待完成的读取和写入操作请求的数量。	计数	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Sum : 与附加到 Nitro 实例的卷无关</li> <li>• Minimum   Maximum : 仅适用于附加到 Nitro 实例的卷</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
VolumeStalledIOCheck	<div data-bbox="349 310 381 346" style="border: 1px solid #00a0e3; border-radius: 50%; width: 15px; height: 15px; display: inline-block; margin-right: 5px;"></div> <b>Note</b> 仅适用于 Nitro 实例。未针对附加到 Amazon ECS 的卷和 AWS Fargate 任务发布。  报告卷在最后一分钟内是否通过停滞 IO 检查。此指标可以是 0 (通过) 或 1 (未通过)。有关更多信息，请参阅 <a href="#">使用监控 I/O 特性 CloudWatch</a> 。			



指标	描述	单位	尺寸	有意义的统计数据
VolumeThroughputPercentage	<div data-bbox="349 310 657 546" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b>            仅限预调配 IOPS SSD 卷。            启用多重挂载的卷不支持此指标。</p> </div> <p>每秒传输的 I/O 操作数 ( IOPS ) 在为 Amazon EBS 卷预置的总 IOPS 中所占的百分比。预置 IOPS SSD 卷在 99.9% 的时间里可提供预置性能。</p> <p>写入过程中，如果一分钟内没有其他待处理的 I/O 请求，指标值就会是 100%。另外，卷的 I/O 性能可能由于已执行的操作而暂时下降 ( 例如，在使用高峰期创建卷的快照，在非 EBS 优化的实例上运行卷，或者首次访问卷上的数据 )。</p>	百分比	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Minimum</li> <li style="text-align: center;"> </li> <li>• Maximum</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
VolumeConsumedReadWriteOps	<div data-bbox="318 268 690 491" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> Note 仅限预调配 IOPS SSD 卷。</p> </div> <p>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>	计数	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Sum</li> <li>• Minimum</li> <li> </li> <li>Maximum</li> </ul>

指标	描述	单位	尺寸	有意义的统计数据
BurstBalance	<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b> gp2st1、和仅限sc1卷。</p> </div> <p>提供有关突增存储桶中剩余的 I/O 积分百分比（对于 gp2）或吞吐量积分（对于 st1 和 sc1）的信息。只有当卷处于活动状态时，CloudWatch 才会向其报告数据。如果未附加卷，则不会报告任何数据。</p> <p>如果卷的基准性能超过了最大突发性能，则绝不会使用积分。如果卷附加到基于 Nitro 系统构建的实例，则不会报告突增余额。对于其他实例，报告的突增余额是 100%。有关更多信息，请参阅 <a href="#">gp2 卷性能</a>。</p>	百分比	VolumeId	<ul style="list-style-type: none"> <li>• Average</li> <li>• Sum：与附加到 Nitro 实例的卷无关。</li> <li>• Minimum   Maximum</li> </ul>

## Nitro 实例的指标

AWS/EC2 命名空间包括所添加的卷的基于 Nitro 的实例（非裸机实例）的其他 Amazon EBS 指标。

指标	描述	单位	有意义的统计数据
EBSReadOps	<p>在指定时间段内在挂载到实例的所有 Amazon EBS 卷中完成的读取操作数。</p> <p>要计算该时间段的平均每秒读取 I/O 操作数 (读取 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算读取 IOPS。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的运算次数。例如，如果您将图表绘EBSReadOps 制 CloudWatch 为m1，则指标数学公式将<math>m1 / (DIFF\_TIME(m1))</math> 返回以运算/秒为单位的量度。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的<a href="#">使用公制数学</a>。</p>	计数	<ul style="list-style-type: none"> <li>• 总和</li> <li>• 平均值</li> <li>• 最低</li> <li>• 最高</li> </ul>
EBSWriteOps	<p>在指定时间段内在附加到实例的所有 EBS 卷中完成的写入操作数。</p> <p>要计算该时间段的平均每秒写入 I/O 操作数 (写入 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算写入 IOPS。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的运算次数。例如，如果您将图表绘EBSWriteOps 制 CloudWatch 为m1，则指标数学公式将<math>m1 / (DIFF\_TIME(m1))</math> 返回以运算/秒为单位的量度。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的<a href="#">使用公制数学</a>。</p>	计数	<ul style="list-style-type: none"> <li>• 总和</li> <li>• 平均值</li> <li>• 最低</li> <li>• 最高</li> </ul>
EBSReadBytes	在指定时间段内从附加到实例的所有 EBS 卷中读取的字节数。	字节	<ul style="list-style-type: none"> <li>• 总和</li> <li>• 平均值</li> </ul>

指标	描述	单位	有意义的统计数据
	<p>报告的数字是在该时间段内读取的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒读取的字节数。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒字节数。例如，如果您将图形化EBSReadBytes CloudWatch 为m1，则指标数学公式将<math>m1/(DIFF\_TIME(m1))</math> 返回以字节/秒为单位的指标。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的<a href="#">使用公制数学</a>。</p>		<ul style="list-style-type: none"> <li>• 最低</li> <li>• 最高</li> </ul>
EBSWriteBytes	<p>在指定时间段内写入附加到实例的所有 EBS 卷的字节数。</p> <p>报告的数字是在该时间段内写入的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒写入的字节数。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒字节数。例如，如果您将图形化EBSWriteBytes CloudWatch 为m1，则指标数学公式将<math>m1/(DIFF\_TIME(m1))</math> 返回以字节/秒为单位的指标。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的<a href="#">使用公制数学</a>。</p>	字节	<ul style="list-style-type: none"> <li>• 总和</li> <li>• 平均值</li> <li>• 最低</li> <li>• 最高</li> </ul>

指标	描述	单位	有意义的统计数据
EBSIOBalance%	<p>提供有关突增存储桶中剩余的 I/O 积分百分比的信息。此指标仅对基本监控可用。</p> <p>此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关更多信息，请参阅<a href="#">默认为 EBS 优化</a>。</p> <p>Sum 统计数据不适用于该指标。</p>	百分比	<ul style="list-style-type: none"> <li>• 最低</li> <li>• 最高</li> </ul>
EBSByteBalance%	<p>提供有关突增存储桶中剩余的吞吐量积分百分比的信息。此指标仅对基本监控可用。</p> <p>此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关更多信息，请参阅<a href="#">默认为 EBS 优化</a>。</p> <p>Sum 统计数据不适用于该指标。</p>	百分比	<ul style="list-style-type: none"> <li>• 最低</li> <li>• 最高</li> </ul>

## 快速快照还原的指标

AWS/EBS 命名空间包含以下用于[快速快照还原](#)的指标。

指标	描述	单位	尺寸	有意义的统计数据
FastSnapshotRestoreCreditsBucketSize	可以累积的最大卷创建积分。将为每个可用区的每个快照报告该指标。	计数	SnapshotId   AvailabilityZone	<ul style="list-style-type: none"> <li>• Average</li> <li>• Minimum   Maximum</li> </ul> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>最有意义的统计数据是 Average。Minimum</p> </div>

指标	描述	单位	尺寸	有意义的统计数据
				和 Maximum 统计数据的结果与 Average 相同，可以替换使用。
FastSnapshotRestoreCreditsBalance	可用的卷创建积分数。将为每个可用区的每个快照报告该指标。	计数	SnapshotId   AvailabilityZone	<ul style="list-style-type: none"> <li>Average</li> <li>Minimum   Maximum</li> </ul> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。</p> </div>

## Amazon EC2 控制台图表

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。右边的列描述了如何使用 CloudWatch API 中的原始数据指标来生成每个图表。所有的图表周期都是 5 分钟。

图表	使用原始指标描述
读取吞吐量 (KiB/s)	$\text{Sum}(\text{VolumeReadBytes}) / \text{Period} / 1024$
写入吞吐量 (KiB/s)	$\text{Sum}(\text{VolumeWriteBytes}) / \text{Period} / 1024$
读取操作 (Ops/s)	$\text{Sum}(\text{VolumeReadOps}) / \text{Period}$
写入操作 (Ops/s)	$\text{Sum}(\text{VolumeWriteOps}) / \text{Period}$

图表	使用原始指标描述
平均队列长度 (操作数)	$Avg(\text{VolumeQueueLength})$
空闲花费时间 (%)	$\text{Sum}(\text{VolumeIdleTime}) / \text{Period} \times 100$
平均读取大小 (KiB/op)	<p><math>Avg(\text{VolumeReadBytes}) / 1024</math></p> <p>对于基于 Nitro 的实例，以下公式使用<a href="#">CloudWatch公式</a>计算出平均读取大小：</p> $(\text{Sum}(\text{VolumeReadBytes}) / \text{Sum}(\text{VolumeReadOps})) / 1024$ <p><code>VolumeReadBytes</code> 和 <code>VolumeReadOps</code> 指标可在 EBS CloudWatch 控制台中找到。</p>
平均写入大小 (KiB/op)	<p><math>Avg(\text{VolumeWriteBytes}) / 1024</math></p> <p>对于基于 Nitro 的实例，以下公式使用<a href="#">CloudWatch公式</a>计算出平均写入大小：</p> $(\text{Sum}(\text{VolumeWriteBytes}) / \text{Sum}(\text{VolumeWriteOps})) / 1024$ <p><code>VolumeWriteBytes</code> 和 <code>VolumeWriteOps</code> 指标可在 EBS CloudWatch 控制台中找到。</p>
平均读取延迟 (ms/op)	<p><math>Avg(\text{VolumeTotalReadTime}) \times 1000</math></p> <p>对于基于 Nitro 的实例，以下公式使用<a href="#">CloudWatch指标</a>数学推导出平均读取延迟：</p> $(\text{Sum}(\text{VolumeTotalReadTime}) / \text{Sum}(\text{VolumeReadOps})) \times 1000$ <p><code>VolumeTotalReadTime</code> 和 <code>VolumeReadOps</code> 指标可在 EBS CloudWatch 控制台中找到。</p>



图表	使用原始指标描述
平均写入延迟 ( ms/op )	$\text{Avg}(\text{VolumeTotalWriteTime}) \times 1000$ <p>对于基于 Nitro 的实例，以下公式使用<a href="#">CloudWatch指标</a>数学推导出平均写入延迟：</p> $(\text{Sum}(\text{VolumeTotalWriteTime}) / \text{Sum}(\text{VolumeWriteOps})) * 1000$ <p>VolumeTotalWriteTime 和VolumeWriteOps 指标可在 EBS CloudWatch 控制台中找到。</p>

对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

## Amazon f EventBridge or Amazon EBS

Amazon EBS 会向亚马逊发送 EventBridge 针对卷和快照执行的操作的事件。借 EventBridge 助，您可以建立触发编程操作以响应这些事件的规则。例如，您可以创建一个规则，在启用快照以快速恢复快照时向您的电子邮件发送通知。

中的 EventBridge 事件以 JSON 对象的形式表示。该事件独有的字段包含在 JSON 对象的“详细信息”部分。“事件”字段包含事件名称。“结果”字段包含触发事件的操作的已完成状态。有关更多信息，请参阅《[亚马逊 EventBridge 用户指南](#)》中的[亚马逊 EventBridge 事件模式](#)。

有关更多信息，请参阅[什么是亚马逊 EventBridge？](#) 在《亚马逊 EventBridge 用户指南》中。

### 事件

- [EBS 卷事件](#)
- [EBS 卷修改事件](#)
- [EBS 快照事件](#)
- [EBS 快照归档事件](#)
- [EBS 快速快照还原事件](#)
- [AWS Lambda 用于处理 EventBridge 事件](#)

## EBS 卷事件

当发生以下卷事件 EventBridge 时，Amazon EBS 会向发送事件。

### 事件

- [创建卷 \( createVolume \)](#)
- [删除卷 \( deleteVolume \)](#)
- [卷附加或重新附加 \( attachVolume、reattachVolume \)](#)
- [分离音量 \( 分离音量 \)](#)

### 创建卷 ( createVolume )

创建卷的操作完成后，该createVolume事件就会发送到您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 available 或 failed。如果提供的内容无效 AWS KMS key ，则创建将失败，如以下示例所示。

### 事件数据

下面的列表是 EBS 为成功的 createVolume 事件发送的 JSON 对象示例。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
  ],
  "detail": {
    "result": "available",
    "cause": "",
    "event": "createVolume",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
  }
}
```

下面的列表是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥被禁用。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

以下是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥正等待导入。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

```
}  
}
```

## 删除卷 ( deleteVolume )

删除卷的操作完成后，该deleteVolume事件就会发送到您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件具有 deleted 结果。如果删除操作未完成，绝不会发送此事件。

### 事件数据

下面的列表是 EBS 为成功的 deleteVolume 事件发送的 JSON 对象示例。

```
{  
  "version": "0",  
  "id": "01234567-0123-0123-0123-012345678901",  
  "detail-type": "EBS Volume Notification",  
  "source": "aws.ec2",  
  "account": "012345678901",  
  "time": "yyyy-mm-ddThh:mm:ssZ",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"  
  ],  
  "detail": {  
    "result": "deleted",  
    "cause": "",  
    "event": "deleteVolume",  
    "request-id": "01234567-0123-0123-0123-0123456789ab"  
  }  
}
```

## 卷附加或重新附加 ( attachVolume、reattachVolume )

如果卷无法附加或重新附加到实例，系统会将 attachVolume 或 reattachVolume 事件发送至您的 AWS 账户。不过，不会保存、记录或存档该事件。如果您使用 KMS 密钥 加密 EBS 卷并且该 KMS 密钥 变为无效，则日后使用该 KMS 密钥 将卷附加或重新附加到实例时，EBS 会发送一个事件，如下示例所示。

### 事件数据

下面的列表是 EBS 在 attachVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 处于待删除状态。

**Note**

AWS 服务器例行维护后，可能会尝试重新连接到卷。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
    "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

下面的列表是 EBS 在 `reattachVolume` 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥处于待删除状态。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
    "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
```

```

    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}

```

## 分离音量 ( 分离音量 )

当卷与 Amazon EC2 实例分离时，该detachVolume事件就会发送到您的 AWS 账户。

### 事件数据

以下是成功detachVolume事件的示例。

```

{
  "version": "0",
  "id": "2ec37298-1234-e436-70fc-c96b1example",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2024-03-18T16:35:52Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJT12345SQ2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/administrator",
        "accountId": "123456789012",
        "accessKeyId": "AKIAJ67890A6EXAMPLE",
        "userName": "administrator"
      },
      "eventTime": "2024-03-18T16:35:52Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "DetachVolume",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "12.12.123.12",
      "userAgent": "aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/ec2.detach-volume",
    }
  }
}

```

```

"requestParameters":
{
  "volumeId":"vol-072577c46bexample",
  "force":false
},
"responseElements":
{
  "requestId":"1234513a-6292-49ea-83f8-85e95example",
  "volumeId":"vol-072577c46bexample",
  "instanceId":"i-0217f7eb3dexample",
  "device":"/dev/sdb",
  "status":"detaching",
  "attachTime":1710776815000
},
"requestID":"1234513a-6292-49ea-83f8-85e95example",
"eventID":"1234551d-a15a-43eb-9e69-c983aexample",
"readOnly":false,
"eventType":"AwsApiCall",
"managementEvent":true,
"recipientAccountId":"123456789012",
"eventCategory":"Management",
"tlsDetails":
{
  "tlsVersion":"TLSv1.3",
  "cipherSuite":"TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
}
}
}

```

## EBS 卷修改事件

修改卷 EventBridge 时，Amazon EBS 会向发送 modifyVolume 事件。不过，不会保存、记录或存档该事件。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",

```

```
"resources": [
  "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
],
"detail": {
  "result": "optimizing",
  "cause": "",
  "event": "modifyVolume",
  "request-id": "01234567-0123-0123-0123-0123456789ab"
}
}
```

## EBS 快照事件

当发生以下卷事件 EventBridge 时，Amazon EBS 会向发送事件。

### 事件

- [创建单个快照 \( createSnapshot \)](#)
- [创建多个快照 \( createSnapshots \)](#)
- [复制快照 \( copySnapshot \)](#)
- [共享快照 \( shareSnapshot \)](#)

### 创建单个快照 ( createSnapshot )

创建快照的操作完成后，该createSnapshot事件就会发送到您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 succeeded 或 failed。

### 事件数据

下面的列表是 EBS 为成功的 createSnapshot 事件发送的 JSON 对象示例。在 detail 部分，source 字段包含源卷的 ARN。startTime 和 endTime 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
```



```

"resources": [
  "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
],
"detail": {
  "event": "createSnapshot",
  "result": "succeeded",
  "cause": "",
  "request-id": "",
  "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
  "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
  "startTime": "yyyy-mm-ddThh:mm:ssZ",
  "endTime": "yyyy-mm-ddThh:mm:ssZ" }
}

```

## 创建多个快照 ( createSnapshots )

创建多卷快照的操作完成后，该createSnapshots事件就会发送到您的 AWS 账户。此事件的结果可能是 succeeded 或 failed。

### 事件数据

下面的列表是 EBS 为成功的 createSnapshots 事件发送的 JSON 对象示例。在 detail 部分中，source 字段包含多卷快照集的源卷的 ARN。startTime 和 endTime 字段表示快照的创建何时开始以及何时完成。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",

```

```

"endTime": "yyyy-mm-ddThh:mm:ssZ",
"snapshots": [
  {
    "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
    "status": "completed"
  },
  {
    "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
    "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
    "status": "completed"
  }
]
}
}

```

下面的列表是 EBS 在 createSnapshots 事件失败后发送的 JSON 对象的示例。失败的原因是多卷快照集的一个或多个快照未能完成。snapshot\_id 的值是失败的快照的 ARN。startTime 和 endTime 表示创建快照操作开始和结束的时间。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",

```

```
    "status": "error"
  },
  {
    "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
    "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
    "status": "error"
  }
]
}
```

## 复制快照 ( copySnapshot )

复制快照的操作完成后，该copySnapshot事件就会发送到您的 AWS 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 succeeded 或 failed。

如果您要跨区域复制快照，则事件将在目标区域中发出。

### 事件数据

下面的列表是 EBS 在 copySnapshot 事件成功后发送的 JSON 对象的示例。snapshot\_id 的值为新创建快照的 ARN。在 detail 部分，source 的值是源快照的 ARN。startTime 和 endTime 表示 copy-snapshot 操作的开始和结束时间。incremental 指示快照是否为增量快照 ( true )，或者完整快照 ( false )。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
```

```

    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true"
  }
}

```

下面的列表是 EBS 在 copySnapshot 事件失败后发送的 JSON 对象的示例。失败原因是源快照 ID 无效。snapshot\_id 的值为失败快照的 ARN。在 detail 部分中，source 的值为源快照的 ARN。startTime 和 endTime 表示 copy-snapshot 操作何时开始以及何时结束。

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}

```

## 共享快照 ( shareSnapshot )

当另一个 AWS 账户与其共享快照时，该shareSnapshot事件就会发送到您的账户。不过，不会保存、记录或存档该事件。结果始终是 succeeded。

### 事件数据

下面是 EBS 在 shareSnapshot 事件完成后发送的 JSON 对象的示例。在该detail部分中，的值source是与您共享快照的用户的 AWS 账号。startTime并endTime表示共享快照操作的开始和

结束时间。仅在与其它用户共享私有快照时，系统才会发送 shareSnapshot 事件。共享公有快照不会触发该事件。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "012345678901",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

## EBS 快照归档事件

Amazon EBS 发出与快照归档操作相关的事件。有关更多信息，请参阅 [监控快照归档](#)。

## EBS 快速快照还原事件

当快照的快速还原状态发生变化 EventBridge 时，Amazon EBS 会向发送事件。尽最大努力发出事件。

以下是此事件的示例数据。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Fast Snapshot Restore State-change Notification",
```

```
"source": "aws.ec2",
"account": "123456789012",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
],
"detail": {
  "snapshot-id": "snap-1234567890abcdef0",
  "state": "optimizing",
  "zone": "us-east-1a",
  "message": "Client.UserInitiated - Lifecycle state transition",
}
}
```

可能的 state 值为 enabling、optimizing、enabled、disabling 和 disabled。

message 的可能值如下所示：

`Client.InvalidSnapshot.InvalidState` - The requested snapshot transitioned to an invalid state (Error)

启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。无法为该快照启用快速快照还原。

`Client.UserInitiated`

状态成功转换为 enabling 或 disabling。

`Client.UserInitiated - Lifecycle state transition`

状态成功转换为 optimizing、enabled 或 disabled。

`Server.InsufficientCapacity` - There was insufficient capacity available to satisfy the request

由于容量不足而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Server.InternalError` - An internal error caused the operation to fail

由于内部错误而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked

快照的快速快照还原状态已转换为 disabling 或 disabled，因为快照已被快照所有者删除或取消共享。无法为已删除或不再与您共享的快照启用快速快照还原。

## AWS Lambda 用于处理 EventBridge 事件

您可以使用 Amazon EBS 和 Amazon EventBridge 来自动执行数据备份工作流程。这要求您创建 IAM 策略、处理事件的 AWS Lambda 函数以及匹配传入事件并将其路由到 Lambda 函数的 EventBridge 规则。

以下过程使用 createSnapshot 事件自动将已完成的快照复制到其他区域，以用于灾难恢复。

将已完成的快照复制到其他区域

1. 创建一个 IAM 策略（如以下示例所示的策略），以提供使用该 CopySnapshot 操作和写入 EventBridge 日志的权限。将策略分配给将处理 EventBridge 事件的用户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 在 Lambda 中定义一个可在控制台中使用的函数。EventBridge 下面用 Node.js 编写的示例 Lambda 函数是在亚马逊 EBS 发出匹配 createSnapshot 的事件（表示快照已完成）EventBridge 时调用的。该函数被调用后，它会将快照从 us-east-2 复制到 us-east-1。

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
    initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
            ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
        }
    });
}
```



```
        callback(errorMessage);
    } else {
        const successMessage = `Successfully started copy of snapshot
${snapshotId} to Region ${destinationRegion}.`;
        console.log(successMessage);
        console.log(data);
        callback(null, successMessage);
    }
});
};
```

为确保您的 Lambda 函数可在 EventBridge 控制台使用，请在 EventBridge 事件发生的区域创建该函数。有关更多信息，请参见[AWS Lambda 开发人员指南](#)。

3. 打开亚马逊 EventBridge 控制台，[网址为 https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/)。
4. 在导航窗格中，选择规则，然后选择创建规则。
5. 对于 Step 1: Define rule detail ( 步骤 1：定义规则详细信息 )，请执行以下操作：
  - a. 为 Name ( 名称 ) 和 Description ( 描述 ) 输入值。
  - b. 对于 Event bus ( 事件总线 )，保持 default ( 默认 )。
  - c. 确保 Enable the rule on the selected event bus ( 在选定的事件总线上启用该规则 ) 已开启。
  - d. 对于 Event type ( 事件类型 )，选择 Rule with an event pattern ( 具有事件模式的规则 )。
  - e. 选择下一步。
6. 对于 Step 2: Build event pattern ( 步骤 2：构建事件模式 )，执行以下操作：
  - a. 在事件源中，选择 AWS 事件或 EventBridge 合作伙伴事件。
  - b. 在事件模式部分，对于事件源，请确保选择 AWS 服务，对于 AWS 服务，选择 EC2。
  - c. 对于事件类型，选择 EBS 快照通知，选择特定事件，然后选择 createSnapshot。
  - d. 选择特定结果，然后选择已成功。
  - e. 选择下一步。
7. 对于 Step 3: Select targets ( 步骤 3：选择目标 )，请执行以下操作：
  - a. 对于目标类型，选择 AWS 服务。
  - b. 对于 Select target ( 选择目标 )，选择 Lambda function ( Lambda 函数 )，对于 Function ( 函数 )，选择之前创建的函数。
  - c. 选择 Next ( 下一步 )。

8. 对于 Step 4: Configure tags ( 步骤 4 : 配置标签 ) , 如果需要 , 为规则指定标签 , 然后选择 Next ( 下一步 ) 。
9. 对于 Step 5: Review and create ( 步骤 5 : 查看并创建 ) , 查看规则 , 然后选择 Create rule ( 创建规则 ) 。

现在 , 您的规则应该会显示在规则选项卡中。在所示的示例中 , 当您下次复制快照时 , EBS 应该会发送您所配置的事件。

## Amazon f GuardDuty or Amazon EBS

Amazon GuardDuty 是一项威胁检测服务 , 可帮助保护您的账户、容器、工作负载和 AWS 环境中的数据。使用机器学习 (ML) 模型以及异常和威胁检测功能 , GuardDuty 持续监控不同的日志源和运行时活动 , 以识别环境中的潜在安全风险和恶意活动并确定其优先级。

其中的[恶意软件保护](#)功能 GuardDuty 会扫描与您的 Amazon EC2 实例关联的 Amazon EBS 卷和容器工作负载 , 以检测潜在威胁。GuardDuty 提供了两种方法来做到这一点 :

- 启用恶意软件防护 — 当 GuardDuty 生成表明在 Amazon EC2 实例或容器工作负载中可能存在恶意软件的发现结果时 , 它将自动对可能受感染的资源启动恶意软件扫描。
- 在@@ 不启用恶意软件保护的情况下使用按需恶意软件扫描 — 提供您的 Amazon EC2 实例的 Amazon 资源名称 (ARN) 以启动按需扫描。

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

## Amazon EBS 的限额

对于每个 AWS 服务，您的 AWS 账户都具有默认配额（以前称为“限额”）。除非另有说明，否则，每个配额都特定于区域。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Amazon EBS 的限额，请打开[“服务限额”控制台](#)。在导航窗格中，选择 AWS 服务，然后选择 Amazon Elastic Block Store ( Amazon EBS )。要请求提高配额，请参阅《Service Quotas 用户指南》中的[请求提高配额](#)。

您的 AWS 账户 具有以下与 Amazon EBS 相关的限额。

名称	默认值	可调整	描述
每卷的已归档快照	每个受支持的区域：25 个	<a href="#">是</a>	每个卷的存档快照的最大数量。
每个账户的 CompleteSnapshot 请求数	每个受支持的区域：每秒 10 个	否	每个账户允许的 CompleteSnapsho 的最大数量。
每个目标区域的并发快照副本	每个受支持的区域：20 个	否	针对单个目标区域的并发快照副本的最大数量。
每个 Cold HDD ( sc1 ) 卷的并发快照数	每个受支持的区域：1 个	否	此区域中每个冷 HDD (sc1) 卷的并发快照的最大数量。
每个通用型 SSD ( gp2 ) 卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个通用型 SSD (gp2) 卷的并发快照的最大数量。
每个通用型 SSD ( gp3 ) 卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个通用型 SSD (gp3) 卷的并发快照的最大数量。

名称	默认值	可调整	描述
每个磁介质（标准）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个磁介质（标准）卷的并发快照的最大数量。
每个预置 IOPS SSD (io1) 卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个预调配 IOPS SSD (io1) 卷的并发快照的最大数量。
每个预置 IOPS SSD (io2) 卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个预调配 IOPS SSD (io2) 卷的并发快照的最大数量。
每个吞吐量优化型 HDD (st1) 卷的并发快照数	每个受支持的区域：1 个	否	此区域中每个吞吐量优化型 HDD (st1) 卷的并发快照的最大数量。

名称	默认值	可调整	描述
快速快照还原	us-east-1 : 5 个 us-east-2 : 5 个 us-west-1 : 5 个 us-west-2 : 5 个 af-south-1 : 5 个 ap-east-1 : 5 个 ap-northeast-1 : 5 个 ap-northeast-2 : 5 个 ap-northeast-3 : 5 个 ap-south-1 : 5 个 ap-southeast-1 : 5 个 ap-southeast-2 : 5 个 ap-southeast-3 : 5 个 ca-central-1 : 5 个 eu-central-1 : 5 个 eu-north-1 : 5 个	<u>是</u>	此区域中可为快速快照还原启用的快照的最大数量。

名称	默认值	可调整	描述
	eu-south-1 : 5 个 eu-west-1 : 5 个 eu-west-2 : 5 个 eu-west-3 : 5 个 me-south-1 : 5 个 sa-east-1 : 5 个 每个其他支持的区域 : 5 个		
每个账户的 GetSnapshotBlock 请求数	每个受支持的区域 : 每秒 1000 个	<u>是</u>	每个账户允许的 GetSnapshotBlock 请求的最大数量。
每个快照的 GetSnapshotBlock 请求数	每个受支持的区域 : 每秒 1000 个	否	每个快照允许的 GetSnapshotBlock 请求的最大数量。
预调配 IOPS SSD ( io1 ) 卷	每个受支持的区域 : 30 万个	<u>是</u>	此区域中可跨预调配 IOPS SSD (io1) 卷预调配的 IOPS 的最大聚合数量。
预置 IOPS SSD ( io2 ) 卷的 IOPS	每个受支持的区域 : 10 万个	<u>是</u>	此区域中可跨预调配 IOPS SSD (io2) 卷预调配的 IOPS 的最大聚合数量。

名称	默认值	可调整	描述
预置 IOPS SSD ( io1 ) 卷的 IOPS 修改	每个受支持的区域：50 万个	<a href="#">是</a>	此区域中可跨预调配 IOPS SDD (io1) 卷在卷修改中请求的 IOPS 的最大聚合数量。
预置 IOPS SSD ( io2 ) 卷的 IOPS 修改	每个受支持的区域：10 万个	<a href="#">是</a>	此区域中，跨预调配 IOPS SSD ( io2 ) 卷的卷修改请求中的最大当前 ( 从 ) IOPS 值和请求的 ( 到 ) IOPS 值。
每个账户正在进行的快照存档	每个受支持的区域：25 个	<a href="#">是</a>	每个账户正在进行的快照存档的最大数量。
每个账户正在通过存档进行的快照还原	每个受支持的区域：5 个	<a href="#">是</a>	每个账户正在通过存档进行的快照还原的最大数量。
每个账户的 ListChangedBlocks 请求数	每个受支持的区域：每秒 50 个	否	每个账户允许的 ListChangedBlocks 请求的最大数量。
每个账户的 ListSnapshotBlocks 请求数	每个受支持的区域：每秒 50 个	否	每个账户允许的 ListSnapshotBlocks 请求的最大数量。
每个账户的待创建快照数	每个受支持的区域：100 个	否	每个账户处于待处理状态的快照的最大数量。
每个账户的 PutSnapshotBlock 请求数	每个受支持的区域：每秒 1000 个	<a href="#">是</a>	每个账户允许的 PutSnapshotBlock 请求的最大数量。

名称	默认值	可调整	描述
每个快照的 PutSnapshotBlock 请求数	每个受支持的区域：每秒 1000 个	否	每个快照允许的 PutSnapshotBlock 请求的最大数量。
每个区域的快照数	每个受支持的区域：10 万个	<u>是</u>	每个区域的快照的最大数量
每个账户的 StartSnapshot 请求数	每个受支持的区域：每秒 10 个	否	每个账户允许的 StartSnapshot 请求的最大数量。
Cold HDD ( sc1 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<u>是</u>	此区域中可跨冷 HDD (sc1) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。



名称	默认值	可调整	描述
通用型 SSD ( gp2 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<u>是</u>	此区域中可跨通用型 SSD (gp2) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。
通用型 SSD ( gp3 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<u>是</u>	此区域中可跨通用型 SSD (gp3) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。

名称	默认值	可调整	描述
磁介质 ( 标准 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<a href="#">是</a>	此区域中可跨磁介质 ( 标准 ) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。
预置 IOPS SSD ( io1 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<a href="#">是</a>	此区域中可跨预调配 IOPS SSD ( io1 ) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。
预置 IOPS SSD ( io2 ) 卷存储 ( 单位 TiB )	每个受支持的区域 : 20 个	<a href="#">是</a>	此区域中可跨预调配 IOPS SSD ( io2 ) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。

名称	默认值	可调整	描述
吞吐量优化型 HDD ( st1 ) 卷存储 ( 单位 TiB )	af-south-1 : 300 个 ap-east-1 : 300 个 eu-south-1 : 300 个 me-south-1 : 300 个 每个其他支持的区域 : 50 个	<u>是</u>	此区域中可跨吞吐量优化型 HDD (st1) 卷预调配的最大聚合存储容量 ( 以 TiB 为单位 )。
冷 HDD ( sc1 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨冷 HDD (sc1) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。
通用型 SSD ( gp2 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨通用型 SSD (gp2) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。
通用型 SSD ( gp3 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨通用型 SSD (gp3) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。
磁介质 ( 标准 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨磁介质 ( 标准 ) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。

名称	默认值	可调整	描述
预置 IOPS SSD ( io1 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨预调配 IOPS SDD (io1) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。
预置 IOPS SSD ( io2 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 20 个	<u>是</u>	此区域中可跨预调配 IOPS SDD (io2) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。
吞吐量优化型 HDD ( st1 ) 卷存储修改 ( 单位 TiB )	每个受支持的区域 : 500 个	<u>是</u>	此区域中可跨吞吐量优化型 HDD (st1) 卷在卷修改中请求的最大聚合存储容量 ( 以 TiB 为单位 )。

## 注意事项

- 限额可能会随时间而改变。Amazon EBS 将持续监控您在每个区域内的预调配存储和 IOPS 使用情况，并可能根据您的使用量自动增加您在每个区域内的配额。尽管 Amazon EBS 可以根据使用情况自动提高限额，您仍可以在需要时请求提高限额。例如，假设您计划在美国东部 ( 弗吉尼亚州北部 ) 使用超过当前限额的 gp3 存储量，则可以在计划的使用量基础上请求提高该区域对该卷类型的限额。
- 每个目标区域的并发快照副本限额无法使用服务限额进行调整。但您可以通过联系 AWS Support，请求提高此限额。
- IOPS 修改和存储修改限额适用于可并发进行修改的卷的当前聚合值 ( 大小或 IOPS，具体取决于限额 )。您可对当前总值 ( 大小或 IOPS ) 不超过限额的卷提出并发修改请求。例如，如果预调配 IOPS SSD ( io1 ) 卷的 IOPS 修改的限额为 50,000，则可对任意数量的 io1 卷并发提出 IOPS 修改请求，前提是它们的当前 IOPS 总和等于或小于 50,000。如果您有三个 io1 卷，每个卷都预调配了 20,000 IOPS，则可并发请求对两个卷进行 IOPS 修改 (  $20,000 * 2 < 50,000$  )。如果您并发提出第三个卷的 IOPS 修改请求，则超出了限额，该请求将失败 (  $20,000 * 3 > 50,000$  )。

## 《Amazon EBS 用户指南》的文档历史记录

下表介绍了 Amazon EBS 的文档版本。

变更	说明	日期
<a href="#">跨账户启用 Amazon Data Lifecycle Manager 默认策略</a>	您可以使用 AWS CloudFormation StackSets 启用跨 AWS 组织或特定 AWS 账户的 Amazon Data Lifecycle Manager 默认策略。	2024 年 4 月 26 日
<a href="#">AWSDataLifecycleManagerSSMFullAccess AWS 托管策略</a>	使用 AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA SSM 文档更新了政策，以支持 SAP HANA 的应用程序一致性快照。	2023 年 11 月 17 日
<a href="#">VolumeStalledIOCheck 指标</a>	您可以使用 VolumeStalledIOCheck 指标来检查卷在最后一分钟是否通过停滞的 IO 检查。	2023 年 11 月 16 日
<a href="#">Amazon Data Lifecycle Manager 默认策略</a>	现在，您可以为 EBS 快照和 EBS 支持的 AMI 创建 Amazon Data Lifecycle Manager 默认策略，以备份一个区域中的所有卷和实例。	2023 年 11 月 16 日
<a href="#">Amazon EBS 快照锁</a>	您可以锁定 Amazon EBS 快照以保护其免受意外或恶意删除，或者将其以 WORM 格式存储一段特定的时间。	2023 年 11 月 15 日

<a href="#">屏蔽对快照的公共访问权限</a>	现在，您可以屏蔽对快照的公共访问权限，以防止公开共享快照。	2023 年 11 月 9 日
<a href="#">Amazon Data Lifecycle Manager 前置和后置脚本</a>	现在，您可以在 Amazon Data Lifecycle Manager 快照策略中使用前置和后置脚本来自动化应用程序一致快照的生命周期。	2023 年 11 月 7 日
<a href="#">NVMe 预留</a>	启用多重挂载的 io2 卷支持 NVMe 预留，这是一组行业标准的存储隔离栏协议。	2023 年 9 月 18 日
<a href="#">在 Amazon EBS 上进行故障测试</a>	AWS FIS 用于暂时停止 EBS 卷与其连接的实例之间的 I/O，以测试您的工作负载如何处理 I/O 中断。	2023 年 1 月 27 日
<a href="#">io2 Block Express 卷</a>	您可以修改 io2 Block Express 卷的大小和预调配 IOPS，并为其启用快速快照还原。	2022 年 5 月 31 日
<a href="#">Amazon EBS 快照回收站</a>	Amazon EBS 快照回收站是一项快照还原功能，能够使您还原意外删除的快照。	2021 年 11 月 29 日
<a href="#">Amazon EBS 快照归档</a>	Amazon EBS 快照归档是一个新存储层，可用于长期低成本地存储很少访问的快照。	2021 年 11 月 29 日
<a href="#">CloudWatch Amazon Data Lifecycle Manager 的指标</a>	您可以使用亚马逊监控您的 Amazon Data Lifecycle Manager 政策 CloudWatch。	2021 年 7 月 28 日

<a href="#">CloudTrail EBS 直接 API 的数据事件</a>	ListSnapshotBlocks、ListChangedBlocks、GetSnapshotBlock、和 PutSnapshotBlock API 可以在中记录数据事件 CloudTrail。	2021 年 7 月 27 日
<a href="#">io2 Block Express 卷</a>	io2 Block Express 卷现已正式发布。	2021 年 7 月 19 日
<a href="#">Amazon EBS local snapshots on Outposts</a>	您现在可以使用 Outposts 上的 Amazon EBS 本地快照将卷快照存储在 Outpost 本地，Outpost 自身的 Amazon S3 中。	2021 年 2 月 4 日
<a href="#">对 io2 卷的多重挂载支持</a>	您现在可以为 Amazon EBS 多重挂载启用预置 IOPS SSD ( io2 ) 卷。	2020 年 12 月 18 日
<a href="#">Amazon Data Lifecycle Manager</a>	使用 Amazon Data Lifecycle Manager 自动执行共享快照和跨 AWS 账户复制快照的过程。	2020 年 12 月 17 日
<a href="#">gp3 卷</a>	一种新 Amazon EBS 通用型 SSD 卷类型。您可以在创建或修改卷时指定预置 IOPS 和吞吐量。	2020 年 12 月 1 日
<a href="#">吞吐量优化型 HDD h 和 Cold HDD 卷大小</a>	吞吐量优化 HDD (st1) 和冷 HDD (sc1) 卷的大小范围可为 125 GiB 到 16 TiB。	2020 年 11 月 30 日
<a href="#">Amazon Data Lifecycle Manager</a>	您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除 EBS 支持的 AMI。	2020 年 11 月 9 日

<a href="#">Amazon Data Lifecycle Manager</a>	Amazon Data Lifecycle Manager 策略最多可配置四个计划。	2020 年 9 月 17 日
<a href="#">适用于 Amazon EBS 的预调配 IOPS SSD ( io2 ) 卷</a>	预置 IOPS SSD ( io2 ) 卷旨在提供 99.999% 的容量耐用性且 AFR 不高于 0.001%。	2020 年 8 月 24 日
<a href="#">快速快照还原</a>	您可以为与您共享的快照启用快速快照还原。	2020 年 7 月 21 日
<a href="#">Amazon EBS 多重挂载</a>	现在，您可以将单个预置 IOPS SSD (io1) 卷附加到位于同一可用区中的多达 16 个基于 Nitro 的实例。	2020 年 2 月 14 日
<a href="#">Amazon EBS 快速快照还原</a>	您可以在 EBS 快照上启用快速快照还原，以确保从快照创建的 EBS 卷在创建时已完全初始化，并立即交付所有预配置性能。	2019 年 11 月 20 日
<a href="#">Amazon EBS 多卷快照</a>	您可以跨连接到 EC2 point-in-time 实例的多个 EBS 卷拍摄精确、数据协调和崩溃一致的快照。	2019 年 5 月 29 日
<a href="#">Amazon EBS 默认加密</a>	在区域中启用默认加密后，将使用用于 EBS 加密的默认 KMS 密钥 加密在区域中创建的所有新 EBS 卷。	2019 年 5 月 23 日
<a href="#">自动化快照生命周期</a>	您可以使用 Amazon Data Lifecycle Manager 来自动创建和删除 EBS 卷的快照。	2018 年 7 月 12 日



<a href="#">在挂载的 EBS 卷上进行修改</a>	对于附加到大多数 EC2 实例的 大多数 EBS 卷，您可以在不分离卷或不停止实例的情况下修改卷大小、类型和 IOPS。	2017 年 2 月 13 日
<a href="#">在两者之间复制加密的 Amazon EBS 快照 AWS 账户</a>	您现在可以在 AWS 账户之间复制加密的 EBS 快照。	2016 年 6 月 21 日
<a href="#">吞吐量优化型 HDD 和 Cold HDD 卷类型</a>	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。	2016 年 4 月 19 日
<a href="#">通用型 SSD 卷类型</a>	通用型 SSD 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷可提供不超过 10 毫秒的延迟，能突增至 3000 IOPS 很长时间，基准性能为 3 IOPS/GiB。通用型 SSD 卷的大小范围为 1 GiB 到 1 TiB。	2014 年 6 月 16 日
<a href="#">Amazon EBS 加密</a>	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 AWS 托管式密钥加密数据，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。	2014 年 5 月 21 日
<a href="#">增量快照副本</a>	您现在可以执行增量快照副本。	2013 年 6 月 11 日
<a href="#">EBS 快照副本</a>	您可以使用快照备份创建数据备份、创建新 Amazon EBS 卷，或创建亚马逊机器映像 (AMI)。	2012 年 12 月 17 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。