aws

开发人员指南

AWS Backup

AWS Backup: 开发人员指南

Table of Contents

什么是 AWS Backup？

AWS Backup 是一项完全托管的服务，可以轻松地跨 AWS 服务、云端和本地集中和自动化数据保护。使用此服务，您可以一站式配置备份策略并监控 AWS 资源活动。它允许您自动执行和整合以前执行的备份任务 service-by-service，并且无需创建自定义脚本和手动流程。只需在 AWS Backup 控制台中单击几下，即可自动执行数据保护策略和计划。

AWS Backup 不控制您在外部 AWS 环境中进行的备份 AWS Backup。因此，如果您想要一个集中的 end-to-end 解决方案来满足业务和监管合规性要求，请 AWS Backup 立即开始使用。

功能概述

AWS Backup 提供了许多特性和功能，包括以下内容。

集中式备份管理

AWS Backup 提供了集中式备份控制台、一组备份 API 和 AWS Command Line Interface (AWS CLI)，用于管理应用程序使用的各项 AWS 服务的备份。使用 AWS Backup，您可以集中管理满足备份要求的备份策略。然后，您可以将它们应用于跨 AWS 服务的 AWS 资源，从而能够以一致且合规的方式备份应用程序数据。 AWS Backup 集中式备份控制台提供了备份和备份活动日志的整合视图，使审计备份和确保合规性变得更加容易。

基于策略的备份

使用 AWS Backup，您可以创建称为备份计划的备份策略。使用这些备份计划来定义您的备份要求，然后将其应用于要跨所使用的 AWS 服务保护的 AWS 资源。您可以创建单独的备份计划，分别满足特定业务及监管合规性要求。这有助于确保根据您的要求备份每种 AWS 资源。通过备份计划，您可以使用可扩展的方式，轻松地在组织中跨您的应用程序实施备份策略。

有关备份计划的所有配置选项，请参见备份计划选项和配置。

基于标记的备份策略

您可以使用多种方式 AWS Backup 将备份计划应用于您的 AWS 资源，包括对其进行标记。通过标记，可以更轻松地在所有应用程序中实施备份策略，并确保所有 AWS 资源都得到备份和保护。 AWS 标签是组织和分类 AWS 资源的绝佳方式。通过与 AWS 标签集成，您可以快速将备份计划应用于一组 AWS 资源，从而以一致且合规的方式对其进行备份。

有关将资源分配给备份计划的所有方法，请参阅将资源分配给备份计划。

生命周期管理策略

AWS Backup 使您能够满足合规性要求，同时通过将备份存储在低成本的冷存储层中来最大限度地降低备份存储成本。您可以配置生命周期策略，它将根据您定义的计划自动将备份从热存储转换到冷存储。

有关可以转移到冷存储的资源的列表，请参阅按资源划分的功能可用性。有关在备份计划中开启冷存储的步骤，请参阅生命周期和存储层。

跨区域备份

使用 AWS Backup，您可以按需将备份复制到多个不同的 AWS 区域 备份中，也可以自动将其作为定时备份计划的一部分。如果您需要将备份存储在最接近生产数据的位置以满足业务连续性或合规性要求，则跨区域备份会特别有用。有关更多信息，请参阅跨 AWS 区域创建备份副本。

跨账户管理和跨账户备份

您可以使用 AWS Backup 来管理AWS Organizations结构 AWS 账户 内所有内容的备份。借助跨账户管理，您可以自动使用备份策略跨组织内的 AWS 账户 应用备份计划。这使得合规性和数据保护能够大规模产生效用，并减少了运营开销。它还有助于避免跨各个账户手动复制备份计划。有关更多信息，请参阅跨多个 AWS 账户管理 AWS Backup 资源。

您也可以将备份复制到 AWS Organizations 管理结构 AWS 账户 中的多个不同位置。这样，您就可以将备份“扇入”到单个存储库账户，然后“扇出”备份以提高弹性。跨 AWS 账户创建备份副本。

在使用跨账户管理和跨账户备份功能之前，必须已在 AWS Organizations中配置了现有组织结构。组织单位 (OU) 是一组可以作为单个实体进行管理的账户。 AWS Organizations 是可以按组织单位分组并作为单个实体进行管理的账户列表。

使用 Audit Manager 进行 AWS Backup 审计和报告

AWS Backup Audit Manager 可帮助您简化整个备份的数据治理和合规性管理 AWS。 AWS Backup Audit Manager 提供了内置的可自定义控件，您可以根据自己的组织要求进行调整。您还可以使用这些控件自动跟踪备份活动和资源。

AWS Backup Audit Manager 可以帮助您找到尚未符合您定义的控制措施的特定活动和资源。您还可以使用它生成每日报告，这些报告可作为在一段时间内遵守控制的证据。

要将备份合规性与总体合规状况一起包括在内，您可以自动将 Audit Man AWS Backup ager 的调查结果导入 AWS Audit Manager。

增量备份

AWS Backup 以增量方式高效存储定期备份。 AWS 资源的第一次备份会备份数据的完整副本。对于每次连续的增量备份，仅备份对 AWS 资源的更改。通过增量备份，您能够从频繁备份的数据保护中受益，同时最大限度降低存储成本。

有关哪些资源支持增量备份的列表，请参见按资源划分的功能可用性。

全面 AWS Backup 管理

某些资源类型支持完全 AWS Backup 管理。全面 AWS Backup 管理的好处包括：

- 独立加密。 AWS Backup 使用 AWS Backup 保管库的 KMS 密钥自动加密您的备份，而不是使用与源资源相同的加密密钥。这会增强防御功能。请参阅对中的备份进行加密 AWS Backup了解更多信息。
- **awsbackup** Amazon 资源名称 (ARN)。Backup ARN 以 `arn:aws:backup` 开头，而不是以 `arn:aws:`*`source-resource`* 开头。这使您可以创建专门适用于备份而不是源资源的访问策略。请参阅访问控制了解更多信息。
- 集中式备份计费和 Cost Explorer 成本分配标签。费用 AWS Backup （包括存储、数据传输、恢复和提前删除）显示在账 Amazon Web Services 单的 “Backup” 下，而不是显示在每个支持的资源下。您还可以使用 Cost Explorer 成本分配标签来跟踪和优化备份成本。请参阅计量、成本和计费了解更多信息。

要查看哪些资源类型符合完全 AWS Backup 管理条件，请参阅按资源划分的功能可用性。

备份活动监控

AWS Backup 提供了一个仪表板，便于跨 AWS 服务审计备份和恢复活动。只需在 AWS Backup 控制台上单击几下，即可查看最近备份任务的状态。您还可以跨 AWS 服务恢复作业，以确保您的 AWS 资源得到适当的保护。

AWS Backup 与亚马逊 CloudWatch 和亚马逊集成 EventBridge。 CloudWatch 允许您跟踪指标并创建警报。 EventBridge 允许您查看和监视 AWS Backup 事件。有关更多信息，请参阅使用监控 AWS Backup 事件 EventBridge和使用监控 AWS Backup 指标 CloudWatch。

AWS Backup 与。集成 AWS CloudTrail。 CloudTrail 为您提供了备份活动日志的整合视图，便于您快速轻松地审核资源的备份情况。 AWS Backup 还与亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 集成，为您提供备份活动通知，例如何时备份成功或恢复已启动。有关更多信息，请参阅记录 AWS Backup API 调用 CloudTrail和使用 Amazon SNS 跟踪 AWS Backup 事件。

保护备份保管库中的数据

每个 AWS Backup 备份的内容都是不可变的，这意味着任何人都无法更改该内容。 AWS Backup 进一步保护备份存储库中的备份，从而将它们与源实例安全地分开。例如，即使您删除了源 Amazon EC2 实例和 Amazon EBS 卷，您的保管库也将根据您选择的生命周期策略保留您的 Amazon EC2 和 Amazon EBS 备份。

备份保管库提供加密和基于资源的访问策略，以便定义能够访问备份的人员。您可以为备份保管库定义访问策略，用于定义有权访问备份保管库中备份的人员以及这些人员可以采取的操作。这提供了一种简单而安全的方法来控制跨 AWS 服务对备份的访问。要查看 AWS 和客户托管的策略 AWS Backup，请参阅的托管策略 AWS Backup。

您可以使用 AWS Backup Vault Lock 来防止任何人（包括您）删除备份或更改其保留期。 AWS Backup Vault Lock 可帮助您强制执行 write-once-read-many（WORM）模型，并为您的防御添加另一层深度防御。要开始使用，请参阅 AWS Backup 保管库锁定。

对合规义务的支持

AWS Backup 帮助您履行全球合规义务。 AWS Backup 属于以下 AWS 合规计划的范围：

- FedRAMP 高
- GDPR
- SOC 1、2 和 3
- PCI
- HIPAA
- 及其他计划

开始使用

要了解更多信息 AWS Backup，我们建议您从开始入门 AWS Backup。

支持的 AWS 资源和应用程序

以下是您可以用来备份和恢复的 AWS 资源和第三方应用程序 AWS Backup。有关更多信息，请参阅 the section called “功能可用性”。

服务	支持的资源类型
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 实例（不包括实例存储支持的 AMI）
Amazon Simple Storage Service (Amazon S3)	Amazon S3 数据
Amazon Elastic Block Store （Amazon EBS)	Amazon EBS 卷
Amazon DynamoDB	Amazon DynamoDB 表
Amazon Relationa l Database Service (Amazon RDS)	Amazon RDS 数据库实例（包括所有数据库引擎）；多可用区集群
Amazon Aurora	Aurora 集群
Amazon Elastic File System (Amazon EFS)	Amazon EFS 文件系统
FSx for Lustre	FSx for Lustre 文件系统
FSx for Windows File Server	FSx for Windows File Server 文件系统
适用于 ONTAP 的亚马逊 FSx NetApp	FSx for ONTAP 文件系统
Amazon FSx for OpenZFS	FSx for OpenZFS 文件系统
AWS Storage Gateway （卷网关）	AWS Storage Gateway 卷
Amazon DocumentDB	基于亚马逊 DocumentDB 实例的集群
Amazon Neptune	Amazon Neptune 集群

服务	支持的资源类型
Amazon Redshift	Amazon Redshift 集群
Amazon Timestream	亚马逊 Timestream 表
VMware Cloud AWS™	开启了 VMware Cloud™ AWS
VMware Cloud AWS Outposts™	开启了 VMware Cloud™ AWS Outposts
AWS CloudFormation	AWS CloudFormation 堆栈
SAP HANA 数据库	Amazon EC2 实例上的 SAP HANA 数据库

定价

使用 AWS Backup，您可以为备份存储、数据恢复、还原测试、跨区域数据传输和 Audit Manager AWS Backup 付费。有关更多信息，请参阅AWS Backup 定价。

AWS Backup 功能可用性

AWS Backup 功能是根据资源提供的， AWS 区域. 以下各节和表格可以帮助您确定功能的可用性。

内容

适用于所有受支持资源的功能

AWS Backup 为其支持的 AWS 服务以及支持的第三方应用程序提供以下功能。除非明确提及，否则不应假定支持某项功能或服务。

- 自动备份计划和保留期管理
- 集中式备份监控

- 加密备份
- 增量备份
- 跨账户管理 AWS Organizations
- 使用 Audit Manager 自动进行备份 AWS Backup 审计和报告
- 带保管库锁定功能的一次写入、多次读取 (WORM) AWS Backup

按资源划分的功能可用性

要 AWS Backup 与特定区域的受支持 AWS 服务一起使用，该服务必须在该地区可用。要确定某个区域的服务可用性，请在中查看服务终端节点AWS 一般参考。

AWS Backup 支持	跨区域备份	跨账户备份	AWS Backup Audit Manager	增量备份	持续备份和 point-in-time 恢复	全面管理	冷库的生命周期	物品等级恢复 [1]	恢复测试
Amazon EC2	✓	✓	✓	✓					✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
亚马逊 RDS 单实例	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Amazon RDS 集群	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓

AWS Backup 支持	跨区域备份	跨账户备份	AWS Backup Audit Manager	增量备份	持续备份和 point-in-time 恢复	全面管理	冷库的生命周期	物品等级恢复 1	恢复测试
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx for Lustre	✓	✓	✓	✓					✓
FSx for Windows File Server	✓	✓	✓	✓					✓
FSx for ONTAP			✓[2]	✓					✓
FSx for OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon DocumentDB	✓[3]	✓[3]	✓						✓
Amazon Neptune	✓[3]	✓[3]	✓						✓

AWS Backup 支持	跨区域备份	跨账户备份	AWS Backup Audit Manager	增量备份	持续备份和 point-in-time 恢复	全面管理	冷库的生命周期	物品等级恢复 1	恢复测试
Amazon Redshift								✓	
Timestream	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					
虚拟机	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation 模板	✓	✓		✓ [5]		✓	✓ [5]		
Amazon DynamoDB			✓						✓
DynamoDB 带 AWS Backup 高级功能	✓	✓	✓			✓	✓		✓

AWS Backup 支持	跨区域备份	跨账户备份	AWS Backup Audit Manager	增量备份	持续备份和 point-in-time 恢复	全面管理	冷库的生命周期	物品等级恢复 1	恢复测试
Amazon EC2 实例上的 SAP HANA 数据库				✓	✓	✓	✓		

某些资源类型同时可以使用连续备份功能及跨区域和跨账户复制。对连续备份进行跨区域或跨账户复制时，复制的恢复点（备份）将变为快照（定期）备份。亚马逊 RDS 和 Amazon S3 支持增量快照副本；亚马逊 Aurora 仅支持完整快照副本。PITR（时间点还原）不适用于这些复制。

[1] 项目级还原中的 “项目” 因支持的资源而异。例如，文件系统项目是文件或目录，S3 项目是 S3 对象。VMware 项目就是磁盘。有关更多信息，请参阅支持的资源的还原备份部分。

[2] AWS Backup 除了跨账户复制和跨区域复制之外，Audit Manager 在所有控件中都支持此资源。

[3] RDS、Aurora、DocumentDB 和 Neptune 不支持同时执行跨区域和跨账户备份的单个复制操作。您可以选择其中一项。您也可以使用 AWS Lambda 脚本来监听第一个副本的完成情况，执行第二个副本，然后删除第一个副本。可以复制 RDS 多可用区数据库实例，但多可用区集群目前不支持跨区域或跨账户复制。有关更多信息特定资源的跨区域复制注意事项，请参阅。

[4] 有关支持 Backup Audi t Manager 的区域，请参阅 RDS 多可用区域备份。

[5] 在CloudFormation 堆栈备份中，嵌套资源保留其源资源的特征。但是，堆栈中的资源不保留时间点恢复 (PITR) 功能（例如 Amazon S3 和 Amazon RDS）。上面矩阵中的属性仅适用于 CloudFormation 模板，不适用于堆栈中的资源。

[6] 对于 Aurora，快照是完整的，增量备份是通过 PITR 提供的。

功能可用性来自 AWS 区域

AWS Backup 在以下所有版本中都可用 AWS 区域。 AWS Backup 除非下表中另有说明，否则所有这些区域均提供功能。

AWS Backup 支持	跨区域备份	跨账户管理	跨账户备份	AWS Backup A@@ udit Manager 和 Jobs 控制面	恢复测试
美国东部（弗吉尼亚州北部）	✓	✓	✓	✓	✓
美国东部（俄亥俄州）	✓	✓	✓	✓	✓
美国西部（加利福尼亚北部）	✓	✓	✓	✓	✓
美国西部（俄勒冈州）	✓	✓	✓	✓	✓
非洲（开普敦）	✓		✓	✓	✓
亚太地区（香港）	✓		✓	✓	✓
亚太地区（海得拉巴）	✓		✓		✓
亚太地区（雅加达）	✓		✓		✓
亚太地区（墨尔本）	✓		✓		✓

AWS Backup 支持	跨区域备份	跨账户管理	跨账户备份	AWS Backup A@@ udit Manager 和 Jobs 控制面	恢复测试
亚太地区（孟买）	✓	✓	✓	✓	✓
亚太地区（大阪）	✓	✓	✓		✓
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）	✓	✓	✓	✓	✓
加拿大西部（卡尔加里）	✓（亚马逊 S3 除外）		✓		
中国（北京）	✓				
中国（宁夏）	✓				
欧洲地区（法兰克福）	✓	✓	✓	✓	✓
欧洲地区（爱尔兰）	✓	✓	✓	✓	✓

AWS Backup 支持	跨区域备份	跨账户管理	跨账户备份	AWS Backup A@@ udit Manager 和 Jobs 控制面	恢复测试
欧洲地区（伦敦）	✓	✓	✓	✓	✓
欧洲地区（米兰）	✓		✓	✓	✓
欧洲地区（巴黎）	✓	✓	✓	✓	✓
欧洲（西班牙）	✓		✓		✓
欧洲地区（斯德哥尔摩）	✓	✓	✓	✓	✓
欧洲（苏黎世）	✓		✓		✓
以色列（特拉维夫）	✓		✓		
中东（巴林）	✓		✓	✓	✓
中东（阿联酋）	✓		✓		✓
南美洲（圣保罗）	✓	✓	✓	✓	✓
AWS GovCloud（美国东部）	✓	✓	✓	✓	

AWS Backup 支持	跨区域备份	跨账户管理	跨账户备份	AWS Backup A@@ udit Manager 和 Jobs 控制面	恢复测试
AWS GovCloud （美国西部）	✓	✓	✓	✓	

中国（北京）和中国（宁夏）支持跨区域复制，即从这两个区域中的一个区域复制到另一个区域。不支持从 这些区域跨区域复制到其他区域或这些区域。这些区域不支持跨账户复制。

AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）不提供职位控制面板。作业控制面板聚合仅适用于支持跨账户管理和 Audit Manager AWS Backup 的区域。

适用于 Windows File Server 的 Amazon FsX 和 Amazon Neptune 不支持可选区域中的跨区域备份副本。

支持的服务由 AWS 区域

AWS Backup 在所有支持的区域中都支持以下内容：

- Aurora
- DynamoDB
- 具有高级功能的 DynamoD AWS Backup B
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

下表按地区显示了对其他 AWS 服务 地区的 AWS Backup 支持。

区域和服务	Amazon FSx	EC2 实例上的 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 和备份网关
美国东部（弗吉尼亚州北部）	✓	✓	✓	✓	✓	✓
美国东部（俄亥俄州）	✓	✓	✓	✓	✓	✓
美国西部（加利福尼亚北部）	Windows；Lustre；ONTAP	✓	✓	✓		✓
美国西部（俄勒冈州）	Windows；Lustre；ONTAP	✓	✓	✓	✓	✓
非洲（开普敦）	Windows；Lustre；ONTAP	✓	✓ [1]	✓		✓
亚太地区（香港）	✓	✓	✓ [1]	✓		✓
亚太地区（海得拉巴）	Windows；Lustre；ONTAP		✓ [1]	✓		
亚太地区（雅加达）	Windows；Lustre；ONTAP		✓	✓		
亚太地区（墨尔本）	Windows；Lustre；ONTAP		✓ [1]	✓		

区域和服务	Amazon FSx	EC2 实例上的 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 和备份网关
亚太地区（孟买）	✓	✓	✓	✓		✓
亚太地区（大阪）	Windows；Lustre	✓	✓ [1]	✓		✓
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）	✓	✓	✓	✓		✓
加拿大西部（卡尔加里）						
中国（北京）	Windows；Lustre		✓ [1]	✓	✓	
中国（宁夏）	Windows；Lustre		✓ [1]	✓	✓	
欧洲地区（法兰克福）	✓	✓	✓	✓	✓	✓

区域和服务	Amazon FSx	EC2 实例上的 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 和备份网关
欧洲地区（爱尔兰）	✓	✓	✓	✓	✓	✓
欧洲地区（伦敦）	✓	✓	✓	✓		✓
欧洲地区（米兰）	Windows；Lustre；ONTAP	✓	✓ [1]	✓		✓
欧洲地区（巴黎）	Windows；Lustre；ONTAP	✓	✓	✓		✓
欧洲（西班牙）	Windows；Lustre；ONTAP		✓ [1]	✓		
欧洲地区（斯德哥尔摩）	✓	✓	✓	✓		✓
欧洲（苏黎世）	Windows；Lustre；ONTAP		✓ [1]	✓		
以色列（特拉维夫）	Windows；Lustre；ONTAP		✓ [1]	✓		
中东（巴林）	Windows；Lustre；ONTAP	✓	✓ [1]	✓		✓

区域和服务	Amazon FSx	EC2 实例上的 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 和备份网关
中东（阿联酋）			✓ [1]	✓		
南美洲（圣保罗）		✓	✓	✓		✓
AWS GovCloud（美国西部）	Windows；Lustre；ONTAP		✓ [1]	✓		✓
AWS GovCloud（美国东部）	Windows；Lustre；ONTAP		✓ [1]	✓		✓

Amazon FSx 下的勾选表明，该地区都支持 Windows 文件服务器的 FSx、Lustre 的 fsX、ONTAP 的 fsX 和 OpenZFS 的 fsX；否则，将列出支持的配置。 AWS Backup

[1] 不支持跨区域和跨账户复制。

AWS Backup：工作原理

AWS Backup 是一项完全托管的备份服务，可以轻松地跨 AWS 服务集中和自动备份数据。使用 AWS Backup，您可以创建名为备份计划的备份策略。您可以使用这些计划来定义备份要求，例如数据的备份频率以及这些备份的保留时间。

AWS Backup 只需为资源添加标签，即可将备份计划应用于 AWS 资源。 AWS Backup 然后根据您定义的备份计划自动备份您的 AWS 资源。

以下各节描述了 AWS Backup 工作原理、其实现细节和安全注意事项。

主题

AWS Backup 如何使用支持的 AWS 服务

某些 AWS Backup支持的 AWS 服务提供自己的独立备份功能。无论您是否使用 AWS Backup，都可以使用这些功能。但是，其他 AWS 服务创建的备份无法用于中央治理 AWS Backup。

AWS Backup 要配置为集中管理所有受支持服务的数据保护，您必须选择使用管理该服务 AWS Backup，创建按需备份或使用备份计划计划计划备份，并将备份存储在备份存储库中。

主题

- 使用 Amazon RDS 和 Aurora
- 与... 合作 AWS BackInt
- 与... 合作 AWS Storage Gateway
- 使用 Amazon DocumentDB
- 使用 Amazon Neptune
- 使用 Amazon Timestream
- 与... 合作 AWS Organizations
- 与... 合作 AWS CloudFormation
- 与 SAP 合作 AWS BackInt、 AWS Systems Manager 为 SAP 和 SAP HANA 工作
- AWS 服务如何备份自己的资源

选择使用管理服务 AWS Backup

当有新 AWS 服务可用时，必须启用 AWS Backup 才能使用这些服务。如果您尝试使用未启用的服务中的资源来创建按需备份或备份计划，则会收到错误消息，并且无法完成此过程。

AWS Backup 控制台有两种方法可以在备份计划中包含资源类型：在备份计划中明确分配资源类型或包含所有资源。请参阅以下要点，了解如何将这些选择与“选择加入服务”设置一起使用。

- 如果资源分配仅基于标签，将应用“选择加入服务”设置。
- 如果为备份计划明确分配了资源类型，则即使该特定服务未启用选择加入功能，该资源类型也将包含在备份中。这不适用于 Aurora、Neptune 和亚马逊 DocumentDB。要包含这些服务，必须启用选择加入。
- 如果在资源分配中同时指定了资源类型和标签，则首先筛选指定的资源类型，然后标签会进一步筛选这些资源。

  大多数资源类型都将忽略服务选择加入设置。但是 Aurora、Neptune 和亚马逊 DocumentDB 需要选择加入服务。
- 对于适用于 NetApp ONTAP 的 Amazon FSx，在使用基于标签的资源选择时，请将标签应用于单个卷而不是整个文件系统。

服务选择加入设置特定于某个区域。当账户在某个地区使用 AWS Backup （创建备份库或备份计划）时，该账户会自动选择该区域当时支持的所有资源类型。 AWS Backup 稍后添加到该区域的支持服务将不会自动包含在备份计划中。一旦这些资源类型获得支持，您就可以选择使用它们。

配置与使用的服务 AWS Backup

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择 Settings（设置）。
3. 在选择加入服务页面上，选择配置资源。
4. 使用拨动开关启用或禁用与使用的服务 AWS Backup。

> **Important**
>
> RDS、Aurora、Neptune 和 DocumentDB 共享相同的 Amazon 资源名称 (ARN)。选择管理其中一种资源类型，并在将其分配给备份计划时 AWS Backup 选择加入所有资源类型。无论如何，我们建议您选择所有选项，以准确反映您的选择加入状态。

5. 选择确认。

使用 Amazon S3 数据

AWS Backup 为 Amazon S3 备份提供完全托管的备份和恢复。要了解更多信息，请参阅Amazon S3 备份。

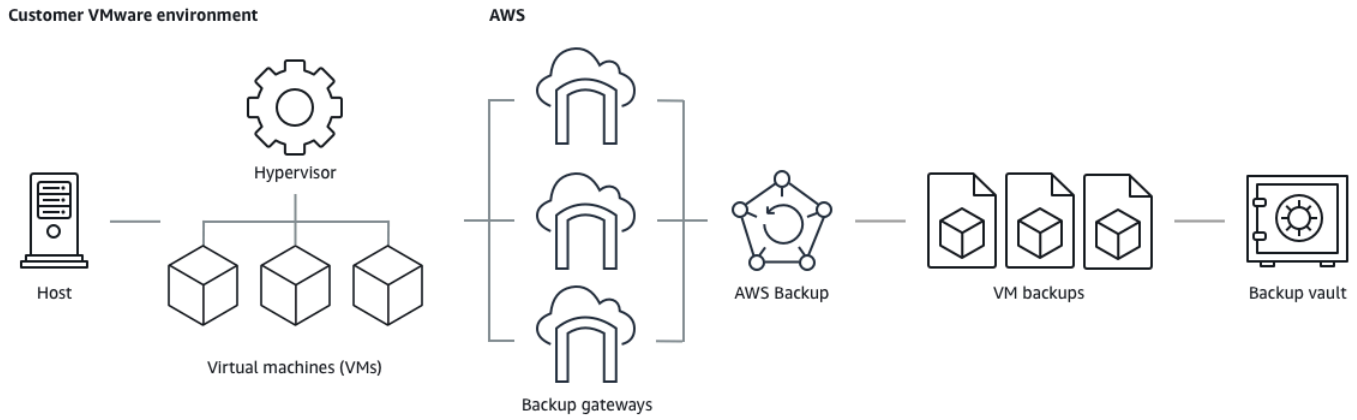
- 如何备份资源：入门 AWS Backup
- 如何使用 AWS Backup以下方法恢复 Amazon S3 数据：还原 S3 数据

有关 S3 数据的详细信息，请参阅 Amazon S3 文档。

使用 VMware 虚拟机

AWS Backup 支持为本地 VMware 虚拟机 (VM) 以及 VMware Cloud™ (VMC) 中的虚拟机提供集中和自动的数据保护。 AWS您可以从本地和 VMC 虚拟机备份到。 AWS Backup然后，您可以从本地或 VMC 恢复 AWS Backup 到。

Backup Gateway 是可下载的 AWS Backup 软件，您可以将其部署到 VMware 虚拟机上以 AWS Backup进行连接。该网关连接到您的虚拟机管理服务器以发现虚拟机、发现您的虚拟机、加密数据并高效地将数据传输到 AWS Backup。下图阐述了 Backup Gateway 如何连接到您的虚拟机：



- 如何备份资源：虚拟机备份
- 如何还原虚拟机资源：使用恢复虚拟机 AWS Backup

使用 Amazon DynamoDB

AWS Backup 支持备份和恢复 Amazon DynamoDB 表。DynamoDB 是一项完全托管的 NoSQL 数据库服务，提供快速而可预测的性能，能够实现无缝扩展。

自推出以来， AWS Backup 一直支持 DynamoDB。从 2021 年 11 月起， AWS Backup 还推出了用于 DynamoDB 备份的高级功能。这些高级功能包括跨 AWS 区域 账户复制备份、将备份分层到冷存储，以及使用标签进行权限和成本管理。

2021 年 11 月之后注册的新 AWS Backup 客户将默认启用高级 DynamoDB 备份功能。

我们建议所有现有 AWS Backup 客户启用 DynamoDB 的高级功能。启用高级功能后，热备份存储的定价没有区别，您可以通过将备份分层到冷存储来节省资金，并通过使用成本分配标签来优化成本。

有关高级功能的完整列表以及如何启用这些功能，请参阅高级 DynamoDB 备份。

- 如何备份资源：入门 AWS Backup
- 如何还原 DynamoDB 资源：还原 Amazon DynamoDB 表

有关 DynamoDB 的详细信息，请参阅《Amazon DynamoDB 开发人员指南》中的什么是 Amazon DynamoDB？。

使用 Amazon FSx 文件系统

AWS Backup 支持备份和恢复 Amazon FSx 文件系统。Amazon FSx 为完全托管的第三方文件系统提供原生兼容性和工作负载功能集。 AWS Backup 使用 Amazon FSx 的内置备份功能。因此，从 AWS Backup 控制台进行的备份与通过 Amazon FSx 控制台进行的备份具有相同级别的文件系统一致性和性能，以及相同的还原选项。

如果您使用 AWS Backup 管理这些备份，则可以获得其他功能，例如无限的保留选项，以及可以像每小时一样频繁地创建定时备份。此外，即使删除了源文件系统，也会 AWS Backup 保留您的备份。这样可以防止意外或恶意删除。

如果您想 AWS Backup 通过同时扩展对其他 AWS 服务的支持的中央备份控制台配置备份策略和监控备份任务，请使用它来保护 Amazon FSx 文件系统。

- 如何备份资源：入门 AWS Backup
- 如何还原 Amazon FSx 资源：还原 FSX 文件系统

有关 Amazon FSx 文件系统的详细信息，请参阅 Amazon FSx 文档。

使用 Amazon EC2

AWS Backup 支持 Amazon EC2 实例。

- 如何备份资源：入门 AWS Backup
- 如何还原 Amazon EC2 资源：还原 Amazon EC2 实例

您可以计划或执行按需备份任务，包括整个 EC2 实例，包括其 Amazon EBS 卷。因此，您可以从单个恢复点恢复整个 Amazon EC2 实例，包括根卷、数据卷和一些实例配置设置，例如实例类型和 key pair。

您还可以备份和还原启用 VSS 的 Microsoft Windows 应用程序。作为按需备份或定时备份计划的一部分，您可以安排应用程序一致性备份，定义生命周期策略，并执行一致的还原。有关更多信息，请参阅创建 Windows VSS 备份。

AWS Backup 在任何时候都不会重启您的 EC2 实例。

图像和快照

备份 Amazon EC2 实例时， AWS Backup 会拍摄根 Amazon EBS 存储卷、启动配置和所有关联的 EBS 卷的快照。 AWS Backup 存储 EC2 实例的某些配置参数，包括实例类型、安全组、Amazon VPC、监控配置和标签。备份数据将存储为 Amazon EBS 卷支持的 Amazon Machine Image (AMI)。

如果您删除 AWS Backup 使用管理的亚马逊系统映像 (AMI) 或 Amazon EBS 快照， AWS Backup 并且配置了 Amazon EC2 回收站，则根据 Amazon EC2 回收站政策，该映像或快照可能会产生费用。如果您从回收站中恢复快照和图像，Amazon EC2 回收站中的快照 AWS Backup 和图像将不再由 AWS Backup 策略管理，也不会由策略管理。

AWS Backup 如果快照锁定持续时间超过备份生命周期，则不能在恢复点生命周期中删除与 AWS Backup 托管 Amazon EC2 AMI 关联的已应用 Amazon EBS 快照锁定的托管 Amazon EBS 快照和快照。相反，这些恢复点的状态将为 `EXPIRED`。如果您选择先删除 Amazon EBS 快照锁，则可以手动删除这些恢复点。

AWS Backup 可以加密与 Amazon EC2 备份关联的 EBS 快照。这与其加密 EBS 快照的方式类似。 AWS Backup 在创建 Amazon EC2 AMI 的快照时，使用与底层 EBS 卷相同的加密，并且原始实例的配置参数保留在还原元数据中。

快照从卷中获取其加密，并且对相应的快照应用相同的加密。复制的 AMI 的 EBS 快照始终处于加密状态。如果您在复制过程中指定 KMS 密钥，则会应用指定的密钥。如果您未指定 KMS 密钥，则会应用默认 KMS 密钥。

有关更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 实例和亚马逊 EBS 用户指南中的亚马逊 EBS 加密。

使用 Amazon EFS

AWS Backup 支持亚马逊 Elastic File System（亚马逊 EFS）。

- 如何备份资源：入门 AWS Backup
- 如何还原 Amazon EFS 资源：还原 Amazon EFS 文件系统

有关 Amazon EFS 文件系统的详细信息，请参阅《Amazon Elastic File System 用户指南》中的什么是 Amazon Elastic File System？。

使用 Amazon EBS

AWS Backup 支持亚马逊 Elastic Block Store (Amazon EBS) 卷。

AWS Backup 如果快照锁定持续时间超过备份生命周期，则不能在恢复点生命周期中删除与 AWS Backup 托管 Amazon EC2 AMI 关联的已应用 Amazon EBS 快照锁定的托管 Amazon EBS 快照和快照。相反，这些恢复点的状态将为 EXPIRED。如果您选择先删除 Amazon EBS 快照锁，则可以手动删除这些恢复点。

- 如何备份资源：入门 AWS Backup
- 如何还原 Amazon EBS 卷：还原 Amazon EBS 卷

有关更多信息，请参阅《亚马逊 EBS 用户指南》中的 Amazon EBS 卷。

使用 Amazon RDS 和 Aurora

AWS Backup 支持 Amazon RDS 数据库引擎和 Aurora 集群。

- 如何备份资源：入门 AWS Backup
- 如何还原 Amazon RDS 资源：还原 SSAS 数据库
- 如何还原 Aurora 集群：还原 Amazon Aurora 集群

有关 Amazon RDS 的更多信息，请参阅《Amazon RDS 用户指南》中的什么是 Amazon Relational Database Service？。

有关 Aurora 的详细信息，请参阅《Amazon Aurora 用户指南》中的什么是 Amazon Aurora？。

> **Note**
>
> 如果您从 Amazon RDS 控制台启动备份作业，则可能会与 Aurora 集群的备份作业发生冲突，从而导致错误备份作业在完成之前过期。如果出现这种情况，请在 AWS Backup中配置更长的备份时段。

> **Note**
>
> AWS Backup目前不支持 RDS Custom for SQL Server 和 RDS Custom for Oracle。

> **Note**
>
> AWS 只要 Aurora 启用了自动备份，并且 Aurora 自动备份的保留期超过 Aurora 快照的保留期，则不对存储在备份库中的 Aurora 快照收费。如果删除了快照的数据库（删除可能是意外发生的，也可能在蓝/绿部署期间发生），将对备份保管库中的所有快照收费。
> 大型快照和从已删除的数据库中频繁备份可能会导致收取大量存储费用。访问 AWS Backup 计算器估算潜在 AWS Backup 费用。

与... 合作 AWS BackInt

AWS Backup 与 AWS Backint 配合使用，支持 Amazon EC2 实例上的 SAP HANA 数据库备份和恢复。

- 备份和恢复 SAP HANA 资源的说明：S AP HANA Amazon EC2 实例备份和还原
- 设置 AWS Backint Agent AWS ：适用于 SAP HANA 的 Backint Agent

与... 合作 AWS Storage Gateway

AWS Backup 支持 Storage Gateway 卷网关。您也可以将 Amazon EBS 快照还原到 Storage Gateway 卷。

- 如何备份资源：入门 AWS Backup
- 如何还原 Storage Gateway 资源：还原 Storage Gateway 卷。

使用 Amazon DocumentDB

AWS Backup 支持亚马逊 DocumentDB 集群。

- 如何备份资源：入门 AWS Backup
- 如何恢复亚马逊文档数据库资源：。还原 DocumentDB 集群

使用 Amazon Neptune

AWS Backup 支持 Amazon Neptune 集群。

- 如何备份资源：入门 AWS Backup

- 如何还原 Amazon Neptune 集群：还原 Neptune 集群。

使用 Amazon Timestream

AWS Backup 支持 Amazon Timestream 表。

- 如何备份 Timestream 表。
- 如何还原 Timestream 表。

与... 合作 AWS Organizations

AWS Backup 与 AWS Organizations 之配合使用可简化跨账户监控和管理

- 在 Organizations 中创建管理账户。
- 启用跨账户管理。
- 指定委托管理员账户和委托策略。

与... 合作 AWS CloudFormation

AWS Backup 支持 AWS CloudFormation 模板和应用程序堆栈

- AWS CloudFormation 堆栈备份

与 SAP 合作 AWS BackInt、 AWS Systems Manager 为 SAP 和 SAP HANA 工作

AWS Backup AWS BackInt 与适用于 SAP 的 SSM 配合使用，支持 SAP HANA 备份和还原功能。

- Amazon EC2 实例上的 SAP HANA 数据库备份
- 开始使用 f AWS Systems Manager or SAP
- AWS 适用于 SAP HANA 的 Backint Agent

AWS 服务如何备份自己的资源

您可以参考技术文档，了解特定 AWS 服务的备份和还原过程，尤其是在还原期间，您需要配置该 AWS 服务的新实例时。以下是文档列表：

- Amazon EC2 相关服务
- AWS Backup 与 Amazon EFS 搭配使用
- DynamoDB 的按需备份和还原
- Amazon EBS 快照
- 备份和还原 Amazon RDS 数据库实例
  - 备份和还原 Aurora 数据库集群概述
- AWS Backup 与适用于 Windows File Server 的 fsX 一起使用
- AWS Backup 与 FSx 一起使用 for Lustre
- 将您的卷备份到 AWS Storage Gateway
- 在 Amazon DocumentDB 中进行备份和还原
- 备份和还原 Amazon Neptune 集群

计量、成本和计费

AWS Backup 定价

当前 AWS Backup 价格按AWS Backup 定价提供。

> **Important**
>
> 为避免额外收费，请为保留策略配置至少一周的温存储持续时间。
> 例如，假设您每天进行备份并将其保留一天。此外，假设您的受保护资源如此之大，需要一整天的时间才能完成备份。 AWS Backup 将您的保留期限定为一天，并在备份任务完成后将备份从温存储中移除。第二天， AWS Backup 无法创建增量备份，因为您的温存储空间中没有备份。由于此保留期未遵循最佳实践，因此，您需要冒着风险，每天创建完整备份，并承担相应费用。
> 如 AWS Support 需进一步帮助，请联系。

AWS Backup 账单

当资源类型支持完全 AWS Backup 管理时，账 Amazon Web Services 单的 “Backup” 部分会显示 AWS Backup 活动费用（包括存储、数据传输、恢复和提前删除）。有关支持完全 AWS Backup 管理的服务列表，请参阅按资源划分的功能可用性表中的 “完全 AWS Backup 管理” 部分。

当某种资源类型不支持完全 AWS Backup 管理时，您的某些 AWS Backup 活动（例如备份的存储成本）将由相应的 AWS 服务反映出来。

复制作业失败

只有在目的地保管库中创建了恢复点后，才会向您收费。当复制作业失败且未创建恢复点时，不收取任何费用。

成本分配标签

您可以使用成本分配标签在详细层面上跟踪和优化 AWS Backup 成本，并使用查看和筛选这些标签 AWS Cost Explorer。

要使用成本分配标签，请参阅使用 AWS Backup自动备份 Amazon EFS 和优化备份成本以及使用成本分配标签。

AWS Backup Audit Manager 定价

AWS Backup Audit Manager 根据控制评估的次数收取使用费。控制评估是针对一种控制对一种资源进行评估。控制评估费用显示在您的 AWS Backup 账单上。有关当前控制评估定价，请参阅 AWS Backup 定价。

要使用 Au AWS Backup dit Manager 控件，必须启用 AWS Config 录制功能以跟踪备份活动。 AWS Config 记录的每个配置项目的费用，这些费用将显示在您的 AWS Config 账单上。有关当前配置项目记录的定价，请参阅 AWS Config 定价。

Amazon Aurora 定价

在 Aurora 连续备份的配置保留期内（最长 35 天），快照不会产生存储费用。超过此时段保留的快照按完整备份计费。

AWS Backup 博客、视频、教程和其他资源

有关的更多信息 AWS Backup，请参阅以下内容：

- 使用备份和恢复本地 VMware 虚拟机 AWS Backup。作者：Olumuyiwa Koya 和 Ezekiel Oyerinde（2022 年 6 月）。
- AWS Backup 用于保护亚马逊 Aurora 数据库。作者：Chris Hendon、Brandon Rubadou 和 Thomas Liddle（2022 年 5 月）。
- 使用跨账户和跨区域备份来保护加密的 Amazon RDS 实例。作者：Evan Peck 和 Sabith Venkitachalapathy（2022 年 5 月）。
- 使用 AWS Backup 和自动化并改善您的安全状况 AWS PrivateLink。作者：Bilal Alam（2022 年 4 月）。
- 获取汇总的每日跨账户多区域报告 AWS Backup。作者：Wali Akbari 和 Sabith Venkitachalapathy（2022 年 2 月）。
- 使用 AWS Backup 和自动查看备份结果 AWS Security Hub。作者：Kanishk Mahajan（2022 年 1 月）。
- 中保护备份的十大安全最佳实践 AWS。作者：Ibukun Oyewumi（2022 年 1 月）。
- AWS 使用 FSx for Lustre 优化 SAS 网格（并使用优化灾难 AWS Backup恢复）。作者：Matt Saeger 和 Shea Lutton（2022 年 1 月）。
- 在 Amazon Neptun AWS Backup e 中集中数据保护和合规性。作者：Brian O'Keefe（2021 年 11 月）。
- 使用 AWS Backup管理 Amazon DocumentDB（与 MongoDB 兼容）的备份和还原。作者：Karthik Vijayraghavan（2021 年 11 月）。
- 使用 A@@ udit Manager 简化对数据保护策略的 AWS Backup 审计。作者：Jordan Bjorkman 和 Harshitha Putta（2021 年 11 月）。
- 使用 AWS Backup Vault Lock 增强备份的安全性。作者：Rolland Miller（2021 年 10 月）。
- 如何在 AWS Backup 还原任务中保留资源标签。作者：Ibukun Oyewumi、Amee Shah 和 Sabith Venkitachalapathy（2021 年 9 月）。
- 使用服务控制策略管理对备份的访问权限 AWS Backup。作者：Sabith Venkitachalapathy 和 Ibukun Oyewumi（2021 年 8 月）。
- 使用实现跨 AWS 服务大规模集中备份的自动化 AWS Backup。作者：Ibukun Oyewumi 和 Sabith Venkitachalapathy（2021 年 7 月）。
- 博客：如何使用 AWS Backup 和 VSS 简化 Microsoft SQL Server 备份。作者：Siavash Irani 和 Sepehr Samiei（2021 年 7 月）。
- 使用自动进行数据恢复验证 AWS Backup。作者：Mahanth Jayadeva（2021 年 6 月）。
- 配置通知以监控 AWS Backup 作业。作者：Virgil Ennes（2021 年 6 月）。

- 使用 AWS Backup自动执行 Amazon EFS 备份并优化备份成本。作者：Prachi Gupta 和 Rohit Verma（2021 年 6 月）。
- 管理 Amazon EFS 备份成本： AWS Backup 支持成本分配标签。作者：Aditya Maruvada（2021 年 5 月）。
- 使用跨账户和地区创建和共享加密备份 AWS Backup。作者：Prachi Gupta（2021 年 5 月）。
- AWS Backup 现已获得 FedRAMP High 认证，可满足您的合规性和数据保护需求。作者：Andy Grimes（2021 年 5 月）。
- ZS Associates 通过提高备份效率 AWS Backup。作者：Mitesh Naik、Hiranand Mulchandani 和 Sushant Jadhav（2021 年 5 月）。
- 教程：使用 AWS Backup Amazon EBS Backup 和还原。作者：Fathima Kamal（2021 年 4 月）。
- 视频教程：管理跨区域备份复制。和大卫在一起 DeLuca （2021 年 4 月）。
- 使用 AWS 工具删除多个 AWS Backup 恢复点 PowerShell。作者：Sherif Talaat（2021 年 4 月）。
- 使用 Amazon FSx 进行跨区域和跨账户备份。 AWS Backup作者：Adam Hunter 和 Fathima Kamal（2021 年 4 月）。
- 的@@ 亚马逊 CloudWatch 事件和指标 AWS Backup. 作者：Rolland Miller（2021 年 3 月）。
- 教程：使用亚马逊关系数据库 (RDS) Service 进行备份和恢复。 AWS Backup作者：Fathima Kamal（2021 年 3 月）。
- 使用 Amazon RDS 的 P oint-in-time 恢复和持续备份 AWS Backup。作者：Kelly Griffin（2021 年 3 月）。
- AWS Backup 使用 Ser AWS vice Catalog 实现自动化。与 John Husemoller 合作（2021 年 1 月）。
- 借助 AWS Backup的跨账户备份和跨区域复制功能保障数据恢复。作者：Cher Simon（2021 年 1 月）。
- AWS re: Invent 回顾：数据保护和合规性。 AWS Backup作者：Nancy Wang（2020 年 12 月）。
- AWS Backup 为您的 AWS 资源提供集中式数据保护。作者：Nancy Wang（2020 年 11 月）。
- 技术研讨会：通过 AWS Backup实现大规模数据保护。作者：Kareem Behairy（2020 年 9 月）。
- 使用@@ 跨区域复制实现集中式跨账户管理。 AWS Backup作者：Cher Simon（2020 年 9 月）。
- 视频教程：在 AWS Organizations 使用中大规模管理备份 AWS Backup。作者：Ildar Sharafeev（2020 年 7 月）。
- 在您的 AWS Organizations 使用中大规模管理备份 AWS Backup。作者：Nancy Wang、Avi Drabkin、Ganesh Sundaresan 和 Vikas Shah（2020 年 6 月）。

- 使用@@ 恢复 Amazon EFS 文件和文件夹 AWS Backup。作者：Abrar Hussain 和 Gurudath Pai（2020 年 5 月）。
- 使用 Amazon EFS 和 AWS Backup安排自动备份。作者：Rob Barnes（2019 年 12 月）。
- re: Invent Recording：re AWS : Invent 2019：深入探索 ft AWS Backup 机架空间。作者：Nancy Wang 和 Jason Pavao（2019 年 12 月）。
- 使用. 保护您的数据 AWS Backup。作者：Anthony Fiore（2019 年 7 月）。
- 营销视频： AWS Backup简介。2019 年 1 月。
- 视频： AWS Backup简介。提供 AWS 培训和认证。

AWS 首次设置

在 AWS Backup 首次使用之前，请完成以下任务：

1. 报名参加 AWS
2. 创建 IAM 用户
3. 创建 IAM 角色

报名参加 AWS

当您注册 Amazon Web Services (AWS) AWS 账户 时，系统会自动注册使用中的所有服务 AWS，包括 AWS Backup。您只需为使用的服务付费。

有关 AWS Backup 使用费率的更多信息，请参阅定AWS Backup 价页面。

如果您 AWS 账户 已有，请跳至下一个任务。如果您还没有 AWS 账户，请使用以下步骤创建。

要创建 AWS 账户

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

   在注册时，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。

记下你的 AWS 账户 电话号码，因为你需要它来完成下一个任务。

创建 IAM 用户

中的 AWS服务（例如 AWS Backup）要求您在访问时提供证书，以便服务可以确定您是否有权访问其资源。 AWS 建议您不要使用 AWS 账户 root 用户发出请求。而应创建一个 IAM 用户并授予该用户完全访问权限。我们将这些用户称为管理员用户。您可以使用管理员用户证书（而不是 AWS 账户 根用户证书）与之交互 AWS 并执行任务，例如创建存储桶、创建用户和向他们授予权限。有关更多信息，

请参阅《AWS 一般参考》中的AWS 账户 根用户凭证与 IAM 用户凭证以及《IAM 用户指南》中的 IAM 最佳实践。

如果您已注册 AWS 但尚未为自己创建 IAM 用户，则可以使用 IAM 控制台创建一个。

要创建管理员用户，请选择以下选项之一。

选择一种方法来管理您的管理员	目的	方式	您也可以
在 IAM Identity Center 中（建议）	使用短期凭证访问 AWS。 这符合安全最佳实操。有关最佳实践的信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。	有关说明，请参阅《AWS IAM Identity Center 用户指南》中的入门。	通过在《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中配置 AWS CLI 要使用的来配置编程访问权限。
在 IAM 中（不推荐使用）	使用长期凭证访问 AWS。	按照《IAM 用户指南》中的创建您的首个 IAM 管理员用户和组的说明操作。	按照《IAM 用户指南》中的管理 IAM 用户的访问密钥，配置编程式访问。

要以此新 IAM 用户的身份登录，请退出 AWS Management Console。然后使用以下 URL，其中 your_aws_account_id 是您的电话 AWS 账户 号码，不带连字符（例如，如果您的号码是，则您 AWS 账户 的 ID 是）：1234-5678-9012 AWS 账户 123456789012

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

输入您刚创建的 IAM 用户名和密码。登录后，导航栏显示 your_user_name@your_aws_account_id。

如果您不希望登录页面的 URL 包含您的 AWS 账户 ID，则可以创建账户别名。从 IAM 控制面板中，单击创建账户别名，然后输入一个别名，例如您的公司名称。要在创建账户别名后登录，请使用以下 URL：

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

要为您的账户验证 IAM 用户的登录链接，请打开 IAM 控制台并在控制面板的 AWS 账户 别名下进行检查。

创建 IAM 角色

您可以使用 IAM 控制台创建 IAM 角色来授予访问支持的资源的 AWS Backup 权限。创建 IAM 角色后，您需要创建策略并将其附加到该角色。

使用控制台创建 IAM 角色

1. 登录 AWS 管理控制台并打开 IAM 控制台。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 选择 AWS 服务角色，然后选择 AWS Backup 对应的选择。选择下一步: 权限。
4. 在附加权限策略页面上，同时选中 AWSBackupServiceRolePolicyForBackup 和 AWSBackupServiceRolePolicyForRestores。这些 AWS 托管策略 AWS Backup 授予备份和恢复所有支持的 AWS 资源的权限。要了解有关托管策略的更多信息并查看示例，请参阅托管策略。

   然后，选择下一步: 标签。
5. 选择下一步: 审核。
6. 对于，请键入可描述此角色作用的名称。角色名称在您的角色中必须是唯一的 AWS 账户。由于可能有多种实体引用该角色，在您创建角色后不能编辑角色名称。

   选择创建角色。
7. 在“角色”页面，选择您创建的角色以便打开其详细信息页面。

入门 AWS Backup

本教程向您展示使用 AWS Backup 特性和功能的一般步骤。与本技术文档的任何部分一样，您应该按照另一个窗口中的 AWS 管理控制台进行操作。

您还可以通过阅读以下教程来学习如何使用 AWS Backup 特定服务：

- 使用 Amazon Relational Database Service (Amazon RDS) 备份和还原 AWS Backup
- 教程：使用 Amazon EBS Backup 和还原 AWS Backup

主题

先决条件

在您开始之前，请确保您已拥有以下各项：

- 一个 AWS 账户。有关更多信息，请参阅 AWS 首次设置。
- 至少支持一种资源 AWS Backup。
- 您应该熟悉要备份的 AWS 服务和资源。查看支持的 AWS 资源和第三方应用程序列表。

  当有新 AWS 服务可用时 AWS Backup ，启用使用这些服务。

  配置要与一起使用的 AWS 服务 AWS Backup

  1. 登录 AWS Management Console，然后通过 https://console.aws.amazon.com/backup 打开 AWS Backup 控制台。

2. 在导航窗格中，选择 Settings（设置）。
3. 在选择加入服务页面上，选择配置资源。
4. 在配置资源页面上，使用切换开关启用或禁用与一起使用的服务 AWS Backup。在配置服务时选择确认。确保您选择的 AWS 服务在您的 AWS 区域服务中可用。

   有关更多信息将资源分配给备份计划，请参阅。 AWS Backup 控制台允许用户为备份计划分配资源类型；即使该特定服务未启用选择加入功能，该资源类型也将包括在内。

- 确保您要备份的资源全部位于同一 AWS 区域。

要完成本教程，您可以使用 AWS 账户 root 用户登录 AWS Management Console。但是， AWS Identity and Access Management (IAM) 建议您不要使用 AWS 账户 根用户。而是在您的账户中创建一个管理员，并使用这些凭证来管理您账户中的资源。有关更多信息，请参阅 AWS 首次设置。

AWS Backup 控制台提供了不同的资源备份选项。您可以按需创建备份，安排和配置所需的资源备份方式，或者在创建资源时将资源配置为自动备份。

入门 1：选择加入服务

AWS Backup 控制台有两种方法可以在备份计划中包含资源类型：在备份计划中明确分配资源类型或包含所有资源。请参阅以下要点，了解如何将这些选择与“选择加入服务”设置一起使用。

- 如果资源分配仅基于标签，将应用“选择加入服务”设置。
- 如果为备份计划明确分配了资源类型，则即使该特定服务未启用选择加入功能，该资源类型也将包含在备份中。这不适用于 Aurora、Neptune 和亚马逊 DocumentDB。要包含这些服务，必须启用选择加入。
- 如果在资源分配中同时指定了资源类型和标签，则首先筛选指定的资源类型，然后标签会进一步筛选这些资源。

  对于大多数资源类型，服务选择加入设置都会被忽略。但是 Aurora、Neptune 和亚马逊 DocumentDB 需要选择加入服务。
- 对于适用于 NetApp ONTAP 的 Amazon FSx，在使用基于标签的资源选择时，请将标签应用于单个卷而不是整个文件系统。

选择加入选项适用于特定帐户，以及 AWS 区域. 当账户在某个地区使用 AWS Backup （创建备份库或备份计划）时，该账户会自动选择该区域当时支持的所有资源类型。 AWS Backup 稍后添加到该区域的支持服务将不会自动包含在备份计划中。一旦这些资源类型获得支持，您就可以选择使用它们。

随着对 AWS 服务和第三方应用程序的 AWS Backup 支持越来越多，您可能需要重新访问此步骤才能选择使用这些新支持的资源。

AWS Backup 不控制或管理在除之外的 AWS 环境中进行的备份 AWS Backup。

选择使用 AWS Backup 来保护所有支持的资源类型

1. 登录 AWS Management Console，然后通过 https://console.aws.amazon.com/backup 打开 AWS Backup 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在选择加入服务下，选择配置资源。
4. 将所有切换开 AWS Backup关向右移动，即可选择使用所有支持的资源。
5. 选择 Confirm（确认）。

后续步骤

要使用创建按需备份 AWS Backup，请继续入门 2：创建按需备份。

入门 2：创建按需备份

在 AWS Backup 控制台上，受保护的资源页面列出了 AWS Backup 至少备份过一次的资源。如果您是首次使用 AWS Backup ，则此页面上没有列出任何资源，例如 Amazon EBS 卷或 Amazon RDS 数据库。如果备份计划未作为计划备份作业至少运行一次，即使该资源已分配到该备份计划中也是如此。

在此步骤 1 中，您将创建某个资源的按需备份。然后，您将看到此资源在 Protected resources (受保护资源) 页面上列出。

创建按需备份

1. 登录 AWS Management Console，然后通过 https://console.aws.amazon.com/backup 打开 AWS Backup 控制台。
2. 使用导航窗格选择受保护的资源，然后选择创建按需备份。
3. 在创建按需备份页面上，选择要备份的资源类型；例如，为 Amazon DynamoDB 表选择 DynamoDB。

4. 选择要保护的资源的名称或 ID。确保您选择的资源是您想要的资源。

> **Note**
>
> 对于适用于 Lustre 的 Amazon FSx，“Persistent”和“Persistent_2”部署类型受支持。

5. 确保选中了立即创建备份。这将立即启动备份，使您能够在受保护的资源页面上更快地看到您保存的资源。
6. 指定转换为冷存储值（如果适用）和过期值。

> **Note**
>
> - 要查看可以转换到冷存储的资源列表，请参阅按资源划分的功能可用性表的“转换到冷存储的生命周期”部分。所有其他资源类型都保存到温存储中，并忽略转换到冷存储表达式。过期值对所有资源类型有效。
> - 当备份过期并作为生命周期策略的一部分标记为 AWS Backup 删除时，将在接下来的 8 小时内随机选择的时间点删除备份。此时段有助于确保一致的性能。

7. 选择现有备份保管库。选择新建备份保管库将打开用于创建保管库的新页面，然后在完成时返回到创建按需备份页面。
8. 在 IAM role (IAM 角色) 下，选择 Default role (默认角色)。

> **Note**
>
> 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的角色。

9. 如果您要将一个或多个标签分配到按需备份，请输入键和可选值，然后选择添加标签。

> **Note**
>
> - 对于 Amazon EC2 资源，除了您添加到此备份中的任何标签外，还 AWS Backup 会自动复制现有的组和单个资源标签。有关更多信息，请参阅将标签复制到备份。
> - 创建基于标签的备份计划时，如果您选择的角色不是默认角色，请确保该角色具有备份所有已标记资源的必要权限。 AWS Backup 尝试处理带有选定标签的所有资源。如果它遇到无权访问的资源，则备份计划将失败。

10. 选择创建按需备份。此操作将您转至作业页面，在其中可以看到作业的列表。

11. 如果您的资源类型为 EC2，则会显示高级备份设置部分。如果您的 EC2 实例运行的是 Microsoft Windows，请选择 Windows VSS。这样，您将能够创建与应用程序保持一致的 Windows VSS 备份。

> **Note**
>
> AWS Backup 目前仅支持在 Amazon EC2 上运行的资源的应用程序一致性备份。Windows VSS 备份并非支持所有实例类型或应用程序。有关更多信息，请参阅 创建 Windows VSS 备份。

12. 为您选择备份的资源选择备份作业 ID 以查看该作业的详细信息。

后续步骤

要自动执行备份活动，请继续执行入门 3：创建计划备份。

入门 3：创建计划备份

AWS Backup 在本教程的这一步中，您将创建备份计划，为其分配资源，然后创建备份保管库。

在开始之前，请确保您满足必需的先决条件。有关更多信息，请参阅 入门 AWS Backup。

主题

步骤 1：基于现有备份计划创建备份计划

备份计划是一个策略表达式，它定义了备份 AWS 资源（例如 Amazon DynamoDB 表或 Amazon Elastic File System (Amazon EFS) 文件系统）的时间和方式。您可以为备份计划分配资源， AWS Backup 然后根据备份计划自动备份和保留这些资源的备份。有关更多信息，请参阅 使用备份计划管理备份。

创建新备份计划有两种方法：您可以从头开始构建，也可以基于现有备份计划构建。此示例使用 AWS Backup 控制台通过修改现有备份计划来创建备份计划。

从现有备份计划创建备份计划

1. 登录 AWS Management Console，然后通过 https://console.aws.amazon.com/backup 打开 AWS Backup 控制台。
2. 从控制面板中，选择管理备份计划。或者，使用导航窗格选择备份计划，并选择创建备份计划。
3. 选择从模板开始，从列表中选择一个计划（例如，Daily-Monthly-1yr-Retention），然后在备份计划名称框中输入一个名称。

> **Note**
>
> 如果您尝试创建与现有计划相同的备份计划，则会收到 AlreadyExistsException 错误。

4. 在计划摘要页面上，选择所需的备份规则，然后选择编辑。
5. 查看并选择您要用于规则的值（有关规则选项，请参阅备份计划选项和配置）。
6. 对于备份保管库，选择默认，或选择新建备份保管库来创建新的保管库。
7. （可选）- AWS 区域 从目标区域的列表中选择一个，将备份复制到其他区域。要添加更多区域，请选择添加副本。
8. 规则编辑完成之后，选择保存备份规则。

在摘要页面上，选择分配资源以准备下一部分。

步骤 2：将资源分配给备份计划

创建备份计划后，必须将 AWS 资源分配给该备份计划。有关分配资源的更多信息，请参阅将资源分配给备份计划。

如果您还没有要分配给备份计划的现有 AWS 资源，请创建一些用于本练习的新资源。使用支持的 AWS 资源和第三方应用程序创建一两个资源。

将资源分配给备份计划

1. 前面的步骤应该会将您带到分配资源页面。
2. 键入资源分配名称。
3. 对于 IAM 角色，选择默认角色。如果您选择其他角色，则该角色必须具有备份您分配的所有资源的权限。

4. 在分配资源部分中，选择包括所有资源类型。资源类型是 AWS Backup支持的 AWS 服务或第三方应用程序。现在，此备份计划将保护您选择使用的所有资源类型 AWS Backup
5. 选择分配资源。

您将返回到备份计划摘要页面。选择创建备份计划来部署您的第一个备份计划！

步骤 3：创建备份保管库

您可以不使用 AWS Backup 控制台上自动为您创建的默认备份保管库，而是创建特定备份保管库，在同一个保管库中保存和组织备份组。

有关备份保管库的更多信息，请参阅备份保管库。

创建备份保管库

1. 在 AWS Backup 控制台的导航窗格中，选择 Backup Vaul ts。

> **Note**
>
> 如果左侧看不到导航窗格，则可以通过选择控制台左上角的菜单图标将其打开。 AWS Backup

2. 选择创建备份保管库。
3. 输入备份保管库的名称。您对保管库的命名可以体现出将要存储在其中的内容，或者便于搜索您所需的备份。例如，您可以将其命名为 **`FinancialBackups`**。
4. 选择一个 AWS Key Management Service (AWS KMS) 密钥。您可以使用已创建的密钥，也可以选择默认 AWS Backup KMS 密钥。

> **Note**
>
> 此处指定的 AWS KMS 密钥仅适用于支持 AWS Backup 独立加密的服务的备份。要查看支持 AWS Backup 独立加密的资源类型列表，请参阅按资源划分的功能可用性表格的 “完全 AWS Backup 管理” 部分。

5. （可选）添加标签可帮助您搜索和标识备份保管库。例如，您可以添加 **`BackupType:Financial`** 标签。
6. 选择创建备份库。
7. 在导航窗格中，选择备份保管库，并确保您的备份保管库已添加。

> **Note**
>
> 现在，您可以在某个备份计划中编辑备份规则，以便将由该规则创建的备份存储在您刚刚创建的备份保管库中。

后续步骤

要专门备份 Amazon EFS 文件系统，请继续执行入门 4：创建 Amazon EFS 自动备份。

入门 4：创建 Amazon EFS 自动备份

当您使用 Amazon EFS 控制台创建 Amazon Elastic File System (Amazon EFS) 文件系统时，自动备份默认处于开启状态。如果您想自动备份现有的 Amazon EFS 文件系统，可以使用 Amazon EFS 控制台、API 或 CLI。

使用控制台自动备份现有 Amazon EFS 文件系统

1. 访问 https://console.aws.amazon.com/efs，打开 Amazon EFS 控制台。
2. 在文件系统页面上，选择要开启自动备份的文件系统。
3. 在常规设置面板中，选择编辑。
4. 要开启自动备份，请选择启用自动备份。

默认备份计划设置为 `daily backups, 35-day retention`。默认备份时段（备份运行的时间区间）设置为凌晨 5 点 UTC（协调世界时）开始，并持续 8 个小时。

> **Note**
>
> Amazon EFS 自动备份保管库 `aws/efs/automatic-backup-vault` 仅用于这些自动备份。
> 此保管库不应用于创建跨账户副本，也不得用作其他非自动备份计划创建的备份的目的地。如果您将其用作其他备份计划的目的地，则会收到“权限不足”错误。

AWS Backup 在您的账户中代表您创建服务相关角色。此角色具有执行 Amazon EFS 备份所需的权限。有关服务相关角色的详细信息，请参阅将服务相关角色用于 AWS Backup。

有关如何使用 Amazon EFS 控制台、API 或 CLI 开启或关闭自动备份的 step-by-step 说明，请参阅 Amaz on Elastic File System 用户指南中的自动备份。

后续步骤

要查看您创建的备份，请继续执行入门 5：查看备份作业和恢复点。

入门 5：查看备份作业和恢复点

使用 AWS Backup，您可以查看所用 AWS 服务的备份和还原活动的状态和其他详细信息。

在 AWS Backup 仪表板上，您可以管理备份计划、创建按需备份、还原备份以及查看备份和还原任务的状态。

主题

查看备份作业的状态

使用 AWS Backup 仪表板快速查看备份和还原活动的状态。

查看备份作业状态

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择控制面板。
3. 要查看备份作业的状态，请选择 Backup jobs details (备份作业详细信息)。这会将您转到作业页面，在其中您可以查看包含备份作业和还原作业的表。
4. 您可以筛选按时间显示的作业。例如，在过去 24 小时、上周或过去 30 天创建的作业。您也可以通过选择齿轮图标，设置每页要显示的作业数。

查看保管库中的所有备份

在 AWS Backup中，按照以下步骤查看在指定保管库中创建的备份。

查看保管库中的所有备份

1. 在 AWS Backup 控制台的导航窗格中，选择 Backup Vaul ts。
2. 选择您在创建按需备份或计划备份时使用的保管库，并查看在此保管库中创建的所有备份。

> **Note**
>
> 每个备份都有一个状态，通常为已完成。如果由于某种原因 AWS Backup 无法根据备份的生命周期配置删除备份，则会将此备份标记为已过期。您需要为过期备份使用的存储空间付费，所以应该将其删除。

查看受保护资源的详细信息

在 Protected resources (受保护资源) 页面上，您可以浏览在 AWS Backup中备份的资源的详细信息。

查看受保护的资源

1. 在 AWS Backup 控制台的导航窗格中，选择受保护的资源。
2. 查看正在备份的 AWS 资源。在列表中选择一个资源以浏览该资源的备份。

后续步骤

要还原已查看的恢复点，请继续执行入门 6：还原备份。

入门 6：还原备份

在资源至少备份一次后，该资源即被视为受保护，可以用它进行恢复 AWS Backup。使用 AWS Backup 控制台，按照以下步骤来还原资源。

有关特定服务的还原参数或使用或 AWS Backup API 恢复备份的信息，请参阅恢复备份。 AWS CLI

还原资源

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的资源 ID。
3. 您的恢复点的列表（包括资源类型）按照资源 ID 显示。选择资源以打开资源详细信息页。

4. 要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
5. 指定还原参数。显示的还原参数特定于所选的资源类型。

> **Note**
>
> 如果只保留一个备份，则只能还原到执行该备份时的文件系统状态。您无法还原到以前的增量备份。

有关如何还原特定资源的说明，请参阅还原备份。

6. 对于还原角色，选择默认角色。

> **Note**
>
> 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的角色。

7. 选择还原备份。

这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

> **Note**
>
> 当您执行还原操作来还原 Amazon EFS 实例中的特定项目时，可以将这些项目还原到新文件系统或现有文件系统。如果您将项目恢复到现有文件系统，则会在根目录之外 AWS Backup 创建一个新的 Amazon EFS 目录来存放这些项目。指定项目的完整层次结构将保留在恢复目录中。例如，如果目录 A 包含子目录 B、C 和 D，则在恢复 A、B、C 和 D 时会 AWS Backup 保留分层结构。
>
> 无论是执行到现有文件系统还是新文件系统的 Amazon EFS 部分还原，每次还原尝试都会在根目录之外创建一个新的恢复目录来包含已还原的文件。如果尝试对同一路径进行多次还原，则可能存在多个包含已还原项目的目录。

还原 Amazon EFS 实例

如果要还原 Amazon EFS 实例，您可以执行完整还原来还原整个文件系统。或者，您可以使用项目级还原来还原特定文件和目录（项目级还原有限制。请参阅还原 EFS 文件系统了解详情）。有关还原其他类型资源的信息，请参阅还原备份。

> **Note**
>
> 要还原 Amazon EFS 实例，您必须“允许”`backup:startrestorejob`。

有关还原备份的详细信息，请参阅还原备份。

后续步骤

使用 A AWS Backup udit Manager，您可以审计您的备份活动和资源。您还可以创建报告，将其用作备份、还原和复制作业的证据。要创建报告，请参阅入门 7：创建审计报告。

入门 7：创建审计报告

在中入门 5：查看备份作业和恢复点，您在 “ AWS Backup 控制面板”、“Backup Vault” 和 “受保护的资源” 视图中观察了备份活动。但是，这些视图是动态视图，会根据您访问它们的时间进行更新。这些视图未必是持续遵守组织数据保护要求和控制措施的最佳证据。

在此步骤中，您将使用 AWS Backup Audit Manager 创建按需备份任务报告。

AWS Backup Audit Manager 每天向您的 Amazon S3 存储桶按需提供 CSV、JSON 或两种格式的各种审计报告。您可以根据许多可自定义的控件来审核备份活动和资源的合规性。您可以收到有关备份、复制和还原作业的报告。备份作业报告可以证明您的备份作业已经完成。

以下是备份计划的示例。

```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
```

```
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```

要创建备份报告（包括按需备份报告），您需要先创建报告计划以自动生成报告并将其提交到 Amazon S3 存储桶。

报告计划要求您有 Amazon S3 存储桶来接收报告。有关设置新 S3 存储桶的说明，请参阅《Amazon Simple Storage Service 用户指南》中的步骤 1：创建您的第一个 S3 存储桶。

创建报告计划

1. 登录 AWS Management Console，然后通过 https://console.aws.amazon.com/backup 打开 AWS Backup 控制台。
2. 在左侧导航窗格中，选择报告。
3. 选择创建报告计划。
4. 从下拉列表中选择备份作业报告。
5. 对于报告计划名称，输入 **`TestBackupJobReport`**。
6. 对于文件格式，同时选择 CSV 和 JSON。
7. 对于 S3 存储桶名称，从下拉列表中选择报告的目的地。
8. 选择创建报告计划。

接下来，您必须允许您的 S3 存储桶接收来自的报告 AWS Backup。 AWS Backup Audit Manager 会自动为您生成 S3 访问策略。

查看和应用此访问策略

1. 在左侧导航窗格中，选择报告。
2. 在报告计划名称下，选择您的报告计划的名称 (TestBackupJobReport)。
3. 选择编辑。
4. 选择查看 S3 存储桶的访问策略。
5. 选择复制权限。
6. 选择编辑存储桶策略以编辑目的地 S3 存储桶的策略，使其能够接收您的备份作业报告。
7. 将权限复制或添加至目的地 S3 存储桶策略。

接下来，创建您的第一份备份作业报告。

创建按需备份报告

1. 在左侧导航窗格中，选择报告。
2. 在报告计划名称下，选择您的报告计划的名称 (TestBackupJobReport)。
3. 选择创建按需报告。

最后，查看您的报告。

查看报告

1. 在左侧导航窗格中，选择报告。
2. 在报告计划名称下，选择您的报告计划的名称 (TestBackupJobReport)。
3. 在报告作业部分中，选择 S3 链接。这样做会将您带到目的地 S3 存储桶。
4. 选择下载。
5. 使用用于处理 CSV 或 JSON 文件的程序打开报告。

后续步骤

要清理入门资源并避免不必要的费用，请继续执行入门 8：清理资源。

入门 8：清理资源

在 入门 AWS Backup 中执行所有任务之后，您可以清除已经创建的资源以免产生不必要的费用。

主题

步骤 1：删除已恢复的 AWS 资源

要删除您从恢复点恢复的 AWS 资源，例如亚马逊弹性区块存储 (Amazon EBS) 卷或亚马逊 DynamoDB 表，您可以使用该服务的控制台。例如，要删除 Amazon Elastic File System (Amazon EFS) 文件系统，请使用 Amazon EFS 控制台。

> **Note**
>
> 此类信息是指还原的资源，而不是存储在备份保管库中的恢复点。

步骤 2：删除备份计划

如果您不希望创建计划备份，则应删除备份计划。必须先删除为备份计划分配的所有资源，然后才能删除该备份计划。

按照以下步骤删除备份计划：

删除备份计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划。
3. 在 Backup plans (备份计划) 页面上，选择要删除的备份计划。这会将您转到该备份的详细信息页面。
4. 要删除计划的资源分配，请选择分配名称旁的单选按钮，然后选择 Delete (删除)。
5. 要删除备份计划，请选择页面右上角的 Delete (删除)。
6. 在确认页面上，输入计划名称，然后选择 Delete plan (删除计划)。

步骤 3：删除恢复点

接下来，您可以删除备份保管库中的备份恢复点。

删除恢复点

1. 在 AWS Backup 控制台的导航窗格中，选择 Backup Vaul ts。
2. 在备份保管库页面上，选择用于存储备份的备份保管库。
3. 检查恢复点并选择删除。
4. 如果您要删除多个恢复点，请按照以下步骤操作：

   a. 如果您的列表包含连续备份，请选择是保留还是删除连续备份数据。

   b. 要删除列出的所有恢复点，请键入 **`delete`**，然后选择删除恢复点。

      保持浏览器选项卡处于打开状态，直到您看到页面顶部显示绿色的成功横幅。过早关闭此选项卡将结束删除过程，并可能留下一些您希望删除的恢复点。相关详情，请参阅删除备份。

步骤 4：删除备份保管库

默认备份保管库通常无法删除。但是，如果一个区域中存在一个或多个其他保管库，则可以使用 AWS CLI删除该区域中的默认备份保管库。

删除其中的所有备份（恢复点）后，您可以删除其他非默认保管库。为此，请在空保管库中选择删除。

步骤 5：删除报告计划

您的报告计划每天自动发送一份新报告。要防止这种情况，请删除报告计划。

删除报告计划

1. 在 AWS Backup 控制台的导航窗格中，选择报告。
2. 在报告计划名称下，选择您的报告计划的名称。
3. 选择删除。
4. 输入您的报告计划名称，然后选择删除报告计划。

步骤 6：删除报告

您可以按照删除每份报告的单个对象的说明，删除报告。如果您不再需要目的地 S3 存储桶，则在从存储桶中删除所有对象后，可以按照删除存储桶的说明，删除存储桶。

使用备份计划管理备份

在中 AWS Backup，备份计划是一种策略表达式，用于定义何时以及如何备份 AWS 资源，例如 Amazon DynamoDB 表或亚马逊弹性文件系统 (Amazon EFS) 文件系统。您可以为备份计划分配资源，并根据备份计划 AWS Backup 自动备份和保留这些资源的备份。如果您的工作负载具有不同的备份要求，则可以创建多个备份计划。默认情况下，备份时段经过 AWS Backup的优化。您可以在控制台或以编程方式自定义备份时段。

AWS Backup 以增量方式高效存储定期备份。 AWS 资源的第一次备份会备份数据的完整副本。对于每次连续的增量备份，仅备份对 AWS 资源的更改。通过增量备份，您能够从频繁备份的数据保护中受益，同时最大限度降低存储成本。

AWS Backup 还可以根据保留设置无缝管理备份计划的生命周期，这样您就可以在需要时进行恢复。

以下各节提供了在中管理备份策略的基础知识 AWS Backup。

主题

创建备份计划

您可以使用 AWS Backup 控制台、API、CLI、SDK 或 AWS CloudFormation 模板创建备份计划。

主题

使用 AWS Backup 控制台创建备份计划

打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。从控制面板中，选择管理备份计划。或者，使用导航窗格选择备份计划，并选择创建备份计划。

启动选项

要启动新的备份计划，您有三种选择：

- 步骤 1：基于现有备份计划创建备份计划
- 创建新计划
- 使用创建备份计划 AWS CLI

在本教程中，我们将选择创建新计划。配置的每个部分都有一个指向页面上扩展部分的链接，您可以在该部分中导航以获取更多详细信息。

1. 在中输入计划名称备份计划名称。计划创建后无法更改其名称。

   如果您尝试创建与现有计划相同的备份计划，则会收到`AlreadyExistsException`错误消息。
2. 您可以选择为备份计划添加标签。
3. 备份规则配置：在备份规则配置部分，您将要设置备份计划、时段和生命周期。
4. 计划：

   a. 在文本字段中输入备份规则名称。

   b. 在“备份保管库”下拉菜单中，选择默认或选择新建备份保管库以创建新的保管库。

   c. 在“备份频率”下拉菜单中，选择您希望此计划创建备份的频率。
5. 备份时段：

   a. 开始时间默认为系统本地时区的上午 12:30（24 小时内为 00:30）。

   b. 开始时间范围默认为 8 小时。您可以对此设置进行更改以指定开始备份的时间段。

   c. 完成时间范围默认为 7 天。
6. 连续备份和 point-in-time 恢复 (PITR)：您可以选择 “启用连续备份以进行 point-in-time 恢复 (PITR)”。要验证支持使用哪些资源进行此类备份，请参阅按资源划分的功能可用性矩阵。
7. 生命周期

   a. 冷存储：选中此框可让符合条件的资源类型根据您在“总保留期”中指定的时间表转移到冷存储。要使用冷存储，您的总保留期必须不短于 90 天。

   b. Amazon EBS 的冷存储是 Amazon EBS 快照归档。转移到归档存储层的快照将作为冷层显示在控制台中。如果启用了冷存储，并且您的备份频率为每月或更长时间一次，则可以让备份计划转移 EBS 快照。

   c. 总保留期是您将资源存储在 AWS Backup中的天数。它是暖存储天数和冷存储天数的总和。

8. （可选）如果您想将备份副本存储在其他 AWS 区域中，请使用复制到目的地来创建符合条件的资源的跨区域副本。
9. （可选）将标签添加到恢复点。
10. 当所有部分均设置为您的规格后，请选择保存备份规则。

使用创建备份计划 AWS CLI

您也可以在 JSON 文档中定义备份计划并使用 AWS Backup 控制台或 AWS CLI提供该计划。以下 JSON 文档包含一个示例备份计划，该计划在太平洋时间 1:00 创建每日备份（如果适用，当地时间会调整为夏令时、标准时间或夏令时条件）。它会在一年后自动删除备份。

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules":[
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone":"America/Los_Angeles",
        "StartWindowMinutes":integer, // Value is in minutes
        "CompletionWindowMinutes":integer, // Value is in minutes
        "Lifecycle":{
          "DeleteAfterDays":integer, // Value is in days
        }
      }
    ]
  }
}
```

您可以使用自己选择的名称存储 JSON 文档。以下 CLI 命令显示的是 `create-backup-plan`，其带有名为 `test-backup-plan.json` 的 JSON：

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

请注意，虽然有些系统将一周中的几天从 0 到 6 进行编号，但我们从 1 到 7 进行编号。有关更多信息，请参阅 Cron 表达式。有关时区的更多信息，请参阅 Amazon Location Service API 参考TimeZone中的。

备份计划选项和配置

在 AWS Backup 控制台中定义备份计划时，需要配置以下选项：

备份计划名称

您必须提供唯一备份计划名称。

如果您选择与现有计划名称相同的名称，将会收到一条错误消息。

备份规则

备份计划由一个或多个备份规则组成。向备份计划添加备份规则或编辑备份计划中的现有规则：

1. 在 AWS Backup 控制台的左侧导航窗格中，选择 Backup 计划。
2. 在备份计划名称下，选择一个备份计划。
3. 在备份规则部分下：
   - 要添加备份规则，请选择添加备份规则。
   - 要编辑现有备份规则，请选择规则，然后选择编辑。

> **Note**
>
> 如果您的备份计划包含多个规则，并且两个规则的时间范围重叠，请 AWS Backup 优化备份并针对保留时间较长的规则进行备份。优化功能考虑了完整的启动时段，而不仅仅是每日备份的时间。

每个备份规则都包含以下元素。

备份规则名称

备份规则名称区分大小写。必须包含 1 到 50 个字母数字字符或连字符。

Backup frequency (备份频率)

备份频率决定了 AWS Backup 创建快照备份的频率。使用控制台，您可从每小时、每 12 个小时、每天、每周或每月中选择频率。您还可以创建 Cron 表达式，以每小时一次的频率创建快照备份。使用 AWS Backup CLI，您可以将快照备份频率安排为每小时一次。

如果选择每周，您可以指定在一周中的星期几进行备份。如果选择每月，您可以选择在一月中具体哪一天进行备份。

您也可以选中 “为支持的资源启用连续备份” 复选框来创建启用 point-in-time 恢复 (PITR) 的连续备份规则。与快照备份不同，连续备份允许您执行 point-in-time 恢复。要详细了解连续备份，请参阅时间点恢复。

备份时段

备份时段由备份时段的开始时间和持续时间（以小时为单位）构成。备份作业会在此时段内启动。控制台中的默认设置为：

- 系统所在时区当地时间@@ 上午 12:30（24 小时系统为 0:30）
- 8 小时内开始
- 7 天内完成

（完成时间范围参数不适用于 Amazon FSx 资源）

您可以使用 cron 表达式来自定义备份频率和备份时段开始时间。要查看 AWS cron 表达式的六个字段，请参阅 A ma CloudWatch zon Events 用户指南中的 Cron 表达式。 AWS cron 表达式的两个示例是`15 * ? * * *`（每小时在过去 15 分钟时进行一次备份）和`0 12 * * ? *`（UTC 每天中午 12 点进行备份）。要查看示例表，请单击前面的链接并向下滚动页面。

AWS Backup 在 00:00 到 23:59 之间评估 cron 表达式。如果您创建了“每 12 小时”的备份规则，但提供的开始时间晚于 11:59，则该规则每天只会运行一次。

连续备份和 point-in-time 恢复 (PITR) 引用一段时间内记录的更改；因此，无法使用时间或 cron 表达式来安排这些更改。

> **Note**
>
> 通常， AWS 数据库服务无法在维护时段前 1 小时或维护时段内启动备份，Amazon FSx 无法在其维护时段或自动备份窗口前 4 小时或期间启动备份（Amazon Aurora 不受此维护时段限制的约束）。在这段时间内安排的快照备份将失败。
> 当您选择使用 AWS Backup 对受支持的服务进行快照和连续备份时，会发生异常。 AWS Backup 将自动安排备份时段以避免冲突。有关支持的服务列表以及如何使用 AWS Backup 进行连续备份的说明，请参阅时间点恢复。

重叠备份规则

有时，备份计划可能包含多个重叠的规则。当不同规则的起始窗口重叠时， AWS Backup 会根据保留期较长的规则保留备份。例如，假设有一个备份计划包含两条规则：

1. 每小时备份一次，起始时间为 1 小时，并保留 1 天。
2. 每 12 小时备份一次，起始时间为 8 小时，并保留 1 周。

24 小时后，第二条规则创建两个备份（因为它的保留期更长）。第一条规则创建八个备份（因为第二条规则的 8 小时启动时间使每小时备份无法运行）。具体来说：

在这个开始时间内	此规则创建 1 个备份
午夜至早上 8 点	12 小时
8 点到 9 点	每小时
9 点到 10 点	每小时
10 点到 11 点	每小时
11 点到中午	每小时
中午至晚上 8 点	12 小时
8 点到 9 点	每小时
9 点到 10 点	每小时
10 点到 11 点	每小时
11 点到午夜	每小时

在启动时段内，备份作业的状态将保持 CREATED 状态，直到成功启动或启动时段结束为止。如果在启动窗口内 AWS Backup 收到允许重试作业的错误消息， AWS Backup 则至少每 10 分钟自动重试一次以开始作业，直到备份成功开始（任务状态更改为RUNNING）或任务状态更改为EXPIRED（预计在启动窗口时间结束时发生）。

生命周期和存储层

备份将存储您指定的天数（即备份生命周期）。备份可以还原，直到其生命周期结束。

在 AWS Backup 控制台中备份规则配置的生命周期部分中，将其设置为总保留期。

如果您使用 AWS CLI，则使用参数进行设置DeleteAfterDays。快照的保留期可以介于 1 天到 100 年之间（如果不输入具体时间，则无限期），而连续备份的保留期可以从 1 天到 35 天不等。备份的创建日期是备份作业的开始日期，而不是其完成的日期。如果您的备份任务未在开始日期完成，请使用开始日期来帮助计算保留期。

备份保存在存储层中。如 AWS Backup 定价所述，每个层的存储和还原成本都不同。每个备份都已创建并存储在暖存储中。根据您选择的备份存储时间长短，您可能希望将备份转移到成本较低的层（名为“冷存储”）。按资源划分的功能可用性中显示了哪些资源具有此可选功能。

Console

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 创建或编辑备份计划。
3. 在备份规则配置的生命周期部分，选中将备份从暖存储移至冷存储框。
4. （可选）如果 Amazon EBS 是您备份的资源之一，并且您的备份频率为每月或更长时间一次，则可以使用 EBS 快照归档将其转移到冷层。
5. 输入您希望将备份保留在温存储空间中的值（以天为单位）。 AWS Backup 建议至少 8 天。
6. 输入总保留期的值（以天为单位）。总保留期和暖存储时间之间的差值将是备份在冷存储中保留的天数。

AWS CLI

1. 使用 create-backup-plan 或者 update-backup-plan。
2.
3. 包括 EBS 资源的布尔参数 OptInToArchiveForSupportedResources。
4. 包含 MoveToColdStorageAfterdays 参数。
5. 使用 DeleteAfterDays 参数。此值必须是 90（天）加上您输入的 MoveToColdStorageAfterDays 值。

冷存储目前可用于以下资源类型：

资源类型	冷存储中的增量备份或完整备份
AWS CloudFormation	增量
DynamoDB，带 高级功能	完整；任何层中都没有增量备份
Amazon EBS（使用 EBS 快照归档）	完整；转移后增量备份将变为完整备份。
Amazon EFS	增量
Amazon EC2 实例上运行的 SAP HANA 数据库	增量
Amazon Timestream	增量
VMware 虚拟机	增量

通过控制台或命令行启用向冷存储的转移后，以下条件对于冷存储（或归档）中的备份是成立的：

- 过渡后的备份除了在温存储中存储的时间外，还必须在冷库中存储至少 90 天。 AWS Backup 要求将保留期设置为 90 天，比 “几天后过渡到低温” 设置长 90 天。在备份转换为冷态后，您无法更改“转换为冷态前经过的天数”设置。
- 一些服务支持增量备份。对于增量备份，必须至少有一个热完整备份。 AWS Backup 建议您将生命周期设置为在至少 8 天后才将备份移至冷存储。如果过早地将完整备份过渡到冷存储（例如，1 天后过渡到冷存储），则 AWS Backup 会创建另一个热完整备份。
- 对于支持增量备份的资源类型，如果热备份不再引用 AWS Backup 过渡后的数据，则会将数据从温存储转换为冷存储。冷备份中保留的仅供其他冷备份引用的备份数据按冷存储层定价计费。其他备份则继续按暖存储层定价计费。

备份保管库

备份保管库是一个用来整理备份的容器。由备份规则创建的备份存储到您在备份规则中指定的备份保管库。您可以使用备份存储库来设置 AWS Key Management Service (AWS KMS) 加密密钥，该密钥用于加密备份库中的备份，并控制对备份库中备份的访问权限。您还可以向备份保管库添加标签来帮助组织备份保管库。如果您不想使用默认保管库，可以自行创建保管库。有关创建备份存储库的 step-by-step 说明，请参阅步骤 3：创建备份保管库。

复制到区域

作为备份计划的一部分，您可以选择在另一个 AWS 区域创建备份副本。有关备份副本的更多信息，请参阅跨 AWS 区域创建备份副本。

在定义备份副本时，您可以配置以下选项：

目的地区域

备份副本的目的地区域。

（高级设置）备份保管库

副本的目的地备份保管库。

（高级设置）IAM 角色

创建副本时 AWS Backup 使用的 IAM 角色。该角色还必须 AWS Backup 列为可信实体，这样 AWS Backup 才能担任该角色。如果您选择默认，但您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的角色。

（高级设置）生命周期

指定将备份副本转换到冷存储的时间以及副本的到期（删除）时间。转换到冷存储的备份必须在冷存储中存储至少 90 天。在副本转换为冷存储后，您无法更改此值。

过期指定副本在创建后多少天删除。这必须比转换为冷存储值多 90 天。

添加到恢复点的标签

您在此处列出的标签，在创建备份时将自动添加到备份。

添加到备份计划的标签

这些标签与备份计划本身关联，帮助您组织和跟踪备份计划。

高级备份设置

为 Amazon EC2 实例上运行的第三方应用程序启用应用程序一致性备份。目前， AWS Backup 支持 Windows VSS 备份。 AWS Backup 从 Windows VSS 备份中排除特定的 Amazon EC2 实例类型。有关更多信息，请参阅 创建 Windows VSS 备份。

AWS CloudFormation 备份计划模板

我们提供了两个示例 AWS CloudFormation 模板供您参考。第一个模板可创建一个简单的备份计划。第二个模板在备份计划中启用 VSS 备份。

> **Note**
>
> 如果您使用的是默认服务角色，请将 *service-role* 替换为 AWSBackupServiceRolePolicyForBackup。

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
```

```
      BackupPlanRule:
        - RuleName: "RuleForDailyBackups"
          TargetBackupVault: !Ref BackupVaultWithDailyBackups
          ScheduleExpression: "cron(0 5 ? * * *)"
  DependsOn: BackupVaultWithDailyBackups

DDBTableWithDailyBackupTag:
  Type: "AWS::DynamoDB::Table"
  Properties:
    TableName: "TestTable"
    AttributeDefinitions:
      - AttributeName: "Album"
        AttributeType: "S"
    KeySchema:
      - AttributeName: "Album"
        KeyType: "HASH"
    ProvisionedThroughput:
      ReadCapacityUnits: "5"
      WriteCapacityUnits: "5"
    Tags:
      - Key: "backup"
        Value: "daily"

BackupRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    ManagedPolicyArns:
      - "arn:aws:iam::aws:policy/service-role/service-role"

TagBasedBackupSelection:
  Type: "AWS::Backup::BackupSelection"
  Properties:
    BackupSelection:
      SelectionName: "TagBasedBackupSelection"
      IamRoleArn: !GetAtt BackupRole.Arn
```

```
        ListOfTags:
          - ConditionType: "STRINGEQUALS"
            ConditionKey: "backup"
            ConditionValue: "daily"
      BackupPlanId: !Ref BackupPlanWithDailyBackups
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
        BackupPlanRule:
```

```
        - RuleName: "RuleForDailyBackups"
          TargetBackupVault: !Ref BackupVaultWithDailyBackups
          ScheduleExpression: "cron(0 5 ? * * *)"

  DependsOn: BackupVaultWithDailyBackups
```

将资源分配给备份计划

资源分配指定 AWS Backup 将使用您的备份计划保护哪些资源。 AWS Backup 为您提供了简单的默认设置和精细的控制来为备份计划分配资源。每次运行备份计划时，它都会扫描您的 AWS 账户 所有符合您的资源分配标准的资源。这种自动化级别允许您只定义一次备份计划和资源分配。 AWS Backup 简化了寻找和备份适合您先前定义的资源分配的新资源的工作。

您可以分配您选择管理的任何 AWS Backup支持的资源类型。 AWS Backup 有关如何选择更多 AWS Backup支持的资源类型的说明，请参阅入门 1：服务选择加入。

AWS Backup 控制台有两种方法可以在备份计划中包含资源类型：在备份计划中明确分配资源类型或包含所有资源。请参阅以下要点，了解如何将这些选择与“选择加入服务”设置一起使用。

- 如果资源分配仅基于标签，将应用“选择加入服务”设置。
- 如果为备份计划明确分配了资源类型，则即使该特定服务未启用选择加入功能，该资源类型也将包含在备份中。这不适用于 Aurora、Neptune 和亚马逊 DocumentDB。要将这些服务包括在内，必须启用选择加入。
- 如果在资源分配中同时指定了资源类型和标签，则首先筛选指定的资源类型，然后标签会进一步筛选这些资源。

  对于大多数资源类型，服务选择加入设置都会被忽略。但是 Aurora、Neptune 和亚马逊 DocumentDB 需要选择加入服务。
- 当账户在某个地区使用 AWS Backup （创建备份库或备份计划）时，该账户会自动选择该区域当时支持的所有资源类型。 AWS Backup 稍后添加到该区域的支持服务将不会自动包含在备份计划中。一旦这些资源类型获得支持，您就可以选择使用它们。
- 对于适用于 NetApp ONTAP 的 Amazon FSx，在使用基于标签的资源选择时，请将标签应用于单个卷而不是整个文件系统。

您的资源分配可以包括（或排除）资源类型和资源。

- 资源类型包括 AWS Backup支持的 AWS 服务或第三方应用程序的每个实例或资源。例如，DynamoDB 资源类型指的是您的所有 DynamoDB 表。

- 资源是某种资源类型的单个实例，例如您的一个 DynamoDB 表。您可以使用其唯一的资源 ID 来指定资源。

您可以使用标签和条件运算符进一步细化资源分配。

主题

使用控制台分配资源

要导航到分配资源页面，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 选择备份计划。
3. 选择创建备份计划。
4. 在选择模板下拉列表中选择任意模板，然后选择创建计划。
5. 键入备份计划名称。
6. 选择创建计划。
7. 选择分配资源。

要开始分配资源，请在常规部分执行以下操作：

1. 键入资源分配名称。
2. 选择默认角色或选择一个 IAM 角色。

> **Note**
>
> 如果您选择 IAM 角色，请验证该角色是否具有备份您要分配的所有资源的权限。如果您的角色遇到它无权备份的资源，则备份计划将失败。

要分配资源，请在分配资源部分，选择定义资源选择下的两个选项之一：

- 包括所有资源类型。此选项可配置您的备份计划，以保护分配给您的备份计划的所有当前和 future AWS Backup支持的资源。使用此选项可以快速轻松地保护您的数据资产。

  选择此选项后，下一步可以选择使用标签来调整选择。

- 包括特定的资源类型。选择此选项时，必须按照以下步骤选择特定的资源类型：

  1. 使用选择资源类型下拉菜单，分配一个或多个资源类型。

     > **Important**
     >
     > RDS、Aurora、Neptune 和 DocumentDB 共享相同的 Amazon 资源名称 (ARN)。在将其中一种资源类型分配给备份计划时，选择使用 AWS Backup 来管理这种资源可以选择管理所有这些资源类型。要细化您的选择，请使用标签和条件运算符。

     完成后，将 AWS Backup 显示您选择的资源类型列表及其默认设置，即保护每种选定资源类型的所有资源。

  2. （可选）如果您想从所选资源类型中排除特定资源，请执行以下操作：

     1. 使用选择资源下拉菜单并取消选择默认选项。
     2. 选择要分配给备份计划的特定资源。

  3. 或者，您可以从所选资源类型中排除特定的资源 ID。如果您想从众多资源中排除一个或几个资源，请使用此选项，因为这样做可能比在上一步中选择许多资源要快。必须先包括资源类型，然后才能从该资源类型中排除资源。使用以下步骤排除资源 ID：

     1. 在从所选资源类型中排除特定资源 ID下，使用选择资源类型选择一个或多个包含的资源类型。
     2. 对于每种资源类型，使用选择资源菜单选择一个或多个要排除的资源。

除了之前的选择外，您还可以使用可选的使用标签优化选择功能，进行更精细的选择。此功能允许您使用标签细化当前的选择，以包含资源子集。

标签是键值对，您可以将其分配给特定资源，以帮助您识别、组织和筛选资源。标签区分大小写。有关更多信息，请参阅《AWS 一般参考》中的标记 AWS 资源。

当您使用两个或更多标签细化您的选择时，效果是 AND 条件。例如，如果您使用 `env: prod` 和 `role: application` 这两个标签来细化选择，则只能将带有 BOTH 标签的资源分配给您的备份计划。

要使用标签细化选择，请执行以下操作：

1. 在使用标签细化选择下，从下拉列表中选择一个密钥。
2. 从下拉列表中选择值条件。
   - 值是指下一个输入，即键值对的值。
   - 条件可以是 Equals、Contains、Begins with 或 Ends with，或者它们的反义词：Does not equal、Does not contain、Does not begin with 或 Does not end with。
3. 从下拉列表中选择一个值。
4. 要使用其他标签进一步细化，请选择添加标签。

以编程方式分配资源

您可以在 JSON 文档中定义资源分配。此示例资源分配将所有 Amazon EC2 实例分配给备份计划 *BACKUP-PLAN-ID*：

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

假设将此 JSON 存储为 backup-selection.json，则您可以使用以下 CLI 命令将这些资源分配给您的备份计划：

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

以下是资源分配示例，以及相应的 JSON 文档。为了便于您阅读此表，示例省略了字段 "BackupPlanId"、"SelectionName" 和 "IamRoleArn"。通配符 * 代表零个或多个非空格字符。

Example 示例：选择我账户中的所有资源

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ]
  }
}
```

Example 示例：选择我账户中的所有资源，但不包括 EBS 卷

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example 示例：选择所有标有 "backup":"true" EBS 卷但不包括 EBS 卷的资源

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
```

```
}
```

Example 示例：选择所有同时"backup":"true"标记了和的 EBS 卷和 RDS 数据库实例 "stage":"prod"

布尔算术与 IAM 策略中的算术类似，"Resources" 中的策略使用布尔 OR 组合，而 "Conditions" 中的策略使用布尔 AND 组合。

"Resources" 表达式 "arn:aws:rds:*:*:db:*" 仅选择 RDS DB 实例，因为没有相应的 Aurora、Neptune 或 DocumentDB 资源。

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Example 示例：选择所有标有"backup":"true"但未标记的 EBS 卷和 RDS 实例 "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
```

```
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 示例：选择所有标记为的资源，"key1"以及一个以开头"include"但不以该词开头的值，"key2"以及包含该词的值 "exclude"

您可以在字符串的开头、结尾和中间使用通配符字符。请注意，上述示例在 `include*` 和 `*exclude*` 中使用了通配符 (*)。您也可以在字符串中间使用通配符，如前面的示例所示，`arn:aws:rds:*:*:db:*`。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/key1",
          "ConditionValue":"include*"
        }
      ],
      "StringNotLike":[
        {
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
  }
}
```

Example 示例：选择"backup":"true"除了 FSx 文件系统以及 RDS、Aurora、Neptune 和 DocumentDB 资源之外的所有标有标签的资源

`NotResources` 中的项目使用布尔 OR 进行组合。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example 示例：选择所有标有标签"backup"和任意值的资源

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Example 示例：选择所有 FSx 文件系统、Aurora 集群"my-aurora-cluster"和所有标有标签的资源"backup":"true"，但标记为的资源除外 "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 示例：选择所有标有标签的资源，但标有标签的 EBS 卷**"backup":"true"**除外**"stage":"test"**

使用两个 CLI 命令创建两个选项来选择这组资源。第一个选项适用于除了 EBS 卷之外的所有资源。第二个选项适用于 EBS 卷。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
```

```
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

使用分配资源 AWS CloudFormation

此 end-to-end AWS CloudFormation 模板创建资源分配、备份计划和目标备份存储库：

- 名为的备份保管库*CloudFormationTestBackupVault*。
- 名为的备份计划*CloudFormationTestBackupPlan*。该计划将运行两个包含两个备份规则的计划，这两个规则均在 UTC 每天中午 12 点进行备份，并保留 210 天。
- 名为的资源选择*BackupSelectionName*。
- • 资源分配会备份以下资源：
  - 任何标记为键值对 backupplan:dsi-sandbox-daily 的资源。

    - 标记为值 prod 或值以 prod/ 开头的任何资源。
- 资源分配不会备份以下资源：
    - 任何 RDS、Aurora、Neptune 或 DocumentDB 集群。
    - 标记为值 test 或值以 test/ 开头的任何资源。

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
```

```
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
          - RuleName: !Ref RuleName2
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
```

```
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod
          StringNotEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test
          StringLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod/*
          StringNotLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test/*
```

资源分配配额

以下配额适用于单个资源分配：

- 500 个不带通配符的 Amazon 资源名称 (ARN)
- 30 个带有通配符表达式的 ARN
- 30 个条件

- 每个资源分配 30 个标签（且每个标签的资源数量不受限制）

删除备份计划

只有在删除了所有关联的资源选择之后，才能删除备份计划。这些选择也称为资源分配。如果在删除备份计划之前未将其删除，则控制台将显示错误："在删除备份计划之前，必须删除相关的备份计划选项。" 使用控制台或使用`DeleteBackupSelection`。

删除备份计划时将删除计划的当前版本。当前版本和以前版本（如果有）仍然存在，但控制台的 Backup plans (备份计划) 下将不再列出它们。

> **Note**
>
> 在删除备份计划时，不会删除现有备份。要删除现有备份，请使用删除备份中的步骤，从备份保管库中将其删除。

使用 AWS Backup 控制台删除备份计划

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在左侧的导航窗格中，选择 Backup plans (备份计划)。
3. 在列表中选择备份计划。
4. 选择与备份计划关联的任意资源分配。
5. 选择删除。

更新备份计划

创建备份计划后，您可以编辑计划，例如，您可以添加标签，也可以添加、编辑或删除备份规则。您对备份计划所做的任何更改都不会影响备份计划已经创建的现有备份。这些更改仅应用到未来创建的备份。

例如，当您更新备份规则中的保留期时，在您更新保留期之前创建的备份，其保留期仍保持相同。该规则以后创建的任何备份将使用更新后的保留期。

计划创建后无法更改其名称。

使用 AWS Backup 控制台编辑备份计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划。
3. 在第二个窗格 “Backup plans” 下，将显示现有的备份计划。选择 “备份计划名称” 列中带下划线的链接，以查看所选备份计划的详细信息。
4. 您可以编辑备份规则、查看资源分配、查看备份作业、管理标签或更改 Windows VSS 设置。
5. 要更新备份规则，请选择备份规则的名称。

   选择管理标签以添加或删除标签。

   选择 “高级备份设置” 旁边的 “编辑” 以打开或关闭 Windows VSS。
6. 更改您喜欢的设置，然后选择 “保存”。

备份保管库

> **Note**
>
> 从 2023 年 8 月 9 日起 AWS Backup ，将提供使用逻辑气隙保管库的预览版。要注册此预览版，请通过电子邮件向 <aws-backup-vault-preview@amazon .com> 发送申请。
> 在预览期间和之后，功能可能会更改或调整。当该服务正式发布 (GA) 时，预览期间提供的数据和配置将不再可用。 AWS 建议在预览中使用测试数据，而不是生产数据。

在中 AWS Backup，备份保管库是一个用于存储和组织备份的容器。

创建备份存储库时，必须指定 AWS Key Management Service (AWS KMS) 加密密钥，该密钥用于加密放置在该存储库中的某些备份。其他备份的加密由其源 AWS 服务管理。有关加密的更多信息，请参阅 AWS中的备份加密。

您的账户将始终有一个默认的备份保管库。如果需要为不同的备份组使用不同的加密密钥或访问策略，您可以创建多个备份保管库。

本节概述如何在 AWS Backup中管理您的备份保管库。

主题

逻辑气隙保管库（预览版）

> **Note**
>
> 从 2023 年 8 月 9 日起 AWS Backup ，将提供使用逻辑气隙保管库的预览版。要注册此预览版，请通过电子邮件向 <aws-backup-vault-preview@amazon .com> 发送申请。
> 在预览期间和之后，功能可能会更改或调整。当该服务正式发布 (GA) 时，预览期间提供的数据和配置将不再可用。 AWS 建议在预览中使用测试数据，而不是生产数据。

概述

AWS Backup 正在预览一种辅助类型的存储库，它可以将备份副本存储在其他存储库中。逻辑气隙保管库是一种专门的保管库，除了备份保管库的功能外，它还提供增强的安全功能，并且能够与其他账户和组织共享保管库访问权限，以便在发生需要快速恢复资源的事件时可以更快、更灵活地进行恢复(RTO)。

从逻辑上讲，气隙保管库还配备了额外的保护功能：每个保管库都使用 AWS 自有密钥加密，每个保管库都设置了合规模式下的文件库锁。

您可以选择在组织和账户之间共享逻辑气隙保管库，以便在需要时可以从与之共享该保管库的账户中恢复存储在其中的备份。

在预览期间，在逻辑气隙保管库中存储备份不会产生额外费用。标准备份保管库和跨区域副本中的备份仍将按公布的费率收费（参见定价），即使这些备份在逻辑气隙保管库中的任何副本都不收费。

应用场景

逻辑气隙保管库是作为数据保护策略一部分的辅助保管库。当您希望为备份使用符合以下条件的保管库时，此保管库可以帮助增强组织的保留和恢复能力

- 在合规模式下使用保管库锁定功能自动设置
- 包含可以与创建备份的账户不同的账户共享和还原的备份
- 使用自有密钥加密 AWS

逻辑气隙保管库中支持的资源包括

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

此逻辑受物理隔离的保管库预览版仅在美国东部（弗吉尼亚州北部）地区提供。由于此功能目前仅在一个地区提供，因此在此预览期内不支持跨区域复制。

与标准备份保管库进行比较和对比

备份存储库是中使用的主要和标准类型的存储库 AWS Backup。创建备份时，每个备份都存储在备份保管库中。您可以分配基于资源的策略来管理存储在保管库中的备份，例如存储在保管库中的备份的生命周期。

逻辑气隙保管库是一种专门的保管库，具有更高的安全性和灵活共享功能，可缩短恢复时间 (RTO)。此保管库存储最初创建并存储在标准备份保管库中的备份副本。

备份保管库可以使用密钥进行加密，这是一种限制目标用户访问权限的安全机制。这些密钥可以由客户管理或 AWS 管理。此外，借助保管库锁定功能，可以更安全地保护备份保管库；逻辑气隙保管库配备了合规模式下的保管库锁定功能。

如果在 AWS KMS 创建初始资源时未手动更改密钥或将其设置为客户托管密钥 (CMK)，则无法将备份复制到逻辑上存在气隙的保管库中。

功能	备份保管库	逻辑气隙保管库（预览版）
备份创建	创建备份时，会将其存储为恢复点	备份在创建时不会存储在此保管库中
备份存储	可以存储资源的初始备份和备份副本	可以存储来自其他保管库的备份副本
安全性	可以选择使用密钥进行加密（客户 AWS 管理或托管） 可以选择使用保管库锁定功能进行锁定	使用 AWS 自有密钥加密 在合规模式下始终使用保管库锁定功能进行锁定
可共享性	可以通过策略和 AWS Organizations 管理访问权限 不兼容 AWS Resource Access Manager	可以选择使用 AWS RAM 跨账户共享
还原	备份可以由拥有保管库的同一个账户进行还原	如果保管库与拥有备份的账户共享，则备份可以由不同的账户还原

功能	备份保管库	逻辑气隙保管库（预览版）
区域性	在所有 AWS Backup 运营地区均可用	预览期间在美国东部（弗吉尼亚州北部）区域可用
资源	可以存储包含所有 AWS Backup 支持资源的备份	可以存储包含 Amazon EC2、Amazon EBS、Amazon EFS、Amazon S3 或 Amazon RDS 数据的备份

从控制台创建逻辑气隙保管库

> **Important**
>
> 一旦创建了保管库，就无法更改保管库名称、保管库类型以及最小和最大保留期；此外，保管库锁定也无法删除。
> 当该服务变为正式可用时，预览期间提供的数据和配置将不再可用。 AWS 建议在预览中使用测试数据而不是生产数据。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择保管库。
3. 将显示两种类型的保管库。选择创建新保管库。
4. 输入备份保管库的名称。您对保管库的命名可以体现出将要存储在其中的内容，或者便于搜索您所需的备份。例如，您可以将其命名为 `FinancialBackups`。
5. 选择逻辑气隙保管库所对应的单选按钮。
6. 设置最短保留期。

   此值（以天、月或年为单位）是可以在此保管库中保留备份的最短时间。无法将保留期短于此值的备份复制到此保管库。
7. 设置最长保留期。

   此值（以天、月或年为单位）是可以在此保管库中保留备份的最长时间。无法将保留期大于此值的备份复制到此保管库。
8. （可选）添加标签，以帮助您搜索和识别逻辑气隙保管库。例如，您可以添加 `BackupType:Financial` 标签。

9. 选择创建保管库。
10. 检查设置。如果所有设置都按预期显示，请选择创建逻辑气隙保管库。
11. 控制台将带您进入新保管库的详细信息页面。验证保管库详细信息是否符合预期。

在控制台中，查看逻辑气隙保管库的详细信息

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 从左侧导航窗格中，选择保管库。
3. 保管库描述下方将显示两个列表，即该账户拥有的保管库和与该账户共享的保管库。选择所需的选项卡以查看保管库。
4. 在保管库名称下，单击保管库名称以打开详细信息页面。您可以查看摘要、恢复点、受保护的资源、账户共享、访问策略和标签详细信息。

在控制台中从标准备份保管库复制到逻辑气隙保管库

逻辑气隙保管库只能是备份计划中的复印作业目的地目标或按需复印作业的目标。

要启动复印作业，您必须

- 具有备份保管库
- 具有逻辑气隙保管库
- 拥有包含 Amazon EC2、Amazon EBS、Amazon RDS、Amazon S3 或 Amazon EFS 数据的备份
- 拥有用于创建副本的角色的权限 `kms:CreateGrant`。
- 没有使用 AWS 托管密钥加密备份到逻辑上空隙的保管库

确认上述内容后，

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 从左侧导航窗格中，选择保管库。
3. 在保管库详细信息页面中，将显示该保管库中的所有恢复点。在要复制的恢复点旁边打勾标记。
4. 选择操作，然后选择下拉菜单中的复制。
5. 在下一个屏幕上，输入目的地详细信息。

    a. 区域必须设置为美国东部（弗吉尼亚州北部）

b. 目的地备份保管库下拉菜单显示符合条件的目的地保管库。按类型 `logically air-gapped vault` 选择一个

6. 将所有详细信息设置为首选项后，选择复制。

在控制台的作业页面上，您可以选择复制作业以查看当前的复制作业。

有关更多信息，请参阅复制备份、跨区域备份和跨账户备份。

从控制台共享逻辑气隙保管库

> **Note**
>
> 只有具有某些 IAM 权限的账户才能共享和管理账户共享。

您可以使用与您 AWS RAM 指定的其他账户共享逻辑上隔绝的保管库。要使用共享 AWS RAM，请确保您具备以下条件：

- 两个或更多可以访问的账户 AWS Backup
- 打算共享的账户拥有必要的 RAM 权限。此过程需要权限 `ram:CreateResourceShare`。策略 `AWSResourceAccessManagerFullAccess` 包含所有必需的 RAM 相关权限。
- 至少一个逻辑气隙保管库

要共享逻辑气隙保管库，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 从左侧导航窗格中，选择保管库。
3. 保管库描述下方将显示两个列表，即该账户拥有的保管库和与该账户共享的保管库。选择所需的列表以查看保管库。
4. 在保管库名称下，选择逻辑气隙保管库的名称以打开详细信息页面。
5. 账户共享窗格显示正在与哪些账户共享保管库。
6. 要开始与其他账户共享或编辑已共享的账户，请选择管理共享。

AWS RAM 选择 “管理共享” 后，控制台将打开。有关使用 AWS RAM 共享资源的步骤，请参阅在 RAM 中 AWS 创建资源共享。

确保您具有适当的权限。Backup Administrator IAM 策略 [AWSBackupFullAccessAWSBackupOperatorAccess] 和 Backup Operator IAM 策略 [] 包含查看共享账户所需的权限；但是，用于共享的角色需要资源访问管理器的写入权限才能从 RAM 共享账户，例如`ram:CreateResourceShare`。

受邀接受共享邀请的账户有 12 小时的时间接受邀请。请参阅《AWS RAM 用户指南》中的接受和拒绝资源共享邀请。

如果共享步骤已完成并被接受，则保管库摘要页面将显示在账户共享 =“已共享 - 参见下面的账户共享表”下方。

使用控制台从逻辑气隙保管库中还原备份

您可以从拥有该保管库的账户或与之共享保管库的任何账户，还原存储在逻辑气隙保管库中的备份。

有关如何还原恢复点的信息，请参阅还原备份。

使用控制台删除逻辑气隙保管库

> **Important**
>
> 当该服务变为正式可用时，预览期间提供的数据和配置将不再可用。 AWS 建议在预览中使用测试数据而不是生产数据。

要删除保管库，请参阅删除备份保管库。如果保管库仍包含备份（恢复点），则无法将其删除。在启动删除操作之前，请确保保管库中没有备份。

通过 CLI/API 对逻辑气隙保管库执行操作

您可以使用以编程方式 AWS CLI 对逻辑上存在气隙的保管库执行操作。每个 CLI 都特定于其来源的 AWS 服务。与共享相关的命令在前面加上 `aws ram`；所有其他命令都应在前面加上 `aws backup`。

创建

可以修改以下示例 CLI 命令 `CreateLogicallyAirGappedBackupVault` 以创建逻辑气隙备份保管库：

```
aws backup create-logically-air-gapped-backup-vault \
--region us-east-1 \
```

```
--backup-vault-name sampleName \
--min-retention-days 7 \
--max-retention-days 35 \
--creator-request-id 123456789012-34567-8901 // optional
```

查看详细信息

可以修改以下示例 CLI 命令 DescribeBackupVault，以获取有关保管库的详细信息：

```
aws backup describe-backup-vault \
--region us-east-1  \
--backup-vault-name testvaultname
```

共享

> **Note**
>
> 只有拥有充足 IAM 权限的账户才能共享和管理账户共享。

您可以通过 AWS Resource Access Manager (RAM) 共享逻辑气隙保管库，RAM 这项服务可帮助用户共享资源。

AWS RAM 使用 CLI 命令create-resource-share。只有拥有足够权限的管理员账户才能访问此命令。有关 CLI 步骤，请参阅在 AWS RAM中创建资源共享。

第 1 步到第 4 步是使用拥有逻辑气隙保管库的账户执行的。第 5 步到第 8 步是使用将与之共享逻辑气隙保管库的账户执行的。

1. 登录所属账户，或者请求您组织中具有足够凭证的用户访问源账户，完成这些步骤。
   - 如果之前创建了资源共享，且您希望向其添加其他资源，请使用 CLI associate-resource-share，而不是新保管库的 ARN。
2. 获取具有足够权限的角色的凭证，以便通过 RAM 进行共享。将这些输入到 CLI 中。
   - 此过程需要权限 ram:CreateResourceShare。该策略AWSResourceAccessManagerFullAccess包含所有与 RAM 相关的权限。
3. 使用create-resource-share。
   a. 包括逻辑气隙保管库的 ARN。

b. 输入示例：

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

示例输出：

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. 在输出中复制资源共享 ARN（后续步骤需要这样做）。将 ARN 交给您邀请接收共享的账户操作员。
5. 获取资源共享 ARN

   a. 如果您没有执行第 1 步 resourceShareArn 到第 4 步，请向执行者索取。

   b. 例如：arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543
6. 在 CLI 中，假设接收账户的凭证。
7. 通过 get-resource-share-invitations 获取资源共享邀请。有关更多信息，请参阅《AWS RAM 用户指南》中的接受和拒绝邀请。
8. 在目的地（恢复）账户中接受邀请。

   - 使用 accept-resource-share-invitation（也可使用 reject-resource-share-invitation）。

列出

可以修改 CLI 命令 ListBackupVaults，以列出该账户拥有和存在的所有保管库：

```
aws backup list-backup-vaults \
--region us-east-1
```

要仅列出逻辑气隙保管库，请添加参数

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

要列出与该账户共享的保管库，请使用

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

Copy（复制）

逻辑气隙保管库只能成为备份复制作业的目标，而不能成为初始备份作业的目标。使用 StartCopyJob 将备份保管库中的现有备份复制到逻辑气隙保管库。

用于向逻辑气隙保管库创建复制作业的角色必须包含权限 kms:CreateGrant。

CLI 输入示例：

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

还原

将备份从逻辑气隙保管库共享到您的账户后，您可以使用 StartRestoreJob 来还原备份。CLI 输入示例：

```
aws backup start-restore-job \
```

```
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

删除

以下示例 CLI 命令 DeleteBackupVault 可用于删除保管库。只有在保管库内没有备份（恢复点）时，才能删除保管库。

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

其他可用的编程选项包括：

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

创建备份保管库

在创建备份计划或开始备份作业之前，您必须至少创建一个保管库。

首次在中使用 AWS Backup 控制台时 AWS 区域，控制台会自动创建默认保管库。

但是，如果您 AWS Backup 通过 AWS CLI、 AWS SDK 或使用 AWS CloudFormation，则不会创建默认保管库。您必须创建自己的保管库。

所需的权限

您必须具有以下权限才能使用创建备份保管库 AWS Backup。

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource":
 "arn:aws:kms:region:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:region:444455556666:backup-vault:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

创建备份保管库（控制台）

有关使用 AWS Backup 控制台创建备份存储库的 step-by-step 说明，请参阅入门指南步骤 3：创建备份保管库中的。

创建备份保管库（以编程方式）

以下 AWS Command Line Interface 命令创建备份保管库：

```
aws backup create-backup-vault --backup-vault-name test-vault
```

您还可以为备份保管库指定以下配置。

备份保管库名称

备份保管库名称区分大小写。名称必须包含 2 到 50 个字母数字字符、连字符或下划线。

AWS KMS 加密密钥

AWS KMS 加密密钥可保护您在此备份保管库中的备份。默认情况下， AWS Backup 使用别名 `aws/backup` 为您创建 KMS 密钥。您可以选择该密钥或选择账户中的任何其他密钥（跨账户 KMS 密钥可通过 CLI 使用）。

您可以按照《AWS Key Management Service 开发人员指南》中的创建密钥过程，创建新的加密密钥。

创建备份保管库并设置 AWS KMS 加密密钥后，您将无法再编辑该备份保管库的密钥。

在 AWS Backup 文件库中指定的加密密钥适用于某些资源类型的备份。有关备份加密的更多信息，请参阅“安全”部分中的对中的备份进行加密 AWS Backup。所有其他资源类型的备份通过用于加密源资源的密钥进行备份。

备份保管库标签

这些标签与备份保管库关联，帮助您组织和跟踪备份保管库。

对备份保管库设置访问策略

使用 AWS Backup，您可以为备份存储库及其包含的资源分配策略。通过分配策略，您可以执行诸多操作，例如，授予用户创建备份计划和按需备份的访问权限，但限制用户在创建恢复点后删除这些恢复点的能力。

有关使用策略授予或限制资源访问权限的信息，请参阅《IAM 用户指南》中的基于身份的策略和基于资源的策略。您还可以使用标签来控制访问。

在使用 AWS Backup 文件库时，您可以使用以下示例策略来限制对资源的访问权限。与其他基于 IAM 的策略不同， AWS Backup 访问策略不支持密钥中的通配符。`Action`

有关可用于标识不同资源类型的恢复点的 Amazon 资源名称 (ARN) 列表，请参阅 AWS Backup 资源 ARN 以获限特定于资源的恢复点 ARN。

文件库访问策略仅控制用户对 AWS Backup API 的访问权限。某些备份类型（例如 Amazon Elastic Block Store (Amazon EBS) 和 Amazon Relational Database Service (Amazon RDS) 快照）也可使用

这些服务的 API 进行访问。您可以在 IAM 中创建单独的访问策略控制对这些 API 的访问，从而完全控制对这些类型备份的访问。

无论 AWS Backup 文件库的访问策略如何，除此之外的任何操作的跨账户访问都`backup:CopyIntoBackupVault`将被拒绝；也就是说， AWS Backup 将拒绝来自与所引用资源账户不同的账户的任何其他请求。

主题

拒绝对备份保管库中资源类型的访问

此策略拒绝针对备份保管库中的所有 Amazon EBS 快照访问指定的 API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
                "backup:StartRestoreJob"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

拒绝对备份保管库的访问

此策略拒绝访问针对备份保管库的指定 API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

拒绝删除备份保管库中的恢复点

根据您授予用户的访问权限来确定这些用户是否可以访问保管库以及是否能够删除存储在其中的恢复点。

请按照以下步骤在备份保管库上创建基于资源的访问策略，阻止删除备份保管库中的任意备份。

在备份保管库上创建基于资源的访问策略

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在左侧的导航窗格中，选择 Backup vaults (备份保管库)。
3. 在列表中选择备份保管库。
4. 在 Access policy (访问策略) 部分中，粘贴以下 JSON 示例。此策略可防止不是委托人的任何用户删除目标备份保管库中的恢复点。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:userId": [
                       "AAAAAAAAAAAAAAAAAAAAA:",
                       "BBBBBBBBBBBBBBBBBBBBB",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

要允许使用其 ARN 列出 IAM 身份，请在以下示例中使用 aws:PrincipalArn 全局条件密钥。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                       "arn:aws:iam::112233445566:role/mys3role",
                       "arn:aws:iam::112233445566:user/shaheer",
                       "112233445566"
                    ]
                }
            }
        }
    ]
```

```
}
```

有关获取 IAM 实体唯一 ID 的信息，请参阅《IAM 用户指南》中的获取唯一标识符。

如果要将此限制为特定资源类型，而不是 `"Resource": "*"`，您可以明确包含要拒绝的恢复点类型。例如，对于 Amazon EBS 快照，请将资源类型更改为以下内容。

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. 选择附加策略。

AWS Backup 文件库锁

> **Note**
>
> AWS Backup Cohasset Associates已对Vault Lock进行了评估，适用于受美国证券交易委员会17a-4、美国商品期货交易委员会和美国金融监管局法规约束的环境。有关 AWS Backup Vault Lock 与这些法规的关系的更多信息，请参阅 Cohasset Associates 合规性评估。

AWS Backup Vault Lock 是备份保管库的一项可选功能，它有助于增强对备份库的安全性和控制力。当锁在合规模式下处于活动状态并且宽限期结束时，客户、账户/数据所有者或 AWS无法更改或删除保管库配置。每个保管库可以有一个保管库锁。

AWS Backup 确保您的备份在保留期到期之前一直可供您使用。如果任何用户（包括 root 用户）尝试删除已锁定文件库中的备份或更改其生命周期属性， AWS Backup 则会拒绝该操作。

- 拥有充足 IAM 权限的用户可以解除锁定在治理模式下的保管库。
- 冷静期（“宽限期”）到期后，无法删除在合规模式下锁定的保管库。在宽限期内，您仍可以移除保管库锁定并更改锁定配置。

保管库锁定模式

创建保管库锁定时，您可以选择两种模式：治理模式或合规模式。治理模式旨在允许只有拥有充足 IAM 权限的用户才能管理保管库。治理模式可帮助组织满足治理要求，确保只有指定的人员才能对备份保管库进行更改。合规模式适用于在数据保留期结束之前永远不会删除或更改保管库（以及其内容）的备份保管库。合规模式下的保管库一旦被锁定，它就不可变，这意味着无法移除锁定。

拥有相应 IAM 权限的用户可以管理或删除在治理模式下锁定的保管库。

任何用户或 AWS都无法更改或删除处于合规模式下的保管库锁定。合规模式下的保管库锁定在锁定并变为不可变之前具有您设置的宽限期。

保管库锁定的好处

AWS Backup 文件库锁有多项好处，包括：

- 针对您在备份保管库中存储和创建的所有备份进行 WORM（一次写入、多次读取）配置。
- 额外防御层，可保护备份保管库中的备份（恢复点）免遭意外或恶意删除。
- 强制执行保留期，防止特权用户（包括 AWS 账户 root 用户）提前删除，并符合贵组织的数据保护策略和程序。

使用控制台锁定备份保管库

您可以使用 Backup 控制台向 AWS Backup 保管库添加文件库锁。

要向备份保管库添加保管库锁定，请执行以下操作：

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，找到备份保管库。单击 Backup 保管库下嵌套的名为保管库锁定的链接。
3. 在保管库锁定的工作原理或保管库锁定下，单击 + 创建保管库锁定。
4. 在保管库锁定详细信息窗格中，选择要应用锁定的保管库。
5. 在保管库锁定模式下，选择要锁定保管库的模式。有关选择模式的更多信息，请参阅本页前面的保管库锁定模式。
6. 对于保留期，选择最小和最大保留期（保留期是可选项）。如果保管库中创建的新备份和复制作业不符合您设置的保留期，则这些作业将失败；这些期限不适用于保管库中已有的恢复点。
7. 如果您选择合规模式，则会显示一个名为保管库锁定开始日期的部分。如果您选择治理模式，则不会显示该部分，并且可以跳过此步骤。

   在合规模式下，保管库锁定的冷静期从创建保管库锁定开始，直到保管库及其锁变为不可变且不可更改。您可以选择此期限的持续时间（称为宽限期），但必须至少为 3 天（72 小时）。

> **Important**
>
> 宽限期到期后，保管库及其锁定将不可变。任何用户或 AWS都不能对其进行更改或删除。

8. 如果您对配置选项感到满意，请单击创建保管库锁定。
9. 要确认您希望在所选模式下创建此锁定，请在文本框中键入 `confirm`，然后选中确认配置符合预期的复选框。

如果步骤已成功完成，则控制台顶部将显示“成功”横幅。

以编程方式锁定备份保管库

要配置 AWS Backup 文件库锁定，请使用 API PutBackupVaultLockConfiguration。要包含的参数将取决于您打算采用哪种保管库锁定模式。如果您想在治理模式下创建保管库锁定，请不要包含 `ChangeableForDays`。如果包含此参数，则将在合规模式下创建保管库锁定。

以下是创建合规模式保管库锁定的 CLI 示例：

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

以下是创建治理模式保管库锁定的 CLI 示例：

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

您可以配置四个选项。

1. **`BackupVaultName`**

   要锁定的保管库的名称。

2. **`ChangeableForDays`**（仅适用于合规模式）

此参数指示 AWS Backup 在合规模式下创建文件库锁。如果您打算在治理模式下创建锁定，请省略此参数。

该值以天数表示。它必须是一个不小于 3 且不大于 36,500 的数字；否则，将返回错误。

从创建此保管库锁定到指定日期到期，可以使用 DeleteBackupVaultLockConfiguration 将保管库锁定从保管库中删除。或者，在此期间，您可以使用 PutBackupVaultLockConfiguration 更改配置。

在此参数确定的指定日期及之后，备份保管库将不可变且无法更改或删除。

3. **MaxRetentionDays**（可选）

   这是一个以天为单位的数值。这是保管库保留其恢复点的最长保留期。

   您选择的最大保留时间范围应与您组织的数据保留政策保持一致。如果您的组织要求将数据保留一段时间，则可以将此值设置为该期限（以天为单位）。例如，可能需要将财务或银行数据保存 7 年（大约 2,557 天，视闰年而定）。

   如果未指定， AWS Backup 文件库锁定将不会强制规定最长保留期。如果指定此参数，则生命周期保留期长于最大保留期的备份和复制到此保管库的作业将失败。保管库锁定创建之前已保存在保管库中的恢复点不受影响。您可以指定的最长保留期为 36500 天（大约 100 年）。

4. **MinRetentionDays**（可选；必填项 CloudFormation）

   这是一个以天为单位的数值。这是保管库保留其恢复点的最短保留期。此设置应设置为您的组织维护数据所需的 时间。例如，如果法规或法律要求将数据保留至少七年，则以天为单位的值约为 2,557，视闰年而定。

   如果未指定， AWS Backup 文件库锁定将不会强制规定最短保留期。如果指定此参数，则生命周期保留期短于最小保留期的备份和复制到此保管库的作业将失败。在保管库锁定之前已保存在 AWS Backup 保管库中的恢复点不受影响。您可以指定的最短保留期为 1 天。

查看备份保管库的保 AWS Backup 管库锁定配置

您可以通过调用DescribeBackupVault或 ListBackupVaults API 随时查看 AWS Backup 文件库的保管库锁定详细信息。

要确定您是否对备份保管库应用了保管库锁定，请调用 DescribeBackupVault 并查看 Locked 属性。如果"Locked": true像以下示例一样，您已将 AWS Backup 文件库锁定应用于备份保管库。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

上述输出确认了以下选项：

1. Locked是一个布尔值，表示您是否已将 AWS Backup 文件库锁定应用于此备份存储库。 True意味着 AWS Backup 文件库锁定会导致对存储在保管库中的恢复点的删除或更新操作失败（无论您是否仍处于冷静期宽限期）。
2. LockDate 是您的冷静宽限期结束时的 UTC 日期和时间。在此时间之后，您将无法删除或更改对此保管库的锁定。使用任何公开可用的时间转换器将此字符串转换为您的本地时间。

如果 "Locked":false 像以下示例一样，说明您尚未应用保管库锁定（或之前的保管库锁定已被删除）。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

在宽限期内移除保管库锁定（合规模式）

要在宽限期（锁定保管库之后但在锁定保管库之前的时间LockDate）使用 AWS Backup 控制台删除文件库锁定，

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在我的账户下的左侧导航栏中，单击“备份保管库”，然后单击“备份保管库锁定”。
3. 单击您要移除的保管库锁定，然后单击管理保管库锁定。
4. 单击删除保管库锁定。
5. 此时，将显示一个警告框，要求您确认删除保管库锁定的意图。在文本框中键入 confirm，然后单击确认。

成功完成所有步骤后，控制台屏幕顶部将显示“成功”横幅。

要在宽限期内使用 CLI 命令删除保管库锁定，请使用 DeleteBackupVaultLockConfiguration，如这个 CLI 示例所示：

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

AWS 账户 用上锁的金库关闭

当您关闭 AWS 账户 包含备份保管库的， AWS 并在备份完好无损的情况下 AWS Backup 暂停您的帐户 90 天。如果您在这 90 天内没有重新打开账户，即使保管库锁定已到位，也会 AWS 删除备份 AWS Backup 保管库中的内容。

其它安全注意事项

AWS Backup Vault Lock 为您的数据保护防御深度增加了一层额外的安全保护。保管库锁定可以与其他安全功能结合使用：

- 针对您的恢复点的加密
- AWS Backup 文件库和恢复点访问策略，允许您在文件库级别授予或拒绝权限，
- AWS Backup 安全最佳实践，包括其客户托管策略库，这些策略允许您通过 AWS 支持的服务授予或拒绝备份和恢复权限，以及
- AWS Backup Audit Manager，它允许您根据自己定义的控制列表自动检查备份的合规性。

您可以遍历使用 AWS Backup API 创建框架以使用 AWS Backup Audit Manager 实施控制备份受 AWS Backup 文件库锁保护，从而帮助确保利用保管库锁的保护您的预期资源。

- 使资源处于非活动状态的机制可能会影响恢复资源的能力。虽然它们仍然无法在锁定的保管库中删除，但它们可能处于非活动状态。例如，允许您禁用 AMI 的 Amazon 弹性计算云设置可以暂时阻止恢复 EC2 实例的备份。这会影响所有 EC2 恢复点，甚至是受文件库锁定或合法保留影响的备份。

  如果禁用 EC2 备份，则可以重新启用已禁用的 AMI。重新启用后，便有资格恢复。要阻止 AMI 禁用功能，您可以使用 IAM 策略来禁用`ec2:DisableImage`。

> **Note**
>
> AWS Backup 文件库锁与 Amazon S3 Glacier 文件库锁的功能不同，后者仅与 S3 Glacier 兼容。

删除备份保管库

为防止意外或恶意大规模删除，只有在删除备份保管库中的所有恢复点（或备份计划生命周期）之后，才能删除 AWS Backup 中的备份保管库。要手动删除恢复点，请参阅清理资源。

删除备份保管库时，请更新您的备份计划以指向新的备份保管库。指向已删除备份保管库的备份计划将导致备份创建失败。

> **Note**
>
> 您无法删除两个备份存储库： AWS Backup 默认备份存储库和 Amazon EFS 自动备份存储库。

使用 AWS Backup 控制台删除备份保管库

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 选择备份库的名称以打开其详细信息页面。
4. 选择并删除与备份保管库关联的任何备份。

5. 选择 “删除保管库”。当系统提示您确认时，输入保管库名称，然后选择 Delete Backup 保管库。

使用备份

备份，也称为恢复点，表示在指定时间的资源内容，例如 Amazon Elastic Block Store (Amazon EBS) 卷或 Amazon DynamoDB 表。恢复点这个术语通常指 AWS 服务中的不同备份，例如 Amazon EBS 快照和 DynamoDB 备份。术语恢复点和备份可以互换使用。

AWS Backup 将恢复点保存在备份存储库中，您可以根据业务需求对其进行整理。例如，您可以保存一组包含 2020 财年财务信息的资源。当您需要恢复资源时，可以使用 AWS Backup 控制台或 AWS Command Line Interface (AWS CLI) 来查找和恢复所需的资源。

每个恢复点都有唯一的 ID。唯一的 ID 位于恢复点的 Amazon 资源名称 (ARN) 末尾。有关恢复点 ARN 和唯一 ID 的示例，请参阅资源和操作中的表。

> **Important**
>
> 为避免额外收费，请为保留策略配置至少一周的温存储持续时间。有关更多信息，请参阅 计量、成本和计费。

以下各节概述了 AWS Backup中的基本备份管理任务。

主题

创建备份

使用 AWS Backup，您可以使用备份计划自动创建备份，也可以通过启动按需备份来手动创建备份。

创建自动备份

当备份计划自动创建备份时，使用在备份计划中定义的生命周期设置来配置备份。它们在备份计划中指定的备份保管库中进行组织。也将为它们分配备份计划中列出的标签。有关备份计划的更多信息，请参阅使用备份计划管理备份。

创建按需备份

创建按需备份时，您可以为所创建的备份配置这些设置。不论是通过自动还是手动创建备份，都将启动备份作业。要了解如何创建按需备份，请参阅使用创建按需备份 AWS Backup。

注意：按需备份会创建备份作业；备份作业将在一小时内（或指定时）转换到 Running 状态。如果您希望在备份计划中定义的计划时间以外的时间创建备份，则可以选择按需备份。例如，可以随时使用按需备份来测试备份和功能。

按需备份不能与 point-in-time 恢复 (PITR) 一起使用，因为按需备份会将资源保留在备份时所处的状态，而 PITR 使用连续备份来记录一段时间内的变化。

备份作业状态

每个备份作业都有唯一的 ID。例如，D48D8717-0C9D-72DF-1F56-14E703BF2345。

您可在 AWS Backup 控制台的作业页面查看备份作业的状态。Backup 任务状态包括CREATEDPENDING、RUNNING、ABORTING、ABORTED、COMPLETED、FAILED、EXPIRED、和。PARTIAL

增量备份的工作方式

许多资源都支持使用进行增量备份 AWS Backup。按资源划分的功能可用性表的增量备份部分提供了完整列表。

尽管第一次备份之后的每个备份都是增量备份（这意味着它仅捕获与上一次备份相比的更改），但使用此备份进行的所有备份都将 AWS Backup 保留必要的参考数据，以便进行完全恢复。即使原始（完整）备份已达到其生命周期的终点并已被删除，也是如此。

例如，如果您的第一天（完整）备份由于 3 天的生命周期策略而被删除，那么您仍然可以使用第 2 天和第 3 天的备份执行完整还原。 AWS Backup 从第一天便维护执行此操作所必要的参考数据。

访问源资源

AWS Backup 需要访问您的源资源才能对其进行备份。例如：

- 要备份 Amazon EC2 实例，该实例可以处于 `running` 或 `stopped` 状态，但不得处于 `terminated` 状态。这是因为`running`或`stopped`实例可以与通信 AWS Backup，但`terminated`实例不能。
- 要备份虚拟机，其管理程序的 Backup Gateway 的状态必须为 `ONLINE`。有关更多信息，请参阅[了解管理程序状态]。
- 要备份 Amazon RDS 数据库、Amazon Aurora 或 Amazon DocumentDB 集群，这些资源的状态必须为 `AVAILABLE`。
- 要备份 Amazon Elastic File System (Amazon EFS)，其状态必须为 `AVAILABLE`。
- 要备份 Amazon FSx 文件系统，其状态必须为 `AVAILABLE`。如果状态为 `UPDATING`，则备份请求将排队，直到文件系统变成 `AVAILABLE`。

  FSx for ONTAP 不支持备份某些卷类型，包括 DP（数据保护）卷、LS（负载共享）卷、完整卷或已满文件系统上的卷。有关更多信息，请参阅 FSx for ONTAP Working with backups。

AWS Backup 无论源资源的运行状况如何，都将保留与您的生命周期策略一致的先前创建的备份。

主题

- 使用创建按需备份 AWS Backup
- 连续备份和 point-in-time 恢复 (PITR)
- Amazon S3 备份
- 虚拟机备份
- 高级 DynamoDB 备份
- Amazon Timestream 备份
- Amazon EC2 实例上的 SAP HANA 数据库备份
- Amazon Redshift 备份
- 亚马逊 Relation Database Service 备份
- AWS CloudFormation 堆栈备份
- 创建 Windows VSS 备份
- 亚马逊 EBS 和 AWS Backup
- 将标签复制到备份
- 停止备份作业

使用创建按需备份 AWS Backup

在 AWS Backup 控制台上，受保护的资源页面列出了 AWS Backup 至少备份过一次的资源。如果您是首次使用 AWS Backup ，则此页面上没有列出任何资源（例如 Amazon EBS 卷或 Amazon RDS 数据库）。即使已将资源分配给备份计划，但是该备份计划未运行至少一次计划备份作业，也会出现此情况。

注意：按需备份会立即开始备份您的资源。如果您希望在备份计划中定义的计划时间以外的时间创建备份，则可以选择按需备份。例如，可以随时使用按需备份来测试备份和功能。

按需备份不能与 point-in-time 恢复 (PITR) 一起使用，因为按需备份会将资源保留在备份时所处的状态，而 PITR 使用连续备份来记录一段时间内的变化。

注意事项

- 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的角色。
- 当备份过期并作为生命周期策略的一部分标记为删除时， AWS Backup 将在接下来的 8 小时内随机选择的时间点删除备份。此时段有助于确保一致的性能。
- 对于 Amazon EC2 资源，除了在此步骤中添加的任何标签外，还 AWS Backup 会自动复制现有的组和单个资源标签。
- AWS Backup 将 “不重启” 作为默认行为的 EC2 备份。 AWS Backup 目前支持在 Amazon EC2 上运行的资源，并且不支持某些实例类型。有关更多信息，请参阅 创建 Windows VSS 备份。

创建按需备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在控制面板中，选择创建按需备份。或者，在导航窗格中，选择受保护的资源，然后选择创建按需备份。
3. 在资源类型页面中，选择要备份的资源类型。例如，为亚马逊 DynamoDB 表选择 DynamoDB。
4. 选择要保护的资源的名称或 ID。例如，为亚马逊 DynamoDB 选择 DynamoDB 表的名称。
5. 确保选中了立即创建备份。
6. 如果资源类型支持过渡到冷存储，则存在冷存储。有关更多信息，请参阅 “按资源划分的功能可用性” 表中的 “冷存储生命周期” 列。

   要指定此备份何时进入冷存储，请选择 “将备份从温存储移至冷存储”，然后指定在温存储中的时间。
7. 在 “总保留期” 中，指定天数。如果您指定了冷存储时间，则保留期将分为温存储和冷存储。

8. 选择现有的备份保管库或创建新的备份保管库。选择新建备份保管库将打开用于创建保管库的新页面，然后在完成时返回到创建按需备份页面。
9. 对于 IAM 角色，请选择默认角色或您创建的角色。
10. 要为按需备份分配标签，请展开添加到恢复点的标签，选择添加新标签，然后输入标签密钥和标签值。
11. 如果资源类型为 EC2，则存在高级备份设置。要使用 Windows 卷影复制服务 (VSS) 拍摄应用程序一致的快照，请选择 Windows VSS。
12. 选择创建按需备份。这将打开 “作业” 页面，您可以在其中查看作业列表并查看作业状态。

连续备份和 point-in-time 恢复 (PITR)

主题

对于某些资源，除了快照备份外，还 AWS Backup 支持连续备份和 point-in-time 恢复 (PITR)。

使用连续备份，您可以将 AWS Backup支持的资源倒带回您选择的特定时间，精确度在 1 秒钟内（最多可追回 35 天）。连续备份的工作原理是，首先创建资源的完整备份，然后不断备份资源的事务日志。PITR 恢复的工作原理是访问您的完整备份，然后将事务日志重放到您要求恢复的时间。 AWS Backup

或者，可以每小时进行一次快照备份。快照备份最多可存储 100 年。可以复制快照进行完整备份或增量备份。

由于连续备份和快照备份具有不同的优势，因此建议您同时使用连续备份和快照备份规则来保护您的资源。

注意：按需备份会立即开始备份您的资源。如果您希望在备份计划中定义的计划时间以外的时间创建备份，则可以选择按需备份。例如，可以随时使用按需备份来测试备份和功能。

按需备份不能与 point-in-time 恢复 (PITR) 一起使用，因为按需备份会将资源保留在备份时所处的状态，而 PITR 使用连续备份来记录一段时间内的变化。

在 AWS Backup 使用 AWS Backup 控制台或 API 创建备份计划时，您可以选择对支持的资源进行持续备份。

使用控制台启用连续备份

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划，然后选择创建备份计划。
3. 在备份计划下，选择添加备份计划。
4. 在备份规则配置部分，选择为支持的资源启用连续备份。

支持的连续备份/时间点恢复 (PITR) 服务

AWS Backup 支持以下服务和应用程序的连续备份和 point-in-time 恢复：

Amazon S3

要为 S3 备份启用 PITR，需要将连续备份设置为备份计划的一部分。

虽然源存储桶的原始备份可能已激活 PITR，但跨区域或跨账户目的地副本不具有 PITR，因此从这些副本还原将还原到它们的创建时间（这些副本将是快照副本），而不是还原到指定的时间点。

RDS

备份计划：当 AWS Backup 计划同时创建 Amazon RDS 快照和连续备份时， AWS Backup 将智能地安排您的备份窗口，使其与 Amazon RDS 维护窗口协调以防止冲突。为了进一步防止冲突，无法手动配置 Amazon RDS 自动备份窗口。无论备份计划的快照备份频率是否为每天一次，RDS 都会每天拍摄一次快照。

设置：将 AWS Backup 持续备份规则应用于 Amazon RDS 实例后，您无法在 Amazon RDS 中创建或修改该实例的连续备份设置；修改必须通过 AWS Backup 控制台或 AWS Backup CLI 完成。

将 Amazon RDS 实例的持续备份控制权移回亚马逊 RDS：

Console

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划。
3. 删除所有包含保护该资源的连续备份的 Amazon RDS 备份计划。
4. 选择备份保管库。从备份保管库中删除连续备份恢复点。或者，等待其保留期过去， AWS Backup 从而自动删除恢复点。

完成这些步骤后， AWS Backup 会将资源的持续备份控制权移回 Amazon RDS。

AWS CLI

调用 `DisassociateRecoveryPoint` API 操作 。

要了解更多信息，请参阅DisassociateRecoveryPoint。

Amazon RDS 连续备份所需的 IAM 权限

- AWS Backup 要使用为您的 Amazon RDS 数据库配置连续备份，请验证 API 权限是否`rds:ModifyDBInstance`存在于您的备份计划配置所定义的 IAM 角色中。要还原 Amazon RDS 连续备份，您必须向为还原任务提交的 IAM 角色添加权限 `rds:RestoreDBInstanceToPointInTime`。您可以使用 `AWS Backup default service role` 执行备份和还原。
- 要描述可用于 point-in-time 恢复的时间范围， AWS Backup 请致电`rds:DescribeDBInstanceAutomatedBackupsAPI`。在 AWS Backup 控制台中，您必须拥有 AWS Identity and Access Management (IAM) 托管策略中的 `rds:DescribeDBInstanceAutomatedBackups` API 权限。您可以使用 `AWSBackupFullAccess` 或 `AWSBackupOperatorAccess` 托管策略。这两个策略都具有所有必需的权限。有关更多信息，请参阅托管策略。

保留期：当您更改 PITR 保留期时，会立即 AWS Backup 致电`ModifyDBInstance`并应用该更改。如果您还有其他配置更新等待下一个维护时段，则更改 PITR 保留期还会立即应用这些配置更新。有关数更多信息，请参阅 Amazon Relational Database Service API 参考中的 `ModifyDBInstance`。

Amazon RDS 连续备份的副本：

- 增量快照复制作业的处理速度比完整快照复制作业的处理速度更快。在新复制作业完成之前保留以前的快照副本可能会缩短复制作业的持续时间。如果您选择从 RDS 数据库实例复制快照，请务必注

意，先删除以前的副本将导致创建完整快照副本（而不是增量副本）。有关优化复制的更多信息，请参阅《Amazon RDS 用户指南》中的增量快照复制

- 创建 Amazon RDS 连续备份的副本 — 您无法创建 Amazon RDS 连续备份的副本，因为 AWS Backup 对于 Amazon RDS，不允许复制事务日志。而是 AWS Backup 创建快照并按照备份计划中指定的频率进行复制。

恢复：您可以使用 Amazon RDS AWS Backup 或 Amazon RDS 执行 point-in-time 恢复。有关 AWS Backup 控制台的说明，请参阅恢复 Amazon RDS 数据库。有关 Amazon RDS 说明，请参阅《Amazon RDS 用户指南》中的将数据库实例还原到指定时间。

> **Tip**
>
> 设置为的多可用区（可用区）数据库实例`Always On`不应将备份保留设置为零。如果出现错误，请使用 AWS CLI 命令`disassociate-recovery-point`代替`delete-recovery-point`，然后在 Amazon RDS 设置中将保留设置更改为 1。

有关使用 Amazon RDS 的一般信息，请参阅 Amazon RDS 用户指南。

Aurora

要启用对您的 Aurora 资源的连续备份，请参阅本页第一部分中的步骤。

将 Aurora 集群还原到某个时间点的过程是还原 Aurora 集群快照的步骤的变体。

当您进行时间点还原时，控制台会显示还原时间部分。请参阅本页下方使用连续备份中的还原连续备份。

Amazon EC2 实例上的 SAP HANA

您可以进行连续备份，这可以与 point-in-time 恢复 (PITR) 一起使用（请注意，按需备份会将资源保留在拍摄时的状态；而 PITR 使用连续备份来记录一段时间内的变化）。

使用连续备份，可以还原 EC2 实例上的 SAP HANA 数据库，方法是将其倒回您选择的特定时间，精确到 1 秒（最多回溯 35 天）。连续备份的工作原理是，首先创建资源的完整备份，然后不断备份资源的事务日志。PITR 恢复的工作原理是访问您的完整备份，然后将事务日志重放到您要求恢复的时间。
AWS Backup

在 AWS Backup 使用 AWS Backup 控制台或 API 创建备份计划时，您可以选择连续备份。

使用控制台启用连续备份

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划，然后选择创建备份计划。
3. 在备份计划下，选择添加备份计划。
4. 在备份规则配置部分，选择为支持的资源启用连续备份。

禁用 SAP HANA 数据库备份的 PITR（point-in-time恢复）后，日志将继续发送到中， AWS Backup 直到恢复点到期（状态等于EXPIRED）。您可以更改到 SAP HANA 中的替代日志备份位置，以停止向 AWS Backup传输日志。

状态为的连续恢复点STOPPED表示连续恢复点已中断；也就是说，从 SAP HANA 传输到 AWS Backup 的显示数据库增量更改的日志存在间隔。在此时间范围间隙内出现的恢复点状态为 STOPPED.。

有关在连续备份（恢复点）的还原作业期间可能遇到的问题，请参阅本指南的 SAP HANA 还原故障排除部分。

查找连续备份

您可以使用 AWS Backup 控制台查找连续备份。

使用 AWS Backup 控制台查找连续备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库，然后在列表中选择您的备份保管库。
3. 在备份部分的备份类型列中，对连续恢复点进行排序。也可以按恢复点 ID 对前缀连续进行排序。

还原连续备份

使用 AWS Backup 控制台恢复连续备份

- 在 PITR 还原过程中， AWS Backup 控制台会显示 “还原时间” 部分。在此部分，请执行以下操作之一：
  - 选择还原到最新可还原时间。
  - 选择指定日期和时间，输入您自己的保留期内的日期和时间。

使用 AWS Backup API 恢复连续备份

1. 对于 Amazon S3，请参阅使用 AWS Backup API、CLI 或软件开发工具包恢复 S3 恢复点。
2. 对于 Amazon RDS，请参阅使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon RDS 恢复点。

停止或删除连续备份

您可以停止创建连续备份，也可以删除特定的备份（point-in-time-recovery 或 PITR 点）。

如果要停止连续备份，则必须从备份计划中删除连续备份规则。如果您希望停止对一个或多个资源，而不是所有资源的连续备份，请针对那些您仍希望进行连续备份的资源，使用连续备份规则创建新的备份计划。相反，如果仅从备份保管库中删除连续备份恢复点，则您的备份计划仍将继续执行连续备份规则，从而创建一个新的恢复点。

但是，即使您删除了连续备份规则，也会 AWS Backup 记住现已删除的备份规则中的保留期。它将根据您指定的保留期自动从备份保管库中删除连续备份恢复点。

删除 Amazon RDS 恢复点时，请考虑：

- 设置为的多可用区（可用区）数据库实例`Always On`不应将备份保留设置为零。如果出现错误，请使用 AWS CLI 命令`disassociate-recovery-point`代替`delete-recovery-point`，然后在 Amazon RDS 设置中将保留设置更改为 1。
- 删除 Amazon RDS 的 point-in-time 恢复点（通过连续备份创建的备份）时，会触发数据库重启并禁用二进制日志。有关更多详细信息，请参阅《Amazon RDS 用户指南》中的备份保留期。

删除 Aurora 恢复点时，请考虑：

如果为 Amazon Aurora 恢复点选择此选项，则将保留期 AWS Backup 设置为 1 天。在源集群也被删除之前，无法完全删除 Aurora 备份。

复制连续备份

如果连续备份规则还指定跨账户或跨区域复制， AWS Backup 会拍摄连续备份的快照并将该快照复制到目的地保管库。要了解有关跨账户和跨区域复制恢复点的更多信息，请参阅复制备份。

持续备份会根据目标账户和/或地区的备份计划规则中设置的频率创建定期备份。

AWS Backup 不支持连续备份的按需副本。

更改保留期

您可以使用 AWS Backup 来延长或缩短现有连续备份规则的保留期。最短保留期为 1 天。最长保留期为 35 天。

如果延长保留期，将立即生效。如果您缩短了保留期，则 AWS Backup 将等到足够的时间过去后再应用更改以防数据丢失。例如，如果您将保留期从 35 天缩短到 20 天，则 AWS Backup 将继续保留 35 天的连续备份，直到 15 天过去为止。此设计可保护您在进行更改时最近 15 天的备份。

从备份计划中删除唯一的连续备份规则

当您创建包含连续备份规则的备份计划然后删除该规则时， AWS Backup 会记住现已删除的规则中的保留期。保留期过后，它将从您的备份保管库中删除该连续备份。

在同一资源上重叠连续备份

通常，您用来保护每种资源的连续备份规则不应该超过一条。这是因为额外的连续备份实属多余。但是，在扩展备份资产时，单个资源上的多个备份计划、规则和存储库可能会重叠。 AWS Backup 按如下方式处理这些重叠。

如果您在多个具有连续备份规则的备份计划中包含相同的资源，则只 AWS Backup 会为其评估的第一个备份计划创建连续备份。它将为所有其他备份计划创建快照备份。

如果您在单个备份计划中包含多条连续备份规则：

- 如果您的规则指向同一个备份存储库，则 AWS Backup 仅为保留期最长的规则创建连续备份。它将忽略所有其他规则。
- 如果您的规则指向不同的备份存储库，则会以该计划无效为由 AWS Backup 拒绝该计划。

P oint-in-time 恢复注意事项

请注意以下 point-in-time 恢复注意事项：

- 自动回退到快照 - 如果 AWS Backup 无法执行连续备份，则会尝试执行快照备份。
- 不支持按需连续备份 — AWS Backup 不支持按需连续备份，因为按需备份会记录一个时间点，而连续备份的记录会在一段时间内发生变化。
- 不支持转换到冷存储 - 连续备份不支持转换到冷存储，因为转换到冷存储至少需要 90 天的转换期，而连续备份的最大保留期为 35 天。
- 还原近期活动 - Amazon RDS 活动允许还原到最近 5 分钟的活动；Amazon S3 允许还原到最近 15 分钟的活动。

Amazon S3 备份

AWS Backup 支持将数据单独存储在 S3 中或与其他数据库、存储和计算 AWS 服务一起存储数据的应用程序的集中备份和恢复。许多功能可用于进行 S3 备份，包括 Backup Audit Manager。

您可以在中使用单一备份策略 AWS Backup 来集中自动创建应用程序数据的备份。 AWS Backup 自动将不同 AWS 服务和第三方应用程序的备份组织到一个集中的加密位置（称为备份保管库），以便您可以通过集中式体验管理整个应用程序的备份。对于 S3，您可以创建连续备份，还原存储在 S3 中的应用程序数据，只需单击一下 point-in-time 即可将备份还原到。

使用 AWS Backup，您可以为 S3 存储桶创建以下类型的备份，包括对象数据、标签、访问控制列表 (ACL) 和用户定义的元数据：

- 连续备份允许您还原至最近 35 天内的任何时间点。仅应在一个备份计划中配置 S3 存储桶的连续备份。

  有关支持的服务列表以及如何使用 AWS Backup 进行连续备份的说明，请参阅时间点故障恢复。
- 定期备份使用数据快照，允许您在指定的持续时间内保留数据，最长可达 99 年。您可以按照 1 小时、12 小时、1 天、1 周或 1 个月等频率安排定期备份。 AWS Backup 在备份计划中定义的备份时段内进行定期备份。

  要了解如何将备份计划 AWS Backup 应用于您的资源，请参阅创建备份计划。

跨账户和跨区域副本可用于 S3 备份，但连续备份的副本不具有 point-in-time 还原功能。

S3 存储桶的连续和定期备份必须位于同一个备份保管库中。

对于这两种备份类型，第一次备份是完整备份，而后续备份是对象级别的增量备份。

> **Note**
>
> 您必须在 S3 存储桶上启用 S3 版本控制才能用 AWS Backup 于 Amazon S3。我们保留这一先决条件是因为在 AWS 中，我们建议将 S3 版本控制作为数据保护的最佳实践。
> 建议您为 S3 版本设置生命周期过期时段。不设置生命周期过期可能会增加 S3 成本，因为会 AWS Backup 备份和存储所有未过期的 S3 数据。要了解有关设置 S3 生命周期策略的更多信息，请按照本页上的说明进行操作。

比较 S3 备份类型

您的 S3 资源备份策略可以仅包括连续备份，也可以仅包括定期（快照）备份，或者两者兼而有之。以下信息可以帮助您选择最适合贵组织的方法：

仅连续备份：

- 完成现有数据的第一次完整备份后，系统会实时跟踪您的 S3 存储桶数据的更改。
- 跟踪的更改允许您在连续备份的保留期内使用 PITR（point-in-time 恢复）。要执行还原作业，请选择要还原到的时间点。
- 每次连续备份的保留期最长为 35 天。

仅定期（快照）备份（计划备份或按需备份）：

- AWS Backup 扫描整个 S3 存储桶，检索每个对象的 ACL 和标签，然后为之前的快照中但在正在创建的快照中未找到的每个对象发起 Head 请求。
- 备份是一 point-in-time 致的。
- 记录的备份日期和时间是 AWS Backup 完成存储桶遍历的时间，而不是创建备份任务的时间。
- 存储桶的第一次备份是完整备份。后续的每次备份都是增量备份，表示自上次快照以来数据发生的变化。
- 对于定期备份创建的快照，保留期最长可达 99 年。

连续备份与定期/快照备份相结合：

- 完成现有数据（每一个存储桶）的第一次完整备份后，系统会实时跟踪您的存储桶的更改。
- 您可以从连续 point-in-time 恢复点执行恢复。
- 快照是一 point-in-time 致的。
- 快照直接从连续恢复点拍摄，无需重新扫描存储桶，从而加快处理速度。
- 快照和连续恢复点共享数据沿袭；快照和连续恢复点之间的数据存储不会重复。

支持的 S3 存储类

AWS Backup 允许您备份存储在以下 S3 存储类中的 S3 数据：

- S3 标准

- S3 标准版-不频繁访问 (IA)
- S3 单区 - IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

存储类别 S3 智能分层 (INT) 中的对象的备份可以访问这些对象。此访问会触发 S3 智能分层自动将这些对象移至 “频繁访问”。

访问不频繁访问层的备份，包括 S3 标准-不频繁访问 (IA) 和 S3 One Zone-IA 类别，将按频繁访问的 S3 存储费用移动（适用于不频繁访问或存档即时访问层）。

除 Glacier 即时检索外，不支持存档存储类别。

有关 Amazon S3 存储定价的更多信息，请参阅 A mazon S3 定价。

亚马逊 S3 AWS Backup 的注意事项

在备份 S3 资源时，应考虑以下几点：

- 重点对象元数据支持： AWS Backup 支持以下元数据：标签、访问控制列表 (ACL)、用户定义的元数据、原始创建日期和版本 ID。您也可以还原除原始创建日期、版本 ID、存储类和电子标签之外的所有备份数据和元数据。
- S3 对象键名称可以由大多数 UTF-8 可编码字符串组成。允许使用以下 Unicode 字符：`#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF`。

  如果对象键名称包含不在此列表中的字符，可以将其从备份中排除。有关更多信息，请参阅字符的 W3C 规范。
- 冷存储过渡： AWS Backup的生命周期管理策略允许您定义备份到期的时间表，但目前不支持 S3 备份的冷存储过渡。
- 目前不支持对具有同一秒钟创建的同一对象的多个版本的 S3 存储桶进行备份。
- 对于定期备份， AWS Backup 请尽最大努力跟踪对象元数据的所有更改。但是，如果您在 1 分钟内多次更新标签或 ACL， AWS Backup 可能无法捕获所有中间状态。
- AWS Backup 目前不支持 SSE-C 加密对象的备份。 AWS Backup 目前也不支持存储桶配置的备份，包括存储桶策略、设置、名称或访问点。
- AWS Backup 目前不支持在上备份 S3 AWS Outposts。

> **Important**
>
> 在记录数据读取事件的账户中，启用 CloudTrail 日志的 S3 存储桶需要将其访问日志保存到不同的目标存储桶中；如果 CloudTrail 日志保存在它们记录的同一个存储桶中，则会形成无限循环。此循环可能会触发意外和不必要的费用。
> 有关更多信息，请参阅《CloudTrail 用户指南》中的数据事件。

S3 备份完成窗口

下表显示了不同大小的存储桶示例，可帮助您估计 S3 存储桶初始完整备份的完成时间。备份时间将因每个存储桶的大小、内容、配置和设置而异。

存储桶大小	对象数	预计完成初始备份所需的时间
425 GB	1.35 亿	31 小时
800 TB	6.7 亿	38 小时
6 PB	50 亿	100 小时
370 TB	75 亿	180 小时

Amazon S3 备份和还原权限和策略

要备份、复制和还原 S3 资源，您的角色中必须有正确的策略。要添加这些策略，请转到 AWS 托管策略。将AWSBackupServiceRolePolicyForS3Backup和AWSBackupServiceRolePolicyForS3Restore添加到您打算用来备份和恢复 S3 存储桶的角色中。

如果您没有足够的权限，需请求贵组织管理（管理员）账户的经理将这些策略添加到目标角色。

有关更多信息，请参阅《IAM 用户指南》中的托管策略与内联策略。

AWS Backup 因为 S3 依赖于通过亚马逊接收 S3 事件 EventBridge。如果在 S3 存储桶通知设置中禁用此设置，则在关闭此设置的情况下，将停止对这些存储桶的连续备份。有关更多信息，请参阅使用 EventBridge。

S3 备份的最佳实践和成本注意事项

最佳实践

对于对象数超过 3 亿的存储桶：

- 对于对象数超过 3 亿的存储桶，在存储桶的初始完整备份期间，备份速率最高可达每秒 17,000 个对象（增量备份的速度会有所不同）；包含的对象数少于 3 亿的存储桶以接近每秒 1,000 个对象的速率进行备份。
- 建议进行连续备份。
- 如果计划的备份生命周期超过 35 天，还可以在存储连续备份的同一个保管库中为存储桶启用快照备份。

成本注意事项

- S3 生命周期策略具有一项名为删除过期对象删除标记的可选功能。此功能停用后，删除标记（有时为数百万个）将在没有清理计划的情况下过期。备份没有此功能的存储桶时，有两个问题会影响时间和成本：
  - 就像对象一样备份删除标记。备份时间和还原时间可能会受到影响，具体取决于对象与删除标记的比例。
  - 备份的每个对象和标记都有最低费用。每个删除标记的费用与 128KiB 对象相同。
- 对于至少每天或更频繁地进行备份的客户，如果备份中的数据在两次备份之间变化最小，则使用连续备份可以实现成本效益。
- 不经常更改的较大存储桶可以从连续备份中受益，因为无需对先前存在的对象（与之前的备份相比未更改的对象）执行整个存储桶的扫描以及每个对象的多个请求时，这可以降低成本。
- 如果备份计划既包含保留期为 2 天的连续备份，又包含保留期更长的快照，则包含超过 1 亿个对象且删除率与总体备份大小相比较小的存储桶可能会实现成本效益。
- 当不需要执行存储桶扫描时，定期（快照）备份时间与备份过程的开始时间一致。在同时包含连续备份和快照的存储桶中不需要执行扫描，因为在这些情况下，快照是从连续恢复点拍摄的。
- 对于单个 S3-GIR（Amazon S3 Glacier 即时检索）中的每个对象， AWS Backup 执行多个调用，这将在执行备份时产生取回费用。

  类似的检索成本适用于对象为 S3-IA 和 S3 One Zone-IA 存储类别的存储桶。
- AWS KMS CloudTrail、和 Amazon 作为备份策略一部分的 CloudWatch 功能可能会导致除 S3 存储桶数据存储之外的额外成本。有关如何调整这些功能的信息，请参阅以下内容：
  - 《Amazon S3 用户指南》中的使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。
  - 您可以通过排除 AWS KMS 事件和禁用 S3 数据事件来降低 CloudTrail 成本：

- 排除 AWS KMS 事件：在《CloudTrail 用户指南》中，在控制台中创建跟踪（基本事件选择器）允许选择排除 AWS KMS 事件，从而将这些事件过滤出您的跟踪（默认设置包括所有 KMS 事件）：
- 只有当您在跟踪中记录管理事件时，用于记录或排除 KMS 事件的选项才可用。如果选择不记录管理事件，则不会记录 KMS 事件，并且您无法更改 KMS 事件日志记录设置。
- AWS KMS 诸如`Encrypt`、`Decrypt`和之类的操作`GenerateDataKey`通常会生成大量事件（超过 99%）。这些操作现在记录为读取事件。`Disable`、`Delete` 和 `ScheduleKey`（通常占不到 KMS 事件量的 0.5%）等少量的相关 KMS 操作记录为写入事件。
- 如果要排除大批量事件（例如 `Encrypt`、`Decrypt` 和 `GenerateDataKey`），但仍然记录相关事件（例如 `Disable`、`Delete` 和 `ScheduleKey`），请选择记录写入管理事件，然后清除排除 AWS KMS 事件复选框。
- 禁用 S3 数据事件：默认情况下，跟踪和事件数据存储不记录数据事件。在初始备份之前禁用 S3 数据事件可降低成本。

- 为了降低 CloudWatch 成本，您可以在更新跟踪以禁用 “ CloudWatch 日志” 设置时停止向 CloudWatch 日志发送 CloudTrail 事件。

还原 S3 备份

您可以将使用 AWS Backup 备份的 S3 数据恢复到 S3 标准存储类别。您可以将 S3 数据还原到现有存储桶，包括原始存储桶。在还原期间，还可以创建一个新的 S3 存储桶作为还原目标。您只能将 S3 备份还原到备份 AWS 区域 所在的位置。

您可以还原整个 S3 存储桶，也可以还原存储桶中的文件夹或对象。 AWS Backup 还原该对象的当前版本。

要使用恢复您的 S3 数据 AWS Backup，请参阅还原 S3 数据。

虚拟机备份

AWS Backup 支持对本地 VMware 虚拟机 (VM) 以及开启 VMware Cloud™ (VMC) 和 VMware Cloud™ (VMC) 中的虚拟机进行集中 AWS 和自动数据保护。 AWS Outposts您可以从本地和 VMC 虚拟机备份到。 AWS Backup然后，您可以从 AWS Backup 还原到本地虚拟机、VMC 或 VMC on AWS Outposts中的虚拟机。

AWS Backup 还为您提供完全托管的 AWS本机虚拟机备份管理功能，例如虚拟机发现、备份计划、保留管理、低成本存储层、跨区域和跨账户复制、对 V AWS Backup ault Lock 和 Audit Manag AWS

Backup er 的支持、独立于源数据的加密以及备份访问策略。有关功能的完整列表和详细信息，请参阅按资源划分的功能可用性表。

您可以使用 AWS Backup 在 VMware Cloud™ 上保护您的虚拟机 AWS Outposts。 AWS Backup 将您的虚拟机备份存储在您的 AWS 区域 VMware Cloud™ AWS Outposts 所连接的中。当您在虚拟机上使用 AWS Backup VMware Cloud™ 时，您可以使用保护 AWS Backup 虚拟机上的 VMware Cloud™，AWS Outposts 以满足应用程序数据的低延迟和本地数据处理需求。根据您的数据驻留要求，您可以选择 AWS Backup 将应用程序数据的备份存储在所连接 AWS 区域 的父级中。 AWS Outposts

支持的虚拟机

AWS Backup 可以备份和恢复由 VMware vCenter 管理的虚拟机。

目前支持：

- vSphere 8、7.0 和 6.7
- 虚拟磁盘大小为 1 KiB 的倍数
- 本地和 VMC 中的 NFS、VMFS 和 VSAN 数据存储库 AWS
- SCSI 热添加和网络块设备安全套接字层 (NBDSSL) 传输模式，用于将数据从源虚拟机复制到本地 VMware AWS
- 热添加模式可保护 VMware Cloud 上的虚拟机 AWS

目前不支持：

- RDM（原始磁盘映射）磁盘或 NVMe 控制器及其磁盘
- 独立永久磁盘模式和独立非永久磁盘模式

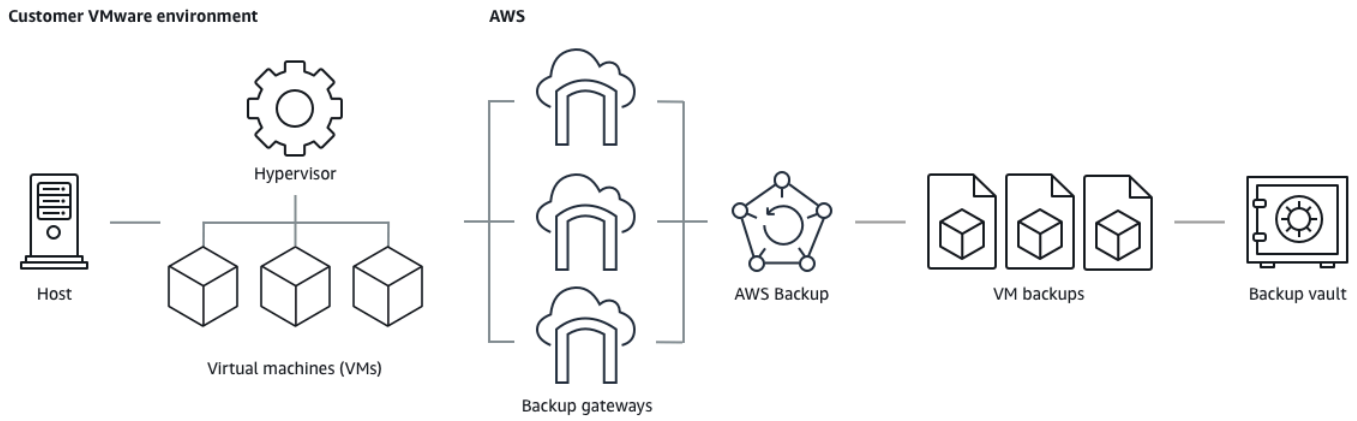
备份一致性

默认情况下，AWS Backup使用虚拟机上的 VMware Tools 静默设置，捕获虚拟机的应用程序一致性备份。如果您的应用程序与 VMware Tools 兼容，将捕获应用程序一致性备份。如果暂停功能不可用，则 AWS Backup 捕获崩溃一致的备份。请通过还原测试，验证您的备份是否满足组织的需求。

Backup Gateway

Backup 网关是可下载的 AWS Backup 软件，您可以将其部署到 VMware 基础架构中，用于将 VMware 虚拟机连接到该 AWS Backup基础架构。该网关连接到您的虚拟机管理服务器以发现虚拟

机、发现您的虚拟机、加密数据并高效地将数据传输到 AWS Backup。下图阐述了 Backup Gateway 如何连接到您的虚拟机：



要下载 Backup Gateway 软件，请按照使用网关的步骤操作。

有关 VPC（虚拟私有云）终端节点的信息，请参阅AWS Backup 和 AWS PrivateLink 连接。

Backup Gateway 附带自己的 API，该接口独立于 AWS Backup API 进行维护。要查看 Backup Gateway API 操作列表，请参阅 Backup Gateway 操作。要查看 Backup Gateway API 数据类型列表，请参阅 Backup Gateway 数据类型。

端点

如果现有用户当前使用的是公有端点，希望切换到 VPC （虚拟私有云）端点，可以使用 AWS PrivateLink 创建带 VPC 端点的新网关，将现有管理程序关联到该网关，然后删除包含公有端点的网关。

将您的基础设施配置为使用 Backup Gateway

Backup Gateway 需要具备以下网络、防火墙和硬件配置才能备份和还原虚拟机。

网络配置

Backup Gateway 要求允许特定端口来执行其操作。请允许使用以下端口：

1. TCP 443 出站
   - 源：Backup Gateway
   - 目的地： AWS

- 使用：允许 Backup 网关与通信 AWS。

2. TCP 80 入站
   - 来源：您用来连接的主机 AWS Management Console
   - 目的地：Backup Gateway
   - 用法：由本地系统用于获取 Backup Gateway 激活密钥。端口 80 仅在激活 Backup 网关期间使用。 AWS Backup 不要求端口 80 可以公开访问。端口 80 所需的访问级别取决于网络配置。如果您从激活网关 AWS Management Console，则从中连接到控制台的主机必须能够访问网关的端口 80。
3. UDP 53 出站
   - 源：Backup Gateway
   - 目的地：域名服务 (DNS) 服务器
   - 用法：允许 Backup Gateway 与 DNS 通信。
4. TCP 22 出站
   - 源：Backup Gateway
   - 目的地： AWS Support
   - 使用： AWS Support 允许访问您的网关以帮助您解决问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时必须将其打开。
5. UDP 123 出站
   - 源：NTP 客户端
   - 目的地：NTP 服务器
   - 用法：由本地系统用于将虚拟机时间同步到主机时间。
6. TCP 443 出站
   - 源：Backup Gateway
   - 目的地：VMware vCenter
   - 用法：允许 Backup Gateway 与 VMware vCenter 通信。
7. TCP 443 出站
   - 源：Backup Gateway
   - 目的地：ESXi 主机
   - 用法：允许 Backup Gateway 与 ESXi 主机通信。
8. TCP 902 出站
   - 源：Backup Gateway

- 目的地：VMware ESXi 主机
- 用法：用于通过 Backup Gateway 传输数据。

以上端口是 Backup 网关所必需的。有关如何创建 AWS Backup VPC 终端节点为其配置 Amazon VPC 终端节点的更多信息，请参阅 AWS Backup。

防火墙配置

Backup 网关需要访问以下服务端点才能与之通信 Amazon Web Services。如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 AWS进行出站通信。不支持在 Backup Gateway 和服务点之间使用 HTTP 代理。

```
proxy-app.backup-gateway.region.amazonaws.com:443
dp-1.backup-gateway.region.amazonaws.com:443
anon-cp.backup-gateway.region.amazonaws.com:443
client-cp.backup-gateway.region.amazonaws.com:443
```

在 VMware 中为多个 NIC 配置网关

您可以将多个虚拟网络接口连接 (NIC) 连接到网关，然后将内部流量（网关到虚拟机管理程序）和外部流量（网关到）分别定向内部和外部流量（网关到），从而为内部和外部流量维护单独的网络。 AWS

默认情况下，连接到 AWS Backup 网关的虚拟机只有一个网络适配器 (eth0)。该网络包括虚拟机管理程序、虚拟机和与更广泛的 Internet 通信的网络网关（Backup 网关）。

下面是一个具有多个虚拟网络接口的设置示例：

```
eth0:
- IP: 10.0.3.83
- routes: 10.0.3.0/24

eth1:
- IP: 10.0.0.241
- routes: 10.0.0.0/24
- default gateway: 10.0.0.1
```

- 在此示例中，如果连接到 IP 为 10.0.3.123 的管理程序，网关将使用 eth0，因为管理程序 IP 是 10.0.3.0/24 块的一部分
- 要连接到 IP 为 10.0.0.234 的管理程序，网关将使用 eth1

- 要连接到本地网络之外的 IP（例如 `34.193.121.211`），网关将回退到默认网关 `10.0.0.1`，该网关位于 `10.0.0.0/24` 块中，因此通过 `eth1`

添加其他网络适配器的第一个步骤序列发生在 vSphere 客户端中：

1. 在 VMware vSphere 客户端中，打开网关虚拟机的上下文菜单（通过右键单击），然后选择编辑设置。
2. 在虚拟机属性对话框的虚拟硬件选项卡上，打开添加新设备菜单，然后选择网络适配器来添加新的网络适配器。
3.
   a. 展开新建网络详细信息以配置新适配器。
   b. 确保选中开机时连接。
   c. 有关适配器类型，请参阅 ESXi 和 vCenter Server 文档中的“网络适配器类型”。
4. 单击确定保存新网络适配器设置。

配置其他适配器的下一个步骤是在 AWS Backup 网关控制台中进行的（请注意，这与管理备份和其他服务的 AWS 管理控制台的界面不同）。

将新 NIC 添加到网关虚拟机中后，您需要

- 转到 `Command Prompt` 并打开新适配器
- 为每个新 NIC 配置静态 IP
- 将首选 NIC 设置为默认值

为此，请执行以下操作：

1. 在 VMware vSphere 客户端中，选择您的网关虚拟机并启动 Web 控制台以访问 Backup 网关本地控制台。
   - 有关访问本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台
2. 退出命令提示符并转到“网络配置”>“配置静态 IP”，然后按照设置说明更新路由表。
   a. 在网络适配器的子网内分配静态 IP。
   b. 设置网络掩码。
   c. 输入默认网关的 IP 地址。这是连接到本地网络之外的所有流量的网络网关。
3. 选择设置默认适配器，指定将作为默认设备连接到云的适配器。

4. 网关的所有 IP 地址都会显示在本地控制台中，以及 VMware vSphere 的虚拟机摘要页面中。

硬件要求

您必须能够在虚拟机主机上为 Backup Gateway 提供以下最低限度的资源：

- 4 个虚拟处理器
- 8 GiB 预留 RAM

VMware 权限

本节列出了使用所需的最低 VMware 权限 AWS Backup gateway。这些权限是 Backup Gateway 发现、备份和还原虚拟机所必需的权限。

要在 VMware Cloud™ 开启 AWS 或开启 AWS Outposts VMware Cloud™ 的情况下使用 Backup 网关，您必须使用默认管理员用户`cloudadmin@vmc.local`或将 CloudAdmin 角色分配给您的专用用户。

要将 Backup 网关与 VMware 本地虚拟机配合使用，请创建一个具有下列权限的专用用户。

全局

- 禁用方法
- 启用方法
- 许可证
- 日志事件
- 管理自定义属性
- 设置自定义属性

vSphere 标记

- 分配或取消分配 vSphere 标签

DataStore

- 分配空间
- 浏览数据存储

- 配置数据存储（适用于 vSAN 数据存储）
- 低级文件操作
- 更新虚拟机文件

Host

- 配置
  - 高级设置
  - 存储分区配置

文件夹

- 创建文件夹

网络

- 分配网络

dvPortGroup

- 创建
- 删除

资源

- 将虚拟机分配到资源池

虚拟机

- 更改配置
  - 获取磁盘租约
  - 添加现有磁盘
  - 添加新磁盘
  - 高级配置

- 更改设置
- 配置原始设备。
- 修改设备设置
- 删除磁盘
- 设置注释
- 切换磁盘变更跟踪

- 编辑清单
  - 从现有创建
  - 新建
  - 注册
  - 删除
  - 取消注册
- 交互
  - 关闭
  - 打开
- 预置
  - 允许访问磁盘
  - 允许只读访问磁盘
  - 允许虚拟机下载
- 快照管理
  - 创建快照
  - 删除快照
  - 恢复为快照

使用网关

要使用备份和恢复虚拟机 (VM) AWS Backup，必须先安装 Backup 网关。网关是 OVF（开放虚拟化格式）模板形式的软件，它将 Amazon Web Services Backup 连接到您的虚拟机管理程序，允许它自动检测您的虚拟机，并允许您对其进行备份和恢复。

一个网关可以同时运行多达 4 个备份或还原作业。要同时运行 4 个以上的作业，请创建更多网关并将其与您的管理程序相关联。

创建网关

要创建网关，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左导航窗格的外部资源部分下，选择网关。
3. 选择创建网关。
4. 在设置网关部分，按照以下说明下载和部署 OVF 模板。

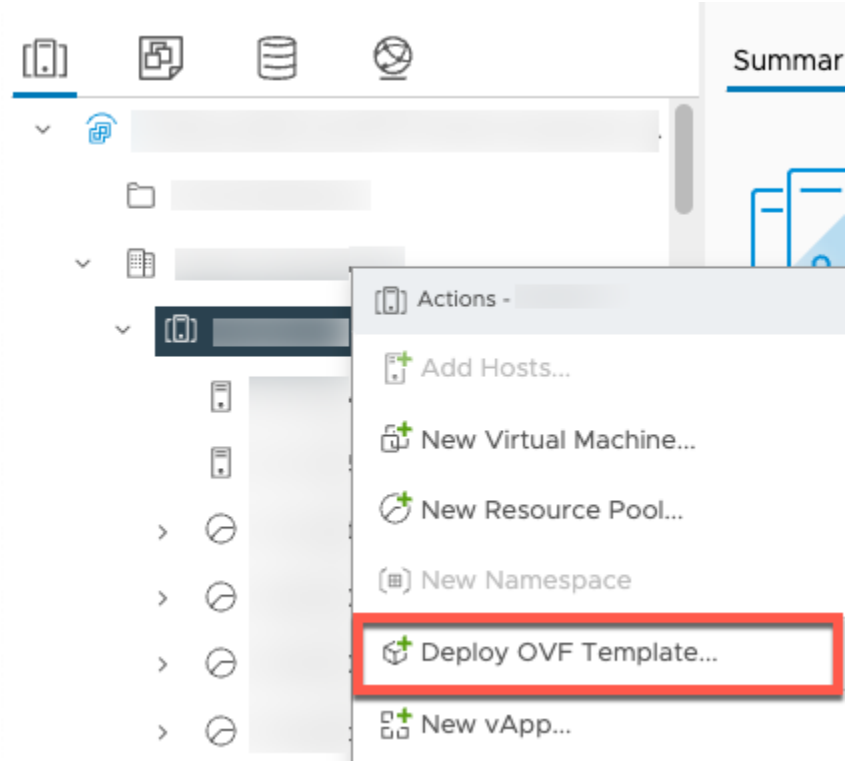
下载 VMware 软件

连接管理程序

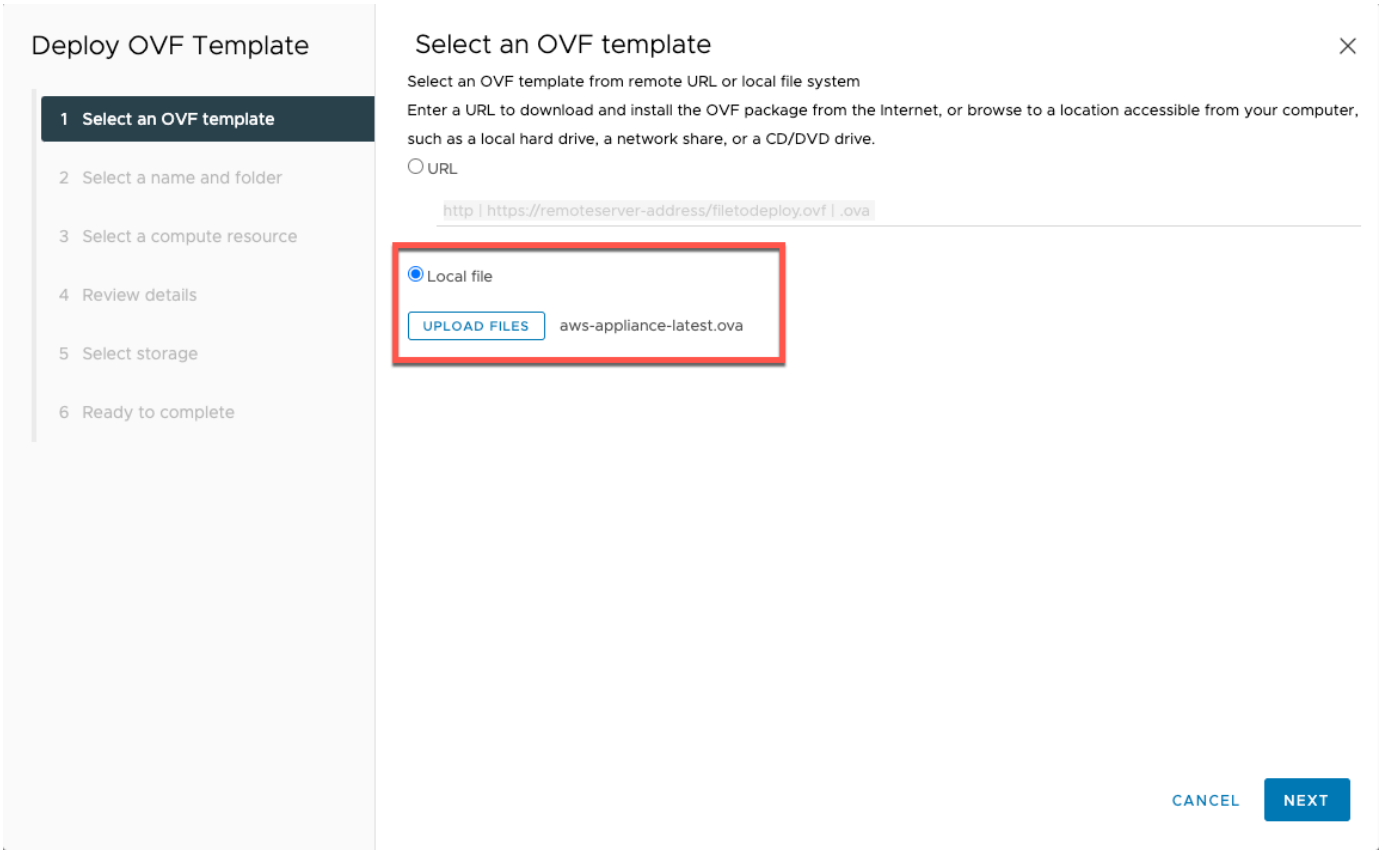
网关 AWS Backup 连接到您的虚拟机管理程序，因此您可以创建和存储虚拟机的备份。要在 VMware ESXi 上设置网关，请下载 OVF 模板。下载可能需要大约 10 分钟。

完成后，继续执行以下步骤：

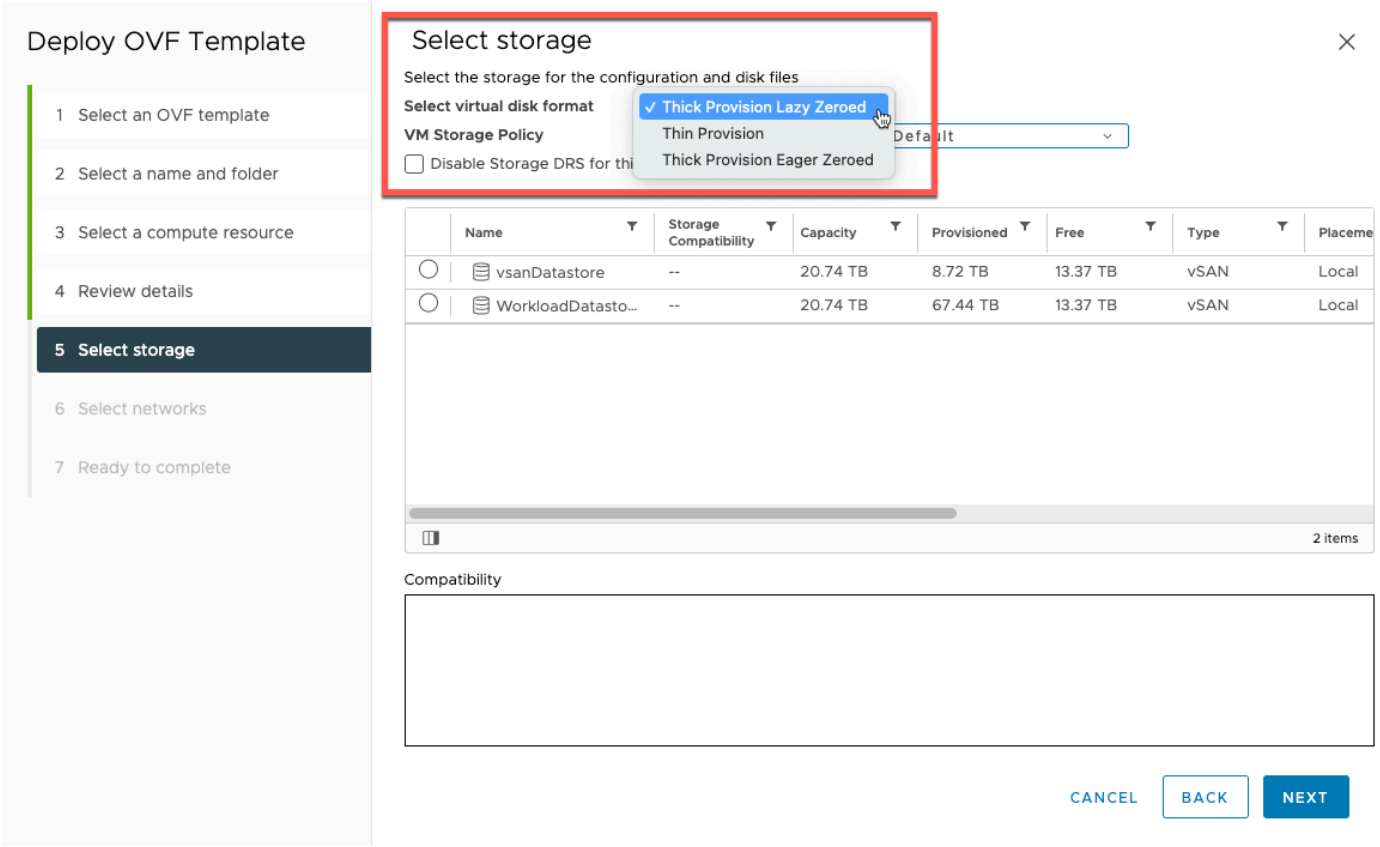
1. 使用 VMware vSphere 连接到您的虚拟机管理程序。
2. 右键单击虚拟机的父对象，然后选择部署 OVF 模板。



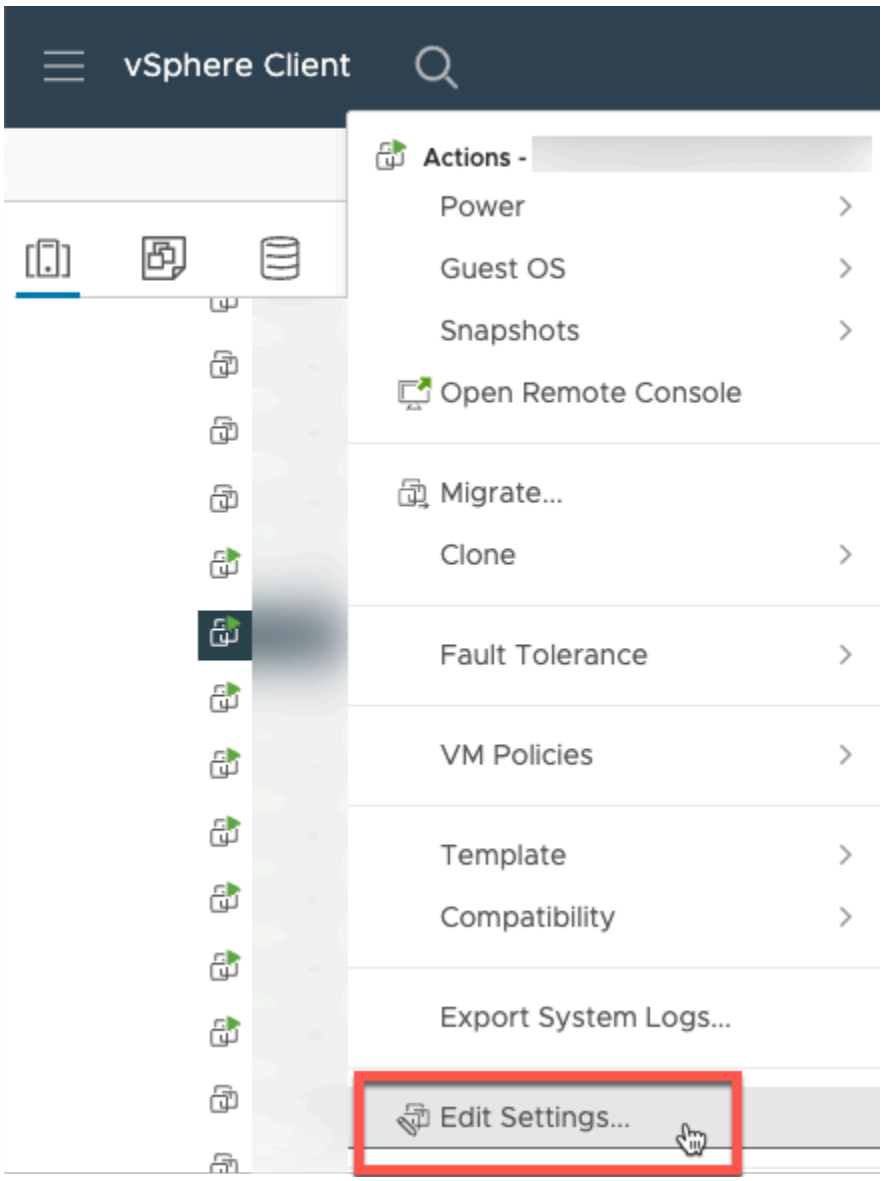
3. 选择本地文件，然后上传您下载的 aws-appliance-latest.ova 文件。



4. 按照部署向导的步骤进行部署。在选择存储页面上，选择虚拟磁盘格式 Thick Provision Lazy Zeroed。

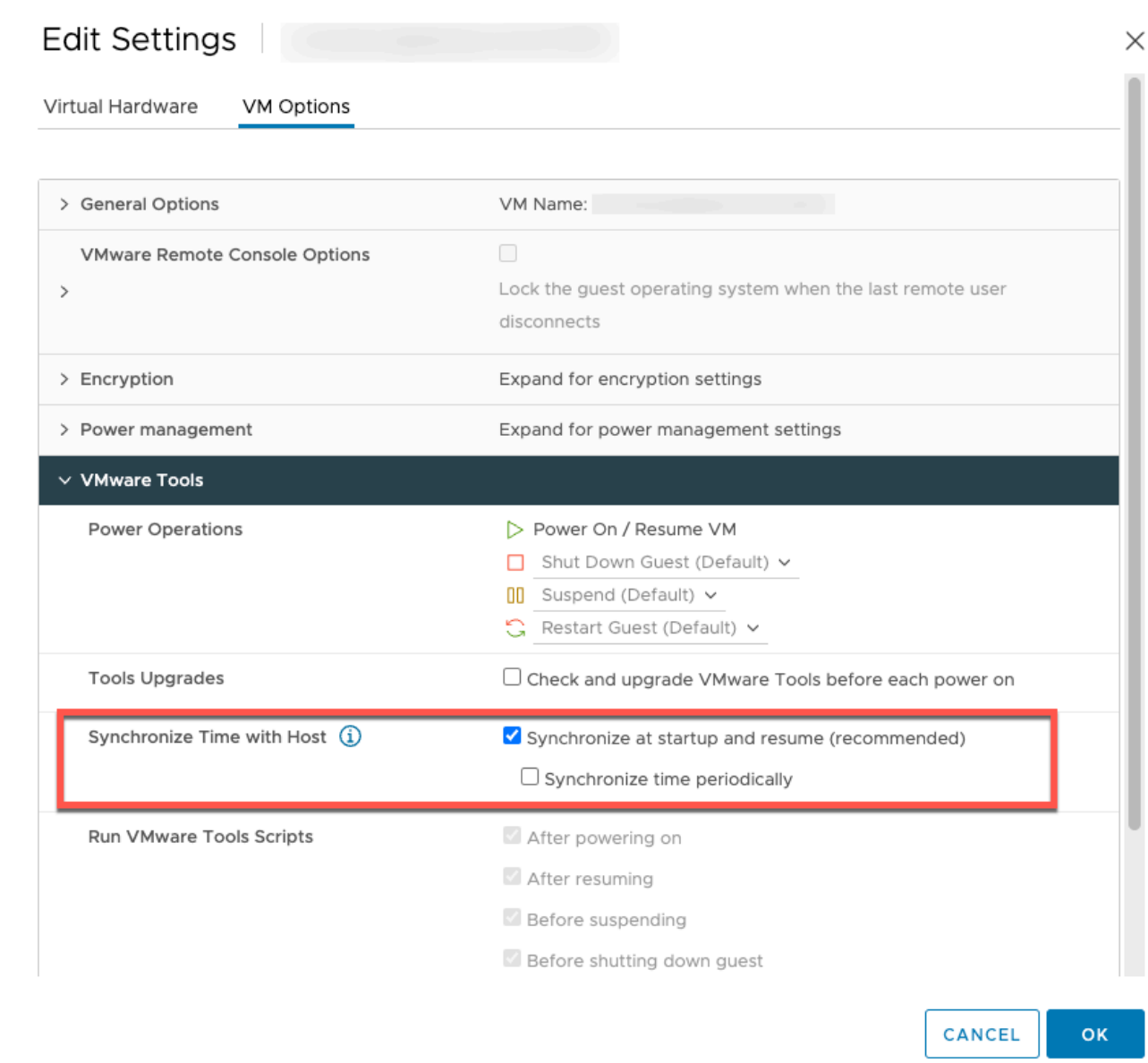


5. 部署 OVF 后，右键单击网关并选择编辑设置。

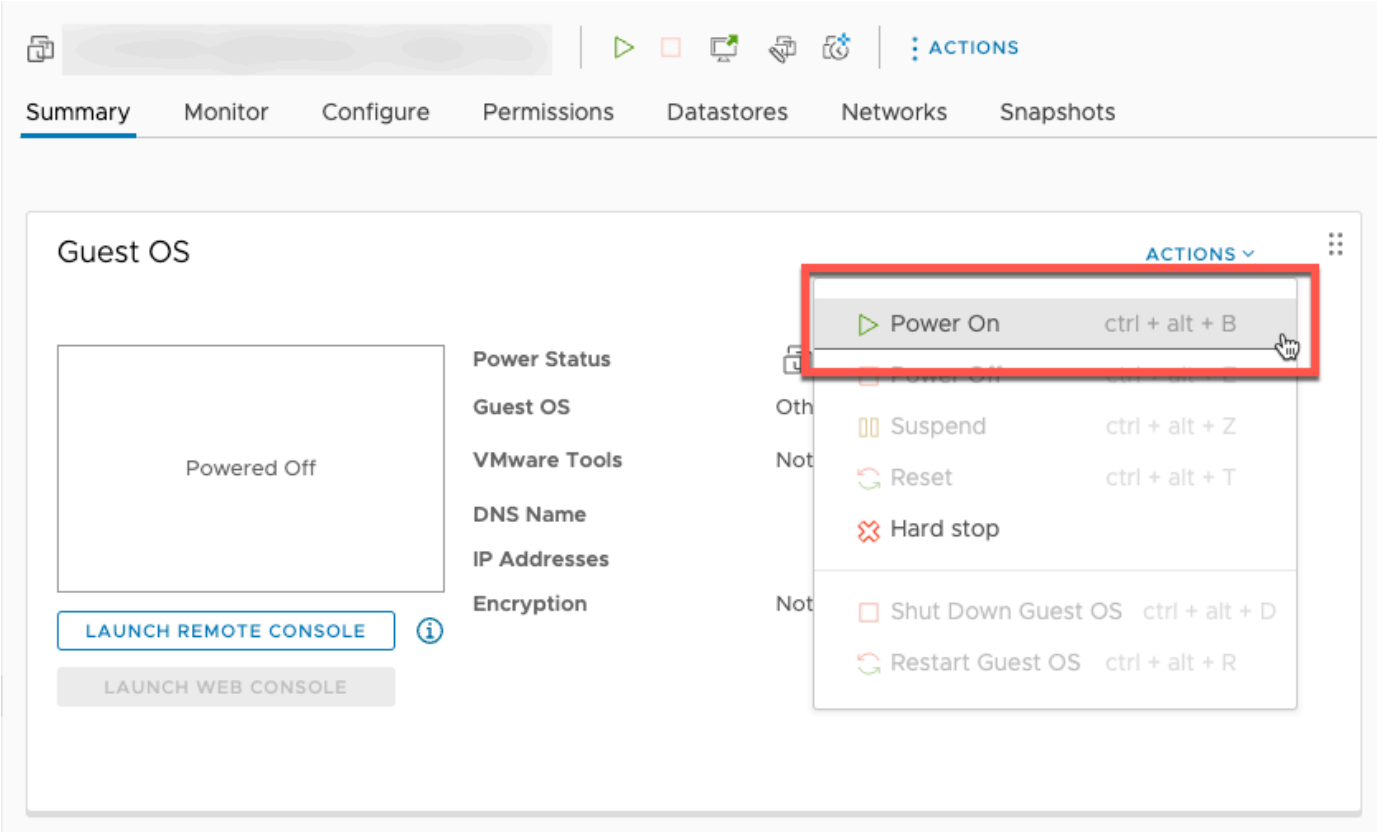


a. 在虚拟机选项 下，转到虚拟机工具。

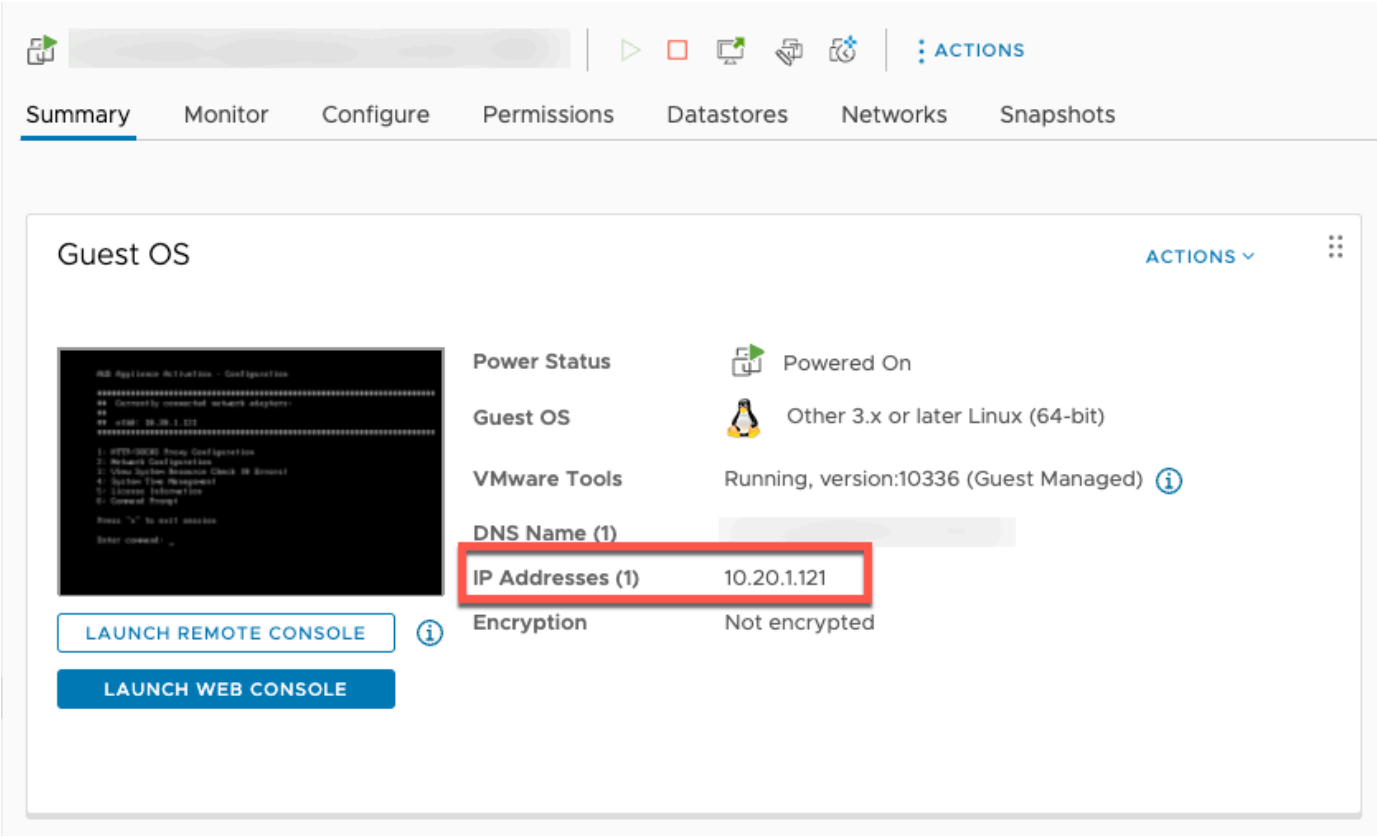
b. 确保在与主机同步时间中选中在启动和恢复时同步。



6. 从操作菜单中选择“开机”，打开虚拟机。



7. 从虚拟机摘要中复制 IP 地址，然后在下面输入它。



下载 VMware 软件后，完成以下步骤：

1. 在网关连接部分，键入网关的 IP 地址。
   a. 要查找此 IP 地址，请前往 vSphere 客户端。
   b. 在摘要选项卡下选择您的网关。
   c. 复制 IP 地址并将其粘贴到 AWS Backup 控制台文本栏中。
2. 在网关设置部分，
   a. 键入网关名称。
   b. 验证 AWS 区域。
   c. 选择端点是可公开访问还是托管在您的虚拟私有云 (VPC) 中。
   d. 根据所选端点，输入 VPC 端点 DNS 名称。

   有关更多信息，请参阅创建 VPC 端点。
3. [可选] 在网关标签部分，可以通过输入键和可选值来分配标签。要添加多个标签，请单击添加另一个标签。
4. 要完成该过程，请单击创建网关，此时将进入网关详细信息页面。

编辑或删除网关

要编辑或删除网关，请执行以下操作：

1. 在左导航窗格的外部资源部分下，选择网关。
2. 在网关部分，按网关名称选择网关。
3. 要编辑网关名称，请选择编辑。
4. 要删除网关，请选择删除，然后选择删除网关。

   您无法重新激活已删除的网关。如果要再次连接到管理程序，请按照创建网关中的过程进行操作。
5. 要连接到管理程序，请在已连接的管理程序 部分，选择连接。

   每个网关都连接到一个管理程序。但是，可以将多个网关连接到同一个管理程序，以便将它们之间的带宽增加到超过第一个网关的带宽。
6. 要分配、编辑或管理标签，请在标签部分选择管理标签。

Backup 网关带宽限制

> **Note**
>
> 此功能将在 2022 年 12 月 15 日之后部署的新网关上提供。对于现有网关，这项新功能将在 2023 年 1 月 30 日当天或之前通过自动软件更新提供。要手动将网关更新到最新版本，请使用 AWS CLI 命令UpdateGatewaySoftwareNow。

您可以将网关的上传吞吐量限制为 AWS Backup ，以控制网关使用的网络带宽量。默认情况下，已激活的网关没有任何速率限制。

您可以使用 AWS Backup 控制台或通过 AWS CLI () PutBandwidthRateLimitSchedule使用 API 配置带宽速率限制计划。使用带宽速率限制计划时，可以将限制配置为在一天或一周内自动进行更改。

带宽速率限制的工作方式是平衡所有上传数据的吞吐量，即每秒的平均值。虽然在任何给定的微秒或毫秒内，上传都可能短暂超过带宽速率限制，但这通常不会导致在较长时间内出现较大的峰值。

最多可以添加 20 个间隔。上传速率的最大值为每秒 8,000,000（百万）兆字节 (Mbps)。

使用控制台查看和编辑网关的带宽速率限制计划。 AWS Backup

本节介绍如何查看和编辑网关的带宽速率限制计划。

查看和编辑带宽速率限制计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择网关。在“网关”窗格中，网关按名称显示。单击要管理的网关名称旁边的单选按钮。
3. 选中单选按钮后，即可单击下拉菜单操作。单击操作，然后单击编辑带宽速率限制计划。此时将显示当前计划。默认情况下，新的或未经编辑的网关没有定义带宽速率限制。

   > **Note**
   >
   > 也可以在网关详细信息页面中单击管理计划，导航到 “编辑带宽” 页面。

4. （可选）选择添加间隔以向计划添加新的可配置间隔。对于每个间隔，请输入以下信息：

   a. 每周日期 - 选择要应用间隔的重复日期。选择后，这些日期将显示在下拉菜单下方。您可以单击该日期旁边的 X 将其删除。

b. 开始时间 - 使用 HH: MM 24 小时格式输入带宽间隔的开始时间。时间以协调世界时 (UTC) 呈现。

注意：您的 bandwidth-rate-limit 间隔从指定分钟开始时开始。

c. 结束时间 - 使用 HH: MM 24 小时格式输入带宽间隔的结束时间。时间以协调世界时 (UTC) 呈现。

> **Important**
>
> bandwidth-rate-limit 间隔在指定的分钟结束时结束。要计划在小时结束时结束的间隔，请输入 59。要计划不间断的连续备份间隔，在小时开始时转换，并且在各个间隔之间没有中断，请对第一个间隔的结束分钟输入 59。对后续间隔的开始分钟输入 00。

d. 上传速率 - 以兆位/秒 (Mbps) 为单位输入上传速率限制。最小值为 102 兆字节/秒 (Mbps)。

5. （可选）根据需要重复上一个步骤，直到带宽速率限制计划完成。如果您需要从计划中删除间隔，请选择删除。

> **Important**
>
> 带宽速率限制间隔不能重叠。间隔的开始时间必须出现在前一个间隔的结束时间之后和下一个间隔的开始时间之前；其结束时间必须出现在下一个间隔的开始时间之前。

6. 完成后，单击保存更改按钮。

使用 AWS CLI查看和编辑网关的带宽速率限制计划。

GetBandwidthRateLimitSchedule 操作可用于查看指定网关的带宽限制计划。如果未设置任何计划，计划将是一个空间隔列表。以下是使用获取网关带宽计划的示例： AWS CLI

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

要编辑网关的带宽限制计划，可以执行 PutBandwidthRateLimitSchedule 操作。请注意，您只能整体更新网关的计划，而不能修改、添加或删除单个间隔。调用此操作将覆盖网关之前的带宽限制计划。

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

使用管理程序

完成后创建网关，您可以将其连接到虚拟机管理程序， AWS Backup 以便与该虚拟机管理程序管理的虚拟机一起使用。例如，VMware 虚拟机的管理程序是 VMware vCenter Server。确保您的管理程序配置了对 AWS Backup的必要权限。

添加管理程序

要添加管理程序，请执行以下操作：

1. 在左导航窗格的外部资源部分下，选择管理程序。
2. 选择添加管理程序。
3. 在管理程序设置 部分，键入管理程序名称。
4. 对于 vCenter Server 主机，使用下拉菜单选择 IP 地址或 FQDN（完全限定域名）。键入相应的值。
5. AWS Backup 要允许在虚拟机管理程序上发现虚拟机，请输入虚拟机管理程序的用户名和密码。
6. 加密您的密码。您可以通过使用下拉菜单选择特定的服务托管 KMS 密钥或客户托管 KMS 密钥来指定此加密，也可以选择创建 KMS 密钥。如果您未选择特定密钥， AWS Backup 将使用服务拥有的密钥对您的密码进行加密。
7. 在连接网关部分，使用下拉列表指定要连接到管理程序的网关。
8. 选择测试网关连接以验证您之前的输入。
9. 或者，在管理程序标签部分，可以通过选择添加新标签为管理程序分配标签。
10. 可选的 VMware 标签映射：您最多可以添加当前在虚拟机上使用的 10 个 VMware 标签来生成 AWS 标签。
11. 在日志组设置面板中，您可以选择与 Amazon Lo CloudWatch g s 集成以维护虚拟机管理程序的日志（标准CloudWatch 日志定价将根据使用情况而定）。每个管理程序可以属于一个日志组。
    a. 如果您尚未创建日志组，请选中创建新的日志组单选按钮。您正在编辑的管理程序将与该日志组关联。
    b. 如果您之前已为不同管理程序创建日志组，则可以将该日志组用于此管理程序。选择使用现有日志组。
    c. 如果您不想 CloudWatch 记录日志，请选择 “停用日志记录”。

12. 选择添加管理程序，此时将进入其详细信息页面。

> **Tip**
>
> 您可以使用 Amazon CloudWatch Logs（参见上面的步骤 11）来获取有关您的虚拟机管理程序的信息，包括错误监控、网关和虚拟机管理程序之间的网络连接以及网络配置信息。有关 CloudWatch 日志组的信息，请参阅 Amazon CloudWatch 用户指南中的使用日志组和日志流。

查看管理程序管理的虚拟机

要查看管理程序上的虚拟机，请执行以下操作：

1. 在左导航窗格的外部资源部分下，选择管理程序。
2. 在管理程序部分，按管理程序名称选择管理程序，进入其详细信息页面。
3. 在管理程序摘要下的部分中，选择虚拟机选项卡。
4. 在已连接的虚拟机部分中，将自动填充虚拟机列表。

查看连接到管理程序的网关

要查看连接到管理程序的网关，请执行以下操作：

1. 选择网关选项卡。
2. 在已连接的网关部分中，将自动填充网关列表。

将管理程序连接到其他网关

您的备份和还原速度可能会受到网关和管理程序之间连接带宽的限制。您可以通过将一个或多个附加网关连接到管理程序来提高这些速度。您可以在已连接的网关部分执行此操作，如下所示：

1. 选择连接。
2. 使用下拉菜单选择其他网关。或者，选择创建网关以创建新网关。
3. 选择连接。

编辑管理程序配置

如果不使用测试网关连接功能，那么您添加管理程序所用的用户名或密码可能会出错。在这种情况下，管理程序的连接状态始终为 Pending。或者，您可能轮换用户名或密码访问管理程序。使用以下过程返回这些信息：

要编辑已添加的管理程序，请执行以下操作：

1. 在左导航窗格的外部资源部分下，选择管理程序。
2. 在管理程序部分，按管理程序名称选择管理程序，进入其详细信息页面。
3. 选择编辑。
4. 顶部面板名为管理程序设置。
   a. 在 vCenter Server 主机下，还可以编辑 FQDN（完全限定域名）或 IP 地址。
   b. （可选）输入管理程序的用户名和密码。
5. 在日志组设置面板中，您可以选择与 Amazon 集成 CloudWatch以维护您的虚拟机管理程序日志（标准CloudWatch 定价将根据使用情况而定）。每个管理程序可以属于一个日志组。
   a. 如果您尚未创建日志组，请选中创建新的日志组单选按钮。您正在编辑的管理程序将与该日志组关联。
   b. 如果您之前已为不同管理程序创建日志组，则可以将该日志组用于此管理程序。选择使用现有日志组。
   c. 如果您不想 CloudWatch 记录日志，请选择 “停用日志记录”。

> **Tip**
>
> 您可以使用 Amazon CloudWatch Logs（参见上面的步骤 5）来获取有关您的虚拟机管理程序的信息，包括错误监控、网关和虚拟机管理程序之间的网络连接以及网络配置信息。有关 CloudWatch 日志组的信息，请参阅 Amazon CloudWatch 用户指南中的使用日志组和日志流。

要以编程方式更新虚拟机管理程序，请使用 CLI 命令 upd ate-hypervisor 和 API 调用。UpdateHypervisor

删除管理程序配置

如果您需要删除已添加的管理程序，请删除管理程序配置并添加另一个管理程序配置。此删除操作适用于连接到管理程序的配置。它不会实际删除管理程序。

要删除连接到已添加的管理程序的配置，请执行以下操作：

1. 在左导航窗格的外部资源部分下，选择管理程序。
2. 在管理程序部分，按管理程序名称选择管理程序，进入其详细信息页面。
3. 选择删除，然后选择删除管理程序。
4. 可选：使用添加管理程序中的步骤替换已删除的管理程序配置。

了解管理程序状态

以下内容描述每个可能的管理程序状态以及补救措施（如果适用）。ONLINE 状态是管理程序的正常状态。在用于备份和恢复由管理程序管理的虚拟机的所有或大部分时间，管理程序都应处于此状态。

管理程序状态

Status	含义和补救措施
ONLINE	您已将虚拟机管理程序添加至 AWS Backup网关，并可通过网络与该网关连接，对由该管理程序管理的虚拟机执行备份和恢复。 您可以随时对这些虚拟机执行按需备份和计划备份。
PENDING	你添加了虚拟机管理程序， AWS Backup 但是： • 它未与任何网关关联，或者 • 它与一个或多个网关关联，但所有这些网关都已删除或者处于非活动状态。 要将管理程序状态从 PENDING 更改为 ONLINE，请创建网关并将管理程序连接到该网关。

Status	含义和补救措施
OFFLINE	您已将虚拟机管理程序添加到网关 AWS Backup 并将其与网关关联，但该网关无法通过您的网络连接到虚拟机管理程序。 要将管理程序状态从 OFFLINE 更改为 ONLINE，请验证您的网络配置是否正确。 如果问题仍然存在，请验证您的管理程序的 IP 地址或完全限定域名是否正确。如果它们不正确，请使用正确的信息再次添加管理程序并测试网关连接。
ERROR	您已将虚拟机管理程序添加到网关并将其 AWS Backup 与网关关联，但该网关无法与虚拟机管理程序通信。 要将管理程序状态从 ERROR 更改为 ONLINE，请验证管理程序的用户名和密码是否正确。如果它们不正确，请编辑管理程序配置。

后续步骤

要在管理程序上备份虚拟机，请参阅备份虚拟机。

备份虚拟机

在添加管理程序之后，Backup Gateway 会自动列出您的虚拟机。您可以通过在左导航窗格中选择管理程序或虚拟机来查看您的虚拟机。

- 选择管理程序可仅查看由特定管理程序管理的虚拟机。使用此视图，可以一次使用一台虚拟机。
- 选择 “虚拟机”，查看添加到您的所有虚拟机管理程序中的所有虚拟机。 AWS 账户使用此视图，可以跨多个管理程序使用部分或全部虚拟机。

无论选择哪个视图，要在特定虚拟机上执行备份操作，请选择其虚拟机名称以打开其详细信息页面。虚拟机详细信息页面是执行以下过程的起点。

创建虚拟机的按需备份

按需备份是您手动启动的一次性完整备份。您可以使用按需备份 AWS Backup来测试备份和还原功能。

要创建虚拟机的按需备份，请执行以下操作：

1. 选择创建按需备份。
2. 配置按需备份。
3. 选择创建按需备份。
4. 检查您的备份作业何时处于 `Completed` 状态。在左导航窗格中，选择作业。
5. 选择备份作业 ID 以查看备份作业信息，例如备份大小以及从创建日期到完成日期之间经过的时间。

增量虚拟机备份

较新的 VMware 版本包含一项名为更改块跟踪的特征，可在虚拟机的存储块随时间发生变化时对其进行跟踪。当您使用 AWS Backup 备份虚拟机时，会 AWS Backup 尝试使用 CBT 数据（如果有）。AWS Backup 使用 CBT 数据来加快备份过程；如果没有 CBT 数据，备份作业通常会变慢，并且会占用更多的虚拟机管理程序资源。即使 CBT 数据无效或不可用，备份仍可以成功完成。例如，如果虚拟机或 ESXi 主机遇到硬关闭，CBT 数据可能无效或不可用。

如果 CBT 数据无效或不可用，则会显示备份状态 `Successful` 和一条消息。在这些情况下，该消息将表明，在没有 CBT 数据的情况下， AWS Backup 使用自己专有的变更检测机制来完成备份，而不是 VMware 的 CBT 数据。随后的备份将重新尝试使用 CBT 数据，并且在大多数情况下，CBT 数据将变为有效且可用。如果问题仍然存在，请参阅 VMware 故障排除了解补救措施。

要让 CBT 正常运行，必须满足以下条件：

- 主机需要具备 ESXi 4.0 或更高版本
- 拥有磁盘的虚拟机必须具有硬件版本 7 或更高版本
- 必须为虚拟机启用 CBT（默认情况下处于启用状态）

要验证虚拟磁盘是否已启用 CBT，请执行以下操作：

1. 打开 vSphere Client，然后选择已关闭的虚拟机。
2. 右键单击虚拟机并导航至**编辑设置** > **选项** > **高级/常规** > **配置参数**。

3. 选项 `ctkEnabled` 需要等于 `True`。

通过为备份计划分配资源自动执行虚拟机备份

备份计划是一种用户定义的数据保护策略，它可以跨许多 AWS 服务和第三方应用程序自动保护数据。首先要通过指定备份频率、保留期、生命周期策略和许多其他选项来创建备份计划。要创建备份计划，请参阅入门教程。

创建备份计划后，您可以将 AWS Backup支持的资源（包括虚拟机）分配给该备份计划。 AWS Backup 提供了多种分配资源的方式，包括分配账户中的所有资源，包括或排除单个特定资源，或者添加带有特定标签的资源。

除了现有的资源分配功能外，对虚拟机的 AWS Backup 支持还引入了多项新功能，可帮助您快速将虚拟机分配给备份计划。在虚拟机页面上，可以为多个虚拟机分配标签，也可以使用新的将资源分配给计划功能。使用这些功能来分配 AWS Backup 网关已发现的虚拟机。

如果您预计将来会发现和分配其他虚拟机，并希望自动执行资源分配步骤以包括这些未来的虚拟机，请使用新的创建组分配功能。

VMware 标签

标签是键值对，可用于管理、筛选和搜索您的资源。

VMware 标签由类别和标签名称组成。VMware 标签用于对虚拟机进行分组。标签名称是分配给虚拟机的标签。类别是标签名称的集合。

在 AWS 标签中，可以使用 UTF-8 字母、数字、空格和特殊字符之间的字符`+ - = . _ : /`。

如果要在虚拟机上使用标签，可以在 AWS Backup 中添加最多 10 个匹配标签帮助进行整理。您最多可以将 10 个 VMware 标签映射到 AWS 标签。在AWS Backup 控制台中，可以在我的组织 > 虚拟机 > AWS 标签或 VMware 标签中找到这些标签。

VMware 标签映射

如果要在虚拟机上使用标签，可以在 AWS Backup 中添加最多 10 个匹配标签进行额外的澄清和整理。映射适用于管理程序上的任何虚拟机。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在控制台中，转到编辑管理程序（依次单击外部资源、管理程序和管理程序名称，然后单击管理映射）。

3. 最后一个窗格是 VMware 标签映射，它包含四个文本框字段，您可以在这些字段中将现有的 VMware 标签信息输入到相应的 AWS 标签中。这四个字段是 VMware 标签类别、VMware AWS 标签名称、标签键和AWS 标签值（例如：类别 = 操作系统；标签名称 = Windows；标签键 = OS-Windows， AWS 标签值 = Windows， AWS 标签值 = Windows）。
4. 输入首选值后，单击添加映射。如果出错，可以单击删除删除输入的信息。
5. 添加映射后，指定要用于将这些 AWS 标签应用于 VMware 虚拟机的 IAM 角色。

   策略 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 包含所需的权限。您可以将此策略附加到您要使用的角色（或让管理员附加此策略），也可以为要使用的角色创建自定义策略。
6. 最后，单击添加管理程序或保存。

应修改 IAM 角色信任关系以添加 backup-gateway.amazonaws.com 和 backup.amazonaws.com 服务。如果没有此服务，则在映射标签时可能会遇到错误。要编辑现有角色的信任关系，请执行以下操作：

1. 登录 IAM 控制台。
2. 在控制台的导航窗格中，选择角色。
3. 选择要修改的角色的名称，然后在详细信息页面中选择信任关系选项卡。
4. 在策略文档下，粘贴以下内容：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. 选择更新信任策略。

有关更多详细信息，请参阅《AWS Directory Service 管理指南》中的编辑现有角色的信任关系。

查看 VMware 标签映射

在 AWS Backup 控制台中，单击外部资源，然后单击管理程序，然后单击“管理程序名称” 链接以查看所选管理程序的属性。在摘要窗格下，有四个选项卡，最后一个选项卡是 VMware 标签映射。请注意，如果还没有映射，将显示“没有 VMware 标签映射” 。

在这里，您可以同步虚拟机管理程序发现的虚拟机的元数据，可以将映射复制到您的虚拟机管理程序，可以将映射到 VMware AWS 标签的标签添加到备份计划的备份选择中，或者您可以管理映射。

在控制台中，要查看将哪些标签应用于选定虚拟机，请单击虚拟机，单击虚拟机名称，然后单击 AWS 标签或 VMware 标签。您可以查看与此虚拟机关联的标签，此外还可以管理这些标签。

使用 VMware 标签映射将虚拟机分配给计划

要使用映射的标签将虚拟机分配给备份计划，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在控制台中，转到管理程序详细信息页面上的 VMware 标签映射（单击外部资源，单击管理程序，然后单击管理程序名称）。
3. 选中映射的多个标签旁边的复选框，将这些标签分配给同一个备份计划。
4. 单击添加到资源分配。
5. 从下拉列表中选择一个现有的备份计划。或者，可以选择创建备份计划创建新的备份计划。
6. 单击确认。这将打开分配资源页面，其中的使用标签优化选择字段已预先填充值。

使用 VMware 标签的 AWS CLI

AWS Backup 使用 API 调用PutHypervisorPropertyMappings将内部管理程序实体属性映射到中的属性。 AWS

在中 AWS CLI，使用以下操作put-hypervisor-property-mappings：

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

示例如下：

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

还可以使用 GetHypervisorPropertyMappings 帮助获取属性映射信息。在中 AWS CLI，使用操作get-hypervisor-property-mappings。示例模板如下：

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

示例如下：

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

AWS 使用 API、CLI 或 SDK 同步虚拟机管理程序发现的虚拟机的元数据

您可以同步虚拟机的元数据。当这样做时，将对虚拟机上作为映射一部分存在的 VMware 标签进行同步。此外，映射到虚拟机上的 VMware 标签的 AWS 标签将应用于 AWS 虚拟机资源。

AWS Backup 使用 API 调StartVirtualMachinesMetadataSync用同步虚拟机管理程序发现的虚拟机的元数据。要使用 AWS CLI同步管理程序发现的虚拟机的元数据，请执行操作 start-virtual-machines-metadata-sync。

示例模板：

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

例如：

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

您还可以使用 GetHypervisor 来帮助获取管理程序信息，例如主机、状态、最新元数据同步的状态，还可以检索上次成功的元数据同步时间。在中 AWS CLI，使用操作get-hypervisor。

示例模板：

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

例如：

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

有关更多信息，请参阅 API 文档VmwareTag和 VmwareToAwsTagMapping。

此功能将在 2022 年 12 月 15 日之后部署的新网关上提供。对于现有网关，这项新功能将在 2023 年 1 月 30 日当天或之前通过自动软件更新提供。要手动将网关更新到最新版本，请使用 AWS CLI 命令 UpdateGatewaySoftwareNow。

例如：

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

使用标签分配虚拟机

您可以为当前发现的 AWS Backup虚拟机以及其他 AWS Backup 资源分配一个您已经分配给现有备份计划的标签。您还可以创建新备份计划和新的基于标签的资源分配。备份计划每次运行备份作业时都会检查是否有新分配的资源。

要使用同一标签标记多个虚拟机，请执行以下操作：

1. 在左侧导航窗格中，选择虚拟机。
2. 选中虚拟机名称旁边的复选框以选择您的所有虚拟机。或者，选中要标记的虚拟机名称旁边的复选框。
3. 选择添加标签。
4. 键入标签键。

5. 推荐：键入标签值。
6. 选择确认。

使用“将资源分配给计划” 功能分配虚拟机

您可以使用 “将资源分配给计划” 功能将当前发现的虚拟机分配给现有或新的备份计划。 AWS Backup

要使用“将资源分配给计划” 功能分配虚拟机，请执行以下操作：

1. 在左侧导航窗格中，选择虚拟机。
2. 选中虚拟机名称旁边的复选框以选择您的所有虚拟机。或者，选中多个虚拟机名称旁边的复选框，将它们分配给同一个备份计划。
3. 选择分配，然后选择将资源分配给计划。
4. 键入资源分配名称。
5. 选择资源分配 IAM 角色以创建备份和管理恢复点。如果您没有特定 IAM 角色可供使用，我们建议使用具有正确权限的默认角色。
6. 在备份计划部分，从下拉列表中选择现有备份计划。或者，选择创建备份计划创建新的备份计划。
7. 选择分配资源。
8. 可选：选择查看备份计划，验证您的虚拟机是否已分配到备份计划。然后，在资源分配部分，选择资源分配名称。

使用“创建组分配”功能分配虚拟机

与前两个虚拟机的资源分配功能不同，创建组分配功能不仅可以分配当前发现的虚拟机 AWS Backup，还可以分配将来在您定义的文件夹或虚拟机管理程序中发现的虚拟机。

此外，您无需选中任何复选框即可使用创建组分配功能。

要使用“将资源分配给计划” 功能分配虚拟机，请执行以下操作：

1. 在左侧导航窗格中，选择虚拟机。
2. 选择分配，然后选择创建组分配。
3. 键入资源分配名称。
4. 选择资源分配 IAM 角色以创建备份和管理恢复点。如果您没有特定 IAM 角色可供使用，我们建议使用具有正确权限的默认角色。
5. 在资源组部分，选择组类型下拉菜单。选项包括文件夹或管理程序。

a. 选择文件夹可分配管理程序文件夹中的所有虚拟机。使用下拉菜单选择文件夹组名称，例如 `datacenter/vm`。您也可以选择包括子文件夹。

> **Note**
>
> 要进行基于文件夹的分配，请在发现过程中使用虚拟机在发现过程中找到的文件夹来 AWS Backup 标记虚拟机。如果您稍后将虚拟机移至其他文件夹，则由于标记最佳做法， AWS Backup 无法为您更新 AWS 标记。此分配方法可能会导致继续备份已移出所分配文件夹的虚拟机。

b. 选择管理程序可分配由管理程序管理的所有虚拟机。使用下拉菜单选择管理程序 ID 组名称。

6. 在备份计划部分，从下拉列表中选择现有备份计划。或者，选择创建备份计划创建新的备份计划。
7. 选择创建组分配。
8. 可选：选择查看备份计划，验证您的虚拟机是否已分配到备份计划。在资源分配部分，选择资源分配名称。

后续步骤

要还原虚拟机，请参阅使用恢复虚拟机 AWS Backup。

有关 Backup Gateway 的第三方源组件的信息

在本节中，您可以找到有关我们提供 Backup Gateway 功能所依赖的第三方工具和许可证的信息。

可在以下网址下载 Backup Gateway 软件附带的某些第三方源软件组件的源代码：

- 对于在 VMware ESXi 上部署的网关，请下载 sources.tgz。

该产品包括由 OpenSSL 项目开发的用于 OpenSSL 工具包的软件 (https://www.openssl.org/)。

该产品包括由 VMware® vSphere 软件开发工具包 (https://www.vmware.com) 开发的软件。

有关所有依赖的第三方工具的相关许可证，请参阅第三方许可证。

AWS 设备的开源组件

一些第三方工具和许可证用于为 Backup Gateway 提供功能。

使用以下链接下载 AWS 设备软件中包含的某些开源软件组件的源代码：

- 对于在 VMware ESXi 上部署的网关，请下载 sources.tar

该产品包括由 OpenSSL 项目开发的用于 OpenSSL 工具包的软件 (https://www.openssl.org/)。有关所有依赖的第三方工具的相关许可证，请参阅 Third-Party Licenses。

排查虚拟机问题

增量备份/CBT 问题和消息

失败消息：**"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."**

如果此消息仍然存在，请按照 VMware 的指示重置 CBT。

消息说明 CBT 未开启或不可用：“VMware 更改块跟踪 (CBT) 不适用于此虚拟机，但是已使用我们专有的更改机制成功完成增量备份。”

检查以确保 CBT 已开启。要验证虚拟磁盘是否已启用 CBT，请执行以下操作：

1. 打开 vSphere Client，然后选择已关闭的虚拟机。
2. 右键单击虚拟机并导航至编辑设置 > 选项 > 高级/常规 > 配置参数。
3. 选项 `ctkEnabled` 需要等于 `True`。

如果已开启，请确保您使用的是 up-to-date VMware 功能。主机必须是 ESXi 4.0 或更高版本，并且具有待跟踪磁盘的虚拟机必须是硬件版本 7 或更高版本。

如果 CBT 已开启（启用）并且软件和硬件为最新，请关闭虚拟机，然后再次将其打开。确保 CBT 已开启。然后，再次执行备份。

高级 DynamoDB 备份

AWS Backup 支持其他高级功能，可满足您的 Amazon DynamoDB 数据保护需求。在中启用高级功能后 AWS 区域，您可以为创建 AWS Backup的 DynamoDB 表备份解锁以下所有新功能：

- 成本节省和优化：
  - 将备份分层到冷存储以降低存储成本
  - 用于 Cost Explorer 的成本分配标记

- 业务连续性：
  - 跨区域复制
  - 跨账户复制
- 安全性：
  - 将备份存储在加密的 AWS Backup 保管库中，您可以使用 AWS Backup 保管库锁定、AWS Backup 策略和加密密钥来保护这些保管库。
  - 备份从其源 DynamoDB 表继承标签，使您能够使用这些标签来设置权限和服务控制策略 (SCP)。

2021 年 11 月 AWS Backup 之后注册的新客户会默认启用高级 DynamoDB 备份功能。具体而言，为在 2021 年 11 月 21 日之前未创建备份保管库的客户默认启用高级 DynamoDB 备份功能。

我们建议所有现有 AWS Backup 客户启用 DynamoDB 的高级功能。在启用高级功能后，热备份存储的定价没有区别。您可以通过将备份分层到冷存储来节省资金，并通过使用成本分配标签来优化成本。您也可以开始利用 AWS Backup的业务连续性和安全功能。

> **Note**
>
> 如果您使用自定义角色或策略而不是默认服务角色，则必须向您的自定义角色添加或使用以下权限策略（或添加其等效权限）： AWS Backup
>
> - `AWSBackupServiceRolePolicyForBackup` 可执行高级 DynamoDB 备份。
> - `AWSBackupServiceRolePolicyForRestores` 可还原高级 DynamoDB 备份。
>
> 要了解有关 AWS托管策略的更多信息并查看客户托管策略的示例，请参阅。的托管策略 AWS Backup

主题

使用控制台启用高级 DynamoDB 备份

您可以使用 AWS Backup 或 DynamoDB 控制台为 DynamoDB 备份启用 AWS Backup 高级功能。

要从控制台启用高级 DynamoDB 备份功能，请执行以下操作： AWS Backup

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左导航菜单中，选择设置。
3. 在支持的服务部分下，验证 DynamoDB 是否已启用。

   如果未启用，请单击选择加入并启用 DynamoDB 作为 AWS Backup 支持的服务。
4. 在 DynamoDB 备份的高级功能部分下，选择启用。
5. 选择启用功能。

有关如何使用 DynamoDB 控制台启用 AWS Backup 高级功能，请参阅亚马逊 Dynam o DB 用户指南中的 AWS Backup 启用功能。

以编程方式启用高级 DynamoDB 备份

您也可以使用 AWS Command Line Interface (CLI) 为 DynamoDB 备份启用 AWS Backup 高级功能。将以下两个值都设置为 `true`，即可启用高级 DynamoDB 备份：

要以编程方式启用 DynamoDB 备份的 AWS Backup 高级功能，请执行以下操作：

1. 使用以下命令检查您是否已经为 DynamoDB 启用了 AWS Backup 高级功能：

   ```
   $ aws backup describe-region-settings
   ```

   如果 `"ResourceTypeManagementPreference"` 和 `"ResourceTypeOptInPreference"` 下均为 `"DynamoDB":true`，则表示已经启用高级 DynamoDB 备份。

   如以下输出所示，如果至少有一个 `"DynamoDB":false` 实例，则表示尚未启用高级 DynamoDB 备份，请继续执行下一步。

   ```
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
   ```

```
  "ResourceTypeOptInPreference":{
    "Aurora":true,
    "DocumentDB":false,
    "DynamoDB":false,
    "EBS":true,
    "EC2":true,
    "EFS":true,
    "FSx":true,
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. 使用以下 UpdateRegionSettings 操作将 "ResourceTypeManagementPreference" 和 "ResourceTypeOptInPreference" 设置为 "DynamoDB":true：

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

编辑高级 DynamoDB 备份

在 AWS Backup 启用高级功能后创建 DynamoDB 备份时，您可以使用： AWS Backup

- 跨区域复制备份
- 跨账户复制备份
- 更改将备份 AWS Backup 分层到冷存储的时间
- 标记备份

要对现有备份使用这些高级功能，请参阅编辑备份。

如果您稍后禁用 DynamoDB 的 AWS Backup 高级功能，则可以继续对您在启用高级功能期间创建的 DynamoDB 备份执行这些操作。

还原高级 DynamoDB 备份

您可以还原启用高级功能的 DynamoDB 备份，就像恢复启用高级功能之前拍摄 AWS Backup 的 DynamoDB 备份一样。 AWS Backup 您可以使用 DynamoDB AWS Backup 或 DynamoDB 执行恢复。

您可以使用以下选项指定如何加密新还原的表：

- 当还原到与原始表相同的区域时，您可以选择为还原的表指定加密密钥。如果您未指定加密密钥，则 AWS Backup 将使用与加密原始表相同的密钥自动加密已恢复的表。
- 当还原到与原始表不同的区域时，必须指定加密密钥。

要使用恢复 AWS Backup，请参阅还原 Amazon DynamoDB 表。

要使用 DynamoDB 进行还原，请参阅《Amazon DynamoDB 用户指南》中的从备份还原 DynamoDB 表。

删除高级 DynamoDB 备份

您无法在 DynamoDB 中删除使用这些高级功能创建的备份。必须使用 AWS Backup 删除备份才能在整个 AWS 环境中保持全局一致性。

要删除 DynamoDB 备份，请参阅删除备份。

启用高级 DynamoDB 备份时进行全面 AWS Backup 管理的其他优势

当你为 DynamoDB 启用 AWS Backup 高级功能时，你可以完全管理你的 DynamoDB 备份。 AWS Backup这样做会给您带来以下额外优势：

加密

AWS Backup 使用目标 AWS Backup 文件库的 KMS 密钥自动加密备份。以前，它们使用与源 DynamoDB 表相同的加密方法进行加密。这增加了可用于保护数据的防御措施的数量。请参阅对中的备份进行加密 AWS Backup了解更多信息。

Amazon 资源名称 (ARN)

每个备份 ARN 的服务命名空间都是 `awsbackup`。以前，服务命名空间是 `dynamodb`。换句话说，每个 ARN 的开头将从 `arn:aws:dynamodb` 变为 `arn:aws:backup`。请参阅《服务授权参考》中的AWS Backup的 ARN。

通过这项更改，您或您的备份管理员可以使用 `awsbackup` 服务命名空间为备份创建现在适用于在启用高级功能后创建的 DynamoDB 备份的访问策略。使用 `awsbackup` 服务命名空间，还可以将策略应用于 AWS Backup进行的其他备份。请参阅访问控制了解更多信息。

账单上的费用位置

备份费用（包括存储、数据传输、恢复和提前删除）显示在账 AWS 单的 “Backup” 下。以前，费用显示在账单的 “DynamoDB” 下。

此更改可确保您可以使用 AWS Backup 账单来集中监控备份成本。请参阅计量、成本和计费了解更多信息。

Amazon Timestream 备份

Amazon Timestream 是一个可扩展的时间序列数据库，允许每天存储和分析多达数万亿个时间序列数据点。Timestream 经过优化，可将最新数据保存在内存中，并根据您的策略将历史数据存储在成本优化的存储层中，从而节省成本和时间。

Timestream 数据库包含表。这些表包含记录，而每条记录都是时间序列中的单个数据点。时间序列是按时间间隔记录的一系列记录，例如股票价格、Amazon EC2 实例的内存使用水平或温度读数。 AWS Backup 可以集中备份和恢复 Timestream 表。您可以将这些表备份复制到其他账户以及同一组织 AWS 区域 内的其他多个账户。

Timestream 目前不提供本机备份和恢复服务，因此使用 AWS Backup 创建 Timestream 表的安全副本可以为您的资源增加额外的安全性和弹性。

备份 Timestream 表

您可以通过 AWS Backup 控制台或使用来备份 Timestream 表。 AWS CLI

使用 AWS Backup 控制台备份 Timestream 表有两种方法：按需备份或作为备份计划的一部分。

创建按需 Timestream 备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 使用导航窗格选择受保护的资源，然后选择创建按需备份。
3. 在创建按需备份页面上，选择 Amazon Timestream。
4. 选择资源类型 Timestream，然后选择要备份的表名称。
5. 在“备份”窗口中，确保选中立即创建备份。这将立即启动备份，使您能够在受保护的资源页面上更快地看到您的集群。
6. 在转换为冷存储下拉菜单中，可以设置转换设置。
7. 在保留期中，您可以选择将备份保留多长时间。
8. 选择现有的备份保管库或创建新的备份保管库。选择新建备份保管库将打开用于创建保管库的新页面，然后在完成时返回到创建按需备份页面。

9. 在 IAM 角色下，选择 AWS Backup 默认角色（如果您的账户中不存在默认角色，则系统将使用正确的权限为您创建该角色）。
10. 或者，可以将标签添加到您的恢复点。如果您要将一个或多个标签分配到按需备份，请输入键和可选值，然后选择添加标签。
11. 选择创建按需备份。此操作将您转至作业页面，在其中可以看到作业的列表。
12. 选择集群的备份作业 ID 以查看该作业的详细信息。它将显示 `Completed`、`In Progress` 或 `Failed` 状态。您可以单击刷新按钮更新显示的状态。

在备份计划中创建 Timestream 计划备份

如果 Timestream 表是受保护的资源，则您的计划备份可以包括这些表。要选择保护 Amazon Timestream 表，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 使用导航窗格，选择受保护的资源。
3. 将 Amazon Timestream 切换为开启。
4. 请参阅为控制台分配资源以在现有计划或新计划中包含 Timestream 表。

在管理备份计划下，您可以选择创建备份计划并包含 Timestream 表，也可以更新现有计划以包含 Timestream 表。添加资源类型 Timestream 时，您可以选择添加所有 Timestream 表，也可以在选择特定的资源类型下选中要添加的表旁边的复选框。

对 Timestream 表所进行的第一个备份将是完整备份。后续备份将是增量备份。

创建或修改备份计划后，导航至左导航窗格中的“备份计划”。您指定的备份计划应该会在资源分配下显示您的集群。

以编程方式进行备份

您可以使用操作名称 `start-backup-job`。包括以下参数：

```
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region AWS ## \
```

```
--endpoint-url URL
```

查看 Timestream 表备份

要在控制台中查看和修改 Timestream 表备份，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 选择备份保管库。然后，单击包含您的 Timestream 表的备份保管库名称。
3. 备份保管库将显示摘要和备份列表。
   a. 您可以单击恢复点 ID 列中的链接，或者
   b. 您可以选中恢复点 ID 左侧的复选框，然后单击操作以删除不再需要的恢复点。

还原 Timestream 表

请参阅如何还原 Timestream 表

Amazon EC2 实例上的 SAP HANA 数据库备份

> **Note**
>
> 支持的服务由 AWS 区域包含目前支持的 Amazon EC2 实例上可用 SAP HANA 数据库备份的区域。

AWS Backup 支持在 Amazon EC2 实例上备份和恢复 SAP HANA 数据库。

主题

- 使用 SAP HANA 数据库概述 AWS Backup
- 通过以下方式备份 SAP HANA 数据库的先决条件 AWS Backup
- AWS Backup 控制台中的 SAP HANA 备份操作
- 查看 SAP HANA 数据库备份
- 用 AWS CLI 于 SAP HANA 数据库 AWS Backup
- 对 SAP HANA 数据库的备份进行故障排除
- 使用时的 SAP HANA 术语表 AWS Backup
- AWS Backup 在 EC2 实例上支持 SAP HANA 数据库发行说明

使用 SAP HANA 数据库概述 AWS Backup

除了能够创建备份和还原数据库外， AWS Backup 与 Amazon EC2 Systems Manager for SAP 集成还可帮助客户识别和标记 SAP HANA 数据库。

AWS Backup 已与 AWS Backint Agent 集成，用于执行 SAP HANA 备份和恢复。有关更多信息，请参阅 AWS Backint。

通过以下方式备份 SAP HANA 数据库的先决条件 AWS Backup

在执行备份和还原活动之前，必须满足以下几个先决条件。请注意，您需要对 SAP HANA 数据库具有管理访问权限，并且需要在 AWS 账户中创建新 IAM 角色和策略的权限才能执行这些步骤。

在 Amazon EC2 Systems Manager 完成这些先决条件。

1. 为运行 SAP HANA 数据库的 Amazon EC2 实例设置所需的权限
2. 在中注册凭证 AWS Secrets Manager
3. 安装 AWS Backint 和 AWS Systems Manager 适用于 SAP 代理
4. 验证 SSM Agent
5. 验证参数
6. 注册 SAP HANA 数据库

最好只注册每个 HANA 实例一次。多个注册可能导致同一个数据库有多个 ARN。维护单个 ARN 和注册可以简化备份计划的创建和维护，还可以帮助减少计划外的备份重复。

AWS Backup 控制台中的 SAP HANA 备份操作

设置这些先决条件和 SSM for SAP，即可备份和还原 EC2 上的 SAP HANA 数据库。

选择保护 SAP HANA 资源

AWS Backup 要用于保护您的 SAP HANA 数据库，必须将 SAP HANA 作为受保护的资源之一开启。要选择加入，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择设置。
3. 在选择加入服务下，选择配置资源。

4. 选择加入 Amazon EC2 上的 SAP HANA。
5. 单击确认。

现在，将启用 Amazon EC2 上 SAP HANA 的选择加入服务。

创建 SAP HANA 数据库的定时备份

您可以编辑现有备份计划并向其中添加 SAP HANA 资源，也可以仅为 SAP HANA 资源创建新的备份计划。

如果您选择创建新的备份计划，则有三个选项：

1. 选项 1：从模板开始
    1. 选择备份计划模板。
    2. 指定备份计划名称。
    3. 单击创建计划。
2. 选项 2：构建新计划
    1. 指定备份计划名称。
    2. （可选）指定要添加到备份计划的标签。
    3. 指定备份规则配置。
        a. 指定备份规则名称。
        b. 选择现有的保管库或创建新的备份保管库。这是存储备份的位置。
        c. 指定备份频率。
        d. 指定备份时段。

            请注意，当前不支持转换到冷存储。
        e. 指定保留期。

            当前不支持复制到目的地
        f. （可选）指定要添加到恢复点的标签。
    4. 单击创建计划。
3. 选项 3：使用 JSON 定义计划
    1. 通过修改现有备份计划的 JSON 表达式或创建新表达式，为您的备份计划指定 JSON。

2. 指定备份计划名称。
3. 单击验证 JSON。

成功创建备份计划后，可以在下一步中为备份计划分配资源。

无论使用哪种计划，都要确保分配资源。您可以选择要分配的 SAP HANA 数据库，包括系统数据库和租户数据库。还可以选择排除特定资源 ID。

创建 SAP HANA 数据库的按需备份

您可以创建完整的按需备份，该备份在创建后立即运行。请注意，Amazon EC2 实例上的 SAP HANA 数据库的按需备份是完整备份；不支持增量备份。

现在已创建按需备份。它将开始备份您的指定资源。控制台会将您转到备份作业页面，您可以在其中查看作业进度。请记下屏幕顶部蓝色横幅中的备份作业 ID，因为您需要它才能轻松找到备份作业的状态。备份完成后，状态将变为 `Completed`。备份可能需要几小时的时间。

刷新备份作业列表可查看状态变化。您也可以搜索并单击备份作业 ID 以查看详细作业状态。

持续备份 SAP HANA 数据库

您可以进行连续备份，这可以与 point-in-time 恢复 (PITR) 一起使用（请注意，按需备份会将资源保留在拍摄时的状态；而 PITR 使用连续备份来记录一段时间内的变化）。

使用连续备份，可以还原 EC2 实例上的 SAP HANA 数据库，方法是将其倒回您选择的特定时间，精确到 1 秒（最多回溯 35 天）。连续备份的工作原理是，首先创建资源的完整备份，然后不断备份资源的事务日志。PITR 恢复的工作原理是访问您的完整备份，然后将事务日志重放到您要求恢复的时间。AWS Backup

在 AWS Backup 使用 AWS Backup 控制台或 API 创建备份计划时，您可以选择连续备份。

使用控制台启用连续备份

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划，然后选择创建备份计划。
3. 在备份计划下，选择添加备份计划。
4. 在备份规则配置部分，选择为支持的资源启用连续备份。

禁用 SAP HANA 数据库备份的 PITR（point-in-time恢复）后，日志将继续发送到中， AWS Backup 直到恢复点到期（状态等于EXPIRED）。您可以更改到 SAP HANA 中的替代日志备份位置，以停止向 AWS Backup传输日志。

状态为的连续恢复点STOPPED表示连续恢复点已中断；也就是说，从 SAP HANA 传输到 AWS Backup 的显示数据库增量更改的日志存在间隔。在此时间范围间隙内出现的恢复点状态为 STOPPED.。

有关在连续备份（恢复点）的还原作业期间可能遇到的问题，请参阅本指南的 SAP HANA 还原故障排除部分。

查看 SAP HANA 数据库备份

查看备份和还原作业的状态：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择作业。
3. 选择备份作业、还原作业或复制作业以查看您的作业列表。
4. 搜索并单击作业 ID 以查看详细作业状态。

查看保管库中的所有恢复点：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 搜索并单击备份保管库以查看该保管库中的所有恢复点。

查看受保护资源的详细信息：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源。
3. 您也可以按资源类型进行筛选，以查看该资源类型的所有备份。

用 AWS CLI 于 SAP HANA 数据库 AWS Backup

备份控制台中的每个操作都有相应的 API 调用。

要以编程方式配置 AWS Backup 和管理其资源，请使用 API 调StartBackupJob用在 EC2 实例上备份 SAP HANA 数据库。

使用 `start-backup-job` 作为 CLI 命令。

对 SAP HANA 数据库的备份进行故障排除

如果您在工作流程中遇到错误，请查阅以下错误示例和建议的解决方案：

Python 必备

- 错误：自适用于 SAP 的 SSM 以来，Zypper 错误与 Python 版本有关，需要 AWS Backup Python 3.6 但是 SUSE 12 SP5 默认支持 Python 3.4。

  解决方案：通过执行以下步骤在 SUSE12 SP5 上安装多个版本的 Python：

  1. 运行 update-alternations 命令在 “/usr/local/bin/” 中为 Python 3 创建符号链接，而不是直接使用 “/usr/bin/python3”。此命令会将 Python 3.4 设置为默认版本。命令是：`# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.45`
  2. 通过运行以下命令将 Python 3.6 添加到备选配置中：`# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. 通过运行以下命令将替代配置更改为 Python 3.6：`# sudo update-alternatives –config python3`

     应显示以下输出：

     ```
     There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
      Selection Path Priority Status
     * 0 /usr/bin/python3.4 5 auto mode
      1 /usr/bin/python3.4 5 manual mode
      2 /usr/bin/python3.6 2 manual mode
     Press enter to keep the current choice[*], or type selection number:
     ```

  4. 输入与 Python 3.6 对应的数字。
  5. 检查 Python 版本并确认正在使用 Python 3.6。
  6. （可选，但建议使用）验证 Zypper 命令是否按预期运行。

适用于 SAP 发现和注册的 Amazon EC2 Systems Manager

- 错误：由于禁止访问和 SSM 的公共端点，SAP 版 SSM 无法发现工作负载。 AWS Secrets Manager

解决方案：测试您的 SAP HANA 数据库是否可以访问终端节点。如果无法访问它们，则可以为 SAP 创建 Amazon VPC 终端节点 AWS Secrets Manager ，为 SAP 创建 SSM。

1. 运行以下命令，测试从 AMAZON EC2 主机对 HANA 数据库的 Secrets Manager 的访问权限：`aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp`。如果该命令未能返回值，则防火墙将阻止对 Secrets Manager 服务端点的访问。日志将在 “从 Secrets Manager 中检索机密” 步骤停止。
2. 通过运行命令`aws ssm-sap list-registration`测试与 SSM for SAP 端点的连接。如果该命令未能返回值，则防火墙将阻止对 SSM for SAP 端点的访问。

   错误示例:`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application".`

如果无法访问端点，则有两个选项可以继续。

- 打开防火墙端口以允许访问 Secrets Manager 的公共服务端点和适用于 SAP 的 SSM；或者，
- 为 Secrets Manager 创建 VPC 终端节点，为 SAP 创建 SSM，然后：
  - 确保已为 DNSSupport 和 dnsHostName 启用亚马逊 VPC。
  - 确保您的 VPC 终端节点已启用允许私有 DNS 名称。
  - 如果 SSM for SAP 发现成功完成，则日志将显示已发现主机。

- 错误： AWS Backup 由于访问 AWS Backup 服务公共端点受阻，Backint 连接失败。 `aws-backint-agent.log`可以显示类似于以下内容的错误：`time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id"`或`level=fatal msg="Error performing backup missing backup data plane Id`。此外， AWS Backup 控制台可以显示 `Fatal Error: An internal error occured.`

  解决方案：如果无法访问端点，则有两个选项可以继续：

  - 打开防火墙端口以允许访问公共服务端点 (HTTPS)。使用此选项后，DNS 将通过公有 IP 地址解析对 AWS 服务的请求。
  - 创建 VPC 终端节点以私密方式路由往 AWS 返所需服务的流量 AWS Backup。使用此选项后，DNS 将通过私有 IP 地址解析对这些服务的请求。此选项可能需要更新 DNS 服务器，以添加将请求转发到私有终端节点的规则。

- 错误：由于 HANA 密码包含特殊字符，SAP 的 SSM 注册失败。示例错误可能包括使用`Error connecting to database HBX/HBX when validating its credentials.hdbsql`或

测试连接`Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.`之后，`tenantdb`该连接已通过 HANA 数据库 Amazon EC2 实例进行测试。`systemdb`

在 AWS Backup控制台的 “作业” 页面中，备份任务详细信息可以显示错误`FAILED`的状态`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`。

解决方案：确保您的密码中没有特殊字符，例如 $。

- 错误：**`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  解决方案：适用于 SAP HANA 的 AWS BackInt 代理安装可能未成功完成。重试在 SAP 应用程序服务器上部署 AWS Backint Agent 和 Amazon EC2 Systems Manager 代理的过程。
- 错误：注册后，控制台与日志文件不匹配。

  尽管适用于 SAP 的 SAP Application Manager 的 SSM for SAP Application Manager for SAP 控制台显示注册成功，但发现日志显示在尝试连接 HANA 数据库时注册失败。它无法确认注册成功。如果控制台显示注册成功，但日志显示未成功，则备份将失败。

  确认注册状态：

  1. 登录 SSM 控制台
  2. 从左侧导航栏中选择 “运行命令”。
  3. 在文本字段命令历史记录下输入`Instance ID:Equal:`，其值等于您用于注册的实例。这将筛选命令历史记录。
  4. 使用命令 ID 列查找带有状态的命令`Failed`。然后，找到 AWSSystemsManagerSAP-Discovery 的文档名称。
  5. 在中 AWS CLI，运行命令`aws ssm-sap register-application status`。如果显示返回值`Error`，则表示注册失败。

  解决方案：确保您的 HANA 密码中没有特殊字符（例如 '$'）。

创建 SAP HANA 数据库的备份

- 错误：创建 AWS Backup SystemDB 或 TenantDB 的按需备份时，控制台会显示 “致命错误” 消息。之所以发生这种情况，是因为无法访问公共端点 cell-1.prod.us-west-west-2.storage.cryo.aws.a2z.com。这是由阻止访问此端点的客户端防火墙造成的。

aws-backint-agent.log可以显示错误，例如level=error msg="Storage configuration validation failed: missing backup data plane Id"或 level=fatal msg="Error performing backup missing backup data plane Id."

解决方案：打开对公共端点的防火墙访问权限 c ell-1.prod.us-west- 2.storage.cryo.aws.a2z.com。

- 错误：Database cannot be backed up while it is stopped。

  解决方案：确保要备份的数据库处于活动状态。只有在数据库处于在线状态时，才能备份数据库数据和日志。

- 错误：Getting backup metadata failed. Check the SSM document execution for more details.

  解决方案：确保要备份的数据库处于活动状态。只有在数据库处于在线状态时，才能备份数据库数据和日志。

监控备份日志

- 错误：Encountered an issue with log backups, please check SAP HANA for details.

  解决方案：检查 SAP HANA，确保日志备份是 AWS Backup 从 SAP HANA 发送到的。

- 错误：One or more log backup attempts failed for recovery point.

  解决方案：有关详细信息，请检查 SAP HANA。确保 AWS Backup 从 SAP HANA 向发送日志备份。

- 错误：Unable to determine the status of log backups for recovery point.

  解决方案：有关详细信息，请检查 SAP HANA。确保 AWS Backup 从 SAP HANA 向发送日志备份。

- 错误：Log backups for recovery point %s were interrupted due to a restore operation on the database.

  解决方案：等待还原任务完成。日志备份应该会恢复。

使用时的 SAP HANA 术语表 AWS Backup

数据备份类型：SAP HANA 支持两种类型的数据备份：完整备份和 INC（增量）备份。 AWS Backup 优化了每次备份操作期间使用的类型。

目录备份：SAP HANA 维护自己的名为目录的清单。 AWS Backup 与这个目录互动。每个新备份都会在该目录中创建一个条目。

连续日志备份（事务日志）：对于时间点故障恢复 (PITR) 功能，SAP HANA 会跟踪自最近一次备份以来的所有事务。

系统复制：一种还原作业，其中的还原目标数据库与创建恢复点的源数据库不同。

破坏性还原：破坏性还原是一种还原作业，在此期间，还原的数据库会删除或覆盖源数据库或现有数据库。

FULL：完整备份是指备份整个数据库。

INC：增量备份是指备份自上次备份以来对 SAP HANA 数据库进行的所有更改。

有关其他详细信息，请参阅 AWS 术语表。

AWS Backup 在 EC2 实例上支持 SAP HANA 数据库发行说明

当前不支持某些功能：

- 当前不支持跨账户和跨区域复制。
- 当前不支持 Backup Audit Manager 和报告。
- 支持的服务由 AWS 区域包含目前支持 Amazon EC2 实例上的 SAP HANA 数据库备份区域。

Amazon Redshift 备份

Amazon Redshift 是一个完全托管的可扩展云数据仓库，可通过快速、简单且安全的分析，使您更快地获得见解。您可以使用不可变 AWS Backup 的备份、单独的访问策略以及对备份和还原作业的集中组织管理来保护您的数据仓库。

Amazon Redshift 数据仓库是一组名为节点的计算资源，这些资源被组织成一个名为集群的组。 AWS Backup 可以备份这些集群。

有关 Amazon Redshift 的信息，请参阅 Amazon Redshift 入门指南、Amazon Redshift 数据库开发人员指南和 Amazon Redshift 集群管理指南。

备份 Amazon Redshift 预置集群

您可以使用 AWS Backup 控制台保护您的 Amazon Redshift 集群，也可以使用 API 或 CLI 以编程方式保护。这些集群可以作为备份计划的一部分定期备份，也可以根据需要通过按需备份进行备份。

您可以还原单个表（也称为项目级还原），也可以还原整个集群。请注意，表不能自行备份；需在备份集群时将表作为集群的一部分进行备份。

使用 AWS Backup 允许您以集中方式查看您的资源；但是，如果 Amazon Redshift 是您使用的唯一资源，则可以继续使用 Amazon Redshift 中的自动快照计划程序。请注意，如果您选择通过管理手动快照设置，则无法继续使用 Amazon Redshift 管理这些设置。 AWS Backup

您可以通过 AWS Backup 控制台或使用来备份 Amazon Redshift 集群。 AWS CLI

使用 AWS Backup 控制台备份 Amazon Redshift 集群有两种方法：按需备份或作为备份计划的一部分。

创建按需 Amazon Redshift 备份

有关更多信息，请参阅创建按需备份类型页面。

要创建手动快照，请在创建包含 Amazon Redshift 资源的备份计划时取消选中持续备份复选框。

在备份计划中创建 Amazon Redshift 计划备份

如果 Amazon Redshift 集群是受保护的资源，则您的计划备份可以包括这些集群。要选择保护 Amazon Redshift 集群，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 使用导航窗格，选择受保护的资源。
3. 将 Amazon Redshift 切换为开启。
4. 请参阅为控制台分配资源以在现有计划或新计划中包含 Amazon Redshift 集群。

在管理备份计划下，您可以选择创建备份计划并包含 Amazon Redshift 集群，也可以更新现有计划以包含 Amazon Redshift 集群。添加资源类型 Amazon Redshift 时，您可以选择添加所有 Amazon Redshift 集群，也可以选中集群旁边的复选框。

以编程方式进行备份

您也可以在 JSON 文档中定义备份计划并使用 AWS Backup 控制台或提供该计划 AWS CLI。有关如何以编程方式创建备份计划的信息，请参阅使用 JSON 文档和 AWS Backup CLI 创建备份计划。

您可以使用 API 执行以下操作：

- 启动备份作业
- 描述备份作业
- 获取恢复点元数据
- 按资源列出恢复点
- 列出恢复点的标签

查看 Amazon Redshift 集群备份

要在控制台中查看和修改 Amazon Redshift 集群备份，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 选择备份保管库。然后，单击包含您的 Amazon Redshift 集群的备份保管库名称。
3. 备份保管库将显示摘要和备份列表。您可以单击恢复点 ID 列中的链接。
4. 要删除一个或多个恢复点，请选中要删除的复选框。在操作按钮下，可以选择删除。

还原 Amazon Redshift 集群

有关更多信息，请参阅如何还原 Amazon Redshift 集群。

亚马逊 Relation Database Service 备份

亚马逊 RDS 和 AWS Backup

在考虑备份 Amazon RDS 实例和集群的选项时，务必明确要创建和使用哪种备份。包括 Amazon RDS 在内的多种 AWS 资源都提供了自己的原生备份解决方案。

Amazon RDS 提供了自动备份和手动备份的选项。在 Amazon RDS 术语中 AWS Backup，由创建的所有恢复点（包括备份计划中的恢复点）都考虑手动备份。

当您使用 AWS Backup 创建 Amazon RDS 实例的备份（恢复点）时， AWS Backup 会检查您之前是否使用 Amazon RDS 创建过自动备份。如果存在自动备份，则 AWS Backup 创建此快照的副本（`copy-db-snapshot`操作）。如果不存在现存的备份，则 AWS Backup 创建您指定的实例的快照，而不是副本（`create-db-snapshot`操作）。

通过 AWS Backup任一操作创建的第一个快照都将生成 1 个完整快照。只要存在完整备份，其所有后续副本都将是增量备份。

> **Important**
>
> 当 AWS Backup 备份计划计划为一个 Amazon RDS 实例创建多个每日快照时，当其中一个计划的 “AWS Backup 开始备份” 窗口与 Amazon RDS 备份窗口相吻合时，备份的数据谱系可能会分支到不相同的备份，从而创建计划外且相互冲突的备份。为防止出现这种情况，请确保您的 AWS Backup 备份计划或 Amazon RDS 窗口的时间不一致。

Amazon RDS 持续备份和时间点恢复

持续备份包括使用 AWS Backup 创建您的 Amazon RDS 资源的完整备份，然后通过事务日志捕获所有更改。通过回放到想要恢复的时间点，而不是选择以前按固定时间间隔拍摄的快照，可以获得更高的粒度。

有关更多信息，请参阅持续备份和 PITR 支持的服务以及管理连续备份设置。

Amazon RDS 多可用区备份

AWS Backup 备份并支持 Amazon RDS for MySQL 和 PostgreSQL 多可用区（可用区）部署选项，包括一个主数据库实例和两个可读备用数据库实例。

多可用区备份在以下区域可用：亚太地区（悉尼）区域、亚太地区（东京）区域、欧洲地区（爱尔兰）区域、美国东部（俄亥俄州）区域、美国西部（俄勒冈州）区域、欧洲地区（斯德哥尔摩）区域、亚太地区（新加坡）区域、美国东部（弗吉尼亚州北部）区域和欧洲地区（法兰克福）区域。

多可用区部署选项可优化写入事务，当您的工作负载需要额外的读取容量、更低的写入事务延迟、更高的网络抖动（这会影响写入事务延迟的一致性）弹性以及高可用性和持久性时，它是理想的选择。

要创建多可用区集群，您可以选择 MySQL 或 PostgreSQL 作为引擎类型。

在 AWS Backup 控制台中，有三个部署选项：

- 多可用区数据库集群：创建包含一个主数据库实例和两个可读备用数据库实例的数据库集群，每个数据库实例均位于不同的可用区。为服务器就绪型工作负载提供高可用性、数据冗余并增加容量。
- 多可用区数据库实例：创建一个主数据库实例并在不同可用区中创建一个备用数据库实例。这提供了高可用性和数据冗余，但备用数据库实例不支持读取工作负载的连接。
- 单个数据库实例：创建单个数据库实例，没有备用数据库实例。

要为 Amazon RDS 创建备份，请参阅创建备份中的作为备份计划的一部分计划备份或创建按需备份。

> **Note**
>
> 时间点故障恢复 (PITR) 可以支持实例，但不支持集群。
> 不支持复制多可用区数据库集群快照。

多可用区集群和 RDS 实例之间的区别

单个可用区或两个可用区中的备份是 RDS 实例；使用三个或更多实例进行部署和备份是集群，类似于 Amazon Aurora、Amazon Neptune 和 Amazon DocumentDB 集群。

ARN（Amazon 资源名称）的呈现方式会有所不同，具体取决于使用的是实例还是集群：

一个 RDS 实例 ARN：`arn:aws:rds:region: account:db:name`

一个 RDS 多可用集群：`arn:aws:rds:region:account :cluster:name`

有关更多信息，请参阅《Amazon RDS 用户指南》中的多可用区数据库集群部署。

有关如何创建多可用区数据库集群快照的更多信息，请参阅《Amazon RDS 用户指南》。

AWS CloudFormation 堆栈备份

CloudFormation 堆栈由多个有状态和无状态资源组成，您可以将这些资源作为一个单元进行备份。换句话说，您可以通过备份堆栈和还原其中的资源来备份和还原包含多个资源的应用程序。堆栈中的所有资源均由堆栈的 AWS CloudFormation 模板定义。

备份堆 CloudFormation 栈时，会为该 CloudFormation 模板以及堆栈 AWS Backup 中支持的每个其他资源创建恢复点。这些恢复点一起分组在一个称为复合的总体恢复点中。

此复合恢复点无法还原，但嵌套恢复点可以还原。您可以使用控制台或 AWS CLI还原复合备份中的一个或所有嵌套备份。

CloudFormation 应用程序堆栈术语

- 复合恢复点：用于将嵌套恢复点以及其他元数据分组在一起的恢复点。
- 嵌套恢复点：资源的恢复点，该资源属于 CloudFormation 堆栈并作为复合恢复点的一部分进行备份。每个嵌套恢复点都属于一个复合恢复点的堆栈。
- 复合作业：堆栈的备份、复制或还原作业，可以触发 CloudFormation堆栈中单个资源的其他备份作业。

- 嵌套作业： AWS CloudFormation 堆栈内资源的备份、复制或还原作业。

CloudFormation 堆栈备份作业

创建备份的过程称为备份作业。堆 CloudFormation 栈备份任务有状态。当备份作业完成时，其状态为 Completed。这表示已创建 AWS CloudFormation 恢复点（备份）。

CloudFormation 堆栈可以使用控制台进行备份，也可以通过编程方式进行备份。要备份任何资源，包括 CloudFormation 堆栈，请参阅本AWS Backup 开发人员指南其他地方的创建备份。

CloudFormation 可以使用 API 命令StartBackupJob备份堆栈。请注意，文档和控制台指的是复合恢复点和嵌套恢复点；API 语言在相同的上下文关系中使用的是术语“父恢复点和子恢复点”。

CloudFormation 堆栈包含所有 AWS 资源，均由您的CloudFormation 模板指示。请注意，您的模板可能包含 AWS Backup尚不支持的资源。如果您的模板包含 AWS 支持的资源和不支持的资源的组合，则仍 AWS Backup 会将模板备份到复合堆栈中，但是 Backup 只会创建备份支持的服务的恢复点。CloudFormation 模板中包含的所有资源类型都将包含在备份中，即使您尚未选择使用特定服务（在控制台设置中将服务切换为 “已启用”）。 AWS Backup 支持的嵌套备份（恢复点）可以还原，但嵌套堆栈无法备份或还原。

AWS CloudFormation 恢复点

恢复点状态

当堆栈的备份作业完成（作业状态为 Completed）后，则表示已创建该堆栈的备份。此备份也称为复合恢复点。复合恢复点可以具有以下状态之一：Completed、Failed 或 Partial。请注意，备份作业有状态，恢复点（也称为备份）也有单独的状态。

备份任务完成意味着您的整个堆栈和其中的资源都受到保护 AWS Backup。失败状态表示备份作业不成功；导致失败的问题得到纠正后，应重新创建备份。

Partial 状态表示并非堆栈中的所有资源都已备份。如果 CloudFormation 模板包含当前不支持的资源，则可能会发生这种情况 AWS Backup，或者如果属于堆栈内资源（嵌套资源）的一个或多个备份任务的状态不是，则可能会发生这种情况。Completed您可以手动创建按需备份，以重新运行任何导致非 Completed 状态的资源。如果您预期堆栈的状态为 Completed，但它却被标记为 Partial，请检查您的堆栈是否符合上述条件之一。

复合恢复点中的每个嵌套资源都有自己的单独恢复点，每个恢复点都有自己的状态（Completed 或 Failed）。状态为 Completed 的嵌套恢复点可以还原。

管理恢复点

可以复制复合恢复点（备份）；可以复制、删除、取消关联或还原嵌套恢复点。包含嵌套备份的复合恢复点无法删除。在复合恢复点中的嵌套恢复点已删除或解除关联后，您可以手动删除复合恢复点，也可以保留它，直到备份计划生命周期将其删除。

删除恢复点

您可以使用 AWS Backup 控制台或使用删除恢复点 AWS CLI。

要使用 AWS Backup 控制台删除恢复点，

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 单击左导航栏中的受保护的资源。在文本框中，键入`CloudFormation`以仅显示您的CloudFormation堆栈。
3. 复合恢复点将显示在恢复点窗格中。可以单击每个恢复点 ID 左侧的加号 (+) 展开每个复合恢复点，显示复合恢复点中包含的所有嵌套恢复点。您可以选中任何恢复点左侧的复选框，将其包含在要删除的恢复点选择中。
4. 单击删除按钮。

当您使用控制台删除一个或多个复合恢复点时，将弹出一个警告框。此警告框要求您确认删除复合恢复点的意图，包括复合堆栈中的嵌套恢复点。

要使用 API 删除恢复点，请使用 `DeleteRecoveryPoint` 命令。

将 API 与一起使用时， AWS Command Line Interface 必须先删除所有嵌套的恢复点，然后才能删除复合点。如果您通过发送 API 请求删除其中仍包含嵌套恢复点的复合堆栈备份（恢复点），则该请求将返回错误。

取消嵌套恢复点与复合恢复点的关联

您可以取消嵌套恢复点与复合恢复点的关联（例如，您希望保留嵌套恢复点但删除复合恢复点）。此时两个恢复点都将保留，但它们将不再联系在一起；也就是说，在取消关联后，在复合恢复点上发生的操作将不再应用于嵌套恢复点。

您可以使用控制台取消恢复点的关联，也可以调用 API `DisassociateRecoveryPointFromParent`。[请注意，API 调用使用“父级”一词来指代复合恢复点。]

复制恢复点

您可以复制复合恢复点，也可以复制嵌套恢复点（如果资源支持跨账户和跨区域复制）。

要使用 AWS Backup 控制台复制恢复点，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 单击左导航栏中的受保护的资源。在文本框中，键入`CloudFormation`以仅显示您的CloudFormation堆栈。
3. 复合恢复点将显示在恢复点窗格中。可以单击每个恢复点 ID 左侧的加号 (+) 展开每个复合恢复点，显示复合恢复点中包含的所有嵌套恢复点。您可以单击任何恢复点左侧的辐射状圆形按钮进行复制。
4. 选中后，单击窗格右上角的复制按钮。

复制复合恢复点时，不支持复制功能的嵌套恢复点最终不会出现在复制的堆栈中。复合恢复点的状态将为 `Partial`。

常见问题

1. “应用程序备份中包含什么？”

   作为使用定义的应用程序的每次备份的一部分 CloudFormation，都会备份模板、模板中每个参数的处理值以及支持的 AWS Backup 嵌套资源。嵌套资源的备份方式与备份不属于 CloudFormation 堆栈的单个资源的方法相同。请注意，标记为 `no-echo` 的参数的值不会被备份。

2. “我可以备份嵌套 AWS CloudFormation 堆栈的堆栈吗？”

   是。包含嵌套 CloudFormation 堆栈的堆栈可以放在备份中。

3. “*`Partial`* 状态是否意味着创建备份失败？”

   不是。“部分”这一状态表示有些恢复点已备份，而有些则未备份。如果您预期得到 `Completed` 备份结果，可以检查以下三种情况：

   a. 您的 CloudFormation 堆栈是否包含当前不支持的 AWS Backup资源？ 有关支持的资源列表，请参阅我们的《开发人员指南》中的支持的 AWS 资源和第三方应用程序。

   b. 属于堆栈内资源的一个或多个备份作业未成功，必须重新运行该作业。

   c. 已删除嵌套恢复点或已取消它与复合恢复点的关联

4. “如何在 CloudFormation 堆栈备份中排除资源？”

   备份 CloudFormation 堆栈时，可以将资源排除在备份之外。在控制台中，在创建备份计划和更新备份计划的过程中，有一个分配资源步骤。在此步骤中，有一个资源选择部分。如果您选择包括特定的资源类型并已包含 CloudFormation为要备份的资源，则可以从选定的资源类型中排除特定的资源 ID。您还可以使用标签排除堆栈中的资源。

   使用 CLI，您可以：

   - `NotResources`在备份计划中，从 CloudFormation 堆栈中排除特定资源。
   - 使用 `StringNotLike`，通过标签排除项目。

5. “嵌套资源支持哪些类型的备份？”

   嵌套资源的备份可以是完整备份，也可以是增量备份，具体取决于这些资源支持哪种类型的备份。AWS Backup 有关更多信息，请参阅增量备份的工作原理。但是，请注意，Amazon S3 和 Amazon RDS 嵌套资源不支持 PITR（point-in-time 恢复）。

6. “作为 CloudFormation 堆栈一部分的变更集是否已备份？”

   不是。 更改集不会作为 CloudFormation 堆栈备份的一部分进行备份。

7. “ AWS CloudFormation 堆栈的状态对备份有何影响？”

   CloudFormation 堆栈的状态可能会影响备份。可以备份状态为 `COMPLETE` 的堆栈，例如状态 `CREATE_COMPLETE`、`ROLLBACK_COMPLETE`、`UPDATE_COMPLETE`、`UPDATE_ROLLBACK_COMPLETE`、`I` 或 `IMPORT_ROLLBACK_COMPLETE`。

   如果上传新模板失败且堆栈变为 `ROLLBACK_COMPLETE` 状态，则会备份新模板，但嵌套资源的备份将基于回滚的资源。

8. “应用程序堆栈生命周期与其他恢复点生命周期有何不同？”

   嵌套恢复点生命周期由它们所属的备份计划决定。复合恢复点由所有嵌套恢复点中最长的生命周期决定。当复合恢复点中剩下的最后一个嵌套恢复点被删除或取消关联时，复合恢复点也将被删除。

9. “如何将标签 CloudFormation 复制到恢复点？”

   是。这些标签将被复制到每个相应的嵌套恢复点。

10. “删除复合和嵌套恢复点（备份）时是否有一定的顺序？”

是。必须先删除某些备份，然后才能删除其他备份。只有先删除复合恢复点中的所有恢复点，然后才能删除包含嵌套恢复点的复合备份。复合恢复点不再包含嵌套恢复点后，便可以手动将其删除。否则，将根据其备份计划的生命周期将其删除。

还原堆栈中的应用程序

有关还原嵌套恢复点的信息，请参阅如何还原应用程序堆栈备份。

创建 Windows VSS 备份

使用 AWS Backup，您可以备份和恢复在 Amazon EC2 实例上运行的支持 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，则会为该应用程序 AWS Backup 创建一致的快照。

您可以执行一致的恢复，同时使用与保护其他 AWS 资源相同的托管备份服务。借助于 EC2 上的应用程序一致性 Windows 备份，您可以获得与传统备份工具相同的一致性设置和应用程序感知。

> **Note**
>
> AWS Backup 目前仅支持对在 Amazon EC2 上运行的资源进行应用程序一致性备份，特别是在备份场景中，可以通过将现有实例替换为通过备份创建的新实例来恢复应用程序数据。Windows VSS 备份并非支持所有实例类型或应用程序。

有关更多信息，请参阅 Amazon EC 2 用户指南中的创建 VSS 应用程序一致性快照。

要备份和还原运行 Amazon EC2 的支持 VSS 的 Windows 资源，请按照以下步骤完成所需的先决任务。有关说明，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的开始前的准备工作。

1. 在中下载、安装和配置 SSM 代理。 AWS Systems Manager这个步骤为必填项。有关说明，请参阅 S AWS ystems Manager 用户指南中的在 Windows 服务器的 Amazon EC2 实例上使用 SSM 代理。
2. 在进行 Windows VSS（卷影复制服务）备份之前，向 IAM 角色添加 IAM 策略并将该角色附加到 Amazon EC2 实例。有关说明，请参阅 A mazon EC2 用户指南中的为启用 VSS 的快照创建 IAM 角色。如需 IAM 策略示例，请参阅的托管策略 AWS Backup。
3. 下载并安装 VSS 组件到 Amazon EC2 实例上的 Windows

4. 在 AWS Backup以下位置启用 VSS：

   1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
   2. 在控制面板上，选择要创建的备份类型，要么创建按需备份，要么管理备份计划。提供您的备份类型所需的信息。
   3. 分配资源时，选择 EC2。当前仅对 EC2 实例支持 Windows VSS 备份。
   4. 在高级设置部分，选择 Windows VSS。这样，您将能够创建与应用程序保持一致的 Windows VSS 备份。
   5. 创建您的备份。

状态为 Completed 的备份作业并不能保证 VSS 部分成功；是否包含 VSS 是在尽力而为的基础上进行的。请继续执行以下步骤以确定备份具有应用程序一致性、崩溃一致性还是失败：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左导航栏的我的账户下，单击作业。
3. 状态为 Completed 表示应用程序一致性 (VSS) 作业成功。

   状态为 Completed with issues 表示 VSS 操作失败，因此只有崩溃一致性备份成功。此状态还将显示弹出框消息"Windows VSS Backup Job Error encountered, trying for regular backup"。

   如果备份不成功，则状态将为 Failed。
4. 要查看备份作业的其他详细信息，请单击单个作业。例如，详细信息可能显示为 Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation。

如果目标为非 Windows 或非 VSS 组件 Windows 且任务成功的 Windows，则启用 VSS 的备份在没有 VSS 的情况下将保持崩溃一致性。

不受支持的 Amazon EC2 实例

支持 VSS 的 Windows 备份不支持以下 Amazon EC2 实例类型，因为它们是小型实例，可能无法成功进行备份。

- t3.nano
- t3.micro

- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

亚马逊 EBS 和 AWS Backup

Amazon EBS 资源的备份过程与用于备份其他资源类型的步骤类似：

- 创建按需备份
- 创建计划备份

以下各节中说明了资源特定信息。

适用于冷存储的 Amazon EBS 归档层

EBS 是支持将备份转移到冷存储的资源之一。有关更多信息，请参阅 生命周期和存储层。

> **Note**
>
> 此功能不适用于中国（北京）、中国（宁夏）、 AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）区域。

Amazon EBS 多卷、崩溃一致性备份

默认情况下， AWS Backup 为连接到 Amazon EC2 实例的 Amazon EBS 卷创建故障一致性备份。崩溃一致性意味着连接到同一 Amazon EC2 实例的每个 Amazon EBS 卷的快照都是在完全相同的时刻拍摄的。您不再需要停止实例或在多个 Amazon EBS 卷之间进行协调以确保应用程序状态的崩溃一致性。

由于多卷、崩溃一致性快照是默认 AWS Backup 功能，因此您无需执行任何不同的操作即可使用此功能。您可以使用以下过程之一备份 Amazon EBS 卷：

用于创建 EBS 快照恢复点的角色将与该快照相关联。必须使用相同的角色来删除由其创建的恢复点或将其恢复点过渡到存档层。

亚马逊 EBS 快照锁和 AWS Backup

AWS Backup 如果快照锁定持续时间超过备份生命周期，则不能在恢复点生命周期中删除与 AWS Backup 托管 Amazon EC2 AMI 关联的已应用 Amazon EBS 快照锁定的托管 Amazon EBS 快照和快照。相反，这些恢复点的状态将为 EXPIRED。如果您选择先删除 Amazon EBS 快照锁，则可以手动删除这些恢复点。

还原 Amazon EBS 资源

要还原 Amazon EBS 卷，请按照还原 Amazon EBS 卷中的步骤操作。

将标签复制到备份

通常，会 AWS Backup 将标签从其保护的资源复制到您的恢复点。有关如何在还原期间复制标签的更多信息，请参阅在还原期间复制标签。

例如，当您备份 Amazon EC2 卷时，会将其组和单个资源标签 AWS Backup 复制到生成的快照中，但须遵守以下条件：

- 有关在备份中保存元数据标签所需的资源特定权限的列表，请参阅将标签分配给备份所需的权限。
- 最初与资源关联的标签和备份期间分配的标签将分配给存储在备份库中的恢复点，最多 50 个（这是一个 AWS 限制）。备份期间分配的标签优先，并且两组标签均按字母顺序进行复制。
- 除非先启用高级 DynamoDB 备份，否则 DynamoDB 不支持为备份分配标签。
- 附加到 Amazon EC2 实例的 Amazon EBS 卷是嵌套资源。附加到亚马逊 EC2 实例的 Amazon EBS 卷上的标签是嵌套标签。 AWS Backup 尽最大努力复制嵌套标签，但如果不成功，它将创建一个没有嵌套标签的备份并报告状态已完成。
- 当 Amazon EC2 备份创建映像恢复点和一组快照时，会将标签 AWS Backup 复制到生成的 AMI。AWS Backup 还会尽最大努力将标签从与 Amazon EC2 实例关联的卷复制到生成的快照中。

如果您将备份复制到另一个备 AWS Backup 份 AWS 区域，则会将原始备份的所有标签复制到目标 AWS 区域。

停止备份作业

您可以在启动备份任务 AWS Backup 后将其停止。当您执行此操作时，将不创建备份，但会保留备份作业记录，其状态为已中止。

使用 AWS Backup 控制台停止备份作业

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在左侧的导航窗格中，选择作业。
3. 选择要停止的备份作业。
4. 在备份作业详细信息窗格中，选择停止。

复制备份

对于大多数资源类型，您可以 AWS 区域 根据需要将备份复制到多个备份， AWS 账户 也可以将其作为定时备份计划的一部分自动复制。有关详细信息，请参阅the section called “按资源划分的功能可用性”。

对于受支持的大多数资源，还可以自动执行一系列跨账户和跨区域复制，但 Amazon RDS 和 Aurora 除外。对于 Amazon RDS 和 Aurora 快照， AWS Backup 仅支持自动执行跨账户或跨区域复制，具体取决于这些服务创建加密密钥的方式（不支持复制多可用区数据库集群快照）。

某些资源类型同时可以使用连续备份功能及跨区域和跨账户复制。对连续备份进行跨区域或跨账户复制时，复制的恢复点（备份）将变为快照（定期）备份。根据资源类型，快照可能是增量副本或完整副本。PITR（时间点还原）不适用于这些复制。

副本保留其源配置，包括创建日期和保留期。创建日期是指创建源的时间，而不是副本的创建时间。

注意：即使副本设置为永不过期，源配置也会覆盖其副本的过期设置；设置为永不过期的副本仍将保留其源的过期日期。

如果您希望备份副本永不过期，请将源备份设置为永不过期，或者将副本指定为在创建后 100 年过期。

内容

跨创建备份副本 AWS 区域

使用 AWS Backup，您可以按需将备份复制到多个 AWS 区域 备份，也可以将备份作为定时备份计划的一部分自动复制。如果您需要将备份存储在最接近生产数据的位置以满足业务连续性或合规性要求，则跨区域复制会特别有用。有关视频教程，请参阅管理备份的跨区域复制。

首次将备份复制到新 AWS 区域 备份时，会完整 AWS Backup 复制该备份。通常，如果某项服务支持增量备份，则该服务中该备份的后续副本 AWS 区域 将是增量备份。 AWS Backup 将使用目标保管库的客户托管密钥重新加密您的副本。

Amazon EBS 是一个例外，它指出，在复制操作期间更改快照的加密状态会生成完整（非增量）副本。

要求

- 大多数 AWS Backup支持的资源都支持跨区域备份。有关具体信息，请参阅按资源划分的功能可用性。
- 大多数 AWS 地区都支持跨区域备份。有关具体信息，请参阅功能可用性来自 AWS 区域。
- AWS Backup 不支持在冷层中存储跨区域副本。

特定资源的跨区域复制注意事项

Amazon RDS

您不能将一个选项组复制到另一个选项组 AWS 区域。如果尝试这样做，则可能会收到错误，例如 “快照需要具有以下选项的目标选项组：...”

创建 Amazon RDS 快照的新跨区域副本 AWS 区域 时，必须在目标中输入相同的选项组。

执行按需跨区域备份

按需复制现有备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 选择备份保管库。
3. 选择包含要复制的恢复点的保管库。
4. 在备份部分，选择要复制的恢复点。
5. 使用操作下拉按钮，选择复制。
6. 输入以下值：

复制到目的地

选择副本 AWS 区域 的目的地。对于每个副本，您可以将新的复制规则添加到新的目的地。

目的地备份保管库

选择副本的目的地备份保管库。

转换为冷存储

选择何时将备份副本转换为冷存储。转换为冷存储的备份必须在其中存储至少 90 天。在副本转换为冷存储后，无法更改此值。

要查看可以转换到冷存储的资源列表，请参阅按资源划分的功能可用性表的“转换到冷存储的生命周期”部分。对于其他资源，将忽略冷存储表达式。

保留期

选择它可指定副本在创建后多少天删除。此值必须比转换为冷存储值多 90 天。如果保留期为始终，将无限期保留您的副本。

IAM 角色

选择创建副本时 AWS Backup 将使用的 IAM 角色。该角色还必须 AWS Backup 列为可信实体，这样 AWS Backup 才能担任该角色。如果您选择 “默认”，但您的账户中没有 AWS Backup 默认角色，则系统将为您创建一个具有正确权限的角色。

7. 选择复制。

计划跨区域备份

您可以使用定时备份计划跨 AWS 区域复制备份。

使用定时备份计划复制备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在我的账户中，选择备份计划，然后选择创建备份计划。
3. 在创建备份计划页面上，选择构建新计划。
4. 对于备份计划名称，输入备份计划的名称。
5. 在备份规则配置部分，添加定义备份计划、备份时段和生命周期规则的备份规则。您稍后可以添加更多备份规则。

a. 对于备份规则名称，输入规则的名称。

b. 对于备份保管库，从列表中选择一个保管库。此备份的恢复点将保存在此保管库中。您可以创建新的备份保管库。

c. 对于备份频率，选择要进行备份的频率。

d. 对于支持 PITR 的服务，如果您需要此功能，请选择 “启用连续备份以进行 point-in-time 恢复 (PITR)”。有关支持 PITR 的服务列表，请参阅按资源划分的功能可用性表的该部分。

e. 对于备份时段，选择使用备份时段默认值 - 推荐。您可以自定义备份时段。

f. 对于复制到目的地，选择备份副本的目的地 AWS 区域 。您的备份将被复制到该区域。对于每个副本，您可以将新的复制规则添加到新的目的地。然后输入以下值：

复制到其他账户的保管库

请勿切换此选项。要了解有关跨账户复制的更多信息，请参阅跨账户创建备份副本 AWS 账户

目的地备份保管库

在目标区域中选择要复制备份的备份保管库。 AWS Backup

如果您希望为跨区域复制创建新的备份保管库，请选择新建备份保管库。在向导中输入信息。然后选择创建备份保管库。

6. 选择创建计划。

跨创建备份副本 AWS 账户

使用 AWS Backup，您可以按需备份多个 AWS 账户 ，也可以作为定时备份计划的一部分自动备份。如果您出于运营或安全原因想要将备份安全地复制到组织 AWS 账户 中的一个或多个账户，请使用跨账户备份。如果原始备份被无意中删除，则可以将备份从目的地账户复制到其源账户，然后开始还原。在执行此操作之前，您必须在 AWS Organizations 服务中拥有两个属于同一组织的账户。有关更多信息，请参阅《Organizations 用户指南》中的教程：创建和配置组织。

在目的地账户中，您必须创建备份保管库。然后，您可以分配客户托管密钥来加密目标账户中的备份，并分配基于资源的访问策略 AWS Backup 以允许访问您要复制的资源。在源账户中，如果您的资源使用客户托管密钥进行加密，则必须与目的地账户共享此客户托管密钥。然后，您可以创建备份计划并选择在 AWS Organizations中属于您的组织单位的目的地账户。

首次将备份复制到跨账户时，会完整 AWS Backup 复制备份。通常，如果某项服务支持增量备份，则同一账户中该备份的后续副本是增量备份。 AWS Backup 使用目标保管库的客户托管密钥重新加密您的副本。

要求

- 在管理多个 AWS 账户 中的资源之前 AWS Backup，您的账户必须属于 AWS Organizations 服务中的同一个组织。
- 支持的大多数资源都 AWS Backup 支持跨账户备份。有关具体信息，请参阅按资源划分的功能可用性。
- 大多数 AWS 地区都支持跨账户备份。有关具体信息，请参阅功能可用性来自 AWS 区域。
- AWS Backup 不支持将跨账户副本存储在冷层中。

设置跨账户备份

创建跨账户备份需要什么？

- 一个源账户

  源帐户是您的生产 AWS 资源和主备份所在的帐户。

  源账户用户发起跨账户备份操作。源账户用户或角色必须具有相应的 API 权限才能发起该操作。适当的权限可能是 AWS 托管策略`AWSBackupFullAccess`（允许对 AWS Backup 操作进行完全访问权限），也可以是允许执行诸如之类的操作的客户托管策略`ec2:ModifySnapshotAttribute`。有关策略类型的更多信息，请参阅 AWS Backup 托管策略。
- 一个目的地账户

  目的地账户是您要在其中保存备份副本的账户。您可以选择多个目的地账户。在 AWS Organizations 中，目的地账户必须与源账户位于同一个组织中。

  对于您的目的地备份保管库，您必须“允许”访问策略 `backup:CopyIntoBackupVault`。如果没有此策略，将拒绝向目的地账户进行复制的尝试。
- 中的管理账户 AWS Organizations

  管理账户是组织中的主账户，由 AWS Organizations定义，您可以使用它管理各 AWS 账户的跨账户备份。要使用跨账户备份，还必须启用服务信任。启用服务信任后，可以将组织中的任何账户用作目的地账户。在目的地账户中，可以选择使用哪些保管库进行跨账户备份。
- 在 AWS Backup 控制台中启用跨账户备份

有关安全的信息，请参阅跨账户备份的安全注意事项。

要使用跨账户备份，必须启用跨账户备份功能。然后，必须“允许”通过访问策略 backup:CopyIntoBackupVault 访问您的目的地备份保管库。

启用跨账户备份

1. 使用您的 AWS Organizations 管理账户凭据登录。只能使用这些凭证启用或禁用跨账户备份。
2. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
3. 在我的账户中，选择设置。
4. 对于跨账户备份，选择启用。
5. 在备份保管库中，选择目的地保管库。

   对于跨账户复制，源文件库和目标文件库位于不同的账户中。必要时切换到拥有目标账户的账户。
6. 在访问策略 部分，“允许”backup:CopyIntoBackupVault。例如，选择添加权限，然后选择允许从组织访问备份保管库。除此之外的任何跨账户操作都backup:CopyIntoBackupVault将被拒绝。
7. 现在，组织中的任何账户都可以与组织中的任何其他账户共享其备份保管库中的内容。有关更多信息，请参阅与其他 AWS 账户共享备份保管库。要限制哪些账户可以接收其他账户的备份保管库中的内容，请参阅将账户配置为目的地账户。

安排跨账户备份

您可以使用定时备份计划跨 AWS 账户复制备份。

使用定时备份计划复制备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在我的账户中，选择备份计划，然后选择创建备份计划。
3. 在创建备份计划页面上，选择构建新计划。
4. 对于备份计划名称，输入备份计划的名称。
5. 在备份规则配置部分，添加定义备份计划、备份时段和生命周期规则的备份规则。您稍后可以添加更多备份规则。

   对于规则名称，输入规则的名称。
6. 在计划部分的频率下，选择您希望备份的频率。

7. 对于备份时段，选择使用备份时段默认值（推荐）。您可以自定义备份时段。
8. 对于备份保管库，从列表中选择一个保管库。此备份的恢复点将保存在此保管库中。您可以创建新的备份保管库。
9. 在生成副本 - 可选部分，输入以下值：

   目的地区域

   选择备份副本 AWS 区域 的目的地。您的备份将被复制到该区域。对于每个副本，您可以将新的复制规则添加到新的目的地。

   复制到其他账户的保管库

   切换以选择此选项。选中后，此选项将变为蓝色。此时将显示外部保管库 ARN 选项。

   外部保管库 ARN

   输入目的地账户的 Amazon 资源名称 (ARN)。ARN 是一个包含账户 ID 及其 ID 的字符串。AWS 区域 AWS Backup 会将备份复制到目标账户的保管库。目的地区域列表会自动更新到外部保管库 ARN 中的区域。

   对于允许备份保管库访问权限中，选择允许。然后，在打开的向导中选择允许。

   AWS Backup 需要访问外部帐户的权限才能将备份复制到指定值。向导将显示以下策略示例，其中提供了此访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

转换为冷存储

选择将备份副本转换到冷存储的时间以及副本的到期（删除）时间。转换到冷存储的备份必须在冷存储中存储至少 90 天。在副本转换为冷存储后，无法更改此值。

要查看可以转换到冷存储的资源列表，请参阅按资源划分的功能可用性表的“转换到冷存储的生命周期”部分。对于其他资源，将忽略冷存储表达式。

过期指定副本在创建后多少天删除。此值必须比转换为冷存储值多 90 天。

> **Note**
>
> 当备份过期并作为生命周期策略的一部分标记为 AWS Backup 删除时，将在接下来的 8 小时内随机选择的时间点删除备份。此时段有助于确保一致的性能。

10. 选择添加到恢复点的标签以向恢复点添加标签。
11. 对于高级备份设置，选择 Windows VSS，为在 EC2 上运行的选定第三方软件启用应用程序感知快照。
12. 选择创建计划。

执行按需跨账户备份

您可以根据需要将备份复制到其他 AWS 账户 备份。

按需复制备份

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在我的账户中，选择备份保管库以查看列出的所有备份保管库。您可以按备份保管库名称或标签进行筛选。
3. 选择要复制的备份的恢复点 ID。
4. 选择复制。
5. 展开备份详细信息以查看有关您正在复制的恢复点的信息。
6. 在复制配置部分，从目的地区域列表中选择一个选项。
7. 选择复制到其他账户的保管库。选中后，此选项将变为蓝色。

8. 输入目的地账户的 Amazon 资源名称 (ARN)。ARN 是一个包含账户 ID 及其 ID 的字符串。 AWS 区域 AWS Backup 会将备份复制到目标账户的保管库。目的地区域列表会自动更新到外部保管库 ARN 中的区域。
9. 对于允许备份保管库访问权限中，选择允许。然后，在打开的向导中选择允许。

   要创建副本， AWS Backup 需要访问源账户的权限。向导将显示一个策略示例，其中提供了此访问权限。下面显示了此策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

10. 对于转换为冷存储，选择将备份副本转换到冷存储的时间以及副本的到期（删除）时间。转换到冷存储的备份必须在冷存储中存储至少 90 天。在副本转换为冷存储后，无法更改此值。

    要查看可以转换到冷存储的资源列表，请参阅按资源划分的功能可用性表的“转换到冷存储的生命周期”部分。对于其他资源，将忽略冷存储表达式。

    过期指定副本在创建后多少天删除。此值必须比转换为冷存储值多 90 天。
11. 对于 IAM 角色，指定有权复制您的备份的 IAM 角色（例如默认角色）。复制行为由目的地账户的服务关联角色执行。
12. 选择复制。根据要复制的资源的大小，此过程可能需要几个小时才能完成。复制作业完成后，您将在作业菜单的复制作业选项卡中看到该副本。

加密密钥和跨账户副本

跨账户副本加密密钥取决于资源类型。已全面 AWS Backup 管理使用源备份存储库加密密钥的资源。客户托管的 KMS 密钥可用于对这些资源类型进行跨账户副本加密。

未完全由管理的资源类型 AWS Backup 具有相同的源 KMS 密钥和资源 KMS 密钥。对于这些未完全 AWS 由管理的资源类型，不支持使用托管 KMS 密钥进行 AWS Backup跨账户复制。

有关解决跨账户复制失败的其他帮助，请参阅AWS 知识中心。

在跨账户复制期间，源账户 KMS 密钥策略必须允许目标账户使用 KMS 密钥策略。

将备份从一个恢复 AWS 账户 到另一个备份

AWS Backup 不支持从一个资源恢复 AWS 账户 到另一个资源。但是，您可以将备份从一个账户复制到另一个账户，然后在该账户中进行还原。例如，您无法将账户 A 中的备份还原到账户 B，但可以将账户 A 中的备份复制到账户 B，然后在账户 B 中还原备份。

将备份从一个账户还原到另一个账户分为两步。

将备份从一个账户还原到另一个账户

1. 将备份从源文件复制 AWS 账户 到您要还原到的帐户。有关说明，请参阅设置跨账户备份。
2. 使用与您的资源对应的说明来还原备份。

与其他 AWS 账户共享备份保管库

AWS Backup 允许您与一个或多个账户共享备份保管库，或者与您的整个组织共享备份保管库 AWS Organizations。您可以与源 AWS 账户、用户或 IAM 角色共享目的地备份保管库。

共享目的地备份保管库

1. 选择 AWS Backup，然后选择备份保管库。
2. 选择要共享的备份保管库的名称。
3. 在访问策略窗格中，选择添加权限下拉列表。
4. 选择允许备份保管库的账户级别访问权限。或者，您可以选择允许组织级别或角色级别访问权限。
5. 输入要与此目的地备份保管库共享的账户的 AccountID。
6. 选择保存策略。

您可以使用 IAM 策略共享您的备份保管库。

与 AWS 账户 或 IAM 角色共享目的地备份保管库

以下策略与账号 4444555566666 和账号 111122223333 中的 IAM 角色 SomeRole 共享备份保管库。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

将目标备份存储库与组织单位共享 AWS Organizations

以下策略使用 PrincipalOrgPaths 与组织单位共享备份保管库。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
```

```
}
```

与中的组织共享目标备份保管库 AWS Organizations

以下策略与 `PrincipalOrgID` 为“o-a1b2c3d4e5”的组织共享备份保管库。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

将账户配置为目的地账户

当您首次使用 AWS Organizations 管理账户启用跨账户备份时，任何成员账户的用户都可以将其账户配置为目标账户。我们建议在 AWS Organizations 中设置一个或多个服务控制策略 (SCP)，以限制您的目的地账户。要了解有关将服务控制策略附加到 AWS Organizations 节点的更多信息，请参阅附加和分离服务控制策略。

使用标签限制目的地账户

当关联到 AWS Organizations 根账户、OU 账户或个人账户时，此策略将来自该根、OU 或账户的复制目标限制为仅限那些带有您标记`DestinationBackupVault`的备份保管库的账户。权限 `"backup:CopyIntoBackupVault"` 控制备份保管库的行为方式，在此例中还控制哪些目的地备份保管库有效。使用此策略以及应用于已批准的目的地保管库的相应标签，可以控制跨账户复制的目的地仅为已批准的账户和备份保管库。

```
{
```

```
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

使用账号和保管库名称限制目的地账户

当关联到 AWS Organizations 根账户、OU 账户或个人账户时，此政策将来自该根账户、OU 或账户的副本限制为仅限两个目标账户。权限 "backup:CopyFromBackupVault" 控制备份保管库中恢复点的行为方式，在此例中还控制您可以将该恢复点复制到的目的地。只有当一个或多个目的地备份保管库名称以 cab- 开头时，源保管库才允许将副本复制到第一个目的地账户 (112233445566)。只有当目的地是单个名为 fort-knox 的备份保管库时，源保管库才允许将副本复制到第二个目的地账户 (123456789012)。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
      }
    }
  ]
}
```

使用中的组织单位限制目标帐户 AWS Organizations

当关联到包含您的源账户的 AWS Organizations 根账户或 OU 时，或者关联到您的源账户时，以下策略将目标账户限制为两个指定 OU 中的账户。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

跨账户备份的安全注意事项

在 AWS Backup中执行跨账户备份时，请注意以下事项：

- 目的地保管库不能是默认保管库。这是因为默认保管库使用无法与其他账户共享的密钥进行加密。
- 禁用跨账户备份后，跨账户备份可能仍会持续长达 15 分钟。这是因为最终一致性造成的，即使在您禁用跨账户备份后，也可能会有某些跨账户作业开始或完成。
- 如果目的地账户稍后离开组织，则该账户将保留备份。为避免出现潜在数据泄露，请在附加到目的地账户的服务控制策略 (SCP) 中对 `organizations:LeaveOrganization` 权限设置拒绝权限。有关 SCP 的详细信息，请参阅《Organizations 用户指南》中的从组织中删除成员账户。
- 如果您在跨账户复制过程中删除了复印作业角色，则 AWS Backup 无法在复印任务完成时取消源账户的快照共享。在这种情况下，备份作业完成，但复制作业状态显示为无法取消共享快照。

删除备份

我们建议您在创建备份计划时通过配置生命周期来自动删除不再需要的备份。 AWS Backup 例如，如果您将备份计划的生命周期设置为将恢复点保留一年，则 AWS Backup 将在2022年1月1日自动删除其在2021年1月1日或之后的几个小时内创建的恢复点。（在恢复点到期后 8 小时内对其删除内容进行 AWS Backup 随机排序，以保持性能。）要了解有关配置生命周期保留策略的更多信息，请参阅创建备份计划。

但是，您可能希望手动删除一个或多个恢复点。例如：

- 您有 EXPIRED 恢复点。这些恢复点 AWS Backup 无法自动删除，因为您删除或修改了用于创建备份计划的原始 IAM 策略。当 AWS Backup 试图删除它们时，它没有权限这样做。

  如果 AWS 托管的 Amazon EBS 或 Amazon EC2 恢复点应用了 Amazon EBS 快照锁，但无法完成通常会导致恢复点被删除的生命周期过程，也可能会创建过期的恢复点。 AWS Backup 请注意，这些过期的恢复点可以从 Amazon EC2 控制台和 API 或 Amazon EBS 控制台和 API 中还原。

  > **Warning**
  >
  > 此时过期的恢复点将继续存储在您的账户中。这可能会增加存储成本。

  2021 年 8 月 6 日之后， AWS Backup 将在其备份保管库中将目标恢复点显示为 “已过期”。您可以将鼠标悬停在红色的已过期状态上以显示弹出框状态消息，该消息会解释为什么它无法删除备份。您也可以选择刷新以接收最新信息。
- 您不再希望备份计划按照您配置的方式运行。更新备份计划会影响它未来将会创建的恢复点，但不会影响它已经创建的恢复点。要了解更多信息，请参阅更新备份计划。
- 您需要在完成测试或教程后进行清理。

手动删除备份

手动删除恢复点

1. 在 AWS Backup 控制台的导航窗格中，选择 Backup Vaul ts。
2. 在备份保管库页面上，选择用于存储备份的备份保管库。
3. 选择恢复点，选择操作下拉列表，然后选择删除。
4. 1. 如果您的列表包含连续备份，请选择以下选项之一。每个连续备份都有一个恢复点。

- 永久删除我的备份数据或删除恢复点。通过选择其中一个选项，可以停止未来的连续备份，还可以删除现有的连续备份数据。

  > **Note**
  >
  > 连续备份和 point-in-time 恢复 (PITR)有关 Amazon S3、Amazon RDS 和 Aurora 持续备份注意事项，请参阅。

- 保留我的连续备份数据或取消关联恢复点。通过选择其中一个选项，可以停止未来的连续备份，但是会保留现有的连续备份数据，直到它到期为止，具体取决于您的保留期。

  已取消关联的 Amazon S3 持续恢复点（备份）将保留在其备份库中，但其状态将转换为`STOPPED`。

2. 要删除列出的所有恢复点，请键入 delete，然后选择删除恢复点。
3. AWS Backup 开始提交要删除的恢复点并显示进度条。请保持浏览器选项卡处于打开状态，在提交过程中不要离开此页面。
4. 在提交过程结束时，会在横幅中 AWS Backup 显示一个状态。状态可以为：
   - 已成功提交。您可以选择对每个恢复点的删除状态查看进度。
   - 未能提交。您可以选择对每个恢复点的删除状态查看进度或者重试提交。
   - 混合结果，有些恢复点成功提交，而其他恢复点未能提交。
5. 如果选择查看进度，则可以查看每个备份的删除状态。如果删除状态为失败或已过期，则可以单击该状态查看原因。您也可以选择重试失败的删除。

手动删除故障排除

在极少数情况下， AWS Backup 可能无法完成您的删除请求。 AWS Backup 使用服务相关角色`AWSServiceRoleForBackup`执行删除。

如果删除请求失败，请验证您的 IAM 角色是否具有创建服务相关角色的权限。具体而言，请验证您的 IAM 角色是否有 `iam:CreateServiceLinkedRole` 操作。如果没有，请将此权限添加到用于创建备份的角色。添加此权限 AWS Backup 允许执行手动删除。

如果在您确认 IAM 角色已具有 `iam:CreateServiceLinkedRole` 操作后，恢复点仍处于 `DELETING` 状态，则表示我们可能正在调查您的问题。请通过以下步骤完成手动删除：

1. 设置提醒，提醒您在 2-3 天后回来。

2. 2-3 天后，检查是否存在最近处于 EXPIRED 状态的删除点（第一次手动删除操作的结果）。
3. 手动删除这些处于 EXPIRED 状态的恢复点。

有关角色的更多信息，请参阅使用服务相关角色和添加和删除 IAM 身份权限。

编辑备份

使用创建备份后 AWS Backup，您可以更改备份的生命周期或标签。生命周期定义备份何时转换到冷存储以及何时过期。 AWS Backup 将根据您定义的生命周期自动转换备份和使备份过期。

要查看可以转换到冷存储的资源列表，请参阅按资源划分的功能可用性表的“转换到冷存储的生命周期”部分。对于其他资源，将忽略冷存储表达式。

> **Note**
>
> 只有亚马逊弹性文件系统 (Amazon EFS) 文件系统和高级 Amazon DynamoDB 的备份才支持使用 AWS Backup 控制台编辑备份的标签。
> 在创建其他资源时添加到恢复点的标签仍会显示，但是会灰显且不可编辑。尽管这些标签在 AWS Backup 控制台中不可编辑，但您可以使用该服务的控制台或 API 编辑这些其他服务备份的标签。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。当您更新“转换为冷态前经过的天数”设置之后，该值必须至少为备份期限加上一天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

以下示例演示如何更新备份的生命周期。

编辑备份的生命周期

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 在备份部分中，选择备份。
4. 在备份详细信息页面上，选择编辑。
5. 配置生命周期设置，然后选择保存。

还原备份

如何还原

有关控制台还原说明以及每种 AWS Backup支持的资源类型的文档链接，请参阅本页底部的链接。

要以编程方式还原备份，请使用 StartRestoreJob API 操作。

您还原资源所需的配置值（“还原元数据”）因要还原的资源而异。要获取创建备份时使用的配置元数据，可以调用 GetRecoveryPointRestoreMetadata。本页底部链接中还提供了还原元数据示例。

从冷存储还原所需的时间通常比从温存储还原所需的时间长 4 个小时。

对于每次还原，都会使用唯一的作业 ID 创建还原作业，例如 `1323657E-2AA4-1D94-2C48-5D7A423E7394`。

> **Note**
>
> AWS Backup 不提供任何恢复时间的服务级别协议 (SLA)。还原时间可能因系统负载和容量而异，即使包含相同资源的还原也是如此。

非破坏性还原

当您使用还原备份时，它会使用您 AWS Backup 要恢复的备份创建一个新资源。这是为了保护您的现有资源不被还原活动所破坏。

还原测试

您可以对资源执行测试以模拟还原体验。这有助于确定您是否达到组织还原时间目标 (RTO)，并有助于为未来的还原需求做好准备。

有关更多信息，请参阅还原测试。

在还原期间复制标签

> **Note**
>
> 在 Amazon EC2 实例、虚拟机和 Amazon Timestream 资源上还原 Amazon DynamoDB、Amazon S3、SAP HANA 当前不提供此功能。

简介

如果在进行备份时，标签属于受保护的资源，则可以在还原资源时复制标签。标签是包含键值对的标签，它可以帮助您识别和搜索资源。启动还原作业时，可以将属于原始备份资源的标签添加到要还原的资源。

当您选择在还原作业期间包含标签时，此步骤可以取代在还原作业完成后手动将标签应用于资源所需的开销和人力。请注意，这与向已还原的资源添加新标签不同。

在控制台流中还原备份时，默认情况下会复制源标签。如果您希望不将标签复制到已还原的资源，请在控制台中取消选中该复选框。

在 API 操作 `StartRestoreJob` 中，参数 `false` 默认设置为 `CopySourceTagsToRestoredResource`，这将从您要还原的资源中排除原始源标签。如果您希望包含 来自原始来源的标签，请将其设置为 `True`。

注意事项

- 一个资源最多可以有 50 个标签，包括已还原的资源。有关标签限制的更多信息，请参阅为 AWS 资源添加标签。
- 确保用于还原复制标签的角色中存在正确的权限。默认还原角色包含必要的权限。自定义角色必须包括为资源添加标签的额外权限。
- 目前不支持包含恢复标签的以下资源：VMware Cloud™ on、VMware Cloud™ on AWS、本地系统、亚马逊 EC2 实例上 AWS Outposts的 SAP HANA、Timestream、DynamoDB、Advanced DynamoDB 和 Amazon S3。
- 对于连续备份，原始资源上截至最近一次备份的标签将被复制到已还原的资源。
- 不会为项目级还原复制标签。
- 在备份作业完成后添加到备份但在备份之前不存在于原始资源上的标签将不会复制到还原的资源中。只有 2023 年 5 月 22 日之后创建的备份才有资格在还原时复制标签。

标签与特定资源的交互

- Amazon EC2
  - 应用于已恢复的 Amazon EC2 实例的标签也适用于附加的已恢复的 Amazon EBS 卷。
  - 应用于附加到源实例的 EBS 卷的标签不会复制到附加到已还原实例的卷上。如果您有基于标签允许或拒绝用户访问 EBS 卷的 IAM 策略，则必须手动为还原的卷重新分配所需的标签，以确保您的策略保持有效。

- 还原 Amazon EFS 资源时，必须将其复制到新文件系统。还原到现有文件系统不能将标签复制到该文件系统。
- Amazon RDS
  - 如果被备份的 RDS 集群仍处于活动状态，将复制该集群的标签。
  - 如果原始集群不再处于活动状态，将改为复制集群快照中的标签。
  - 无论 `CopySourceTagsToRestoredResource` 的 Boolean 参数是设置为 `True` 还是 `False`，在还原期间都会复制在进行备份时资源上存在的标签。但是，如果快照不包含标签，将使用以上 Boolean 设置。
- 默认情况下，Amazon Redshift 集群在还原作业期间始终包含标签。

通过控制台复制标签

1. 打开 AWS Backup 控制台
2. 在导航窗格中，选择受保护的资源，然后选择要还原的 Amazon S3 资源 ID。
3. 在资源详细信息页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请执行以下操作：
   a. 在备份窗格中，选择资源的恢复点 ID。
   b. 在窗格的右上角，选择还原（或者，可以转到备份保管库，找到恢复点，单击操作，然后单击还原）。
4. 在还原备份页面上，找到名为“带标签还原”的面板。要包含原始资源中的所有标签，请保留此复选框（注意，控制台中此复选框默认处于选中状态）。
5. 选择所有首选设置和角色后，单击还原备份。

以编程方式包含标签

使用 API 操作 `StartRestoreJob`。确保将以下 Boolean 参数设置为 `True`：

```
CopySourceTagsToRestoredResource = true
```

如果 Boolean 参数 `CopySourceTagsToRestoredResource = True`，则还原作业会将标签从原始资源复制到还原的材料中。

> **Important**
>
> 如果为不受支持的资源（VMware、、本地系统、EC2 实例上的 SAP HANA、Timestream AWS Outposts、DynamoDB、高级 DynamoDB 和 Amazon S3）包含此参数，则恢复任务将失败。

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

排查标签还原问题

错误：权限不足

补救措施：确保您的还原角色具有必要的权限，以便可以在还原的资源上包含标签。用于恢复的默认AWS 托管服务角色策略包含此任务所需的权限。AWSBackupServiceRolePolicyForRestores

如果选择使用自定义角色，请确保存在以下权限：

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`

- `cloudformation:TagResource`

有关更多信息，请参阅 API 权限。

还原作业状态

您可在 AWS Backup 控制台的作业页面查看还原作业的状态。还原作业的状态包括待处理、正在运行、已完成、已中止和失败。

主题

- 还原 S3 数据
- 使用恢复虚拟机 AWS Backup
- 还原 FSX 文件系统
- 还原 Amazon EBS 卷
- 还原 Amazon EFS 文件系统
- 还原 Amazon DynamoDB 表
- 还原 SSAS 数据库
- 还原 Amazon Aurora 集群
- 还原 Amazon EC2 实例
- 还原 Storage Gateway 卷
- 还原 Amazon Timestream 表
- 还原 Amazon Redshift 集群
- 还原 Amazon EC2 实例上的 SAP HANA 数据库
- 还原 DocumentDB 集群
- 还原 Neptune 集群
- 恢复 CloudFormation 堆栈备份

还原 S3 数据

您可以将使用 AWS Backup 备份的 S3 数据恢复到 S3 标准存储类别。您可以还原存储桶中的所有对象或特定对象。您可以将它们还原到现有存储桶或新存储桶。

亚马逊 S3 恢复权限

在开始恢复资源之前，请确保您使用的角色具有足够的权限。

有关更多信息，请参阅以下有关策略的条目：

1. AWSBackupServiceRolePolicyForS3Restore
2. AWSBackupServiceRolePolicyForRestores
3. 的托管策略 AWS Backup

亚马逊 S3 恢复注意事项

- AWS Backup 创建所有 S3 版本的备份，但在任何时候都只能从版本堆栈中恢复最新版本。
- 必须在目的地存储桶中启用访问控制列表 (ACL)，否则作业将失败。要启用 ACL，请按照配置 ACL 页面中的说明进行操作。
- 如果源存储桶的对象名称或版本 ID 相同，则会跳过对象的还原。
- 如果还原特定对象，则可以还原对象的当前版本。
- 当您恢复到原来的 S3 存储桶时，
  - AWS Backup 不执行破坏性恢复，这意味着无论版本如何，都不会 AWS Backup 将对象代替已存在的对象放入存储桶中。
  - 当前版本中的删除标记被视为不存在的对象，因此可以进行恢复。
  - AWS Backup 在还原期间不会从存储桶中删除对象（不带删除标记）（例如：备份期间不存在的当前存储桶中的密钥将保留）。
- 恢复跨区域副本
  - 虽然 S3 备份可以跨区域复制，但还原作业只能在原始备份或副本所在的同一区域进行。

    Example

    示例：在美国东部（弗吉尼亚北部）地区创建的 S3 存储桶可以复制到加拿大（中部）区域。还原作业可以使用美国东部（弗吉尼亚州北部）区域的原始存储桶启动并还原到该区域，也可以使用加拿大（中部）区域的副本启动并还原到该区域。
  - 原始加密方法不能用于恢复从其他区域复制的恢复点（备份）。跨区域副本 AWS KMS 加密不适用于 Amazon S3 资源；相反，对还原任务使用不同的加密类型。

使用 AWS Backup 控制台恢复 Amazon S3 恢复点

要使用 AWS Backup 控制台恢复您的 Amazon S3 数据，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源，然后选择要还原的 Amazon S3 资源 ID。
3. 在资源详细信息页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请执行以下操作：
   a. 在备份窗格中，选择资源的恢复点 ID。
   b. 在窗格的右上角，选择还原。

   （或者，您可以前往备份保管库，找到恢复点，单击操作，然后单击还原。）
4. 如果要还原的是连续备份，请在还原时间窗格中选择以下任一选项：
   a. 接受默认值以还原到最近可还原时间。
   b. 指定要还原的日期和时间。
5. 在设置窗格中，指定是还原整个存储桶还是执行项目级还原。
   a. 如果您选择项目级别还原，则通过指定每个项目的 S3 URI 来唯一标识该对象，每个还原任务最多可以恢复 5 个项目（存储桶中的对象或文件夹）。

      （有关 S3 存储桶 URI 的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的访问存储桶的方法。）
   b. 选择添加项目可指定要还原的其他项目。
6. 选择您的还原目的地。您可以还原到源存储桶、使用现有存储桶或创建新的存储桶。

   > **Note**
   >
   > 您的还原目标存储桶必须开启版本控制。 AWS Backup 如果您选择的存储桶不符合此要求，则会通知您。

   a. 如果您选择使用现有存储桶，请从显示当前 AWS 区域内所有现有存储桶的下拉菜单中选择目标 S3 存储桶。
   b. 如果您选择创建新的存储桶，请键入新存储桶名称。新存储桶默认为启用 S3 版本控制。默认情况下，阻止公有访问 (BPA) 设置处于关闭状态。在 S3 中创建存储桶后，您可以修改这些设置。

7. 要对 S3 存储桶中的对象进行加密，您可以选择已恢复的对象加密。使用原始加密密钥（默认）、Amazon S3 密钥 (SSE-S3) 或 AWS Key Management Service 秘钥 (SSE-KMS)。

   这些设置仅适用于 S3 存储桶中对象的加密。这不会影响存储桶本身的加密。

   a. 使用原始加密密钥（默认）使用与源对象相同的加密密钥还原对象。如果源对象未加密，则此方法会在不加密的情况下恢复该对象。

      如果原始密钥不可用，此还原选项允许您选择替代加密密钥来加密还原对象。

   b. 如果您选择 Amazon S3 秘钥 (SSE-S3)，则无需指定任何其他选项。

   c. 如果您选择AWS Key Management Service 密钥 (SSE-KMS)，则可以做出以下选择：AWS 托管式密钥 (aws/s3)、从密钥中进行选择或输入 AWS KMS 密钥 ARN。 AWS KMS

      i. 如果您选择 AWS 托管式密钥 (aws/s3)，则无需指定任何其他选项。

      ii. 如果您从 AWS KMS 密钥中选择，请从下拉菜单中选择一个 AWS KMS 密钥。或者，选择创建密钥。

      iii. 如果您输入 AWS KMS 密钥 ARN，请在文本框中键入 ARN。或者，选择创建密钥。

8. 在还原角色窗格中，选择 AWS Backup 将为此还原担任的 IAM 角色。

9. 选择还原备份。这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon S3 恢复点

使用 StartRestoreJob。在 Amazon S3 还原期间，您可以指定以下元数据：

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

恢复点状态

恢复点的状态将显示其所处的状态。

PARTIAL状态表示在备份窗口关闭之前 AWS Backup 无法创建恢复点。要使用 API 延长备份计划窗口，请参阅UpdateBackupPlan。您还可以使用控制台，通过选择和编辑备份计划来延长备份计划时段。

EXPIRED状态表示恢复点已超过其保留期，但 AWS Backup 缺少权限或无法将其删除。要手动删除这些恢复点，请参阅入门章节清理资源部分中的步骤 3：删除恢复点。

当用户执行某些操作导致连续备份被禁用时，连续备份中会出现 STOPPED 状态。这可能是由于移除权限、关闭版本控制、关闭发送到 Amazon EventBridge 的事件或禁用由 AWS Backup制定的 EventBridge 规则造成的。

要解决 STOPPED 状态问题，请确保请求的所有权限均已准备就绪，并且已在 S3 存储桶上启用版本控制。满足这些条件后，下一个运行的备份规则实例将导致创建新的连续恢复点。不需要删除处于 STOPPED 状态的恢复点。

使用恢复虚拟机 AWS Backup

您可以将虚拟机还原到 VMware、VMware Cloud on AWS、VMware Cloud on、亚马逊 EBS 卷或亚马逊 EC2 实例。 AWS Outposts将虚拟机还原（或迁移）到 EC2 需要具有许可证。默认情况下， AWS 将包括许可证（收费）。有关更多信息，请参阅《虚拟机导入/导出用户指南》中的许可选项。

您可以使用 AWS Backup 控制台或通过恢复 VMware 虚拟机 AWS CLI。恢复虚拟机时，不包括 VMware Tools 文件夹。要重新安装 VMware 工具，请参阅 VMware 文档。

AWS Backup 虚拟机的恢复是非破坏性的，这意味着在还原期间 AWS Backup 不会覆盖现有的虚拟机。相反，还原任务会部署一台新的虚拟机。

任务

- 将虚拟机还原到 Amazon EC2 实例时的注意事项
- 使用 AWS Backup 控制台恢复虚拟机恢复点
- 用于 AWS CLI 恢复虚拟机恢复点

将虚拟机还原到 Amazon EC2 实例时的注意事项

- 将虚拟机还原（或迁移）到 EC2 需要具有许可证。默认情况下， AWS 包括许可证（收费）。有关更多信息，请参阅《虚拟机导入/导出用户指南》中的许可选项。

- 每个虚拟机磁盘的最大限制为 5 TB（太字节）。
- 将虚拟机还原到实例时，您无法指定 key pair。您可以在启动`authorized_keys`期间（通过实例用户数据）或启动后向添加密钥对（如 Amazon EC2 用户指南中的故障排除部分所述）。
- 在《虚拟机导入/导出用户指南》中确认您的操作系统支持从 Amazon EC2 导入和导出。
- 在虚拟机导入 /导出用户指南中查看将虚拟机导入到 Amazon EC2 所涉及的限制。
- 使用恢复到 Amazon EC2 实例时 AWS CLI，必须指定`"RestoreTo":"EC2Instance"`。所有其他属性都有默认值。

使用 AWS Backup 控制台恢复虚拟机恢复点

您可以在控制台的左侧导航窗格中从多个位置恢复虚拟 AWS Backup 机：

- 选择管理程序可查看由连接到 AWS Backup的管理程序管理的虚拟机的恢复点。
- 选择虚拟机可查看连接到 AWS Backup的所有管理程序中的虚拟机的恢复点。
- 选择 Backup 保管库可查看存储在特定保 AWS Backup 管库中的恢复点。
- 选择 “受保护的资源”，查看所有 AWS Backup 受保护资源的恢复点。

如果您需要还原不再与 Backup Gateway 有连接的虚拟机，请选择备份保管库或受保护的资源以查找恢复点。

Options

- 恢复到 VMware
- 恢复到 Amazon EBS 卷
- 还原到 Amazon EC2 实例

要将虚拟机恢复到 VMware，请开启 VMware Cloud AWS，开启 VMware C AWS Outposts

1. 在管理程序或虚拟机视图中，选择要还原的虚拟机名称。在受保护的资源视图中，选择要还原的虚拟机资源 ID。
2. 选择要还原的恢复点 ID 旁边的单选按钮。
3. 选择还原。
4. 选择还原类型。

a. 完整还原还原所有虚拟机的磁盘。

b. 磁盘级还原还原用户定义的一个或多个磁盘。使用下拉菜单选择要还原的磁盘。

5. 选择还原位置。选项有 VMware、VM ware Cloud on AWS 和 VMware Cloud on AWS Outposts

6. 如果您要进行完整还原，请跳到下一步。如果您要执行磁盘级还原，则在虚拟机磁盘下会有一个下拉菜单。选择要还原的一个或多个可启动卷。

7. 从下拉菜单中选择管理程序以管理还原后的虚拟机。

8. 对于还原后的虚拟机，请使用贵组织的虚拟机最佳实践指定其：

a. 名称

b. 路径（例如 `/datacenter/vm`）

c. 计算资源名称（例如 VMHost 或集群）

如果主机是集群的一部分，则无法还原到该主机，只能还原到给定的集群。

d. 数据存储

9. 对于还原角色，使用下拉菜单选择默认角色（推荐）或选择 IAM 角色。

10. 选择还原备份。

11. 可选：检查您的还原作业何时处于状态 `Completed`。在左导航窗格中，选择作业。

将虚拟机恢复到 Amazon EBS 卷

1. 在管理程序或虚拟机视图中，选择要还原的虚拟机名称。在受保护的资源视图中，选择要还原的虚拟机资源 ID。

2. 选择要还原的恢复点 ID 旁边的单选按钮。

3. 选择还原。

4. 选择还原类型。

- 磁盘还原可还原用户定义的一个磁盘。使用下拉菜单选择要还原的磁盘。

5. 选择还原位置为 Amazon EBS。

6. 在虚拟机磁盘下拉菜单下，选择要还原的可启动卷。

7. 在 EBS 卷类型下，选择卷类型。

8. 选择您的可用区。

9. 加密（可选）。如果您选择加密 EBS 卷，请选中该复选框。

10. 从菜单中选择您的 KMS 密钥。
11. 对于恢复角色，选择默认角色（推荐）或选择 IAM 角色。
12. 选择还原备份。
13. 可选：检查您的还原作业何时处于状态 Completed。在左导航窗格中，选择作业。
14. 可选：访问如何在整个 Amazon EBS 卷上创建 LVM 逻辑卷？了解有关如何挂载托管卷和访问还原后的 Amazon EBS 卷上的数据的更多信息。

将虚拟机恢复到 Amazon EC2 实例

1. 在管理程序或虚拟机视图中，选择要还原的虚拟机名称。在受保护的资源视图中，选择要还原的虚拟机资源 ID。
2. 选择要还原的恢复点 ID 旁边的单选按钮。
3. 选择还原。
4. 选择还原类型。
   - 完整还原可完全还原文件系统，包括根级别文件夹和文件。
5. 选择还原位置为 Amazon EC2。
6. 对于实例类型，选择在新实例上运行应用程序所需的计算和内存组合。

> **Tip**
>
> 选择符合或超过原始虚拟机规格的实例类型。有关更多信息，请参阅 Amazon EC2 实例类型指南。

7. 对于虚拟私有云 (VPC)，请选择定义实例网络环境的虚拟私有云 (VPC)。
8. 对于子网，选择 VPC 中的一个子网。您的实例会收到来自子网地址范围的私有 IP 地址。
9. 对于安全组，请选择一个安全组，该安全组充当您的实例流量的防火墙。
10. 对于恢复角色，选择默认角色（推荐）或选择 IAM 角色。
11. 可选：要在启动时在实例上运行脚本，请展开高级设置并在用户数据中输入脚本。
12. 选择还原备份。
13. 可选：检查您的还原作业何时处于状态 Completed。在左导航窗格中，选择作业。

用于 AWS CLI 恢复虚拟机恢复点

使用 StartRestoreJob。

您可以指定以下元数据以便虚拟机还原到 Amazon EC2 和 Amazon EBS：

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

您可以为虚拟机恢复到 VMware、开启 VMware Cloud 和 AWS Outpost 上 AWS的 VMware 云时指定以下元数据：

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

此示例演示如何对 VMware 进行完整还原：

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

还原 FSX 文件系统

用于 AWS Backup 恢复 Amazon FSx 文件系统时可用的还原选项与使用原生 Amazon FSx 备份相同。您可以使用备份的恢复点来创建新的文件系统并恢复另一个文件系统的 point-in-time 快照。

恢复 Amazon FSx 文件系统时， AWS Backup 会创建一个新的文件系统并在其中填充数据（适用于 NetApp ONTAP 的 Amazon FSx 允许将卷恢复到现有文件系统）。这与本机 Amazon FSx 备份和还原文件系统的方式类似。将备份还原到新文件系统所需的时间与创建新文件系统所需的时间相同。从备份还原的数据会延迟加载到文件系统中。因此，在此过程中，延迟可能会稍高。

> **Note**
>
> 您无法还原到现有的 Amazon FSx 文件系统，也无法还原单个文件或文件夹。
> FSx for ONTAP 不支持备份某些卷类型，包括 DP（数据保护）卷、LS（负载共享）卷、完整卷或已满文件系统上的卷。有关更多信息，请参阅 FSx for ONTAP Working with backups。
> AWS Backup 包含 Amazon FSx 文件系统恢复点的文件库在外部可见。 AWS Backup您可以使用 Amazon FSx 还原恢复点，但不能将其删除。

您可以从控制台查看由内置的 Amazon FSx 自动备份功能创建的 AWS Backup 备份。您也可以使用恢复这些备份 AWS Backup。但是，您不能使用删除这些备份或更改 Amazon FSx 文件系统的自动备份计划。 AWS Backup

您可以使用 AWS Backup 控制台、API 或恢复创建的备份 AWS CLI。 AWS Backup 本节向您展示如何使用 AWS Backup 控制台恢复 Amazon FSx 文件系统。

使用 AWS Backup 控制台恢复 Amazon FSx 恢复点

还原适用于 Windows File Server 的 FSx 文件系统

还原适用于 Windows File Server 的 FSx 文件系统

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon FSx 资源 ID。

3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。选择资源的恢复点 ID。
4. 在窗格右上角，选择还原以打开还原备份页面。
5. 在文件系统详细信息部分，您的备份 ID 显示在备份 ID 下，文件系统类型显示在文件系统类型下。您可以还原适用于 Windows File Server 的 FSx 和适用于 Lustre 的 FSx 文件系统。
6. 对于部署类型，接受默认值。在还原期间，您无法更改文件系统的部署类型。
7. 选择要使用的存储类型 。如果文件系统的存储容量低于 2,000 GiB，则无法使用 HDD 存储类型。
8. 对于吞吐能力，选择建议的吞吐能力以使用建议的每秒 16 MB (MBps) 的速率，或者选择指定吞吐能力并输入新的速率。
9. 在网络和安全部分，提供所需的信息。
10. 如果要还原适用于 Windows File Server 的 FSx 文件系统，请提供用于访问该文件系统的 Windows 身份验证信息，或者可以新建一个。

    > **Note**
    >
    > 还原备份时，您无法更改文件系统上的 Active Directory 类型。

    有关 Microsoft Active Directory 的更多信息，请参阅《适用于 Windows File Server 的 Amazon FSx 用户指南》中的在适用于 Windows File Server 的 Amazon FSx 中使用 Active Directory。
11. （可选）在备份和维护部分，提供设置备份首选项所需的信息。
12. 在还原角色部分，选择 AWS Backup 将用于代表您创建和管理备份的 IAM 角色。建议您选择默认角色。如果没有默认角色，将使用正确的权限为您创建一个。也可以提供自己的 IAM 角色。
13. 验证所有输入内容，然后选择还原备份。

还原适用于 Lustre 的 Amazon FSx 文件系统

AWS Backup 支持 Amazon FSx for Lustre 文件系统，这些文件系统具有永久存储部署类型且未链接到 Amazon S3 等数据存储库。

还原适用于 Lustre 的 Amazon FSx 文件系统

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon FSx 资源 ID。

3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。选择资源的恢复点 ID。
4. 在窗格右上角，选择还原以打开将备份还原到新文件系统页面。
5. 在设置部分，您的备份 ID 显示在备份 ID 下，文件系统类型显示在文件系统类型下。文件系统类型应为 Lustre。
6. （可选）输入文件系统的名称。
7. 选择部署类型。 AWS Backup 仅支持持久部署类型。在还原期间，您无法更改文件系统的部署类型。

   持久性部署类型针对的是长期存储。有关适用于 Lustre 的 FSx 部署选项的详细信息，请参阅《适用于 Lustre 的 Amazon FSx 用户指南》中的使用适用于 Lustre 的 Amazon FSx 文件系统的可用部署选项。
8. 选择要使用的单位存储吞吐量。
9. 指定要使用的存储容量。输入介于 32 GiB 和 64,436 GiB 之间的容量。
10. 在网络和安全部分，提供所需的信息。
11. （可选）在备份和维护部分，提供设置备份首选项所需的信息。
12. 在还原角色部分，选择 AWS Backup 将用于代表您创建和管理备份的 IAM 角色。建议您选择默认角色。如果没有默认角色，将使用正确的权限为您创建一个。也可以提供您的 IAM 角色。
13. 验证所有输入内容，然后选择还原备份。

为 ONTAP 卷恢复 Amazon FS NetApp x

要恢复 NetApp ONTAP 卷的 Amazon FSx，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon FSx 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。选择资源的恢复点 ID。
4. 在窗格的右上角，选择还原以打开还原页面。

   第一部分文件系统详细信息显示恢复点 ID、文件系统 ID 和文件系统类型。
5. 在还原选项下，有几个选项。首先，从下拉菜单中选择文件系统。
6. 接下来，从下拉菜单中选择首选存储虚拟机。
7. 输入您的卷的名称。

8. 指定交汇点路径，该路径是文件系统中要挂载卷的位置。
9. 指定您正在创建的卷大小，以兆字节 (MB) 为单位。
10. （可选）您可以通过选中复选框来选择提高存储效率。这将允许进行重复数据删除和压缩。
11. 在容量池分层策略下拉菜单中，选择分层首选项。
12. 在还原权限中，选择 AWS Backup 将用于还原备份的 IAM 角色。
13. 验证所有输入内容，然后选择还原备份。

还原适用于 OpenZFS 的 Amazon FSx 文件系统

还原适用于 OpenZFS 的 FSx 文件系统

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon FSx 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。选择资源的恢复点 ID。
4. 在窗格右上角，选择还原以打开还原备份页面。

   在文件系统详细信息部分，您的备份 ID 显示在备份 ID 下，文件系统类型显示在文件系统类型下。文件系统类型应为适用于 OpenZFS 的 FSx。
5. 在还原选项下，您可以选择快速还原或标准还原。快速还原将使用源文件系统的默认设置。如果执行的是快速还原，请跳到步骤 7。

   如果选择“标准还原”，请指定以下其他配置：

   a. 预置的 SSD IOPS：您可以选择自动单选按钮，也可以选择用户配置选项（如果有）。
   b. 吞吐能力：您可以选择建议的吞吐能力 64 MB/秒，也可以选择指定吞吐能力。
   c. （可选）VPC 安全组：您可以指定要与文件系统的网络接口关联的 VPC 安全组。
   d. 加密密钥：指定用于保护已恢复的文件系统静态数据的 AWS Key Management Service 密钥。
   e. （可选）根卷配置：默认情况下，此配置处于折叠状态。您可以通过单击向下箭头将其展开。通过备份创建文件系统将创建一个新的文件系统；卷和快照将保留其源配置。
   f. （可选）备份和维护：要设置计划备份，请单击向下箭头展开该部分。您可以选择备份时段、小时和分钟、保留期以及每周维护时段。
6. （可选）您可以输入卷的名称。

7. SSD 存储容量将显示文件系统的存储容量。
8. 选择可从中访问文件系统的虚拟私有云 (VPC)。
9. 在子网下拉菜单中，选择文件系统网络接口所在的子网。
10. 在还原角色部分，选择 AWS Backup 将用于代表您创建和管理备份的 IAM 角色。建议您选择默认角色。如果没有默认角色，将使用正确的权限为您创建一个。还可以选择 IAM 角色。
11. 验证所有输入内容，然后选择还原备份。

使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon FSx 恢复点

要使用 API 或 CLI 还原 Amazon FSx，请使用 StartRestoreJob。在任何 Amazon FSx 还原期间，您都可以指定以下元数据：

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

适用于 Windows File Server 的 FSx 还原元数据

在适用于 Windows File Server 的 FSx 还原期间，您可以指定以下元数据：

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

适用于 Lustre 的 FSx 还原元数据

在适用于 Lustre 的 FSx 还原期间，您可以指定以下 PerUnitStorageThroughput 和 DriveCacheType。

适用于 ONTAP 的 FSx 还原元数据

在适用于 ONTAP 的 FSx 还原期间，您可以指定以下元数据：

- 要创建的卷的名称 #name
- OntapConfiguration: # ontap 配置
- junctionPath
- sizeInMegabytes
- storageEfficiencyEnabled
- storageVirtualMachineId
- tieringPolicy

适用于 OpenZFS 的 FSx 还原元数据

在适用于 OpenZFS 的 FSx 还原期间，您可以指定以下元数据：

- ThroughputCapacity
- DesklopsConfiguration
- 如果指定 Iops，则必须包含介于 0 到 160,000 之间的值，但不包括模式。

CLI 还原命令示例：

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

还原元数据示例：

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
```

```
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

还原 Amazon EBS 卷

恢复亚马逊弹性区块存储 (Amazon EBS) 快照时，会创建一个新的亚马逊 EBS 卷 AWS Backup ，您可以将其附加到您的亚马逊 EC2 实例。

您可以选择将快照作为 EBS 卷或 AWS Storage Gateway 卷进行还原。

使用 AWS Backup 控制台恢复 Amazon EBS 恢复点

还原 Amazon EBS 卷

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 EBS 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 指定资源的还原参数。您输入的还原参数将特定于所选的资源类型。

   对于资源类型，选择在还原此备份时要创建的 AWS 资源。
5. 如果选择 EBS 卷，请提供卷类型和大小 (GiB) 的值，然后选择可用区。

   - 在吞吐量后，有一个可选复选框加密此卷。如果 EBS 恢复点已加密，则此选项将保持活动状态。

     您可以指定 KMS 密钥或创建 AWS KMS 密钥。

   如果选择 Storage Gateway 卷，请选择处于可访问状态的网关。另外，请选择您的 iSCSI 目标名称。

   - 对于存储卷网关，选择磁盘 ID。
   - 对于卷缓存网关，选择至少与受保护资源一样大的容量。
6. 对于还原角色，请选择 AWS Backup 将担任此还原的 IAM 角色。

> **Note**
>
> 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的默认角色。您可以删除此默认角色或使其无法使用。

7. 选择还原备份。

   这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

还原已归档的 EBS 快照会将其暂时从冷存储移至暖存储，以创建新的 EBS 卷。这种类型的还原会产生一次性检索费用。在此还原期间，将对暖存储和冷存储的存储费用进行计费。冷存储中的 EBS 卷无法恢复到 Backup 网关卷。

您可以使用 AWS Backup 控制台或命令行在冷存储中还原已归档的 EBS 快照。从冷存储中还原最长可能需要 72 小时。有关更多信息，请参阅《Amazon EBS 用户指南》中的归档 Amazon EBS 快照。

Console

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 依次导航到备份保管库 > ### > 还原已归档的 EBS 快照。
3. 在设置部分中，输入一个介于 0 到 180（含）之间的值，以指定临时还原归档快照的天数。
4. 输入其他设置：卷类型、大小、IOPS、可用区、吞吐量和加密。
5. 选择您的还原角色。
6. 选择还原备份。在确认弹出窗口中，确认快照和还原类型。然后，选择还原快照。

AWS CLI

1. 使用 `start-restore-job`
2. 添加相应参数。
3.
4.
5.

使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon EBS 恢复点

要使用 API 或 CLI 还原 Amazon EBS，请使用 StartRestoreJob。在任何 Amazon EBS 还原期间，您都可以指定以下元数据：

```
availabilityZone
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

例如：

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

还原 Amazon EFS 文件系统

如果要还原 Amazon Elastic File System (Amazon EFS) 实例，您可以执行完整还原或项目级还原。

完整还原

在执行完整还原时，整个文件系统都将被还原。

AWS Backup 不支持使用 Amazon EFS 进行破坏性恢复。破坏性还原是指还原的文件系统会删除或覆盖源文件系统或现有文件系统。相反， AWS Backup 将文件系统还原到根目录中的恢复目录。

项目级还原

执行项目级还原时， AWS Backup 还原特定的文件或目录。必须指定相对于文件系统根目录的路径。例如，如果文件系统挂载到 `/user/home/myname/efs` 并且文件路径为 `user/home/myname/efs/file1`，则输入 **`/file1`**。路径区分大小写。不支持通配符和正则表达式字符串。如果使用接入点挂载文件系统，则您的路径可能与主机中的路径不同。

使用控制台执行 EFS 还原时，最多可以选择 10 个项目。使用 CLI 进行还原时没有项目数限制；但是，可以传递的还原元数据长度有 200 KB 的限制。

可以将这些项目还原到新的或现有的文件系统。无论哪种方式， AWS Backup 都会从根目录创建一个新的 Amazon EFS 目录 (`aws-backup-restore_datetime`) 来包含这些项目。指定项目的完整层次结构将保留在恢复目录中。例如，如果目录 A 包含子目录 B、C 和 D，则在恢复 A、B、C 和 D 时， AWS Backup 会保留分层结构。无论是执行到现有文件系统还是新文件系统的 Amazon EFS 项目级还原，每次还原尝试都会从根目录创建一个新的恢复目录来包含已还原的文件。如果尝试对同一路径进行多次还原，则可能存在多个包含已还原项目的目录。

> **Note**
>
> 如果只保留一个每周备份，则只能还原到执行该备份时的文件系统状态。您无法还原到以前的增量备份。

使用 AWS Backup 控制台恢复 Amazon EFS 恢复点

还原 Amazon EFS 文件系统

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 您的 EFS 备份保管库在创建后会收到访问策略 Deny `backup:StartRestoreJob`。如果是第一次还原备份保管库，则必须按以下步骤更改访问策略。

   a. 选择备份保管库。

   b. 选择包含要还原的恢复点的备份保管库。

   c. 向下滚动到保管库访问策略。

   d. 如果存在，请从 `Statement` 中删除 `backup:StartRestoreJob`。为此，请选择编辑、删除 `backup:StartRestoreJob`，然后选择保存策略。
3. 在导航窗格中，选择受保护的资源和要还原的 EFS 文件系统 ID。
4. 在资源详细信息页面上，将显示所选文件系统 ID 的恢复点列表。要还原文件系统，请在备份窗格中，选择文件系统的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
5. 指定文件系统的还原参数。您输入的还原参数将特定于所选的资源类型。

   您可以执行完整还原，这会还原整个文件系统。或者，您可以使用项目级还原来还原特定的文件和目录。

   - 选择完整还原选项可还原整个文件系统，包括所有根级别的文件夹和文件。
   - 选择项目级还原选项可还原特定的文件或目录。您最多可以选择并还原 Amazon EFS 中的五个项目。

要还原特定文件或目录，您必须指定与挂载点相关的相对路径。例如，如果文件系统挂载到 `/user/home/myname/efs` 并且文件路径为 `user/home/myname/efs/file1`，则输入 **`/file1`**。路径区分大小写，不能包含特殊字符、通配符和正则表达式字符串。

1. 在项目路径文本框中，输入文件或文件夹的路径。
2. 选择添加项目以添加其他文件或目录。您可以在 EFS 文件系统中选择并还原最多 5 个项目。

6. 对于还原位置

   - 如果要还原到源文件系统，请选择还原到源文件系统中的目录。
   - 如果要还原到其他文件系统，请选择还原到新文件系统。

7. 对于文件系统类型

   - （推荐）如果要跨多个 AWS 可用区恢复文件系统，请选择 “区域”。
   - 如果要将文件系统还原到单个可用区，请选择单区。然后，在可用区下拉列表中，选择还原的目的地。

   有关更多信息，请参阅《Amazon EFS 用户指南》中的管理 Amazon EFS 存储类。

8. 对于性能

   - 如果您选择执行区域还原，请选择（推荐）通用型或最大 I/O。
   - 如果您选择执行单区还原，则必须选择（推荐）通用型。单区还原不支持最大 I/O。

9. 对于启用加密

   - 如果要对文件系统进行加密，请选择启用加密。使用 AWS Key Management Service (AWS KMS) 控制台创建 KMS 密钥 ID 和别名后，它们会出现在列表中。
   - 在 KMS 密钥文本框中，从列表中选择要使用的密钥。

10. 对于还原角色，请选择 AWS Backup 将担任此还原的 IAM 角色。

> **Note**
>
> 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的默认角色。您可以删除此默认角色或使其无法使用。

11. 选择还原备份。

    这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

> **Note**
>
> 如果只保留一个每周备份，则只能还原到执行该备份时的文件系统状态。您无法还原到以前的增量备份。

使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon EFS 恢复点

使用 StartRestoreJob。在还原 Amazon EFS 实例时，您可以还原整个文件系统或特定的文件或目录。要还原 Amazon EFS 资源，您需要以下信息：

- `file-system-id`— 由备份的 Amazon EFS 文件系统的 ID AWS Backup。在 `GetRecoveryPointRestoreMetadata` 中返回。恢复新文件系统时不需要这样做（如果参数`newFileSystem`是，则忽略此值`True`）。
- `Encrypted` - 一个布尔值，如果设为 true，则指定文件系统已加密。如果指定了 `KmsKeyId`，`Encrypted` 必须设置为 `true`。
- `KmsKeyId`— 指定用于加密已恢复文件系统的密 AWS KMS 钥。
- `PerformanceMode` - 指定文件系统的吞吐量模式。
- `CreationToken` - 用户提供的值，确保请求的唯一性（幂等性）。
- `newFileSystem` - 一个布尔值，如果设为 true，则指定恢复点将还原到新的 Amazon EFS 文件系统。
- `ItemsToRestore` - 最多包含五个字符串的一个数组，其中每个字符串均为一个文件路径。使用 `ItemsToRestore` 可还原特定文件或目录而不是整个文件系统。此参数为可选的。

您也可以添加 `aws:backup:request-id`。

可以通过包含以下参数来执行 One Zone 恢复：

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

有关 Amazon EFS 配置值的更多信息，请参阅create-file-system。

在 Amazon EFS 中禁用自动备份

默认情况下，Amazon EFS 自动创建数据备份。这些备份在中表示为恢复点 AWS Backup。尝试删除恢复点将导致出现错误消息，指出没有足够的权限来执行该操作。

最佳实践是保持此自动备份处于活动状态。特别是在意外删除数据的情况下，此备份允许将文件系统内容还原到上次创建恢复点的日期。

万一您希望将其关闭，则必须将访问策略从 `"Effect": "Deny"` 更改为 `"Effect": "Allow"`。有关开启或关闭自动备份的更多信息，请参阅《Amazon EFS 用户指南》。

还原 Amazon DynamoDB 表

使用 AWS Backup 控制台恢复 DynamoDB 恢复点

还原 DynamoDB 表

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 DynamoDB 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 对于设置，在新表名称文本字段中输入新表的名称。
5. 对于还原角色，请选择 AWS Backup 将担任此还原的 IAM 角色。
6. 对于加密设置：

   a. 如果您的备份由 DynamoDB 管理（其 ARN 开头为），则`arn:aws:dynamodb`使用拥有的密钥对还原 AWS Backup 后的表进行加密。 AWS

      要选择其他密钥来加密已恢复的表，您可以使用该 AWS Backup StartRestoreJob操作或从 DynamoDB 控制台执行恢复。

   b. 如果您的备份支持完全 AWS Backup 管理（其 ARN 开头为`arn:aws:backup`），则可以选择以下任何加密选项来保护已恢复的表：

      - （默认）DynamoDB 拥有的 KMS 密钥（加密不收取额外费用）
      - DynamoDB 托管的 KMS 密钥（收取 KMS 费用）
      - 客户托管的 KMS 密钥（收取 KMS 费用）

“DynamoDB 拥有”和“DynamoDB 托管”的密钥分别与“AWS拥有”和“AWS托管”的密钥相同。如需澄清，请参阅《Amazon DynamoDB 开发人员指南》 中的静态加密：工作原理。

有关完全 AWS Backup 管理的更多信息，请参阅高级 DynamoDB 备份。

> **Note**
>
> 仅当您还原复制的备份并希望使用与加密原始表相同的密钥对还原后的表进行加密时，以下准则才适用。
> 恢复跨区域备份时，要使用与加密原始表相同的密钥来加密已恢复的表，您的密钥必须是多区域密钥。 AWS自有密钥和 AWS托管密钥不是多区域密钥。要了解更多信息，请参阅《AWS Key Management Service 开发人员指南》中的多区域密钥。
> 恢复跨账户备份时，要使用与加密原始表相同的密钥来加密已恢复的表，则必须与目标账户共享源账户中的密钥。 AWS账户之间不能共享拥有的密钥和 AWS托管的密钥。要了解更多信息，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。

7. 选择还原备份。

   这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

使用 AWS Backup API、CLI 或 SDK 恢复 DynamoDB 恢复点

使用 `StartRestoreJob`。在任何 DynamoDB 还原期间，您都可以指定以下元数据。此元数据不区分大小写。

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

以下是 CLI 中某项 `StartRestoreJob` 操作的 `restoreMetadata` 参数示例：

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
```

```
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

前面的示例使用 AWS拥有的密钥对还原后的表进行加密。恢复元数据中指定使用 AWS拥有的密钥进行加密的部分是:\"encryptionType\":\"Default\","kmsMasterKeyArn\":\"Not Applicable\".

要使用 AWS托管密钥加密已恢复的表，请指定以下还原元数据："encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"。

要使用客户托管的密钥加密还原后的表，请指定以下还原元数据："encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"*arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab*\"。

还原 SSAS 数据库

还原 Amazon RDS 数据库需要指定多个还原选项。有关这些选项的更多信息，请参阅《Amazon RDS 用户指南》中的备份和还原 Amazon RDS 数据库实例。

使用 AWS Backup 控制台恢复 Amazon RDS 恢复点

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon RDS 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 在实例规格窗格中，接受数据库引擎、许可证模型、数据库实例类、多可用区和存储类型设置的默认值或指定这些选项。例如，如果需要备用数据库实例，请指定多可用区。
5. 在设置窗格中，为当前区域中您拥有的所有数据库实例和集群指定一个唯一 AWS 账户 的名称。数据库实例标识符不区分大小写，但它以全小写形式存储，例如“mydbinstance”。此字段为必填字段。
6. 在 “网络和安全” 窗格中，接受默认值或指定虚拟私有云 (VPC) 、子网组、公共可访问性 (通常是 “是”) 和可用区域设置的选项。
7. 在数据库选项窗格中，接受数据库端口、数据库参数组、选项组、将标签复制到快照 和已启用 IAM 数据库身份验证设置的默认值或指定这些选项。

8. 在加密窗格中，使用默认设置。如果快照的源数据库实例已加密，则还原后的数据库实例也会加密。无法删除此加密。
9. 在日志导出窗格中，选择要发布到 Amazon Logs 的 CloudWatch 日志类型。已定义 IAM 角色。
10. 在维护窗格中，接受自动次要版本升级选项的默认值或指定该选项。
11. 在还原角色窗格中，选择 AWS Backup 将为此还原担任的 IAM 角色。
12. 指定所有设置后，选择还原备份。

    这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

使用 AWS Backup API、CLI 或软件开发工具包恢复 Amazon RDS 恢复点

使用 `StartRestoreJob`。有关接受的元数据和值的信息，请参阅《Amazon RDS API 参考》中的 `RestoreDBInstanceFromDBSnapshot`。此外，还 AWS Backup 接受以下仅提供信息的属性。但是，添加它们不会影响还原：

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

还原 Amazon Aurora 集群

使用 AWS Backup 控制台恢复 Aurora 恢复点

AWS Backup 恢复您的 Aurora 集群；它不会创建 Amazon RDS 实例或将其附加到您的集群。在以下步骤中，将使用 CLI 创建 Amazon RDS 实例并将其附加到还原后的 Aurora 集群。

还原 Aurora 集群需要指定多个还原选项。有关这些选项的信息，请参阅《Amazon Aurora 用户指南》中的备份和还原 Aurora DB 集群概述。还原选项的规格可在的 API 指南中找到`RestoreDBClusterFromSnapshot`。

还原 Amazon Aurora 集群

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Aurora 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。

4. 在实例规格窗格中，接受数据库引擎、数据库引擎版本和容量类型设置的默认值或指定这些选项。

> **Note**
>
> 如果选择了无服务器容量类型，则会显示容量设置窗格。指定最小 Aurora 容量单位和最大 Aurora 容量单位设置的选项，或从其他扩展配置部分选择不同的选项。

5. 在设置窗格中，为当前区域中您拥有的所有数据库集群实例指定一个唯一 AWS 账户 的名称。
6. 在网络和安全 窗格中，接受虚拟私有云 (VPC)、子网组和可用区设置的默认值或指定这些选项。
7. 在数据库选项 窗格中，接受数据库端口、数据库集群参数组和已启用 IAM 数据库身份验证设置的默认值或指定这些选项。
8. 在备份窗格中，接受将标签复制到快照设置的默认值或指定此选项。
9. 在回溯窗格中，接受启用回溯或禁用回溯设置的默认值或指定这些选项。
10. 在加密) 窗格中，接受启用加密和禁用加密设置的默认值或指定这些选项。
11. 在日志导出窗格中，选择要发布到 Amazon Logs 的 CloudWatch 日志类型。已定义 IAM 角色。
12. 在还原角色窗格中，选择 AWS Backup 将为此还原担任的 IAM 角色。
13. 指定所有设置后，选择还原备份。

    这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。
14. 还原完成后，将还原的 Aurora 集群连接到 Amazon RDS 实例。

    使用 C AWS LI：

    - 对于 Linux、macOS 或 Unix：

```
aws rds create-db-instance --db-instance-identifier sample-instance \
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

    - 对于 Windows：

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

有关连续备份和 point-in-time 恢复到选定时间点的信息，请参阅连续备份和恢复 (PITR)。

使用 AWS Backup API、CLI 或软件开发工具包恢复 Aurora 恢复点

使用 StartRestoreJob。在 Aurora 还原期间，您可以指定以下元数据：

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

例如：

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"
```

还原 Amazon EC2 实例

恢复 EC2 实例时， AWS Backup 会创建亚马逊系统映像 (AMI)、实例、亚马逊 EBS 根卷、亚马逊 EBS 数据卷（如果受保护的资源有数据卷）和 Amazon EBS 快照。您可以使用 AWS Backup 控制台自定义一些实例设置，也可以使用或 AWS SDK 自定义更多设置。 AWS CLI

以下注意事项适用于恢复 EC2 实例：

- AWS Backup 将还原的实例配置为使用与受保护资源最初使用的密钥对相同。在还原过程中，您不能为还原的实例指定不同的密钥对。
- AWS Backup 不会备份和还原启动 Amazon EC2 实例时使用的用户数据。
- 配置已还原的实例时，您可以选择使用与受保护资源最初使用的相同实例配置文件或在没有实例配置文件的情况下启动。这是为了防止可能出现权限升级。您可以使用 Amazon EC2 控制台更新已恢复实例的实例配置文件。

  如果您使用原始实例配置文件，则必须授予 AWS Backup 以下权限，其中资源 ARN 是与实例配置文件关联的 IAM 角色的 ARN。

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

- 在还原期间，所有 Amazon EC2 配额和配置限制均适用。
- 如果包含您的 Amazon EC2 恢复点的文件库有文件库锁，其它安全注意事项请参见以获取更多信息。

使用 AWS Backup 控制台恢复 Amazon EC2 恢复点

您可以从单个恢复点恢复整个 Amazon EC2 实例，包括根卷、数据卷和一些实例配置设置，例如实例类型和密钥对。

使用 AWS Backup 控制台恢复 Amazon EC2 资源

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源，然后选择 Amazon EC2 资源的 ID 以打开资源详情页面。
3. 在恢复点窗格中，选择要还原的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 在网络设置窗格中，我们使用受保护实例的设置为实例类型、VPC、子网、安全组和实例 IAM 角色选择默认值。您可以使用这些默认值或根据需要进行更改。
5. 在还原角色窗格中，使用默认角色或使用选择 IAM 角色来指定授予还原备份 AWS Backup 权限的 IAM 角色。
6. 在受保护的资源标签窗格中，我们选择默认将标签从受保护的资源复制到还原的资源。如果您不想复制这些标签，请清除该复选框。

7. 在高级设置窗格中，接受实例设置的默认值或根据需要进行更改。有关这些设置的信息，请选择该设置的 “信息” 以打开其帮助窗格。
8. 完成实例配置后，选择恢复备份。

使用恢复亚马逊 EC2 AWS CLI

在命令行界面中，start-restore-job允许您使用最多 32 个参数（包括一些无法通过 AWS Backup 控制台自定义的参数）进行恢复。

以下列表中所列的是接受的元数据，您可以传递它们以还原 Amazon EC2 恢复点。

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
aws:backup:request-id
```

AWS Backup 接受以下仅提供信息的属性。但是，添加它们不会影响还原：

```
vpcId
```

您还可以在不包含任何存储的参数的情况下还原 Amazon EC2 实例。 AWS Backup 控制台的“受保护的资源”选项卡上提供了此选项。

还原 Storage Gateway 卷

如果您要恢复 AWS Storage Gateway 卷快照，则可以选择将快照恢复为 Storage Gateway 卷或 Amazon EBS 卷。这是因为与这两项服务 AWS Backup 集成，并且任何 Storage Gateway 快照都可以恢复到 Storage Gateway 卷或 Amazon EBS 卷。

通过 AWS Backup 控制台恢复 Storage Gateway

还原 Storage Gateway 卷

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Storage Gateway 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 指定资源的还原参数。您输入的还原参数将特定于所选的资源类型。

   对于资源类型，选择在还原此备份时要创建的 AWS 资源。
5. 如果选择 Storage Gateway 卷，请选择处于可访问状态的网关。另外，请选择您的 iSCSI 目标名称。

   1. 对于“存储卷”网关，选择磁盘 ID。
   2. 对于“卷缓存”网关，选择至少与受保护资源一样大的容量。

   如果选择 EBS 卷，请提供卷类型和大小 (GiB) 的值，然后选择可用区。
6. 对于还原角色，请选择 AWS Backup 将担任此还原的 IAM 角色。

   > **Note**
   >
   > 如果您的账户中没有 AWS Backup 默认角色，则会为您创建一个具有正确权限的默认角色。您可以删除此默认角色或使其无法使用。
7. 选择还原备份。

这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。

使用恢复 Storage Gateway AWS CLI

在命令行界面中，使用 `start-restore-job` 可以还原 Storage Gateway 卷。

以下列表中所列的是接受的元数据。

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and AWS ##.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

还原 Amazon Timestream 表

还原 Amazon Timestream 表时，需要配置多个选项，包括新表名称、目的地数据库、存储分配首选项（内存和磁性存储）以及将使用哪个角色来完成还原作业。您还可以选择一个 Amazon S3 存储桶来存储错误日志。磁性存储写入异步进行，因此您可能希望记录错误。

Timestream 数据存储有两层：内存存储和磁性存储。内存存储为必需项，但您可以选择在指定的内存时间结束后将还原后的表传输到磁性存储。内存存储针对高吞吐量数据写入和快速 point-in-time 查询进行了优化。磁性存储针对吞吐量较低的延迟数据写入、长期数据存储和快速分析查询进行了优化。

还原 Timestream 表时，您可以确定希望该表在每个存储层中保留多长时间。您可以使用控制台或 API 为两者设置存储时间。请注意，存储采用线性和顺序方式。Timestream 会先将还原后的表存储在内存存储中，然后在达到内存存储时间后自动将其转换到磁性存储。

> **Note**
>
> 磁性存储保留期必须等于或大于原始保留期（显示在控制台右上角），否则数据将丢失。

示例：您将内存存储分配设置为将数据保存一周，并将磁性存储分配设置为将相同的数据保存一年。当内存存储中的数据保存一周后，它会自动移至磁性存储。然后，它会保存在磁性存储中一年时间。在该时间结束时，会从 Timestream 和 AWS Backup中将其删除。

使用控制台恢复 Amazon Timestream 表 AWS Backup

您可以在 AWS Backup 控制台中恢复由 AWS Backup创建的 Timestream 表。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon Timestream 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 指定新的表配置设置，包括：
   a. 新表名称，由 2 到 256 个字符（字母、数字、短划线、句点和下划线）组成。
   b. 目的地数据库，从下拉菜单中选择。
5. 存储分配：设置还原后的表首先驻留在内存存储中的时间，并设置还原后的表随后驻留在磁性存储中的时间。内存存储可以设置为小时、天、周或月。磁性存储可以设置为天、周、月或年。
6. （可选）启用磁性存储写入：您可以选择允许磁性存储写入。选中此选项后，延迟到达的数据（即时间戳超出内存存储保留期的数据）将直接写入磁性存储。
7. （可选）Amazon S3 错误日志位置：您可以指定存储错误日志的 S3 位置。浏览您的 S3 文件或复制并粘贴 S3 文件路径。

   > **Note**
   >
   > 如果您选择指定 S3 错误日志位置，则用于此还原的角色必须具有写入 S3 存储桶的权限，或者它必须包含具有该权限的策略。

8. 选择要传递的用于执行还原的 IAM 角色。您可以使用默认 IAM 角色或指定其他角色。
9. 单击还原备份。

您的还原作业将显示在受保护的资源下。您可以通过单击刷新按钮或 CTRL-R 来查看还原作业的当前状态。

使用 API、CLI 或 SDK 还原 Amazon Timestream 表

使用 `StartRestoreJob` 通过 API 还原 Timestream 表。

要使用恢复时间流 AWS CLI，请使用操作`start-restore-job`.并指定以下元数据：

```
TableName: string;
DestinationDatabase: string;
```

```
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

示例模板如下：

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

还可以使用 DescribeRestoreJob 帮助获取还原信息。

在中 AWS CLI，使用操作describe-restore-job并使用以下元数据：

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

示例模板如下：

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

还原 Amazon Redshift 集群

您可以在 AWS Backup 控制台中或通过 CLI 恢复自动和手动快照。

在还原 Amazon Redshift 集群时，默认情况下将原始集群设置输入到控制台中。您可以为以下配置指定不同的设置。在还原表时，必须指定源数据库和目标数据库。有关这些配置的更多信息，请参阅《Amazon Redshift 管理指南》中的从快照还原集群。

- 单个表或集群：您可以选择还原整个集群或单个表。如果您选择还原单个表，则需要提供源数据库、源架构和源表名称，以及目标集群、架构和新表名称。
- 节点类型：每个 Amazon Redshift 集群均由一个领导节点和至少一个计算节点组成。在还原集群时，您需要指定符合您的 CPU、RAM、存储容量和驱动器类型要求的节点类型。
- 节点数：在还原集群时，您需要指定需要的节点数量。
- 配置摘要
- 集群权限

使用控制台恢复 Amazon Redshift 集群或表 AWS Backup

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择设置和要还原的 Amazon Redshift 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在恢复点窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 还原选项
   a. 从快照还原集群，或者
   b. 将快照中的单个表还原到新集群。如果选择此选项，则必须配置以下各项：
      i. 开启或关闭区分大小写的名称。
      ii. 输入源表值，包括数据库、架构和表。源表信息可以在 Amazon Redshift 控制台中找到。
      iii. 输入目标表值，包括数据库、架构和新表名称。
5. 指定新的集群配置设置。
   a. 对于集群还原：选择集群标识符、节点类型和节点数量。
   b. 指定可用区和维护时段。
   c. 您可以通过单击关联 IAM 角色关联其他角色。
6. 可选：其他配置：
   a. 默认情况下，使用默认值处于开启状态。

b. 使用下拉菜单选择网络和安全、VPC 安全组、集群子网组和可用区的设置。

c. 开启或关闭增强型 VPC 路由。

d. 确定是否要使您的集群端点可公开访问。如果是，VPC 之外的实例和设备可以通过集群端点连接到您的数据库。如果将其开启，请输入弹性 IP 地址。

7. 可选：数据库配置。您可以选择输入

   a. 数据库端口（通过在文本字段中键入）

   b. 参数组

8. 维护：您可以选择

   a. 维护时段

   b. 维护记录，从当前、尾随或预览中进行选择。这控制将在维护时段内应用的集群版本。

9. 自动快照设置为默认值。

   a. 自动快照保留期。保留期必须为 0 到 35 天。选择 0 将不创建自动快照。

   b. 手动快照保留期为 1 到 3653 天。

   c. 有一个可选复选框用于集群重新定位。如果选中此复选框，则允许将您的集群重新定位到另一个可用区。启用重新定位后，您可以使用 VPC 端点。

10. 监控：集群恢复后，您可以通过 CloudWatch 或 Amazon Redshift 设置监控。

11. 选择要传递的用于执行还原的 IAM 角色。您可以使用默认角色或指定其他角色。

您的还原作业将显示在作业下。您可以通过单击刷新按钮或 CTRL-R 来查看还原作业的当前状态。

使用 API、CLI 或 SDK 还原 Amazon Redshift 集群

使用 `StartRestoreJob` 还原 Amazon Redshift 集群。

要使用恢复 Amazon Redshift AWS CLI，请使用命令`start-restore-job`并指定以下元数据：

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
```

```
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

有关更多信息，请参阅《Amazon Redshift API 参考》中的 RestoreFromClusterSnapshot 和《AWS CLI 指南》中的 restore-from-cluster-snapshot。

示例模板如下：

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region AWS ##
-\-endpoint-url URL
```

示例如下：

```
aws backup start-restore-job \
```

```
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

还可以使用 DescribeRestoreJob 帮助获取还原信息。

在中 AWS CLI，使用操作describe-restore-job并使用以下元数据：

```
Region
```

示例模板如下：

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region AWS ##
```

示例如下：

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

还原 Amazon EC2 实例上的 SAP HANA 数据库

可以使用 AWS Backup 控制台、API 或使用恢复 EC2 实例上的 SAP HANA 数据库 AWS CLI。

主题

- 使用 AWS Backup 控制台恢复 Amazon EC2 实例数据库上的 SAP HANA
- StartRestoreJob EC2 上适用于 SAP HANA 的 AP@@ I
- 适用于 EC2 上 SAP HANA 的 CLI
- 故障排除

使用 AWS Backup 控制台恢复 Amazon EC2 实例数据库上的 SAP HANA

请注意，涉及同一数据库的备份作业和还原作业不能同时进行。在执行 SAP HANA 数据库还原作业时，尝试备份同一数据库可能会导致错误：“数据库在停止时无法备份”。

1. 使用先决条件中的凭证访问 AWS Backup 控制台。
2. 在目标还原位置下拉菜单下，选择要使用您要用于还原的恢复点覆盖的数据库（请注意，托管还原目标数据库的实例也必须具有先决条件中的权限）。

   > **Important**
   >
   > SAP HANA 数据库还原具有破坏性。还原数据库将覆盖位于指定目标还原位置的数据库。

3. 只有在执行系统副本还原时才完成此步骤；否则，请跳至步骤 4。

   系统副本还原是一种还原作业，它还原到目标数据库与生成恢复点的源数据库不同。对于系统副本还原，请注意控制台上为您提供的 `aws ssm-sap put-resource-permission` 命令。必须在满足先决条件的计算机上复制、粘贴和执行此命令。运行此命令时，请使用设置注册应用程序所需权限的先决条件中的角色中的凭证。

   ```
   // Example command
   aws ssm-sap put-resource-permission \
   --region us-east-1 \
   --action-type RESTORE \
   --source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
   --resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
   ```

4. 选择还原位置后，可以看到目标数据库的资源 ID、应用程序名称、数据库类型和 EC2 实例。
5. 或者，可以打开高级还原设置以更改目录还原选项。默认选择是从 AWS Backup中还原最新的目录。
6. 单击还原备份。
7. 由于将在还原期间覆盖目标位置（破坏性还原），因此您必须在接下来的弹出对话框中确认允许这样做。

   a. 要继续，您必须明白，现有数据库将被您要还原的数据库所覆盖。

   b. 明白这一点后，您必须确认现有数据将被覆盖。要确认这一点并继续，请在文本输入字段中键入 overwrite。

8. 单击还原备份。

如果该过程操作成功，控制台顶部将显示一条蓝色横幅。这表示还原作业正在进行中。您将被自动重定向到“作业”页面，您的还原作业将出现在还原作业列表中。这个最新作业的状态将为 `Pending`。您可

以搜索并单击还原作业 ID，以查看每个还原作业的详细信息。您可以通过单击“刷新”按钮来刷新还原作业列表，以查看还原作业状态的更改。

StartRestoreJob EC2 上适用于 SAP HANA 的 AP@@ I

此操作将恢复由一个 Amazon 资源名称 (ARN) 标识的已保存资源。

请求语法

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 请求参数：该请求不使用任何 URI 参数。

请求体：请求接受采用 JSON 格式的以下数据：

IdempotencyToken客户选择的字符串，可用于区分原本相同的调用。StartRestoreJob使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

元数据

一组元数据键值对。包含还原恢复点所需的信息，例如资源名称。您可以通过调用 GetRecoveryPointRestoreMetadata 来获取在备份资源时有关该资源的配置元数据。但是，除了 GetRecoveryPointRestoreMetadata 提供的值之外，可能还需要其他值才能还原资源。例如，如果原始资源名称已存在，您可能需要提供一个新的资源名称。

您需要包含特定元数据才能还原 Amazon EC2 实例上的 SAP HANA。请参阅 SAP HANA 特定项目的 StartRestoreJob 元数据。

要检索相关元数据，您可以使用调用 GetRecoveryPointRestoreMetadata。

标准 SAP HANA 数据库恢复点示例：

```
"RestoreMetadata": {
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

连续 SAP HANA 数据库恢复点示例：

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

适用于 EC2 上 SAP HANA 的 CLI

`start-restore-job` 命令将恢复由一个 Amazon 资源名称 (ARN) 标识的已保存资源。CLI 将遵循上面的 API 准则。

摘要：

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

Options

`--recovery-point-arn`（字符串）是 Amazon 资源编号 (ARN) 形式的字符串，用于唯一地标识恢复点；例如 `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata`（映射）：一组元数据键值对。包含还原恢复点所需的信息，例如资源名称。您可以通过调用 `GetRecoveryPointRestoreMetadata` 来获取在备份资源时有关该资源的配置元数据。但是，除了 `GetRecoveryPointRestoreMetadata` 提供的值之外，可能还需要其他值才能还原资源。您需要指定特定元数据才能还原 Amazon EC2 实例上的 SAP HANA：

- aws:backup:request-id: 这是用于幂等性的任何 UUID 字符串。它不会以任何方式改变您的还原体验。
- aws:backup:TargetDatabaseArn：指定要还原到的数据库。这是 Amazon EC2 上的 SAP HANA 数据库 ARN。
- CatalogRestoreOption：指定从何处还原目录。选择 NO_CATALOG、LATEST_CATALOG_FROM_AWS_BACKUP 和 CATALOG_FROM_LOCAL_PATH 之一：
- LocalCatalogPath：如果 CatalogRestoreOption 元数据值为CATALOG_FROM_LOCAL_PATH，则在您的 EC2 实例上指定本地目录的路径。它应该是您的 EC2 实例中的有效文件路径。
- RecoveryType：当前支持 FULL_DATA_BACKUP_RECOVERY、POINT_IN_TIME_RECOVERY 和 MOST_RECENT_TIME_RECOVERY 恢复类型。

键 =（字符串）；值 =（字符串）。速记语法：

```
KeyName1=string,KeyName2=string
```

JSON 语法：

```
{"string": "string"
  ...}
```

--idempotency-token 是客户选择的字符串，可用于区分对 StartRestoreJob 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

--resource-type 是一个字符串，它启动用于还原以下资源之一的恢复点的作业：SAP HANA on Amazon EC2（适用于 SAP HANA on Amazon EC2）。或者，可以使用命令 aws ssm-sap tag-resource 标记 SAP HANA 资源。

输出：RestoreJobId 是一个字符串，用于唯一地标识还原恢复点的作业。

故障排除

如果在尝试备份操作时出现以下任何错误，请参阅相关的解决方案。

- 错误：连续备份日志错误

  为了维护连续备份的恢复点，SAP HANA 会为所有更改创建日志。当日志不可用时，每个连续恢复点的状态都将变为 STOPPED。最后一个可用于还原的可行恢复点的状态为 AVAILABLE。如果在状

态为 STOPPED 的恢复点和状态为 AVAILABLE 的恢复点之间的时间内出现日志数据丢失，则无法保证这些时间能够成功还原。如果您输入的日期和时间在此范围内，AWS Backup 将尝试备份，但会使用最接近的可恢复时间。出现此错误时，将显示消息“Encountered an issue with log backups. Please check SAP HANA for details."

解决方案：在控制台中，将基于日志显示最近可还原时间。您可以输入比显示的时间更近的时间。但是，如果日志中没有该时间的数据，则 AWS Backup 将使用最新的可恢复时间。

- 错误：Internal error

  解决方案：通过控制台创建支持案例，或联系 AWS Support 并提供还原任务编号等还原详情。

- 错误：The provided role arn:aws:iam::*ACCOUNT_ID*:role/ServiceLinkedRole cannot be assumed by AWS Backup

  解决方案：确保调用还原时担任的角色具有创建服务相关角色所需的权限。

- 错误：User: arn:aws:sts::*ACCOUNT_ID*:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:*ACCOUNT_ID*:...

  解决方案：确保正确输入了调用先决条件中概述的还原权限时所担任的角色。

- 错误：b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n

  解决方案：确保正确安装了 Backint Agent。检查所有先决条件，尤其是在 SAP 应用程序服务器上安装 AWS BackInt 代理和适用 AWS Systems Manager 于 SAP 的必备条件，然后再次尝试安装 BackInt 代理。

- 错误：IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED

  解决方案：服务工作流程已取消还原作业。重试还原作业。

- 错误：RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"

  解决方案：实例上出现暂时性网络不稳定。请重试还原。如果此问题持续发生，请尝试将 ForceRetry: "true" 添加到 /hana/shared/aws-backint-agent/aws-backint-agent-config.yaml. 处的代理配置文件

有关任何其他与 AWS Backint 代理相关的问题，请参阅针对 SAP HANA 的 AWS Backint 代理进行故障排除。

还原 DocumentDB 集群

使用 AWS Backup 控制台恢复 Amazon DocumentDB 恢复点

还原 Amazon DocumentDB 集群需要指定多个还原选项。有关这些选项的信息，请参阅《Amazon DocumentDB 开发人员指南》中的从集群快照还原。

还原 Amazon DocumentDB 集群

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Amazon DocumentDB 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 在配置窗格中，接受集群标识符、引擎版本、实例类和实例的数量的默认值或指定这些选项。
   - 注意：如果还原时不存在默认 VPC，则必须在其他 VPC 中指定子网。
5. 在网络和安全窗格中，将显示“无首选项”。
6. 在 E ncryption-at-rest 窗格中，接受默认设置或指定启用加密或禁用加密设置的选项。
7. 在集群选项窗格中，键入端口，然后选择集群参数组。
8. 在 “备份” 窗格中，选择连续备份以进行 point-in-time 恢复 (PITR)、定时快照备份或两者兼而有之。
9. 在日志导出窗格中，选择要发布到 Amazon Logs 的 CloudWatch 日志类型。已定义 IAM 角色。
10. 在维护窗格中，指定维护时段或选择无首选项。
11. 在标签窗格中，可以选择添加标签。
12. 在删除保护窗格中，可以选中启用删除保护复选框。
13. 指定所有设置后，选择还原备份。

    这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。
14. 还原完成后，将还原的 Amazon DocumentDB 集群连接到 Amazon RDS 实例。

使用 AWS Backup API、CLI 或软件开发工具包恢复亚马逊 DocumentDB 恢复点

首先，还原您的集群。使用 StartRestoreJob。在 Amazon DocumentDB 还原期间，您可以指定以下元数据：

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

然后，使用 `create-db-instance` 将还原后的 Amazon DocumentDB 集群连接到 Amazon RDS 实例。

- 对于 Linux、macOS 或 Unix：

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- 对于 Windows：

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

还原 Neptune 集群

使用 AWS Backup 控制台恢复 Amazon Neptune 恢复点

还原 Amazon Neptune 数据库需要指定多个还原选项。有关这些选项的信息，请参阅《Neptune 用户指南》中的从数据库集群快照还原。

还原 Neptune 数据库

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源和要还原的 Neptune 资源 ID。
3. 在 Resource details (资源详细信息) 页面上，将显示所选资源 ID 的恢复点列表。要还原资源，请在备份窗格中，选择资源的恢复点 ID 旁边的单选按钮。在窗格的右上角，选择还原。
4. 在实例规格窗格中，接受默认值或指定数据库引擎和版本。
5. 在设置窗格中，为当前区域中您拥有的所有数据库集群实例指定一个唯一 AWS 账户 的名称。数据库集群标识符不区分大小写，但它以全小写形式存储，例如“mydbclusterinstance”。此字段为必填字段。
6. 在数据库选项窗格中，接受数据库端口、数据库集群参数组的默认值或指定这些选项。
7. 在加密) 窗格中，接受启用加密和禁用加密设置的默认值或指定这些选项。
8. 在日志导出窗格中，选择要发布到 Amazon Logs 的 CloudWatch 日志类型。已定义 IAM 角色。
9. 在还原角色窗格中，选择 AWS Backup 将为此还原担任的 IAM 角色。
10. 指定所有设置后，选择还原备份。

    这将显示还原作业窗格。页面顶部的消息提供了有关还原作业的信息。
11. 还原完成后，将还原的 Neptune 集群连接到 Amazon RDS 实例。

使用 AWS Backup API、CLI 或 SDK 恢复 Neptune 恢复点

首先，还原您的集群。使用 `StartRestoreJob`。在 Amazon DocumentDB 还原期间，您可以指定以下元数据：

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
```

```
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

然后，使用 `create-db-instance` 将还原后的 Neptune 集群连接到 Amazon RDS 实例。

- 对于 Linux、macOS 或 Unix：

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- 对于 Windows：

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

有关更多信息，请参阅《Neptune Management API 参考》中的 RestoreDBClusterFromSnapshot 和《Neptune CLI 指南》中的 restore-db-cluster-from-snapshot。

恢复 CloudFormation 堆栈备份

CloudFormation 复合备份是 CloudFormation 模板和所有关联的嵌套恢复点的组合。虽然可以还原任意数量的嵌套恢复点，但无法还原复合恢复点（即顶级恢复点）。

恢复 CloudFormation 模板恢复点时，您会创建一个新的堆栈，其中包含用于表示备份的更改集。

使用 AWS Backup 控制 CloudFormation 台恢复；

在CloudFormation 控制台中，您可以看到新的堆栈和更改集。要了解有关更改集的更多信息，请参阅《AWS CloudFormation 用户指南》中的使用更改集更新堆栈。

确定要使用 CloudFormation堆栈恢复的嵌套恢复点，然后使用 AWS Backup 控制台将其恢复。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 转到备份保管库，选择包含所需恢复点的备份保管库，然后单击恢复点。
3. 恢复 AWS CloudFormation 模板恢复点。
   a. 单击包含要还原的嵌套恢复点的复合恢复点，打开复合恢复点的“详细信息”页面。
   b. 在嵌套恢复点下，将显示嵌套的恢复点。每个恢复点都有恢复点 ID、状态、资源 ID、资源类型、备份类型和创建恢复点的时间。单击 AWS CloudFormation 恢复点旁边的单选按钮，然后单击 “恢复”。确保您选择的恢复点的资源类型为 AWS CloudFormation，备份类型为备份。
4. CloudFormation 模板的还原任务完成后，您恢复的 AWS CloudFormation 模板将在AWS CloudFormation 控制台的 Stacks 下方可见。
5. 在堆栈名称下，您应该查找状态为 `REVIEW_IN_PROGRESS` 的已还原模板。
6. 单击堆栈的名称以查看堆栈的详细信息。
7. 堆栈名称下有选项卡。单击更改集。
8. 执行更改集。
9. 此过程完成后，将在新堆栈中重新创建原始堆栈中的资源。有状态的资源将重新创建为空资源。要恢复有状态资源，请返回 AWS Backup 控制台中的恢复点列表，选择所需的恢复点，然后启动恢复。

CloudFormation 使用恢复 AWS CLI

在命令行界面中，`start-restore-job`允许您恢复堆 CloudFormation栈。

以下列表是恢复 CloudFormation 资源时可接受的元数据。

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

还原测试

主题

概述

恢复测试是提供的一项功能 AWS Backup，它可以自动定期评估恢复的可行性，并能够监控恢复作业的持续时间。

首先，创建还原测试计划，在其中提供计划的名称、还原测试的频率和目标开始时间。然后，分配要包含在计划中的资源。然后，您可以选择在测试中包括特定或随机的恢复点。 AWS Backup backup 可以智能地推断成功还原任务所需的元数据。

当计划中的预定时间到来时， AWS Backup 会根据您的计划启动恢复作业，并监控完成恢复所需的时间。

在还原测试计划完成运行后，您可以使用结果来证明是否符合组织或监管要求，例如，成功完成还原测试方案或还原作业的完成时间。

或者，您可以使用恢复测试验证来确认恢复测试结果。

在可选验证完成或验证窗口关闭后，将 AWS Backup 删除与还原测试相关的资源，并根据服务 SLA 删除这些资源。

在测试过程结束时，您可以查看测试的结果和完成时间。

还原测试与还原过程的比较

还原测试以与按需还原相同的方式运行还原作业，并使用与按需还原相同的恢复点（备份）。对于通过恢复测试启动`StartRestoreJob`的每项作业，你将看到调用 CloudTrail （如果选择加入）

但是，计划还原测试的操作和按需还原操作之间有一些区别：

	还原测试	还原
账户	推荐的最佳做法是指定一个用于还原测试的账户	您可以从账户还原资源
AWS Backup Audit Manager	可以启用控制功能以确认还原测试是否达到指定的还原目标	
节奏	作为计划的一部分定期实施。	按需
区域性	在除以色列（特拉维夫）以外的所有 AWS Backup 运营区域均可用 不可用 AWS GovCloud （美国东部）、 AWS GovCloud （美国西部）、中国（北京）和中国（宁夏）。	在所有 AWS Backup 运营的商业区域都可用
资源	您可以为测试计划分配的资源类型包括：Aurora、Amazon DocumentDB、Amazon DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、Amazon FSx（Lustre、ONTAP、OpenZFS、Windows）、Amazon	所有资源均可还原。

	还原测试	还原
	Neptune、Amazon RDS 和 Amazon S3。	
结果	恢复测试任务完成后，还原的资源将在恢复测试验证窗口结束后删除。	还原作业完成后，资源的还原版本将保留。
标签	对于在还原时支持标签的资源类型，测试功能会在还原时应用标签。	对于支持的资源，标签是可选的。

还原测试管理

您可以在 AWS Backup 控制台中创建、查看、更新或删除还原测试计划。

您可以使用 AWS CLI 以编程方式执行还原测试计划的操作。每个 CLI 都特定于其来源的 AWS 服务。命令应前缀 `aws backup`。

数据删除

恢复测试完成后， AWS Backup 开始删除测试中涉及的资源。此删除操作不会即时完成。每种资源都有一个底层配置，用于确定这些资源的存储方式和生命周期方式。例如，如果 Amazon S3 存储桶是还原测试的一部分，则会将生命周期规则添加到存储桶。执行规则和完全删除存储桶及其对象最多可能需要几天时间，但对于这些资源，只会在生命周期规则启动日之前（默认情况下为 1 天）收费。删除速度将取决于资源类型。

作为还原测试计划一部分的资源包含一个名为 `awsbackup-restore-test` 的标签。如果用户删除了此标签，则 AWS Backup 无法在测试期结束时删除该资源，用户必须手动将其删除。

要检查未按预期删除资源的原因，可以在控制台中搜索失败的作业，或者使用命令行界面调用 API 请求 `DescribeRestoreJob` 来检索删除状态消息。

Backup 计划（非恢复测试计划）会忽略恢复测试创建的资源（标签`awsbackup-restore-test`或名称以开头的资源`awsbackup-restore-test`）。

成本控制

对于还原测试，按每次还原测试收费。根据您的还原测试计划中包含的资源，作为计划一部分的还原作业也可能产生费用。有关详细信息，请参阅 AWS Backup 定价。

首次设置还原测试计划时，您可能会发现包括最少数量的资源类型和受保护资源会很有用，这样可以熟悉相关的功能、流程和平均成本。您可以在创建计划后对其进行更新，以添加更多资源类型和受保护的资源。

创建还原测试计划

还原测试计划分为两个部分：创建计划和分配资源。

使用控制台时，这些部分是按顺序进行的。在第一部分中，您将要设置名称、频率和开始时间。在第二部分中，您将要为测试计划分配资源。

使用 AWS CLI 和 API 时，请先使用`create-restore-testing-plan`。收到成功响应且已创建计划后，请针对要包含在计划中的每种资源类型使用 `create-restore-testing-selection`。

Console

第 I 部分：使用控制台创建还原测试计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，找到还原测试并将其选中。
3. 选择创建还原测试计划。
4. 一般性问题

    a. 名称：键入新还原测试计划的名称。名称一经创建便无法更改。名称只能包含字母数字字符和下划线。

    b. 测试频率：选择还原测试的运行频率。

    c. 开始时间：设置您希望开始测试的时间（以小时和分钟为单位）。您还可以设置本地时区以运行还原测试计划。

    d. 开始时间：此值（以小时为单位）是指定开始恢复测试的时间段。 AWS Backup 尽最大努力在一定时间内开始所有指定的恢复作业，并在此时间段内随机安排开始时间。
5. 恢复点选择：在这里，您可以设置源保管库、恢复点范围以及对要在计划中包含的恢复点（备份）的选择标准。

a. 源保管库：选择是包含所有可用的保管库，还是仅包含特定保管库，以帮助筛选您的计划中可以包含哪些恢复点。如果您选择特定保管库，请从下拉菜单中选择要包含的保管库。

b. 符合条件的恢复点：指定将从中选择恢复点的时间范围。您可以选择 1 到 365 天、1 到 52 周、1 到 12 个月或 1 年。

c. 选择标准：指定恢复点的日期范围后，您可以选择是将最新的恢复点还是随机选择的恢复点包含在计划中。您可能希望随机选择一个来以更规则的频率衡量恢复点的总体运行状况，以防需要还原到旧版本。

d. P oint-in-time 恢复点：如果您的计划包括具有连续备份 (point-in-time-restore/PITR) 点的资源，则可以选中此复选框，让您的测试计划包括连续备份作为符合条件的恢复点（请参阅按资源类型划分的功能可用性，哪些资源类型具有此功能）。

6. （可选）已添加到还原测试计划的标签：您最多可以选择在还原测试计划中添加 50 个标签。每个标签必须单独添加。要添加新标签，请选择添加新标签。

第 II 部分：使用控制台为计划分配资源

在本节中，您可以选择已备份的资源以包含在还原测试计划中。您将选择资源分配的名称，选择用于还原测试的角色，并设置清理前的保留期。然后，您将要选择资源类型，选择范围，并有选择地使用标签来细化选择。

> **Tip**
>
> 要返回到要向其中添加资源的还原测试计划，您可以转到 AWS Backup 控制台，选择还原测试，然后找到您的首选测试计划并将其选中。

1. 一般性问题

a. 资源分配名称：使用一串字母数字字符和下划线输入此资源分配的名称，不要含空格。

b. 还原 IAM 角色：测试必须使用您指定的 Identity and Access Management（IAM）角色。您可以选择 AWS Backup 默认角色或其他角色。如果在完成此过程时 AWS Backup 默认值尚不存在，则 AWS Backup 将使用必要的权限自动为您创建默认值。您为还原测试选择的 IAM 角色必须包含在 AWSBackupServicePolicyForRestores 中找到的权限。

c. 清理前的保留期：在还原测试期间，会临时还原备份数据。默认情况下，将在测试完成后删除这些数据。如果您希望在还原时运行验证，则可以选择延迟删除这些数据。

如果您计划运行验证，请选择保留特定的小时数，然后输入一个介于 1 到 168 小时（含）之间的值。请注意，验证可以通过编程方式运行，但不能从 AWS Backup 控制台运行。

2. 受保护的资源：

   a. 选择资源类型：选择要包含在资源测试计划中的资源类型以及这些类型的备份的范围。每个计划可以包含多种资源类型，但必须将每种类型的资源单独分配给计划。

   b. 资源选择范围：选择类型后，选择是要包括该类型的所有可用受保护资源，还是只想包括特定的受保护资源。

   c. （可选）使用标签优化资源选择：如果您的备份具有标签，则可以按标签筛选以选择特定的受保护资源。输入标签键、包含或不包含此键的条件以及该键的值。然后，选择添加标签按钮。

      通过检查包含受保护资源的备份保管库中最新恢复点上的标签来评估受保护资源上的标签。

3. 还原参数：某些资源需要指定参数以便为执行还原作业做好准备。在大多数情况下， AWS Backup 将根据存储的备份推断出值。

   在大多数情况下，建议保留这些参数；但是，您可以通过从下拉菜单中选择不同的选项来更改这些值。例如，最好更改值的情况可以包括：覆盖加密密钥、无法推断数据的 Amazon FSx 设置以及创建子网。

   例如，如果 RDS 数据库是您分配给还原测试计划的资源类型之一，则可用区、数据库名称、数据库实例类和 VPC 安全组等参数将显示并带有推断出的值，您可以根据情况对其进行更改。

AWS CLI

CLI 命令 `CreateRestoreTestingPlan` 用于制定还原测试计划。

测试计划必须包含：

- `RestoreTestingPlan`，它必须包含一个唯一的 `RestoreTestingPlanName`
- `ScheduleExpression` cron 表达式
- `RecoveryPointSelection`

  尽管命名类似，但这与不一样`RestoreTestingSelection`。

RecoveryPointSelection有五个参数（三个必填参数和两个可选参数）。您指定的值决定了恢复测试中包括哪个恢复点。您必须使用指明您Algorithm是否想要最新的恢复点，SelectionWindowDays或者是否想要一个随机恢复点，并且必须指明可以IncludeVaults从哪些保管库中选择恢复点。

一个选项可以具有一个或多个受保护的资源 ARN，也可以具有一个或多个条件，但不能同时具有这两者。

您也可以添加：

- ScheduleExpressionTimezone
- Tags
- CreatorRequestId
- StartWindowHours

使用 CLI 命令 create-restore-testing-plan。

成功创建计划后，您需要使用 create-restore-testing-selection 为其分配资源。

它包括 RestoreTestingSelectionName、ProtectedResourceType 和以下项之一：

- ProtectedResourceArns

- ProtectedResourceConditions

每种受保护的资源类型可以具有一个单一值。还原测试选择可以包括带通配符值（“*”）的 ProtectedResourceArns 以及 ProtectedResourceConditions。或者，您最多可以在 ProtectedResourceArns 中包括 30 个特定的受保护资源 ARN。

恢复点确定

每次运行测试计划时（根据您指定的频率和开始时间），还原测试都会为所选的每个受保护资源恢复一个符合条件的恢复点。如果某个资源的恢复点不符合恢复点选择标准，则该资源将不包括在测试中。

如果满足指定时间范围内的标准并将文件库包含在还原测试计划中，则测试选择中受保护资源的恢复点符合条件。

如果资源测试选择包括资源类型，并且满足以下任一条件，则会选择受保护的资源：

- 资源 ARN 在该选择中指定；或者，
- 该选择的标签条件与资源最新恢复点上的标签相匹配

更新还原测试计划

您可以通过控制台或 AWS CLI更新部分还原测试计划以及其中的资源选项。

Console

在控制台中更新还原测试计划和选项

在控制台中查看还原测试计划详细信息页面时，可以编辑（更新）计划的许多设置。为此，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，找到还原测试并将其选中。
3. 选择编辑按钮。
4. 调整频率、开始时间，以及所选开始时间后的测试开始时间范围。
5. 保存您的更改。

AWS CLI

通过更新恢复测试计划和选择 AWS CLI

请求UpdateRestoreTestingPlan和UpdateRestoreTestingSelection可用于向指定计划或选择发送部分更新。名称无法更改，但您可以更新其他参数。在每个请求中仅包含您想要更改的参数。

在发送更新请求之前，请使用GetRestoreTestingPlan和GetRestoreTestingSelection来确定您的请求是 RestoreTestingSelection包含特定的 ARN 还是使用通配符和条件。

如果您的还原测试选择指定了 ARN（而不是通配符），并且您希望将其更改为带条件的通配符，则更新请求必须同时包含 ARN 通配符和条件。选项可以具有受保护的资源 ARN，也可以使用带条件的通配符，但不能两者兼而有之。

- `get-restore-testing-plan`
- `get-restore-testing-selection`

- update-restore-testing-plan
- update-restore-testing-selection

查看现有的还原测试计划

Console

在控制台中查看有关现有还原测试计划和已分配资源的详细信息

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 从左侧导航窗格中，选择还原测试。显示屏中显示您的还原测试计划。默认情况下，会在最后一次运行时之前显示计划。
3. 从计划中选择链接以查看其详细信息，包括计划的摘要、名称、频率、开始时间和开始时间范围值。

您还可以查看此计划中的受保护资源、此计划中包含的最近 30 天的还原测试作业，以及您可以创建的要作为此测试计划一部分的任何标签。

AWS CLI

使用命令行获取有关现有还原测试计划和测试选项的详细信息

- list-restore-testing-plan
- list-restore-testing-selections
- get-restore-testing-plan
- get-restore-testing-selection

查看还原测试作业

Console

查看控制台中的现有还原测试作业

还原测试作业包含在“还原作业”页面上。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。

2. 导航至作业页面。

   或者，您可以选择还原测试，然后选择还原测试计划以查看其详细信息以及与该计划关联的作业。

3. 选择还原作业选项卡。

   在此页面上，您可以查看还原作业的状态、还原时间、还原类型、资源 ID、资源类型、作业所属的还原测试计划、创建时间和恢复点 ID。

   还原测试计划中包含的作业的还原类型为测试。

还原测试作业具有以下几个状态类别：

- 需要注意的状态类型带有下划线；将鼠标悬停在状态上方可查看其他详细信息（如果有）。
- 如果恢复测试验证已在测试中启动，则会显示验证状态（控制台中不可用）。
- 删除状态记录了还原测试生成的数据的状态。可能的删除状态有三种：成功、正在删除和失败。

  如果删除还原测试作业失败，则需要手动删除资源，因为还原测试流程无法自动完成该删除操作。通常，如果从资源中删除标签 `awsbackup-restore-test`，则会导致删除失败。

AWS CLI

在命令行中查看现有还原测试作业

- `list-restore-jobs-by-protected-resource`

删除还原测试计划

Console

在控制台中删除还原测试计划

1. 转至 查看现有的还原测试计划 查看您当前的还原测试计划。
2. 在还原测试计划详细信息页面上，通过选择删除来删除计划。
3. 选择删除后，将出现一个弹出式确认屏幕，以确保您要删除计划。在此屏幕上，您的特定还原测试计划的名称将以粗体显示。要继续，请键入测试计划的确切名称（区分大小写），其中可包括任何下划线、破折号和句点。

如果无法选择删除还原测试计划选项，请重新输入名称，直到它与显示的名称相匹配。一旦它完全匹配，用于删除还原测试计划的选项将变为可选状态。

AWS CLI

通过命令行删除还原测试计划

CLI 命令DeleteRestoreTestingSelection可用于删除恢复测试选项。在请求中包含 `RestoreTestingPlanName` 和 `RestoreTestingSelectionName`。

必须先删除与测试计划关联的所有测试选项，然后才能删除测试计划。删除所有测试选择后，您可以使用 API 请求DeleteRestoreTestingPlan删除恢复测试计划。您需要包括 `RestoreTestingPlanName`。

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

审核还原测试

恢复与 Audit m AWS Backup anager 的测试集成，以帮助您评估恢复的资源是否在目标还原时间内完成。

有关更多信息，请参阅 AWS Backup Audit Manager 控制和修复中的资源还原时间满足目标控制。

还原测试配额和参数

- 100 个还原测试计划
- 可向每个还原测试计划中添加 50 个标签
- 每个计划 30 个选项
- 每个选项 30 个受保护的资源 ARN
- 每个选项 30 个受保护的资源条件（包括 `StringEquals` 和 `StringNotEquals` 中的条件）
- 每个选项 30 个保管库选择器
- 最大选择时段天数：365 天
- 开始时段小时数：最短：1 小时；最长：168 小时（7 天）
- 计划名称的最大长度：50 个字符
- 选项名称的最大长度：50 个字符

有关限制的更多信息，可通过 AWS Backup 配额进行查看。

恢复测试失败疑难解答

如果您的恢复测试任务的恢复状态为Failed，则以下原因可以帮助您确定原因和补救措施。

可以在 AWS Backup 控制台的任务状态详细信息页面中查看错误消息，也可以使用 CLI 命令list-restore-jobs-by-protected-resource或来查看list-restore-jobs。

1. 错误：*No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.*

   解决方案 1：更新您的还原测试选择并覆盖该参数SubnetId。 AWS Backup 控制台将此参数显示为 “子网”。

   解决方案 2：重新创建默认 VPC。

   受影响的资源类型：Amazon EC2

2. 错误：*No subnets found for the default VPC [vpc]. Please specify a subnet.*

   解决方案 1：更新您的还原测试选择并覆盖SubnetId还原参数。 AWS Backup 控制台将此参数显示为 “子网”。

   解决方案 2：在默认 VPC 中创建默认子网。

   受影响的资源类型：Amazon EC2

3. 错误：*No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

   解决方案 1：更新您的还原测试选择并覆盖DBSubnetGroupName还原参数。 AWS Backup 控制台将此参数显示为子网组。

   解决方案 2：在默认 VPC 中创建默认子网。

   受影响的资源类型：亚马逊 Aurora、亚马逊 DocumentDB、亚马逊 RDS、Neptune

4. 错误：*IAM Role cannot be assumed by AWS Backup*。

解决方案：还原角色必须由担任。 AWS Backup要么在 IAM 中更新角色的信任策略以允许其代替，要"backup.amazonaws.com"么更新您的还原测试选择以使用可由 AWS Backup担任的角色。

受影响的资源类型：全部

5. 错误：*Access denied to KMS key.*或 *The specified AWS KMS key* ARN *does not exist, is not enabled or you do not have permissions to access it.*

   解决方案：验证以下各项：

   a. 还原角色可以访问用于加密备份的 AWS KMS 密钥，以及用于加密已还原资源的 KMS 密钥（如果适用）。

   b. 上述 KMS 密钥上的资源策略允许还原角色访问它们。

   如果尚未满足上述条件，请配置还原角色和资源策略以获得适当的访问权限。然后，再次运行恢复测试作业。

   受影响的资源类型：全部

6. 错误：*User ARN is not authorized to perform action on resource because no identity based policy allows the action.*或*Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*。

   解决方案：还原角色没有足够的权限。在 IAM 中更新还原角色的权限。

   受影响的资源类型：全部

7. 错误：*User ARN is not authorized to perform action on resource because no resource-based policy allows the action.*或 *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   解决方案：还原角色对消息中指定的资源没有足够的访问权限。更新上述资源的资源政策。

   受影响的资源类型：全部

还原测试推断出的元数据

还原恢复点需要还原元数据。为了执行还原测试， AWS Backup 会自动推断可能有助于实现成功还原的元数据。该命令`get-restore-testing-inferred-metadata`可用于预览 AWS Backup 将推断出的内容。该命令`get-restore-job-metadata`返回由 AWS Backup推断出的元数据集。请注意，对于某些资源类型 (Amazon FSx) AWS Backup ，无法推断出一组完整的元数据。

推断出的还原元数据是在还原测试过程中确定的。您可以通过在 `RestoreTestingSelection` 的正文中添加参数 `RestoreMetadataOverrides` 来覆盖某些还原元数据键。某些元数据覆盖在 AWS Backup 控制台中不可用。

每个支持的资源都具有推断出的还原元数据键和值，以及可覆盖的还原元数据键。只有 `RestoreMetadataOverrides` 键值对或标有`#######`的嵌套键值对，才必须包括在内；其他键值对都是可选的。请注意，键值不区分大小写。

> **Important**
>
> AWS Backup 可以推断资源应恢复到默认设置，例如 Amazon EC2 实例或 Amazon RDS 集群恢复到默认 VPC。但是，如果不存在默认值，例如默认 VPC 或子网已被删除且未输入任何元数据覆盖，则恢复将无法成功。

资源类型	推断出的还原元数据键和值	可覆盖的元数据

DynamoDB	`deletionProtection` ，其中值设置为 `false`
	
	`encryptionType` 设置为 `Default`
	
	`targetTableName` ，其中值设置为随机值（从 `awsbackup-restore-test-` 开始）
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` ，其值设置为随机可用区
	
	`encrypted` ，其值设置为 `true`
		`availabilityZone`
		
		`kmsKeyId`

资源类型	推断出的还原元数据键和值	可覆盖的元数据
Amazon EC2	disableApiTermination 值设置为 false instanceType 值设置为正在还原的恢复点的实例类型 requiredImdsV2 值设置为 true	iamInstanceProfileName 值可以为空或 UseBackedUpValue instanceType requireImdsV2 securityGroupIds subnetId
Amazon EFS	encrypted 值设置为 true file-system-id 值设置为正在还原的恢复点的文件系统 ID kmsKeyId value 设置为 alias/aws/elasticfilesystem newFileSystem 值设置为 true performanceMode 值设置为 generalPurpose	kmsKeyId
Amazon FSx for Lustre	lustreConfiguration 具有嵌套键。一个嵌套键是 automaticBackupRetentionDays ，其值设置为 0	kmsKeyId lustreConfiguration 具有嵌套键 logConfiguration securityGroupIds subnetIds ，#######

资源类型	推断出的还原元数据键和值	可覆盖的元数据
适用于 ONTAP 的亚马逊 FSx NetApp	name 设置为随机值（从 awsbackup_restore_test_ 开始） ontapConfiguration 具有嵌套键，其中包括： • junctionPath ，其中 / name 是正在还原的卷的名称 • sizeInMegabytes ，其值设置为正在还原的恢复点的大小（以兆字节为单位） • snapshotPolicy ，其值设置为 none	ontapConfiguration 具有特定的可覆盖嵌套键，其中包括： • junctionPath • ontapVolumeType • securityStyle • sizeInMegabytes • storageEfficiencyEnabled • storageVirtualMachineId ，####### • tieringPolicy
Amazon FSx for OpenZFS	openZfzConfiguration ，具有嵌套键，其中包括： • automaticBackupRetentionDays ，其值设置为 0 • deploymentType ，其值设置为正在还原的恢复点的部署类型 • throughputCapacity ，其值基于 deploymentType 。如果 deploymentType 为 SINGLE_AZ_1 ，则该值设置为 64；如果 deploymentType 为 SINGLE_AZ_2 or MULTI_AZ_1 ，则该值设置为 160	kmsKeyId openZfsConfiguration 具有特定的可覆盖嵌套键，其中包括： • deploymentType • throughputCapacity • diskiopsConfiguration securityGroupIds subnetIds

资源类型	推断出的还原元数据键和值	可覆盖的元数据
Amazon FSx for Windows File Server	windowsConfiguration ，具有嵌套键，其中包括： • automaticBackupRetentionDays ，其值设置为 0 • deploymentType ，其值设置为正在还原的恢复点的部署类型 • throughputCapacity ，其值设置为 8	kmsKeyId securityGroupIds subnetIds *#######* windowsConfiguration ，带有特定的可覆盖嵌套键 • throughputCapacity • activeDirectoryId *########selfManagedActiveDirectoryConfiguration #######* • selfManagedActiveDirectoryConfiguration *########activeDirectoryId #######* • preferredSubnetId

资源类型	推断出的还原元数据键和值	可覆盖的元数据
Amazon RDS、Aurora、Amazon DocumentDB、Amazon Neptune 集群	availabilityZones ，其值设置为列有多达三个随机可用区的列表 dbClusterIdentifier ，从 awsbackup-restore-test 开始的随机值 engine，其值设置为正在还原的恢复点的引擎	availabilityZones databaseName dbClusterParameterGroupName dbSubnetGroupName enableCloudwatchLogsExports enableIamDatabaseAuthentication engine engineMode engineVersion kmskeyId port optionGroupName scalingConfiguration vpcSecurityGroupIds

资源类型	推断出的还原元数据键和值	可覆盖的元数据
Amazon RDS 实例	dbInstanceIdentifier ，从 awsbackup-restore-test- 开始的随机值 deletionProtection ，其值设置为 false multiAz，其值设置为 false publiclyAccessible ，其值设置为 false	allocatedStorage availabilityZones dbInstanceClass dbName dbParameterGroupName dbSubnetGroupName domain domainIamRoleName enableCloudwatchLogsExports enableIamDatabaseAuthentication iops licensemodel multiAz optionGroupName port processorFeatures publiclyAccessible storageType vpcSecurityGroupIds

资源类型	推断出的还原元数据键和值	可覆盖的元数据

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` ，从 `awsbackup-restore-test-` 开始的随机值
	
	`encrypted` ，其值设置为 `true`
	
	`encryptionType` ，其值设置为 `SSE-S3`
	
	`newBucket` ，其值设置为 `true`
		`encryptionType`
		
		`kmsKey`

恢复测试验证

您可以选择创建事件驱动的验证，该验证在恢复测试作业完成时运行。

首先，使用 Amazon 支持的任何目标创建验证工作流程 EventBridge，例如 AWS Lambda。其次，添加一条 EventBridge 规则，监听恢复任务是否达到状态`COMPLETED`。第三，制定恢复测试计划（或者让现有计划按计划运行）。最后，在还原测试完成后，监控验证工作流程的日志，确保其按预期运行（验证运行后，AWS Backup 控制台中将显示验证状态）。

1. 设置验证工作流程

   您可以使用 Lambda 或支持的任何其他目标来设置验证工作流程。 EventBridge例如，如果您正在验证包含 Amazon EC2 实例的还原测试，则可以包含用于对运行状况检查终端节点执行 ping 操作的代码。

   您可以使用事件中的详细信息来确定要验证哪些资源。

   您可以使用自定义 Lambda 层来使用最新的软件开发工具包（因为`PutRestoreValidationResult`尚未通过 Lambda 开发工具包提供）。

   以下是一个示例：

```
import { Backup } from "@aws-sdk/client-backup";
```

```
export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. 添加 EventBridge 规则

   创建监听还原作业COMPLETED事件的 EventBridge 规则。

   或者，您可以按资源类型筛选事件或恢复测试计划 ARN。将此规则的目标设置为调用您在步骤 1 中定义的验证工作流程。示例如下：

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
```

```
        "COMPLETED"
      ]
    }
}
```

3. 让恢复测试计划运行并完成

   恢复测试计划将根据您配置的时间表运行。

   如果您还没有恢复测试计划，请参阅创建恢复测试计划；如果要更改设置，请参阅更新恢复测试计划。

4. 监控结果

   恢复测试计划按计划运行后，您可以检查验证工作流程的日志以确保其正确运行。

   您可以调用 API `PutRestoreValidationResult` 来发布结果，然后可以在AWS Backup 控制台中查看，也可以通过描述和列出恢复任务 AWS Backup 的 API 调用（例如`DescribeRestoreJob`或`ListRestoreJob`）进行查看。

   一旦设置了验证状态，就无法对其进行更改。

查看备份列表

您可以使用AWS Backup 控制台或以编程方式查看备份列表。

主题

- 在控制台中按受保护资源列出备份
- 在控制台中按备份保管库列出备份
- 以编程方式列出备份

在控制台中按受保护资源列出备份

在 AWS Backup 控制台上按照以下步骤，查看特定资源的备份列表。

1. 登录并打开 AWS Backup 控制台 AWS Management Console，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择受保护的资源。

3. 在列表中，选择一个受保护的资源来查看备份的列表。只有已由 AWS Backup 备份的资源才会列在“受保护的资源”下。

您可以查看资源的备份。从此视图中，您还可以选择备份并进行还原。

在控制台中按备份保管库列出备份

按照以下步骤，查看备份保管库中组织的备份列表。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 在备份部分中，查看此备份保管库中组织的所有备份的列表。在此视图中，您可以按任意列标题（包括状态）对备份进行排序，也可以选择要还原、编辑或删除的备份。

以编程方式列出备份

您可以使用 `ListRecoveryPoint` API 操作以编程方式列出备份：

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

例如，以下 AWS Command Line Interface (AWS CLI) 命令列出了`EXPIRED`状态为的所有备份：

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

您可以使用 AWS Backup Audit Manager 根据您定义的控制措施来审核 AWS Backup 策略的合规性。控制是一种旨在审核备份要求（例如备份频率或备份保留期）的合规性的程序。

AWS Backup Audit Manager 可帮助您回答以下问题：

- “我是否在备份所有资源？”
- “我的所有备份都加密了吗？”
- “我的备份每天都在进行吗？”

您可以使用 Au AWS Backup dit Manager 来查找尚未符合您定义的控制措施的备份活动和资源。请注意，仅在控制评估资源的合规性时，才会包括活动资源。例如，将评估处于运行状态的 Amazon EC2 实例。处于停止状态的 EC2 实例将不包括在合规性评估中。

您还可以使用它自动生成每日报告和按需报告的审计跟踪，以实现备份治理。

以下步骤概述了如何使用 Audit M AWS Backup anager。有关详细演练，请选择此页面末尾的主题之一。

1. 创建包含一个或多个治理控制模板的框架。前面的问题是三个治理控制模板的示例。您可以自定义某些治理控制模板的参数。例如，您可以自定义最后一个控件，询问，“我的备份是否每周进行一次？”，而不是每天进行。
2. 查看您的框架，了解有多少资源符合（或不符合）您在该框架中定义的控制。
3. 创建备份和合规性状态报告。存储这些报告，以此来证明您的合规性实践，或者用于识别尚不合规的个别备份活动和资源。

   AWS Backup Audit Manager 每 24 小时自动为您生成一份新报告，并将其发布到 Amazon S3。您也可以生成按需报告。

> **Note**
>
> 在创建第一个与合规性相关的框架之前，必须开启资源跟踪功能。这样 AWS Config 做可以跟踪您的 AWS Backup 资源。有关如何管理资源跟踪的技术文档，请参阅AWS Config 开发人员指南中的 AWS Config 使用控制台进行设置。

当您开启资源跟踪功能时，将收取费用。有关 Audit Manager 的 AWS Backup 资源跟踪定价和账单的信息，请参阅计量、成本和账单。

主题

使用审计框架

框架是帮助您评估备份实践的控件集合。您可以使用预构建的可自定义控件来定义策略，并评估您的备份实践是否符合您的策略。您还可以设置自动每日报告，以深入了解框架的合规性状态。

每个框架都适用于一个账户，并且 AWS 区域. 每个区域每个账户最多可以部署 15 个框架。您不能部署重复的框架（即包含相同控件和参数的框架）。

有两种不同类型的框架：

- AWS Backup 框架（推荐）- 使用 AWS Backup 框架部署所有可用的控件，根据我们推荐的最佳实践来监控您的备份活动、覆盖范围和资源。
- 您定义的自定义框架 - 使用自定义框架选择一个或多个特定控件并自定义控件参数。

主题

选择您的控件

下表列出了 Au AWS Backup dit Manager 控件、其可自定义参数和 AWS Config 记录资源类型。每个控件都需要记录资源类型 `AWS Config: resource compliance`，因为这种类型会记录您的合规性状态。

可用控件

控件名称	控件描述	可自定义的参数	AWS Config 录制资源类型
受备份计划保护的备份资源	评估资源是否受备份计划保护。	无	`AWS Backup: backup selection`
备份计划具有最低频率和最低保留期	评估备份频率是否至少为 [1 天]，保留期是否至少为 [35 天]。	备份频率；保留期	`AWS Backup: backup plans`
保管库可防止手动删除恢复点	评估备份库是否不允许手动删除某些 AWS Identity and Access Management (IAM) 角色以外的恢复点。默认情况下，IAM 角色不存在例外。在 AWS Backup 框架中部署此控件时，也没有 IAM 角色异常。	最多 5 个 IAM 角色，以允许手动删除恢复点	`AWS Backup: backup vaults`
恢复点经过加密	评估恢复点是否已加密。	无	`AWS Backup: recovery points`
为恢复点设定的最低保留期	评估恢复点保留期是否至少为 [35 天]。	恢复点保留期	`AWS Backup: recovery points`
计划跨区域备份复制	评估是否将资源配置为将其备份副本创建到另一个 AWS 区域。	AWS 区域	`AWS Backup: backup selection`

控件名称	控件描述	可自定义的参数	AWS Config 录制资源类型
计划跨账户备份复制	评估资源是否配置了跨账户备份副本。	AWS 账号	`AWS Backup: backup selection`
备份受 AWS Backup 文件库锁保护	评估是否将资源配置为在锁定的备份保管库中存放备份。	最小保留天数；最大保留天数	`AWS Backup: backup selection`
已创建上一个恢复点	评估是否在指定的时间范围内创建了恢复点。	以小时 [1 到 744] 或天 [1 到 31] 为单位的值。	`AWS Backup recovery points`
资源还原时间满足目标	评估还原测试作业是否在目标还原时间内完成	以分钟为单位的值	无

有关这些控件的详细信息，请参阅 控制和修复。

有关不支持所有控件的 AWS Backup支持的资源列表，请参阅按资源划分的功能可用性表格的 Audi AWS Backup t Manager 部分。

> **Note**
>
> 如果您不想使用上述任何控件，您仍然可以使用 Audit AWS Backup Manager 创建备份、复制和还原作业的每日报告。请参阅使用审计报告。

开启资源跟踪

在创建第一个与合规性相关的框架之前，必须开启资源跟踪功能。这样 AWS Config 做可以跟踪您的 AWS Backup 资源。有关如何管理资源跟踪的技术文档，请参阅AWS Config 开发人员指南中的 AWS Config 使用控制台进行设置。

当您开启资源跟踪功能时，将收取费用。有关 Audit Manager 的 AWS Backup 资源跟踪定价和账单的信息，请参阅计量、成本和账单。

主题

使用控制台开启资源跟踪

使用控制台开启资源跟踪：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格的 Audit Manager 下，选择框架。
3. 选择管理资源跟踪，以开启资源跟踪。
4. 选择 “前往 AWS Config 设置”。
5. 选择启用或禁用记录。
6. 为以下所有资源类型选择启用记录，或者选择为某些资源类型启用记录。请参阅 AWS Backup Audit Manager 控件和补救措施，了解您的控件需要哪些资源类型。

   - `AWS Backup: backup plans`
   - `AWS Backup: backup vaults`
   - `AWS Backup: recovery points`
   - `AWS Backup: backup selection`

   > **Note**
   >
   > AWS Backup Audit Manager 需要每`AWS Config: resource compliance`项控制。

7. 选择关闭。
8. 等待带有文本打开资源跟踪的蓝色横幅变为带有文本资源跟踪已开启的绿色横幅。

您可以在 AWS Backup 控制台的两个位置查看是否已开启资源跟踪，如果是，则可以查看正在记录哪些资源类型。在左侧导航窗格中，执行以下一项操作：

- 选择框架，然后选择 AWS Config 记录器状态下的文本。
- 选择设置，然后选择 AWS Config 记录器状态下的文本。

使用 AWS Command Line Interface (AWS CLI) 开启资源跟踪

如果您尚未登录 AWS Config，则使用上手可能会更快地上手。 AWS CLI

使用 AWS CLI开启资源跟踪：

1. 键入以下命令以确定是否已启用 AWS Config 记录器。

```
$ aws configservice describe-configuration-recorders
```

   a. 如果 ConfigurationRecorders 列表为空，如下所示：

```
{
  "ConfigurationRecorders": []
}
```

      则表明您的记录器未启用。请继续执行步骤 2 以创建记录器。

   b. 如果您已经为所有资源启用了记录功能，则 ConfigurationRecorders 输出将如下所示：

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

      由于您启用了所有资源，表明您已经开启资源跟踪功能。您无需完成本过程的其余部分即可使用 Audit M AWS Backup anager。

   c. 如果 ConfigurationRecorders 不为空，但您尚未为所有资源启用记录功能，请使用以下命令将备份资源添加到现有记录器中。然后，跳至步骤 3。

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

2. 使用 Au AWS Config dit Manag AWS Backup er 资源类型创建记录器

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. 描述一下你的 AWS Config 录音机。

```
$ aws configservice describe-configuration-recorders
```

通过将您的输出与以下预期输出进行比较，验证其是否具有 Audit Manager 资源类型。 AWS Backup

```
{
  "ConfigurationRecorders":[
```

```
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. 创建一个 Amazon S3 存储桶作为存储 AWS Config 配置文件的目标。

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. 使用 *policy.json* 授予访问您的存储桶的 AWS Config 权限。查看下面的示例 *policy.json*。

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
```

```
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. 将您的存储桶配置为 AWS Config 配送渠道

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. 启用 AWS Config 录制

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. 验证 DescribeFramework 输出最后一行中的 "FrameworkStatus":"ACTIVE"，如下所示。

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
```

```
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[

      ],
      "ControlScope":{
```

```
      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    }
  ],
  "CreationTime":1633463605.233,
  "DeploymentStatus":"COMPLETED",
  "FrameworkStatus":"ACTIVE"
}
```

使用 AWS CloudFormation 模板开启资源跟踪

有关启用资源跟踪的 AWS CloudFormation 模板，请参阅将 Audit Manager 与一起使用 AWS BackupAWS CloudFormation。

使用 AWS Backup 控制台创建框架

开启资源跟踪后，可使用以下步骤创建框架。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择框架。
3. 选择创建框架。
4. 对于框架名称，输入一个唯一名称。框架名称的长度必须介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。
5. （可选）输入框架描述。
6. 在控件中，将显示您的活动控件。默认情况下，会列出所有符合资源条件的控件。

   要更改哪些控件处于活动状态，请单击编辑控件。

   a. 第一个复选框表示控件是否已开启。要关闭控件，请取消选中该复选框。

   b. 在选择要评估的资源下，您可以选择如何按类型、标签或单个资源选择资源。

AWS Backup Audit Manager 控件列表描述了每个控件的自定义选项。

7. （可选）通过选择添加新标签，标记您的框架。您可以使用标签来搜索和筛选您的框架或跟踪成本。
8. 选择创建框架。

AWS Backup Audit Manager 可能需要几分钟才能创建框架。

如果出现错误 `AlreadyExists`，则说明已存在具有相同控件和参数的框架。要成功创建新框架，必须至少有一个控件或参数与现有框架不同。

使用 AWS Backup API 创建框架

下表包含针对每个控件 CreateFramework 的 API 请求示例，以及对相应 DescribeFramework 请求的 API 响应示例。要以编程方式 AWS Backup 使用 Audit Manager，可以参考这些代码片段。

控件	**CreateFramework** 请求	**DescribeFramework** 响应
Backup resources are protected by a backup plan	<pre>{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }],</pre>	<pre>{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope":</pre>

控件	CreateFramework 请求	DescribeFramework 响应
	<pre>"IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>{"Complia nceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }</pre>

控件	**CreateFramework** 请求	**DescribeFramework** 响应
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"}

控件	CreateFramework 请求	DescribeFramework 响应
	<pre>"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>

控件	CreateFramework 请求	DescribeFramework 响应
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

控件	CreateFramework 请求	DescribeFramework 响应
	"Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }	ole/service-role/Q uickSightAction"}], "ControlScope": {"Complia nceResourceIds":[" default"], "Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }

控件	**CreateFramework** 请求	**DescribeFramework** 响应
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"}

控件	CreateFramework 请求	DescribeFramework 响应
		} }

Backup recovery points are encrypted	{"FrameworkName":
	"Control5",
	"FrameworkDescript
	ion": "This is a test
	framework",
	"FrameworkControls":
	[
	{"ControlName":
	"BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	"ControlInputParam
	eters":
	[],
	"ControlScope":
	{} // Default scope
	(no scope input) is all
	recovery points
	}
	],
	"IdempotencyToken":
	"Control5",
	"FrameworkTags":
	{"key1": "foo"}
	}
		{"FrameworkName":
		"Control5",
		"FrameworkArn":
		"arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		"FrameworkDescript
		ion": "This is a test
		framework",
		"FrameworkControls
		":
		[
		{"ControlName":
		"BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		"ControlInputParam
		eters":
		[],
		"ControlScope": {}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control5",
		"FrameworkTags":
		{"key1": "foo"}
		}

控件	CreateFramework 请求	DescribeFramework 响应
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

控件	**CreateFramework** 请求	**DescribeFramework** 响应
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

控件	**CreateFramework** 请求	**DescribeFramework** 响应
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

控件	CreateFramework 请求	DescribeFramework 响应
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

控件	CreateFramework 请求	DescribeFramework 响应
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

控件	**CreateFramework** 请求	**DescribeFramework** 响应
	}	

查看框架合规性状态

创建审计框架后，它会显示在框架表中。您可以通过在 AWS Backup 控制台的左侧导航窗格中选择“框架”来查看此表。要查看框架的审计结果，请选择其框架名称。这样做会将您带到框架详细信息页面，其中包含两个部分：摘要和控件。

摘要部分从左到右列出了以下状态：

- 合规性状态是审计框架的总体合规性状态，由其每个控件的合规性状态决定。每个控件的合规性状态由其评估的每个资源的合规性状态决定。

  只有当控件评估范围内的所有资源都通过这些评估时，框架合规性状态才会为 Compliant。如果一个或多个资源未通过控件评估，则合规性状态将为 Non-Compliant。有关如何查找不合规资源的信息，请参阅查找不合规资源。有关如何使您的资源合规的信息，请参阅 AWS Backup Audit Manager 控件和补救措施的补救措施部分。
- 框架状态是指您是否已为所有资源开启资源跟踪。可能状态包括：
  - Active，当框架评估的所有资源启用记录时。
  - Partially active，当框架评估的至少一种资源启用记录时。
  - Inactive，当框架评估的所有资源关闭记录时。
  - Unavailable当 AWS Backup Audit Manager 此时无法验证录制状态时。

  更正 **Partially active** 或 **Inactive** 状态

  1. 在左侧导航窗格中，选择框架。
  2. 选择管理资源跟踪。
  3. 按照弹出窗口中的说明启用之前未针对您的资源类型启用的记录。

  有关哪些资源类型需要根据您在框架中包含的控件进行资源跟踪的更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施的资源部分。
- 部署状态是指您框架的部署状态。这种状态通常应该是 Completed，但也可以是 Create in progress、Update in progress、Delete in progress 和 Failed。

  - 状态 Failed 表示框架未正确部署。删除框架，然后通过 AWS Backup 控制台 或 AWS Backup API 重新创建框架。
- 合规控件显示所有评估均已通过的框架控件的数量。
- 不合规控件显示至少一项评估未通过的框架控件的数量。

控件部分会显示以下信息：

- 控件状态是指每个控件的合规性状态。控件可以处于 Compliant 状态，表示所有资源都通过了该评估；Non-compliant，表示至少有一个资源未通过该评估，或者 Insufficient data，表示控件在评估范围内找不到可供评估的资源。
- 评估范围可能会将每个控件限制为一种或多种资源类型、一个资源 ID 或一个标签键和标签值，具体取决于您在创建审计框架时如何自定义控件。如果所有字段均为空（如破折号“-”所示），则控件将评估所有适用的资源。

查找不合规资源

AWS Backup Audit Manager 通过两种方式帮助您找出哪些资源不合规。

- 查看框架合规性状态时，请在详细信息部分中选择控件名称。这样做会将你带到 AWS Config 控制台，在那里你可以查看你的Non-Compliant资源列表。
- 使用包含框架的资源合规性模板创建报告计划后，您可以查看报告以识别所有控件中的所有 Non-Compliant 资源。

  此外，Resource compliance report还会显示 AWS Backup Audit Manager 上次评估您的每个控件的时间。

更新审计框架

您可以更新现有审计框架的描述、控件和参数。

更新现有框架

1. 在 AWS Backup 控制台的左侧导航窗格中，选择 “框架”。
2. 按框架名称选择要编辑的框架。
3. 选择编辑。

删除审计框架

删除现有框架

1. 在 AWS Backup 控制台的左侧导航窗格中，选择 “框架”。
2. 按框架名称选择要删除的框架。
3. 选择删除。
4. 键入框架的名称，然后选择删除框架。

使用审计报告

AWS Backup Audit Manager 报告是自动生成的 AWS Backup 活动证据，例如：

- 哪些备份作业已完成以及何时完成
- 您备份了哪些资源

有两种类型的报告。创建报告时，您可以选择要创建的报告类型。

一种是作业报告，它显示过去 24 小时内完成的作业以及所有活动作业。作业报告不显示 `completed with issues` 状态。要查找此状态，您可以筛选包含一条或多条状态消息的`Completed`作业。 AWS Backup 只有当消息需要关注或采取行动时，才会将状态消息作为`Completed`工作状态的一部分。

另一种报告是合规性报告。合规性报告可以监控资源级别或有效的不同控件。

AWS Backup Audit Manager 会将每日报告发送到您的 Amazon S3 存储桶。如果报告针对当前区域和当前账户，则您可以选择接收 CSV 或 JSON 格式的报告。否则，报告将以 CSV 格式提供。每日报告的时间可能会在几个小时内波动，因为 Audit Man AWS Backup ager 会执行随机化以保持其性能。您也可以随时运行按需报告。

所有账户持有人都可以创建跨区域报告；管理和委托管理员账户持有人也可以创建跨账户报告。

每个报告计划最多可以有 20 个 AWS 账户。

> **Note**
>
> 如果诸如 RDS 之类的资源无法显示特定备份的增量字节数据，则值 `backupSizeInBytes` 将显示为 0。

要允许 AWS Backup Audit Manager 创建每日或按需报告，必须先根据报告模板创建报告计划。

主题

选择您的报告模板

报告模板定义了您的报告计划在报告中包含的信息。当您使用报告计划自动生成报告时，Audi AWS Backup t Manager 会为您提供过去 24 小时的报告。 AWS Backup Audit Manager 在世界标准时间凌晨 1 点到 5 点之间创建这些报告。它提供以下报告模板。

备份报告模板

备份报告模板。这些模板为您提供有关备份、还原或复制作业的每日更新。您可以使用这些报告来监控您的操作状态，并识别可能需要采取进一步措施的任何故障。下表列出了每个备份报告模板的名称及其示例输出。

备份报告模板	JSON 格式的示例报告
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2",

备份报告模板	JSON 格式的示例报告


```
      "resourceArn": "arn:aws:ec2:us-
west-2:112233445566:instance/
i-0bc877aee7782ba75",
      "backupPlanArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-plan:349f2247-b48
9-4301-83ac-4b7dd724db9a",
      "backupRuleId": "ab88bbf8-
ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

备份报告模板	JSON 格式的示例报告

COPY_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	"jobStatus": "RUNNING",
	"resourceType": "EC2",
	"resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	"backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	"backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	"creationDate": "2021-07-15T15:42:04.771Z",
	"backupSizeInBytes": 8589934592,
	"sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	"destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	"destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}

备份报告模板	JSON 格式的示例报告
	] }

RESTORE_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E",
	"jobStatus": "RUNNING",
	"recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae",
	"creationDate": "2021-07-15T15:52:49.797Z",
	"backupSizeInBytes": 8589934592,
	"percentDone": "0.00%",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}
	]
	}

合规性报告模板

合规性报告模板为您提供有关根据在一个或多个框架中定义的控件备份活动和资源合规性的每日报告。如果您的某个框架的合规性状态为 Non-compliant，请查看合规性报告以确定不合规资源。

合规性报告模板的类型

- Control compliance report 帮助您跟踪在框架中定义的控件的合规性状态。

- Resource compliance report 帮助您根据在框架中定义的控件跟踪资源的合规性状态。这些报告包括详细的评估结果，包括识别有关不合规资源的信息，您可以使用这些信息来识别和更正这些资源。

下表显示了来自合规性报告的示例输出。

合规性报告模板	JSON 格式的示例报告
CONTROL_COMPLIANCE_REPORT	{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_R ESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08- 17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_H ours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_P LAN_MIN_FREQUENCY_AND_MIN_R ETENTION_CHECK",

合规性报告模板	JSON 格式的示例报告


```
      "controlComplianceStatus":
 "NON_COMPLIANT",
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

合规性报告模板	JSON 格式的示例报告

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

使用 AWS Backup 控制台创建报告计划

有两种类型的报告。一种是作业报告，它显示过去 24 小时内完成的作业以及所有活动作业。另一种报告是合规性报告。合规性报告可以监控资源级别或有效的不同控件。创建报告时，您可以选择要创建的报告类型。

注意：根据您的账户类型，控制台显示可能会有所不同。只有管理账户才能看到多账户功能。

与备份计划类似，您可以创建报告计划来自动创建报告并定义其目的地 Amazon S3 存储桶。报告计划要求您拥有 S3 存储桶才能接收报告。有关设置新 S3 存储桶的说明，请参阅《Amazon Simple Storage Service 用户指南》中的步骤 1：创建您的第一个 S3 存储桶。

在 AWS Backup 控制台中创建您的报告计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 选择创建报告计划。
4. 从下拉列表中选择一个报告模板。
5. 输入唯一报告计划名称。该名称的长度必须介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。
6. （可选）输入报告计划描述。
7. 仅适用于一个账户的合规性报告模板。选择要报告的一个或多个框架。您最多可以向报告计划添加 1,000 个框架。

    1. 使用下拉列表选择您 AWS 所在的地区。
    2. 使用下拉列表从该区域中选择一个框架。
    3. 选择添加框架。
8. （可选）要向报告计划添加标签，请选择向报告计划添加标签。
9. 如果您使用的是管理账户，则可以指定要在此报告计划中包含哪些账户。您可以选择仅我的账户，这将仅针对您当前登录的账户生成报告。或者，您可以选择我的组织中的一个或多个帐户（适用于管理和委派管理员帐户）。
10. （如果您只为一个区域创建合规性报告，请跳过此步骤）。您可以选择要包含在报告中的区域。单击下拉菜单，显示可供您使用的区域。选择所有可用区域或您喜欢的区域。

    - 将新区域合并到 Backup Audit Manager 时将其包括在内复选框将在新区域可用时触发将其包含在您的报告中。

11. 选择报告的文件格式。所有报告均可以 CSV 格式导出。此外，可以以 JSON 格式导出单个区域的报告。
12. 使用下拉列表选择您的 S3 存储桶名称。
13. （可选）输入存储桶前缀。

    AWS Backup 将您的往来账户、当前地区报告发送至`s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name`。

    AWS Backup 将您的跨账户报告发送给 `s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name`

    AWS Backup 将您的跨区域报告发送给 `s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name`
14. 选择创建报告计划。

接下来，您必须允许您的 S3 存储桶接收来自的报告 AWS Backup。创建报告计划后，Audit AWS Backup Manager 会自动生成一个 S3 存储桶访问策略供您应用。

如果您使用自定义 KMS 密钥加密存储桶，则 KMS 密钥策略必须满足以下要求：

- 该`Principal`属性必须包含 Backup Audit Manager 服务相关角色 AR [AWSServiceRolePolicyForBackupReports](#)N。
- 该`Action`属性必须`kms:Decrypt`至少包含`kms:GenerateDataKey`和。

该策略[AWSServiceRolePolicyForBackupReports](#)具有这些权限。

查看此访问策略并将其应用于 S3 存储桶

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划名称下，选择报告计划的名称，来选择报告计划。
4. 选择编辑。
5. 选择查看 S3 存储桶的访问策略。您还可以在此过程结束时使用策略。
6. 选择复制权限。

7. 选择编辑存储桶策略。请注意，在首次创建备份报告之前，S3 存储桶策略中提及的服务相关角色尚不存在，从而导致错误 “委托人无效”。
8. 将权限复制到策略。

示例存储桶策略

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

如果您使用自定义 AWS Key Management Service 来加密存储报告的目标 S3 存储桶，请在策略中包括以下操作：

```
      "Action":[
        "kms:GenerateDataKey",
        "kms:Encrypt"
      ],
      "Resource":[
        "*"
      ],
```

使用 AWS Backup API 创建报告计划

您也可以通过编程方式使用报告计划。

有两种类型的报告。一种是作业报告，它显示过去 24 小时内完成的作业以及所有活动作业。另一种报告是合规性报告。合规性报告可以监控资源级别或有效的不同控件。创建报告时，您可以选择要创建的报告类型。

与备份计划类似，您可以创建报告计划来自动创建报告并定义其目的地 Amazon S3 存储桶。报告计划要求您拥有 S3 存储桶才能接收报告。有关设置新 S3 存储桶的说明，请参阅《Amazon Simple Storage Service 用户指南》中的步骤 1：创建您的第一个 S3 存储桶。

如果您使用自定义 KMS 密钥加密存储桶，则 KMS 密钥策略必须满足以下要求：

- 该`Principal`属性必须包含 Backup Audit Manager 服务相关角色 AR `AWSServiceRolePolicyForBackupReports`N。
- 该`Action`属性必须`kms:Decrypt`至少包含`kms:GenerateDataKey`和。

该策略AWSServiceRolePolicyForBackupReports具有这些权限。

对于单账户、单区域报告，请使用以下语法调用 CreateReportPlan。

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
   },
   "ReportPlanTags": {
       "string" : "string" // Optional.
   },
   "IdempotencyToken": "string"
```

```
}
```

当您使用报告计划的唯一名称调用 DescribeReportPlan 时，AWS Backup API 会响应并返回以下信息。

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

对于多账户、多区域报告，请使用以下语法调用 CreateReportPlan。

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ], // Use string value of "ROOT" to include all
 organizational units
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"], // Use wildcard value in string to include all Regions
      "FrameworkArns": [ "string" ],
```

```
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

当您使用报告计划的唯一名称调用 DescribeReportPlan 时，对于多账户、多区域计划， AWS Backup API 会响应并返回以下信息：

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
         "Regions": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "ReportTemplate": "string"
      }
   }
}
```

创建按需报告

您可以按照以下步骤创建按需报告，从而方便地生成新报告。 AWS Backup Audit Manager 会将您的按需报告发送到您在报告计划中指定的 Amazon S3 存储桶。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划名称下，选择报告计划的名称，来选择报告计划。

4. 选择创建按需报告。

您可以为现有报告计划生成按需报告。

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划下，单击报告计划名称旁边的单选按钮，选择报告计划。
4. 单击操作，然后单击创建按需报告。

即使在生成报告时，也可以对多个报告执行此操作。

查看审计报告

您可以使用通常用于处理 CSV 或 JSON 文件的程序打开、查看和分析 AWS Backup Audit Manager 报告。请注意，多个区域或多个账户的报告仅以 CSV 格式提供。

如果文件总大小超过 50 MB，则大文件会被分成多个报告。如果生成的文件超过 50 MB，Audi AWS Backup t Manager 将使用报告的其余部分创建其他 CSV 文件。

查看报告

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划名称下，选择报告计划的名称，来选择报告计划。
4. 在报告作业下，单击报告链接查看报告。
5. 如果您报告的报告状态带有虚线下划线，请选择它以获取有关报告的信息。
6. 按完成时间选择要查看的报告。
7. 选择 S3 链接。将打开您的目的地 S3 存储桶。
8. 在名称下，选择要查看的报告的名称。
9. 要将报告保存到您的计算机，请选择下载。

更新报告计划

您可以更新现有报告计划的描述、其传送目的地和格式。如果适用，您还可以在报告计划中添加框架或从中删除框架。

更新现有报告计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划名称下，选择报告计划的名称，来选择报告计划。
4. 选择编辑。
5. 您可以编辑报告计划的详细信息，包括报告名称和描述，以及报告中包含哪些账户和区域。

删除报告计划

您可以删除现有报告计划。当您删除报告计划时，该报告计划已创建的所有报告都将保留在其目的地 Amazon S3 存储桶中。

删除现有报告计划

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择报告。
3. 在报告计划名称下，选择报告计划的名称，来选择报告计划。
4. 选择删除。
5. 输入您的报告计划的名称，然后选择删除报告计划。

将 Audi AWS Backup t Manager 与 AWS CloudFormation

我们提供以下示例 AWS CloudFormation 模板供您参考：

主题

- 开启资源跟踪
- 部署默认控件
- 将 IAM 角色排除在控件评估之外
- 创建报告计划

开启资源跟踪

以下模板开启了资源跟踪功能，如开启资源跟踪中所述。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
  AllSupported:
    Type: String
    Default: True
    Description: Indicates whether to record all supported resource types.
```

```
    AllowedValues:
      - True
      - False

  IncludeGlobalResourceTypes:
    Type: String
    Default: True
    Description: Indicates whether AWS Config records all supported global resource
types.
    AllowedValues:
      - True
      - False

  ResourceTypes:
    Type: List<String>
    Description: A list of valid AWS resource types to include in this recording group,
such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
    Default: <All>

  DeliveryChannelName:
    Type: String
    Default: <Generated>
    Description: The name of the delivery channel.

  Frequency:
    Type: String
    Default: 24hours
    Description: The frequency with which AWS Config delivers configuration snapshots.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours

  TopicArn:
    Type: String
    Default: <New Topic>
    Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
Service (Amazon SNS) topic that AWS Config delivers notifications to.

  NotificationEmail:
    Type: String
    Default: <None>
```

```
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>

Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
```

```
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"

  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
```

```
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config

  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
```

```
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

部署默认控件

以下模板使用 AWS Backup Audit Manager 控件和补救措施中所述的默认控件来创建框架。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
```

```
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

将 IAM 角色排除在控件评估之外

控件 BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED 允许您排除最多五个仍可以手动删除恢复点的 IAM 角色。以下模板部署了此控件并排除了两个 IAM 角色。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
```

```
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

创建报告计划

以下模板创建了报告计划。

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"
```

```
Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

将 Audi AWS Backup t Manager 与 AWS Audit Manager

AWS Backup Audit Manager 控件映射到中预建的标准控件 AWS Audit Manager，允许您将 Audit Manager 合规性调查结果导入到 AWS Audit Manager 报告中。 AWS Backup 您可能需要这样做来帮助合规官员、审计经理或其他同事，将备份活动作为组织整体合规态势的一部分进行报告。

您可以将 Audit Manager 控件的合规结果导入到您的 AWS Audit Manager 框架中。 AWS Backup AWS Audit Manager 要启用自动从 Audit Manager 控件收集数据，请 AWS Backup AWS Audit Manager 使用《AWS Audit Manager 用户指南》中有关自定义现有控件的说明在中创建自定义控件。在按照这些说明进行操作时，请注意， AWS Backup 控件的数据源是AWS Config。

有关 AWS Backup 控件列表，请参阅选择控件。

控制和修复

本页列出了 Audit Manager AWS Backup 的可用控件。您可以选择右侧的信息窗格，查看控件列表并跳转到特定控件。要快速比较控件，请参阅选择控件中的表格。要以编程方式定义控件，请参阅使用 AWS Backup API 创建框架中的代码片段。

每个区域每个账户最多可以使用 50 个控件。在两个不同的框架中使用相同的控件相当于使用了 50 个控件限制中的两个控件。

本页列出了每个控件及其以下信息：

- 描述。方括号（“[]”）中的值是默认参数值。
- 控件评估的资源。
- 控件的参数。
- 发生控制失控的情况。
- 控制的范围，如下所示：
  - 您可以选择一个或多个 AWS Backup支持的服务，按类型指定资源。
  - 您可以使用单个标签键和可选值，指定带标签的资源范围。
  - 您可以使用单个资源下拉列表，指定单个资源。

- 使适用资源合规的补救措施。

请注意，仅在控制评估资源的合规性时，才会包括活动资源。例如，处于运行状态的 Amazon EC2 实例将由上一个恢复点已创建控件进行评估。处于停止状态的 EC2 实例将不包括在合规性评估中。

受备份计划保护的备份资源

描述：评估资源是否受备份计划保护。

资源：`AWS Backup: backup selection`

参数：无

发生：每 24 小时自动发生一次

范围：

- 带标签的资源
- 按类型划分的资源（默认）
- 单一资源

补救措施：将资源分配给备份计划。 AWS Backup 会在将资源分配给备份计划后，自动保护您的资源。有关更多信息，请参阅将资源分配给备份计划。

备份计划最低频率和最低保留期

描述：评估备份计划是否包含至少一条备份规则，该规则的备份频率至少为 [1 天]，保留期至少为 [35 天]。

资源：`AWS Backup: backup plans`

参数：

- 所需的备份频率，以小时或天数为单位。
- 所需的保留期，以天、周、月或年为单位。我们建议将热存储保留至少一周， AWS Backup 以便尽可能进行增量备份，从而避免额外收费。

发生：配置更改

范围：

- 带标签的资源
- 单一资源

补救措施：更新备份计划以更改其备份频率、保留期（或两者）。更新备份计划会更改更新后计划创建的恢复点的保留期。

保管库可防止手动删除恢复点

描述：评估备份保管库是否不允许手动删除某些 IAM 角色以外的恢复点。

资源：`AWS Backup: backup vaults`

参数：允许手动删除恢复点的多达五个 IAM 角色的 Amazon 资源名称 (ARN)。

发生：配置更改

范围：

- 带标签的资源
- 单一资源

补救措施：在备份保管库上创建或修改基于资源的访问策略。有关如何设置备份保管库访问策略的策略示例和说明，请参阅拒绝访问以删除备份保管库中的恢复点。

恢复点经过加密

描述：评估恢复点是否已加密。

资源：`AWS Backup: recovery points`

参数：无

发生：配置更改

范围：

- 带标签的资源

补救措施：为恢复点配置加密。为 AWS Backup 恢复点配置加密的方式因资源类型而异。

您可以为支持完全 AWS Backup 管理的资源类型配置加密 AWS Backup。如果资源类型不支持完全 AWS Backup 管理，则必须按照该服务的说明配置其备份加密，例如亚马逊弹性计算云用户指南中的 Amazon EBS 加密。要查看支持完全 AWS Backup 管理的资源类型列表，请参阅按资源划分的功能可用性表格的 “完全 AWS Backup 管理” 部分。

为恢复点设定的最低保留期

描述：评估恢复点保留期是否至少为 [35 天]。

资源：`AWS Backup: recovery points`

参数：所需的恢复点保留期，以天、周、月或年为单位。我们建议将热存储保留至少一周， AWS Backup 以便尽可能进行增量备份，从而避免额外收费。

发生：配置更改

范围：

- 带标签的资源

补救措施：更改恢复点的保留期。有关更多信息，请参阅编辑备份。

计划跨区域备份复制

描述：评估资源是否配置为将其备份副本创建到另一个 AWS 区域。

资源：`AWS Backup: backup selection`

参数：

- 选择备份副本应存在的地方（可选） AWS 区域
- 区域

发生：每 24 小时自动发生一次

范围：

- 带标签的资源

- 按类型划分的资源
- 单一资源

补救：更新备份计划以更改备份副本应存在 AWS 区域 的位置。

计划跨账户备份复制

描述：评估是否将资源配置为将其备份副本创建到另一个账户。您最多可以添加 5 个账户供控件评估。在 AWS Organizations中，目的地账户必须与源账户位于同一个组织中。

资源：`AWS Backup: backup selection`

参数：

- 选择应存放备份副本的 AWS 账户 ID（可选）
- 账户 ID

发生：每 24 小时自动发生一次

范围：

- 带标签的资源
- 按类型划分的资源
- 单一资源

补救：更新备份计划以更改或添加副本应存在的 AWS 账户 ID。

备份受 AWS Backup 文件库锁保护

描述：评估资源是否在锁定的备份保管库中存储了不可变备份。

资源：`AWS Backup: backup selection`

参数：

- 输入 AWS Backup 文件库锁定的最小和最大保留天数（可选）
- 最小保留天数
- 最大保留天数

发生：每 24 小时自动发生一次

范围：

- 带标签的资源
- 按类型划分的资源
- 单一资源

补救措施：锁定备份保管库，以设置其名称，更改其最小保留天数、最大保留天数（或两者）。对于合规模式下的保管库锁，也可以包括 ChangeableForDays。

已创建上一个恢复点

描述：此控件评估是否在指定的时间范围内（以天或小时为单位）创建了恢复点。

如果资源在指定的时间范围内创建了恢复点，则控件合规。如果未在指定的天数或小时数内创建恢复点，则控件不合规。

资源：`AWS Backup: recovery points`

参数：

- 以整数（以小时或天为单位）输入指定的时间范围。
- `hours` 的值可以从 1 到 744。
- `days` 的值可以从 1 到 31。

发生：每 24 小时自动发生一次

范围：

- 带标签的资源
- 按类型划分的资源
- 单一资源

补救措施：

- 更新备份计划，以更改创建恢复点的指定时间范围。
- 此外，您还可以创建按需备份。

资源还原时间满足目标

描述：评估对受保护资源的还原是否在目标还原时间内完成。

此控制功能可检查特定资源的还原时间是否符合目标持续时间。如果某资源类型的 `LatestRestoreExecutionTimeMinutes` 大于 `maxRestoreTime`（以分钟为单位），则该规则为 NON_COMPLIANT。

参数：

- `maxRestoreTime`（以分钟为单位）

发生：每 24 小时自动发生一次

范围：

- 带标签的资源
- 按类型划分的资源
- 单一资源

> **Note**
>
> AWS Backup 不提供任何恢复时间的服务级别协议 (SLA)。还原时间可能因系统负载和容量而异，即使包含相同资源的还原也是如此。

跨多个管理 AWS Backup 资源 AWS 账户

> **Note**
>
> 在管理多个 AWS 账户 中的资源之前 AWS Backup，您的账户必须属于 AWS Organizations 服务中的同一个组织。

您可以使用中的跨账户管理功能 AWS Backup 来管理和监控您配置的备份、还原和复制作业。 AWS 账户 AWS OrganizationsAWS Organizations是一项通过单个管理账户为多个账户提供基于策略 AWS 账户 的管理的服务。它使您能够标准化您实施备份策略的方式，同时最大限度地减少手动错误和工作量。从中央视图中，您可以轻松地识别所有账户中符合您关注条件的资源。

如果您进行了设置 AWS Organizations，则可以配置 AWS Backup 为在一个地方监控所有账户中的活动。您还可以创建备份策略并将其应用于属于您组织的选定账户，并直接从 AWS Backup 控制台查看聚合备份任务活动。此功能使备份管理员能够从单个管理账户有效地监控整个企业中数百个账户的备份作业状态。AWS Organizations 配额适用。

例如，您可以定义一个备份策略 A，该策略每天对特定资源进行备份并将备份保留 7 天。您可以选择将备份策略 A 应用于整个组织。（这意味着组织中的每个账户都会获得该备份策略，该策略会创建一个在该账户中可见的对应备份计划。）然后，您创建一个名为 Finance 的 OU，并决定仅将其备份保留 30 天。在这种情况下，您定义一个备份策略 B，该策略将覆盖生命周期值，并将其附加到 Finance OU。这意味着 Finance OU 下的所有账户都会获得一个新的有效备份计划，该计划每天对所有指定的资源进行备份，并将备份保留 30 天。

在此示例中，备份策略 A 和备份策略 B 合并为一个备份策略，该策略为名为 Finance 的 OU 下的所有账户定义保护策略。组织中的所有其他账户仍受备份策略 A 的保护。仅对共享相同备份计划名称的备份策略执行合并。还可以让策略 A 和策略 B 在该账户中共存，而无需进行任何合并。只能在控制台的 JSON 视图中使用高级合并运算符。有关合并策略的详细信息，请参阅《AWS Organizations 用户指南》中的定义策略、策略语法和策略继承。有关其他参考和用例，请参阅博客 “在 AWS Organizations 使用中大规模管理备份” AWS Backup和视频教程 “在 AWS Organizations 使用中大规模管理备份” AWS Backup。

请查看按 AWS 地区划分的功能可用性，以了解跨账户管理功能在哪些地方可用。

要使用跨账户管理，您必须执行以下步骤：

1. 在中创建管理账户 AWS Organizations ，并在管理账户下添加账户。
2. 在中启用跨账户管理功能。 AWS Backup
3. 创建备份策略以应用于您的管理账户 AWS 账户 下的所有用户。

> **Note**
>
> 对于由 Organizations 管理的备份计划，管理账户中的资源选择加入设置将覆盖成员账户中的该设置，即使配置了一个或多个委派管理员账户也是如此。委派管理员账户是具有增强功能的成员账户，不能像管理账户那样覆盖设置。

4. 管理您的所有备份、还原和复印作业 AWS 账户。

主题

在 Organizations 中创建管理账户

首先，您必须创建您的组织并使用中的 AWS 成员帐户对其进行配置 AWS Organizations。

在中创建管理账户 AWS Organizations 并添加账户

- 有关说明，请参阅《AWS Organizations 用户指南》中的教程：创建和配置组织。

启用跨账户管理

在中使用跨账户管理之前 AWS Backup，必须先启用该功能（即选择启用）。启用此特征后，您可以创建备份策略，以允许您自动同时管理多个账户。

启用跨账户管理

1. 打开网址为 AWS Backup 控制台 https://console.aws.amazon.com/backup/。您必须使用您的管理账户凭证登录。
2. 在左侧导航窗格中，选择设置以打开跨账户管理页面。
3. 在备份策略部分中，选择启用。

   这使您可以访问所有账户，并允许您创建策略以便同时自动管理组织中的多个账户。
4. 在跨账户监控部分中，选择启用。

   这使您能够从管理账户监控组织中所有账户的备份、复制和还原活动。

委派管理员

委托管理为注册成员账户中的分配用户提供了一种便捷的方式来执行大多数 AWS Backup 管理任务。您可以选择将管理权限委托给中的成员账户 AWS Organizations，从而将管理账户外部的管理权限扩展 AWS Backup 到整个组织。 AWS Backup

默认情况下，管理账户是用于编辑和管理策略的账户。使用委托管理员特征，您可以将这些管理功能委托给您指定的成员账户。这样，除了管理账户之外，这些账户也可以管理策略。

成员账户在成功注册委托管理后，就成为委托管理员账户。请注意，指定为委托管理员的是账户（而非用户）。

启用委托管理员账户允许选择管理备份策略，这会最大限度地减少有权访问管理账户的用户数量，并允许跨账户监控作业。

下表显示了管理账户、委托为 Backup 管理员的账户以及作为 AWS 组织成员的账户的职能。

> **Note**
>
> 委派管理员账户是具有增强功能的成员账户，不能像管理账户那样覆盖其他成员账户的服务选择加入设置。

权限	管理账户	委托管理员	成员账户
注册/注销委托管理员账户	是	否	否
在中跨账户管理备份策略 AWS Organizations	是	是	不支持
监控跨账户作业	是	是	不支持

先决条件

在委托备份管理之前，必须先将 AWS 组织中的至少一个成员帐户注册为委托管理员。在将账户注册为委托管理员之前，您必须先配置以下内容：

- AWS Organizations 除了您的默认管理账户外，还@@ 必须启用并配置至少一个成员帐户。
- 在 AWS Backup 控制台中，确保备份策略、跨账户监控和跨账户备份功能已开启。它们位于 AWS Backup 控制台的 “委派管理员” 窗格下方。
  - 跨账户监控允许您通过管理账户以及委托管理员账户，监控组织中所有账户的备份活动。
  - 可选：跨账户备份，允许组织中的账户将备份复制到其他账户（适用于备份支持的跨账户资源）。
  - 使用启用服务访问权限 AWS Backup。

设置委托管理涉及到两个步骤。第一步是委托跨账户作业监控。第二步是委托备份策略管理。

将成员账户注册为委托管理员账户

这是第一部分：使用 AWS Backup 控制台注册委托管理员帐户以监控跨账户作业。要委派 AWS Backup 策略，您将在下一节中使用 Organizations 控制台。

要使用 AWS Backup 控制台注册成员账户，请执行以下操作：

1. 打开网址为 AWS Backup 控制台 https://console.aws.amazon.com/backup/。您必须使用您的管理账户凭证登录。
2. 在控制台左侧导航栏的我的账户下，选择设置。
3. 在委托管理员窗格中，单击注册委托管理员或添加委托管理员。

4. 在注册委托管理员页面上，选择要注册的账户，然后选择注册账户。

此指定账户现在将注册为委托管理员，拥有管理权限，可以监控组织内各个账户的作业，并且可以查看和编辑策略（策略委托）。该成员账户不能注册或注销其他委托管理员账户。您可以使用控制台，将最多五个账户注册为委托管理员。

以编程方式注册成员账户：

使用 `register-delegated-administrator` CLI 命令。您可以在 CLI 请求中指定以下参数：

- `service-principal`
- `account-id`

以下是使用 CLI 请求以编程方式注册成员账户的示例：

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

注销成员账户

使用以下步骤 AWS Backup 通过注销 AWS 组织中以前被指定为授权管理员的成员帐户来移除管理访问权限。

使用控制台注销成员账户

1. 打开网址为 AWS Backup 控制台 https://console.aws.amazon.com/backup/。您必须使用您的管理账户凭证登录。
2. 在控制台左侧导航栏的我的账户下，选择设置。
3. 在委托管理员部分，单击注销账户。
4. 选择要注销的账户。
5. 在注销账户对话框中，查看安全隐患，然后键入 `confirm` 以完成注销。
6. 选择`Deregister account`。

以编程方式注销成员账户：

使用 CLI 命令 `deregister-delegated-administrator` 注销委托管理员账户。您可以在 API 请求中指定以下参数：

- `service-principal`
- `account-id`

以下是使用 CLI 请求以编程方式注销成员账户的示例：

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

通过以下方式委派 AWS Backup 策略 AWS Organizations

在 AWS Organizations 控制台中，您可以委托管理多个策略，包括 Backup 策略。

在登录到 AWS Organizations 控制台的管理账户中，您可以为您的组织创建、查看或删除基于资源的委托策略。有关委托策略的步骤，请参阅《AWS Organizations 用户指南》中的创建基于资源的委托策略。

创建备份策略

启用跨账户管理后，使用您的管理账户创建跨账户备份策略。

> **Warning**
>
> 当您使用 JSON 创建策略时，重复的密钥名称将被拒绝。如果单个策略中包含多个计划、规则或选项，则每个密钥的名称必须是唯一的。

通过 AWS Backup 控制台创建备份策略

1. 在左侧导航窗格中，选择备份策略。在备份策略页上，选择创建备份策略。
2. 在详细信息部分中，输入备份策略名称并提供描述。
3. 在备份计划详细信息部分中，选择可视编辑器选项卡，然后执行以下操作：

    a. 对于备份计划名称，输入名称。

b. 对于区域，从列表中选择一个区域。

4. 在备份规则配置部分中，选择添加备份规则。

   每个备份计划的最大规则数为 10。如果计划包含的规则超过 10 条，则备份计划将被忽略，并且不会根据该计划创建备份。

   a. 对于规则名称，输入规则的名称。规则名称区分大小写，只能包含字母数字字符或连字符。

   b. 对于计划，请在频率列表中选择备份频率，然后选择备份时段选项之一。建议您选择使用备份时段默认值 - 推荐。

5. 对于生命周期，请选择所需的生命周期设置。

6. 对于备份保管库名称，输入一个名称。这是将存储由备份创建的恢复点的备份保管库。

   确保您的所有账户中都存在备份保管库。 AWS Backup 不检查这个。

7. （可选）如果要将备份复制到另一个区域，请从列表中选择目标区域 AWS 区域，然后添加标签。无论跨区域复制设置如何，您都可以为创建的恢复点选择标签。您还可以添加更多规则。

8. 在资源分配部分，提供 AWS Identity and Access Management (IAM) 角色的名称。要使用 AWS Backup 服务角色，请提供`service-role/AWSBackupDefaultServiceRole`。

   AWS Backup 在每个账户中担任此角色是为了获得执行备份和复制任务的权限，包括加密密钥权限（如果适用）。 AWS Backup 还使用此角色执行生命周期删除。

   > **Note**
   >
   > AWS Backup 不验证该角色是否存在或是否可以担任该角色。
   > 对于跨账户管理创建的备份计划， AWS Backup 将使用管理账户中的选择加入设置并覆盖特定账户的设置。
   > 对于要添加备份策略的每个账户，您必须自行创建保管库和 IAM 角色。

9. 添加标签以选择要备份的资源。允许的最大标签数为 30。

   AWS Organizations 如果备份计划是通过 Organizations 策略创建的，则策略最多允许指定 30 个标签。通过使用多个资源分配或参与多个备份计划，可以包含其他标签。

   如果在同一个备份选择中标签的数量超过 30 个，无论是通过修改现有选择还是使用`@@append`，备份计划都将失效，并将从本地帐户中删除。

10. 如果您要备份的资源正在 Amazon EC2 实例上运行 Microsoft Windows，请在高级设置部分选择 Windows VSS。这样，您将能够创建与应用程序保持一致的 Windows VSS 备份。

> **Note**
>
> AWS Backup 目前仅支持在 Amazon EC2 上运行的资源的应用程序一致性备份。Windows VSS 备份并非支持所有实例类型或应用程序。有关更多信息，请参阅 创建 Windows VSS 备份。

11. 选择添加备份计划以将其添加到策略中，然后选择创建备份策略。

    创建备份策略不会保护您的资源，直到您将其附加到账户。您可以选择您的策略名称并查看详细信息。

    以下是创建备份计划的 AWS Organizations 策略示例。如果启用 Windows VSS 备份，则必须添加允许您创建应用程序一致性备份的权限，如策略的 `advanced_backup_settings` 部分所示。

```
{
  "plans": {
    "PiiBackupPlan": {
      "regions": {
        "@@append":[
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 0/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "60"
          },
          "complete_backup_window_minutes": {
            "@@assign": "604800"
          },
          "target_backup_vault_name": {
            "@@assign": "FortKnox"
          },
          "recovery_point_tags": {
            "owner": {
              "tag_key": {
                "@@assign": "Owner"
```

```
              },
              "tag_value": {
                "@@assign": "Backup"
              }
            }
          },
          "lifecycle": {
            "delete_after_days": {
              "@@assign": "365"
            },
            "move_to_cold_storage_after_days": {
              "@@assign": "180"
            }
          },
          "copy_actions": {
            "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
 {
            "target_backup_vault_arn" : {
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        },
        "selections": {
          "tags": {
            "SelectionDataType": {
              "iam_role_arn": {
                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
              },
              "tag_key": {
                "@@assign": "dataType"
              },
              "tag_value": {
                "@@assign": [
                  "PII",
```

```
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
}
```

12. 在目标部分中，选择要将策略附加到的组织单位或账户，然后选择附加。此策略也可以添加到各个组织单位或账户中。

> **Note**
>
> 确保验证您的策略，并确保在策略中包含所有必需的字段。如果策略的某些部分无效，则 AWS Backup 忽略这些部分，但策略的有效部分将按预期工作。目前， AWS Backup 不验证 AWS Organizations 策略的正确性。
>
> 如果您对管理账户应用一种策略，对成员账户应用不同的策略，并且它们存在冲突（例如，备份保留期不同），则这两个策略将毫无问题地运行（也就是说，这些策略将针对每个账户独立运行）。例如，如果管理账户策略每天备份一次 Amazon EBS 卷，而本地策略每周备份一次 EBS 卷，则这两个策略都将运行。
>
> 如果将应用于某个账户的有效策略中缺少必需的字段（可能是由于不同策略之间的合并所致），则 AWS Backup 根本不会将该策略应用于该账户。如果某些设置无效，则对其 AWS Backup 进行调整。

在根据备份策略创建的备份计划中，无论成员账户中的选择加入设置如何，都 AWS Backup 将使用组织管理账户中指定的选择加入设置。

当您将策略附加到组织单位时，加入此组织单位的每个账户都会自动获取此策略，从组织单位中删除的每个账户都会失去此策略。相应的备份计划将自动从该账户中删除。

监控多个 AWS 账户中的活动

要跨账户监控备份、复制和还原作业，必须启用跨账户监控。这样，您就可以从组织管理账户监控所有账户中的备份活动。选择加入后，组织中在选择加入后创建的所有作业都将可见。选择退出时， AWS Backup 将作业在聚合视图中保留 30 天（从到达终点状态开始）。在选择退出后创建的作业不可见，也不显示任何新创建的备份作业。有关选择加入的说明，请参阅启用跨账户管理。

监控多个账户

1. 打开网址为 AWS Backup 控制台 https://console.aws.amazon.com/backup/。您必须使用您的管理账户凭证登录。
2. 在左侧导航窗格中，选择设置以打开跨账户管理页面。
3. 在跨账户监控部分中，选择启用。

   这样，您可以从管理账户监控组织中所有账户的备份和还原活动。
4. 在左侧导航窗格中，选择跨账户监控。
5. 在跨账户监控页面上，选择备份作业、还原作业或复制作业选项卡，以查看在所有账户中创建的所有作业。您可以通过 AWS 账户 ID 查看这些作业，也可以查看特定账户中的所有作业。
6. 在搜索框中，您可以按账户 ID、状态或作业 ID 筛选作业。

   例如，您可以选择备份作业选项卡并查看在您的所有账户中创建的所有备份作业。您可以按账户 ID 筛选列表，并查看在该账户中创建的所有备份作业。

资源选择加入规则

如果成员账户的备份计划是由组织级别的备份策略创建的，则组织管理账户的 AWS Backup 选择加入设置将覆盖该成员账户中的选择加入设置，但仅适用于该备份计划。

如果成员账户还有用户创建的本地级备份计划，则这些备份计划将遵循成员账户中的选择加入设置，而不参照 Organizations 管理账户的选择加入设置。

定义策略、策略语法和策略继承

《 AWS Organizations 用户指南》中记录了以下主题。

- 备份策略 - 请参阅备份策略。
- 策略语法 - 请参阅备份策略语法和示例。
- 管理策略类型的继承 - 请参阅管理策略类型的继承。

AWS Backup 和 AWS CloudFormation

常规信息

借助 AWS CloudFormation，您可以使用自己创建的模板以安全、可重复的方式预配置和管理 AWS 资源。您可以使用 AWS CloudFormation 模板和 StackSets 管理备份计划、备份资源选择和备份保管库。有关使用 AWS CloudFormation 的信息，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation 的工作原理。

在创建 AWS CloudFormation 堆栈之前，您应该考虑以下几点：

- 建议您为备份计划和备份保管库创建单独的模板。您只能删除空的备份保管库。如果包含备份保管库的堆栈包含恢复点，则无法删除它们。
- 在创建堆栈之前，请确保您具有可用的服务角色。首次将资源分配给备份计划时，系统会为您创建 AWS Backup 默认服务角色。如果您尚未为备份计划分配资源，请在创建堆栈之前分配资源。您还可以指定自己创建的自定义角色。有关 角色的更多信息，请参阅IAM 服务角色。

使用 AWS CloudFormation 部署备份保管库、备份计划和资源分配

有关部署备份保管库、备份计划和资源分配的 AWS CloudFormation 模板示例，请参阅使用分配资源 AWS CloudFormation。

使用 AWS CloudFormation 部署备份计划

有关部署备份计划的 AWS CloudFormation 模板示例，请参阅AWS CloudFormation 备份计划模板。

使用 AWS CloudFormation 部署 AWS Backup Audit Manager 框架和报告计划

有关部署 AWS Backup Audit Manager 框架和报告计划的 AWS CloudFormation 模板示例，请参阅 备份计划的 AWS CloudFormation 模板。

使用 AWS CloudFormation 跨账户部署备份计划

您可以在 AWS 组织中，使用 AWS CloudFormation StackSets 跨多个账户部署策略。可在 AWS CloudFormation 用户指南中找到模板示例。

一个很好的起点和参考资料是出版物使用 AWS Backup 跨 AWS 服务自动进行大规模集中备份。作者：Ibukun Oyewumi 和 Sabith Venkitachalapathy（2021 年 7 月）。

了解有关 AWS CloudFormation 的更多信息

有关结合使用 AWS CloudFormation 与 AWS Backup 的信息，请参阅《AWS CloudFormation 用户指南》中的 AWS Backup 资源类型参考。

有关在使用 AWS CloudFormation 时控制对 AWS 服务资源的访问的信息，请参阅《AWS CloudFormation 用户指南》中的使用 AWS Identity and Access Management 控制访问权限。

安全性 AWS Backup

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 AWS Backup，请参阅按合规计划划分的范围内的AWS 服务。
- 云中的安全性 - 您对 AWS Backup 的责任包括但不限于以下各项。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。
  - 回复您收到的来信 AWS。
  - 管理您和您的团队使用的凭证。有关更多信息，请参阅中的身份和访问管理 AWS Backup。
  - 配置您的备份计划和资源分配，以反映组织的数据保护策略。有关更多信息，请参阅管理备份计划。
  - 定期测试您是否有能力找到某些恢复点并还原它们。有关更多信息，请参阅使用备份。
  - 将 AWS Backup 程序纳入组织的灾难恢复和业务连续性书面程序。首先，请参阅 开始使用 AWS Backup。
  - 确保您的员工熟悉并练习在紧急情况下使用 AWS Backup 您的组织程序。有关更多信息，请参阅 AWS 架构完善的框架。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Backup。以下主题向您介绍如何进行配置 AWS Backup 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS Backup 资源。

主题

- AWS PrivateLink
- 韧性在 AWS Backup

合规性验证 AWS Backup

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，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 构建 HIPAA 安全与合规性 Amazon Web Services — 本白皮书描述了公司如何使用 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 可以全面了解您的安全状态 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。

中的数据保护 AWS Backup

AWS Backup 符合 AWS 分担责任模式，其中包括数据保护的法规和指导方针。 AWS 负责保护运行所有 AWS 服务的全球基础架构。 AWS 保持对托管在此基础架构上的数据的控制，包括用于处理客户内容和个人数据的安全配置控制。 AWS 作为数据控制者或数据处理者的客户和 AWS 合作伙伴网络 (APN) 合作伙伴应对他们输入的任何个人数据负责。 AWS Cloud

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置个人用户账户。这可帮助确保仅向每个用户授予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)。
- 使用安全套接字层 (SSL)/传输层安全性 (TLS) 与 AWS 资源通信。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如名称字段）。这包括您使用控制台、 AWS CLI API AWS Backup 或 AWS SDK 使用其他 AWS 服务时。您输入到 AWS Backup 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供网址时，请勿在网址中包含凭证信息来验证您对该服务器的请求。

有关数据保护的更多信息，请参阅AWS 安全性博客 上的AWS 责任共担模式和 GDPR 博客文章。

对中的备份进行加密 AWS Backup

> **Note**
>
> AWS Backup A@@ udit Manager 可帮助您自动检测未加密的备份。

您可以为支持完全 AWS Backup 管理的资源类型配置加密 AWS Backup。如果资源类型不支持完全 AWS Backup 管理，则必须按照该服务的说明配置其备份加密，例如亚马逊弹性计算云用户指南中的 Amazon EBS 加密。要查看支持完全 AWS Backup 管理的资源类型列表，请参阅按资源划分的功能可用性表格的 “完全 AWS Backup 管理” 部分。

下表列出了每种受支持的资源类型、如何为备份配置加密以及是否支持独立的备份加密。当 AWS Backup 独立加密备份时，它会使用行业标准的 AES-256 加密算法。

资源类型	如何配置加密	独立 AWS Backup 加密
Amazon Simple Storage Service (Amazon S3)	Amazon S3 备份使用与备份库关联的 AWS KMS (AWS Key Management Service) 密钥进行加密。 AWS KMS 密钥可以是客户管理的 CMK，也可以是与服务关联的 AWS托管 CMK。 AWS Backup AWS Backup 即使源 Amazon S3 存储桶未加密，也会加密所有备份。	支持
VMware 虚拟机	虚拟机备份始终经过加密。虚拟机备份的 AWS KMS 加密密钥是在存储虚拟机备份的 AWS Backup 保管库中配置的。	支持
启用高级 DynamoDB 备份后的 Amazon DynamoDB	DynamoDB 备份始终加密。DynamoDB 备份的 AWS KMS 加密密钥是在存储 DynamoDB 备份的文件库中 AWS Backup 配置的。	支持
未启用高级 DynamoDB 备份的 Amazon DynamoDB	DynamoDB 备份使用与用于加密源 DynamoDB 表的相同加密密钥自动进行加密。未加密的 DynamoDB 表的快照也不会加密。 **Note** AWS Backup 要创建加密的 DynamoDB 表的备份，您必须向	不支持

资源类型	如何配置加密	独立 AWS Backup 加密
	用于备份的 IAM 角色添加`kms:Decrypt` 权限`kms:GenerateDataKey` 和。或者，您可以使用 AWS Backup 默认服务角色。	
Amazon Elastic File System (Amazon EFS)	Amazon EFS 备份始终加密。Amazon EFS 备份的 AWS KMS 加密密钥是在存储 Amazon EFS 备份 AWS Backup 的文件库中配置的。	支持
Amazon Elastic Block Store （Amazon EBS)	默认情况下，Amazon EBS 备份要么使用用于加密源卷的密钥进行加密，要么未加密。在还原期间，您可以通过指定 KMS 密钥来选择覆盖默认加密方法。	不支持
Amazon Elastic Compute Cloud (Amazon EC2) AMI	AMI 未加密。EBS 快照按照 EBS 备份的默认加密规则进行加密（参见 EBS 条目）。数据和根卷的 EBS 快照可以加密并附加到 AMI。	不支持

资源类型	如何配置加密	独立 AWS Backup 加密
Amazon Relational Database Service (Amazon RDS)	Amazon RDS 快照使用与用于加密源 Amazon RDS 数据库相同的加密密钥自动进行加密。未加密的 Amazon RDS 数据库的快照也不会加密。 **Note** AWS Backup 目前支持所有亚马逊 RDS 数据库引擎，包括亚马逊 Aurora。	不支持
Amazon Aurora	Aurora 集群快照使用与用于加密源 Amazon Aurora 集群相同的加密密钥自动进行加密。未加密的 Aurora 集群的快照也不会加密。	不支持

资源类型	如何配置加密	独立 AWS Backup 加密
AWS Storage Gateway	Storage Gateway 快照使用与用于加密源 Storage Gateway 卷相同的加密密钥自动进行加密。未加密的 Storage Gateway 卷的快照也不会加密。 **Note** 您无需在所有服务中使用客户托管密钥即可启用 Storage Gateway。您只需将 Storage Gateway 备份复制到已配置 KMS 密钥的保管库。这是因为 Storage Gateway 没有特定于服务的 AWS KMS 托管密钥。	不支持
Amazon FSx	Amazon FSx 文件系统的加密功能因底层文件系统而异。要了解您的特定 Amazon FSx 文件系统的更多信息，请参阅相应的 FSx 用户指南。	不支持
Amazon DocumentDB	Amazon DocumentDB 集群快照使用与用于加密源 Amazon DocumentDB 集群相同的加密密钥自动进行加密。未加密的 Amazon DocumentDB 集群的快照也不会加密。	不支持

资源类型	如何配置加密	独立 AWS Backup 加密
Amazon Neptune	Amazon Neptune 集群快照使用与用于加密源 Amazon Neptune 集群相同的加密密钥自动进行加密。未加密的 Amazon Neptune 集群的快照也不会加密。	不支持
Amazon Timestream	Amazon Timestream 表快照备份始终加密。Amazon Timestream 备份的 AWS KMS 加密密钥在存储 Timestream 备份的备份保管库中进行配置。	支持
Amazon Redshift	Amazon Redshift 集群快照使用与用于加密源 Amazon Redshift 集群相同的加密密钥自动进行加密。未加密的 Amazon Redshift 集群的快照也不会加密。	不支持
AWS CloudFormation	CloudFormation 备份始终是加密的。备份的 CloudFormation 加密密钥是在存储 CloudFormation 备份的 CloudFormation 保管库中配置的。 CloudFormation	支持
Amazon EC2 实例上的 SAP HANA 数据库	SAP HANA 数据库备份始终加密。SAP HANA 数据库备份的 AWS KMS 加密密钥是在存储数据库备份的 AWS Backup 保管库中配置的。	支持

备份副本的加密

当您使用 AWS Backup 跨账户或区域复制备份时，即使原始备份未加密，也会 AWS Backup 自动加密大多数资源类型的副本。 AWS Backup 使用目标保管库的 KMS 密钥加密您的副本。但是，未加密的 Aurora、Amazon DocumentDB 和 Neptune 集群的快照也未加密。

加密和备份副本

对于未完全 AWS 由管理的资源，不支持使用托管 KMS 密钥进行跨账户复制。 AWS Backup请参阅，全面 AWS Backup 管理以确定哪些资源是完全托管的。

对于完全由管理的资源 AWS Backup，使用备份库的加密密钥对备份进行加密。对于未完全由管理的资源 AWS Backup，跨账户副本使用与源资源相同的 KMS 密钥。有关更多信息，请参阅加密密钥和跨账户副本

虚拟机管理程序凭证加密

由管理程序管理的虚拟机使用 AWS Backup 网关将本地系统连接到 AWS Backup。管理程序必须具有同样强大而可靠的安全性，这一点很重要。这种安全性可以通过使用 AWS 自有密钥或客户管理的密钥对虚拟机管理程序进行加密来实现。

AWS 自有密钥和客户管理的密钥

AWS Backup 为虚拟机管理程序凭据提供加密，以使用AWS 自有的加密密钥保护敏感的客户登录信息。您可以选择改用客户托管密钥。

默认情况下，用于在虚拟机管理程序中加密凭据的密钥是AWS 自有密钥。 AWS Backup 使用这些密钥自动加密虚拟机管理程序凭据。您既无法查看、管理或使用 AWS 拥有的密钥，也无法审核其使用情况。但是，无需采取任何措施或更改任何计划即可保护用于加密数据的密钥。有关更多信息，请参阅《AWS KMS 开发者指南》中的 AWS 自有密钥。

或者，也可以使用客户托管密钥对凭证进行加密。 AWS Backup 支持使用由您创建、拥有和管理的对称客户托管密钥来执行加密。由于您可以完全控制此加密，因此可以执行以下任务：

- 制定和维护密钥策略
- 制定和维护 IAM policy 和授权
- 启用和禁用密钥策略
- 轮换密钥加密材料

- 添加标签
- 创建密钥别名
- 计划删除密钥

当您使用客户托管密钥时，请 AWS Backup 验证您的角色是否有权使用此密钥进行解密（在运行备份或还原作业之前）。必须将 `kms:Decrypt` 操作添加到用于启动备份或还原作业的角色。

由于无法将 `kms:Decrypt` 操作添加到默认备份角色，因此必须使用默认备份角色以外的角色才能使用客户托管密钥。

有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户托管密钥。

使用客户托管密钥时需要的授权

AWS KMS 需要获得授权才能使用您的客户托管密钥。当您导入使用客户托管密钥加密的虚拟机管理程序配置时， AWS Backup 会通过向发送`CreateGrant`请求来代表您创建授权。 AWS KMS AWS Backup 使用授权访问客户账户中的 KMS 密钥。

您可以随时撤销对授予的访问权限，也可以取消 AWS Backup对客户托管密钥的访问权限。如果这样做，与管理程序关联的所有网关都将无法再访问由客户托管密钥加密的管理程序的用户名和密码，这将影响您的备份和还原作业。具体而言，您在此管理程序中对虚拟机执行的备份和还原作业将失败。

当您删除管理程序时，Backup Gateway 将使用 `RetireGrant` 操作来删除授权。

监控加密密钥

当您对 AWS Backup 资源使用 AWS KMS 客户托管密钥时，您可以使用AWS CloudTrail或 Amazon CloudWatch Logs 来跟踪 AWS Backup 发送到的请求 AWS KMS。

查找具有以下`"eventName"`字段 AWS CloudTrail 的事件，以监控访问由 AWS Backup 您的客户托管密钥加密的数据所调用的 AWS KMS 操作：

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

中的身份和访问管理 AWS Backup

访问 AWS Backup 需要凭证。这些凭证必须有权访问 AWS 资源，例如 Amazon DynamoDB 数据库或 Amazon EFS 文件系统。此外， AWS Backup 为某些 AWS Backup支持的服务创建的恢复点无法使用源服务（例如 Amazon EFS）删除。您可以使用删除这些恢复点 AWS Backup。

以下各节详细介绍了如何使用 AWS Identity and Access Management (IAM) 以及 AWS Backup 如何帮助安全访问您的资源。

> **Warning**
>
> AWS Backup 使用您在分配资源来管理恢复点生命周期时选择的 IAM 角色。如果您删除或修改该角色，则 AWS Backup 无法管理您的恢复点生命周期。发生这种情况时，它将尝试使用服务相关角色来管理您的生命周期。在少数情况下，这也可能不起作用，从而在存储上留下 EXPIRED 恢复点，这可能会产生不必要的成本。要删除 EXPIRED 恢复点，请使用删除备份中的步骤手动将其删除。

主题

身份验证

访问 AWS Backup 或正在备份的 AWS 服务需要 AWS 能够用来验证您的请求的证书。您可以 AWS 作为以下任何类型的身份进行访问：

- AWS 账户 root 用户 — 注册时 AWS，您需要提供与您的 AWS 帐户关联的电子邮件地址和密码。这就是您的 AWS 账户 根用户。其凭证可让您完全访问您的所有 AWS 资源。

> **Important**
>
> 出于安全原因，建议您仅使用根用户来创建管理员。管理员是对您的 AWS 账户拥有完全权限的 IAM 用户。随后，您可以使用此管理员用户来创建具有有限权限的其他 IAM 用户和角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实践和创建您的第一个 IAM 管理员用户和组。

- IAM 用户 - IAM 用户用户是 AWS 账户 中的一种身份，它具有特定的自定义权限（例如，创建备份保管库以存储备份的权限）。您可以使用 IAM 用户名和密码登录安全 AWS 网页 AWS Management Console，例如AWS 讨论论坛或AWS Support 中心。

  除了用户名和密码之外，您还可以为每个用户生成访问密钥。在以编程方式访问 AWS 服务时，您可以使用这些密钥，无论是通过几个软件开发工具包中的一个还是使用 (AWS Command Line Interface CL AWS I)。SDK 和 AWS CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。有关验证请求的更多信息，请参阅《AWS 一般参考》 中的签名版本 4 签名流程。

- IAM 角色 – IAM 角色是可在账户中创建的另一种具有特定权限的 IAM 身份。它类似于 IAM 用户，但未与特定人员关联。IAM 角色使您能够获得可用于访问 AWS 服务和资源的临时访问密钥。具有临时凭证的 IAM 角色在以下情况下很有用：

  - 联合用户访问权限 — 您可以使用企业用户目录或 Web 身份提供商中预先存在的用户身份 AWS Directory Service，而不是创建 IAM 用户。这些用户称为联合用户。在通过身份提供者请求访问权限时， AWS 将为联合用户分配角色。有关联合用户的更多信息，请参阅《IAM 用户指南》中的联合用户和角色。
  - 跨账户管理 — 您可以使用账户中的 IAM 角色授予其他 AWS 账户 权限来管理您的账户的资源。有关示例，请参阅 IAM 用户指南中的教程： AWS 账户 使用 IAM 角色委派访问权限。
  - AWS 服务访问权限 — 您可以使用账户中的 IAM 角色向 AWS 服务授予访问您账户资源的权限。有关更多信息，请参阅 IAM 用户指南中的创建角色以向 AWS 服务委派权限。
  - 在亚马逊弹性计算云 (Amazon EC2) 上运行的应用程序 — 您可以使用 IAM 角色管理在亚马逊 EC2 实例上运行并发 AWS 出 API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该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 角色为在 Amazon EC2 实例上运行的应用程序授予权限。

访问控制

您可以拥有有效的凭证来验证您的请求，但是除非您拥有相应的权限，否则您无法访问备份文件库等 AWS Backup 资源。您也无法备份诸如亚马逊 Elastic Block Store (Amazon EBS) 卷之类的 AWS 资源。

每个 AWS 资源都归人所有 AWS 账户，创建或访问资源的权限受权限策略的约束。账户管理员可以向 AWS Identity and Access Management (IAM) 身份（即用户、群组和角色）附加权限策略。有些服务还支持向资源附加权限策略。

> **Note**
>
> 账户管理员 (或管理员用户) 是具有管理员权限的用户。有关更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

以下各部分介绍了访问策略的工作原理以及如何使用它们来保护备份。

主题

资源和操作

资源是存在于服务中的对象。 AWS Backup 资源包括备份计划、备份存储库和备份。Backup 是一个通用术语，指的是中存在的各种类型的备份资源 AWS。例如，Amazon EBS 快照、Amazon Relational Database Service (Amazon RDS) 快照、Amazon DynamoDB 备份都是备份资源类型。

在中 AWS Backup，备份也称为恢复点。使用时 AWS Backup，您还可以使用您正在尝试保护的其他 AWS 服务的资源，例如 Amazon EBS 卷或 DynamoDB 表。这些资源具有与其关联的唯一 Amazon 资

源名称 (ARN)。ARN 对 AWS 资源进行唯一标识。当您需要在 AWS全局环境中（例如在 IAM 策略或 API 调用中）明确指定一项资源时，您必须拥有 ARN。

下表列出了资源、子资源和 ARN 格式以及一个唯一 ID 示例。

AWS Backup 资源 ARN

资源类型	ARN 格式	唯一 ID 示例
备份计划	arn:aws:backup: *region*:*account-id* :backup-plan:*	
备份保管库	arn:aws:backup: *region*:*account-id* :backup-vault:*	
Amazon EBS 恢复点	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-05f426fd8kdjb4224
Amazon EC2 映像恢复点	arn:aws:ec2: *region*::image/ami-*	image/ami-1a2b3e4f5e6f7g890
Amazon RDS 恢复点	arn:aws:rds: *region*:*account-id* :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Aurora 恢复点	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Storage Gateway 恢复点	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-0d40e49137e31d9e0

资源类型	ARN 格式	唯一 ID 示例
未启用高级 DynamoDB 备份的 DynamoDB 恢复点	arn:aws:dynamodb: *region*:*account-id* :table/*/backup/*	table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3
启用高级 DynamoDB 备份的 DynamoDB 恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Amazon EFS 恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e
Amazon FSx 恢复点	arn:aws:fsx: *region*:*account-id* :backup/backup-*	backup/backup-1a20e49137e31d9e0
虚拟机恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	1801234a-5b6b-7dc8-8032-836f7ffc623b
Amazon S3 连续备份恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -5ec207d0
S3 定期备份恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -20211231900000-5ec207d0
亚马逊 DocumentDB 的恢复点	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012

资源类型	ARN 格式	唯一 ID 示例
Neptune 的恢复点	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
亚马逊 Redshift 的恢复点	arn:aws:redshift: *region*:*account-id* :snapshot: *resource*/awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
亚马逊 Timestream 的恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta
AWS CloudFormation 模板的恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012
亚马逊 EC2 实例上 SAP HANA 数据库的恢复点	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012

支持完全 AWS Backup 管理的资源都有格式的恢复点arn:aws:backup:*region*:*account-id:*:recovery-point:*。这使您可以更轻松地应用权限策略来保护这些恢复点。要查看哪些资源支持完全 AWS Backup 管理，请参阅按资源划分的功能可用性表格的该部分。

AWS Backup 提供了一组使用 AWS Backup 资源的操作。有关可用操作的列表，请参阅 AWS Backup 操作。

资源所有权

AWS 账户 拥有在账户中创建的资源，无论谁创建了这些资源。具体而言，资源所有者是 AWS 账户 对资源创建请求进行身份验证的委托人实体（即 AWS 账户 根用户、IAM 用户或 IAM 角色）。以下示例说明了它的工作原理：

- 如果您使用您的 AWS 账户 root 用户凭证创建备份保管库，则您 AWS 账户 就是该文件库的所有者。 AWS 账户
- 如果您在中创建 IAM 用户 AWS 账户 并向该用户授予创建备份库的权限，则该用户可以创建备份存储库。但是，您的 AWS 账户（即该用户所属的账户）拥有备份保管库资源。
- 如果您在中创建 AWS 账户 具有创建备份库权限的 IAM 角色，则任何能够担任该角色的人都可以创建文件库。角色 AWS 账户所属的您拥有备份库资源。

指定策略元素：操作、效果和主体

对于每个 AWS Backup 资源（请参阅资源和操作），该服务定义了一组 API 操作（请参阅操作）。要授予这些 API 操作的权限，请 AWS Backup 定义一组可在策略中指定的操作。执行一个 API 操作可能需要多个操作的权限。

以下是最基本的策略元素：

- 资源：在策略中，您可以使用 Amazon Resource Name（ARN）标识策略应用到的资源。有关更多信息，请参阅 资源和操作。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。
- 效果 - 您可以指定当用户请求特定操作（可以是允许或拒绝）时的效果。如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体 – 在基于身份的策略（IAM 策略）中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。

要了解 IAM 策略语法和描述的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

有关显示所有 AWS Backup API 操作的表格，请参阅API 权限：操作、资源和条件参考。

在策略中指定条件

当您授予权限时，可使用 IAM 策略语言来指定规定策略何时生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅《IAM 用户指南》中的条件。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

AWS Backup 定义自己的一组条件键。要查看 AWS Backup 条件键列表，请参阅《服务授权参考》AWS Backup中的条件密钥。

API 权限：操作、资源和条件参考

在设置 访问控制 和编写可附加到 IAM 身份的权限策略 (基于身份的策略) 时，可使用下面的列表作为参考。包括每个 AWS Backup API 操作、您可以为其授予执行操作权限的相应操作，以及您可以为其授予权限的 AWS 资源。您可以在策略的 `Action` 字段中指定这些操作，并在策略的 `Resource` 字段中指定资源值。如果 `Resource` 字段为空，则可以使用通配符 (*) 来包含所有资源。

您可以在 AWS Backup 策略中使用 AWS-wide 条件键来表达条件。有关 AWS范围密钥的完整列表，请参阅 IAM 用户指南中的可用密钥。

[1] 使用现有的文件库访问策略。

[2] AWS Backup 资源 ARN 有关特定于资源的恢复点 ARN，请参阅。

[3] `StartRestoreJob` 必须在资源的元数据中包含键值对。要获取资源的元数据，请调用 `GetRecoveryPointRestoreMetadata` API。

[4] `backup:TagResource` 如果您计划在备份中包含原始资源标签或在备份中添加其他标签，则某些资源类型要求执行备份的角色具有特定的标记权限。任何以 ARN 开头的备份`arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:`或连续备份都需要此权限。 `backup:TagResource`必须将许可应用于 "*`resourcetype`*": "`arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*`"

有关更多信息，请参阅《服务授权参考》中的 AWS Backup的操作、资源和条件键。

复制标签权限

AWS Backup 执行备份或复印作业时，它会尝试将标签从您的源资源（如果是复制，则为恢复点）复制到您的恢复点。

> **Note**
>
> AWS Backup 在还原作业期间不会以本机方式复制标签。有关将在还原作业期间复制标签的事件驱动架构，请参阅如何在还原作业中 AWS Backup 保留资源标签。

在备份或复印作业期间， AWS Backup 将您在备份计划（或复制计划或按需备份）中指定的标签与源资源中的标签聚合。但是，对每个资源 AWS 强制执行 50 个标签的限制，该限制 AWS Backup 不能超过。当备份或复制作业聚合计划和源资源中的标签时，它可能会发现总标签数超过 50 个，此时它将无

法完成作业，并且会使作业失败。这与 AWS全域标记最佳实践一致。要了解更多信息，请参阅《AWS一般参考指南》中的标签限制。

- 将备份任务标签与源资源标签聚合后，您的资源有超过 50 个标签。 AWS 每个资源最多支持 50 个标签。有关更多信息，请参阅标签限制。
- 您提供的 IAM 角色 AWS Backup 缺乏读取源标签或设置目标标签的权限。有关更多信息和 IAM 角色策略示例，请参阅托管策略。

您可以使用备份计划创建与源资源标签相矛盾的标签。当两者发生冲突时，您的备份计划中的标签优先。如果您不想从源资源中复制标签值，请使用此方法。使用备份计划指定相同的标签密钥，但使其值不同或为空。

为备份分配标签所需的权限

资源类型	所需的权限
Amazon EFS 文件系统	`elasticfilesystem:DescribeTags`
Amazon FSx 文件系统	`fsx:ListTagsForResource`
Amazon RDS 数据库和 Amazon Aurora 集群	`rds:AddTagsToResource` `rds:ListTagsForResource`
Storage Gateway 卷	`storagegateway:ListTagsForResource`
Amazon EC2 实例和 Amazon EBS 卷	`EC2:CreateTags` `EC2:DescribeTags`

除非先启用高级 DynamoDB 备份，否则 DynamoDB 不支持为备份分配标签。

当 Amazon EC2 备份创建映像恢复点和一组快照时，会将标签 AWS Backup 复制到生成的 AMI。AWS Backup 还将标签从与 Amazon EC2 实例关联的卷复制到生成的快照中。

访问策略

权限策略规定谁可以访问哪些内容。附加到 IAM 身份的策略称为基于身份的策略（IAM 策略）。附加到资源的策略称为基于资源的策略。 AWS Backup 支持基于身份的策略和基于资源的策略。

> **Note**
>
> 本节讨论在的上下文中使用 IAM AWS Backup。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅《IAM 用户指南》中的什么是 IAM？。有关 IAM 策略语法和描述的信息，请参阅《IAM 用户指南》中的IAM JSON 策略参考。

基于身份的策略（IAM 策略）

基于身份的策略是可以附加到 IAM 身份（如用户或角色）的策略。例如，您可以定义一个策略，允许用户查看和备份 AWS 资源，但禁止他们恢复备份。

有关用户、组、角色和权限的更多信息，请参阅《IAM 用户指南》中的身份（用户、组和角色）。

有关如何使用 IAM 策略控制对备份的访问的信息，请参阅的托管策略 AWS Backup。

基于资源的策略

AWS Backup 支持基于资源的备份存储库访问策略。这使您可以定义访问策略，用于控制哪些用户对于存储在备份保管库中的任何备份具有哪种类型的访问权限。备份保管库的基于资源的访问策略提供了一种控制备份访问的简便方法。

Backup 保管库访问策略控制您使用 AWS Backup API 时的用户访问权限。某些备份类型（例如 Amazon Elastic Block Store (Amazon EBS) 和 Amazon Relational Database Service (Amazon RDS) 快照）也可以使用这些服务的 API 进行访问。您可以在 IAM 中创建单独的访问策略控制对这些 API 的访问，从而完全控制对备份的访问。

要了解如何创建备份保管库的访问策略，请参阅对备份保管库设置访问策略。

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， AWS Backup 要求您在该服务代表您执行备份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。

您传递给的角色 AWS Backup 必须具有 IAM 策略，该策略具有执行与备份操作相关的操作的权限，例如创建、还原或过期备份。 AWS Backup AWS Backup 支持的每项 AWS 服务都需要不同的权限。该角色还必须 AWS Backup 列为可信实体，这样 AWS Backup 才能担任该角色。

在为备份计划分配资源或执行按需备份、复制或还原时，必须传递一个有权对指定资源执行底层操作的服务角色。 AWS Backup 使用此角色在您的账户中创建、标记和删除资源。

使用 AWS 角色控制对备份的访问权限

您可以使用角色来控制对备份的访问，方法是定义范围狭窄的角色，并指定谁可以将该角色传递给 AWS Backup。例如，您可以创建一个角色，该角色仅授予备份亚马逊关系数据库服务 (Amazon RDS) 数据库的权限，而仅授予 Amazon RDS 数据库所有者将该角色传递给的权限 AWS Backup。 AWS Backup 为每种支持的服务提供了多个预定义的托管策略。您可以将这些托管策略附加到您创建的角色。这样可以更轻松地创建具有 AWS Backup 所需正确权限的服务特定角色。

有关 AWS 托管策略的更多信息 AWS Backup，请参阅的托管策略 AWS Backup。

的默认服务角色 AWS Backup

首次使用 AWS Backup 控制台时，您可以选择为您 AWS Backup 创建默认服务角色。此角色具有代表您创建和恢复备份 AWS Backup 所需的权限。

> **Note**
>
> 默认角色是在您使用 AWS Management Console时自动创建的。您可以使用 AWS Command Line Interface (AWS CLI) 创建默认角色，但必须手动完成。

如果您更喜欢使用自定义角色，例如为不同的资源类型使用不同的角色，也可以这样做并将您的自定义角色传递给 AWS Backup。要查看为单个资源类型启用备份和还原的角色示例，请参阅客户托管策略表。

默认服务角色名为`AWSBackupDefaultServiceRole`。此服务角色包含两个托管策略，AWSBackupServiceRolePolicyForBackup和AWSBackupServiceRolePolicyForRestores。

`AWSBackupServiceRolePolicyForBackup`包括一个 IAM 策略，该策略授予描述正在备份的资源的 AWS Backup 权限，以及创建、删除、描述备份或向备份添加标签的能力，无论使用何种 AWS KMS 密钥对其进行加密。

`AWSBackupServiceRolePolicyForRestores`包括一个 IAM 策略，该策略授予创建、删除或描述从备份中创建的新资源的 AWS Backup 权限，无论使用何种 AWS KMS 密钥对其进行加密。它还包括权限来标记新创建的资源。

要还原 Amazon EC2 实例，您必须启动一个新实例。

在控制台中创建默认服务角色

您在 AWS Backup 控制台中执行的特定操作将创建 AWS Backup 默认服务角色。

在您的 AWS 账户中创建 AWS Backup 默认服务角色

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 要为您的账户创建角色，请为备份计划分配资源或创建按需备份。
   a. 创建备份计划并为备份分配资源。请参阅创建计划备份。
   b. 或者，创建按需备份。请参阅创建按需备份。
3. 按照以下步骤验证您是否已在账户中创建 `AWSBackupDefaultServiceRole`：
   a. 等待几分钟。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的我所做的更改并不总是立即可见。
   b. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
   c. 在左导航菜单中，选择角色。
   d. 在搜索栏中，键入 `AWSBackupDefaultServiceRole`。如果存在此选择，则表示您已经创建了 AWS Backup 默认角色并完成了此过程。
   e. 如果 `AWSBackupDefaultServiceRole` 仍未出现，请向用于访问控制台的 IAM 用户或 IAM 角色添加以下权限。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
```

```
      ],
      "Resource":"*"
    }
  ]
}
```

对于中国区域，请将 *aws* 替换为 *aws-cn*。对于 AWS GovCloud (US) 区域，将 a *w* s 替换为*aws-us-gov*。

f. 如果您无法向 IAM 用户或 IAM 角色添加权限，请让您的管理员手动创建一个名称不为 AWSBackupDefaultServiceRole 的角色，并将该角色附加到以下托管策略：

- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores

的托管策略 AWS Backup

托管策略是基于身份的独立策略，您可以将其附加到中的多个用户、群组和角色。 AWS 账户将策略附加到主体实体时，便向实体授予了策略中定义的权限。

AWS 托管策略由创建和管理 AWS。您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。

客户托管策略为您提供了精细的控制来设置对备份的访问权限。 AWS Backup例如，您可以使用它们向数据库备份管理员授予对 Amazon RDS 备份，而不是 Amazon EFS 备份的访问权限。

有关更多信息，请参阅 IAM 用户指南中的托管策略。

AWS 托管策略

AWS Backup 为常见用例提供了以下 AWS 托管策略。使用这些策略可以更轻松地定义正确的权限并控制对备份的访问。有两种托管策略。一种类型旨在分配给用户，以控制他们对 AWS Backup的访问。另一种托管策略旨在附加到您传递给 AWS Backup的角色。下表列出了 AWS Backup 提供的所有托管策略，并说明了它们的定义方式。您可以在 IAM 控制台的策略部分找到这些托管策略。

策略

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess

- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

该策略允许用户创建控制和框架，以定义他们对 AWS Backup 资源和活动的期望，并根据其定义的控制和框架对 AWS Backup 资源和活动进行审计。该政策授予权限 AWS Config 和类似的服务，以描述用户期望来执行审计。

此策略还向 Amazon S3 和类似服务授予提供审计报告的权限，并使用户能够查找和打开其审计报告。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupAuditAccess中的。

AWSBackupDataTransferAccess

此策略为 AWS Backup 存储平面数据传输 API 提供权限，允许 AWS Backint 代理使用 AWS Backup 存储平面完成备份数据传输。您可以将此策略附加到使用 Backint 代理运行 SAP HANA 的 Amazon EC2 实例所担任的角色。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupDataTransferAccess中的。

AWSBackupFullAccess

备份管理员拥有 AWS Backup 操作的完全访问权限，包括创建或编辑备份计划、为备份计划分配 AWS 资源以及恢复备份。备份管理员负责通过定义满足其组织的业务和法规要求的备份计划来确定和强制实施备份合规性。Backup 管理员还要确保将其组织的 AWS 资源分配给相应的计划。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupFullAccess中的。

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

要查看此策略的权限，请参阅AWS 托管策略参考中的。

AWSBackupOperatorAccess

备份操作员是这样的用户，他们负责确保正确备份自己负责的资源。Backup 操作员有权为备份管理员创建的备份计划分配 AWS 资源。他们还有权为其 AWS 资源创建按需备份和配置按需备份的保留期。备份操作员无权创建或编辑备份计划，也无权在创建备份计划后删除计划备份。备份操作员可以还原备份。您可以限制备份操作员可分配给备份计划或从备份还原的资源类型。为此，您可以只允许向具有特定资源类型权限的某些服务角色传递。 AWS Backup

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupOperatorAccess中的。

AWSBackupOrganizationAdminAccess

组织管理员拥有 AWS Organizations 操作的完全访问权限，包括创建、编辑或删除备份策略，为账户和组织单位分配备份策略，以及监控组织内的备份活动。组织管理员负责通过定义和分配满足其组织业务和管理法规要求的备份策略来保护其组织中的账户。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupOrganizationAdminAccess中的。

AWSBackupRestoreAccessForSAPHANA

该策略 AWS Backup 允许在亚马逊 EC2 上恢复 SAP HANA 的备份。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupRestoreAccessForSAPHANA中的。

AWSBackupServiceLinkedRolePolicyForBackup

此策略附加到名为的服务相关角色AWSServiceRoleforBackup， AWS Backup 允许您代表您调用 AWS 服务来管理备份。有关更多信息，请参阅 the section called “备份和复制”。

要查看此策略的权限，请参阅AWS 托管策略参考 AWSBackupServiceLinkedRolePolicyforBackup中的。

AWSBackupServiceLinkedRolePolicyForBackupTest

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupServiceLinkedRolePolicyForBackupTest中的。

AWSBackupServiceRolePolicyForBackup

提供代表您创建所有受支持资源类型的备份的 AWS Backup 权限。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupServiceRolePolicyForBackup中的。

AWSBackupServiceRolePolicyForRestores

提供代表您恢复所有受支持资源类型的备份的 AWS Backup 权限。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupServiceRolePolicyForRestores中的。

对于 EC2 实例还原，还必须包括以下权限才能启动 EC2 实例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

此策略包含备份任何 S3 存储桶所需的 AWS Backup 权限。这包括对存储桶中所有对象和任何关联 AWS KMS 密钥的访问权限。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupServiceRolePolicyForS3Backup中的。

AWSBackupServiceRolePolicyForS3Restore

此策略包含将 S3 备份还原 AWS Backup 到存储桶所需的权限。这包括对存储桶的读写权限以及与 S3 操作有关的任何 AWS KMS 密钥的使用。

要查看此策略的权限，请参阅AWS 托管策略参考AWSBackupServiceRolePolicyForS3Restore中的。

AWSServiceRolePolicyForBackupReports

AWS Backup 将此策略用于AWSServiceRoleForBackupReports服务相关角色。此服务相关 AWS Backup 角色允许监控和报告您的备份设置、任务和资源与框架的合规性。

要查看此策略的权限，请参阅AWS 托管策略参考AWSServiceRolePolicyForBackupReports中的。

AWSServiceRolePolicyForBackupRestoreTesting

要查看此策略的权限，请参阅AWS 托管策略参考AWSServiceRolePolicyForBackupRestoreTesting中的。

客户托管策略

以下各节描述了为支持的应用程序和第三方应用程序推荐的备份 AWS 服务 和还原权限 AWS Backup。在创建自己的策略文档时，您可以使用现有的 AWS 托管策略作为模型，然后对其进行自定义以进一步限制对 AWS 资源的访问。

Amazon Aurora

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

还原

从中的`RDSPermissions`语句开始AWSBackupServiceRolePolicyForRestores。

Amazon DynamoDB

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`

- KMSDynamoDBPermissions

还原

从以下语句开始 AWSBackupServiceRolePolicyForRestores：

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamoDBRestorePermissions
- KMSPermissions

Amazon EBS

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- EBSResourcePermissions
- EBSTagAndDeletePermissions
- EBSCopyPermissions
- EBSSnapshotTierPermissions
- GetResourcesPermissions
- BackupVaultPermissions

还原

从中的EBSPermissions语句开始AWSBackupServiceRolePolicyForRestores。

添加以下语句。

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
```

```
        "Resource":"*"
},
```

Amazon EC2

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

还原

从以下语句开始 AWSBackupServiceRolePolicyForRestores：

- EBSPermissions
- EC2DescribePermissions
- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

添加以下语句。

```
{
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

还原

从中的`EFSPermissions`语句开始AWSBackupServiceRolePolicyForRestores。

Amazon FSx

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

还原

从以下语句开始 AWSBackupServiceRolePolicyForRestores：

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`

- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon RDS

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- DynamoDBBackupPermissions
- RDSBackupPermissions
- RDSClusterModifyPermissions
- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

还原

从中的RDSPermissions语句开始AWSBackupServiceRolePolicyForRestores。

Amazon S3

备份

首先是AWSBackupServiceRolePolicyForS3Backup。

如果您需要将备份复制到其他帐户，请添加BackupVaultPermissions和BackupVaultCopyPermissions语句。

还原

首先是AWSBackupServiceRolePolicyForS3Restore。

AWS Storage Gateway

备份

从以下语句开始 AWSBackupServiceRolePolicyForBackup：

- StorageGatewayPermissions
- EBSTagAndDeletePermissions
- GetResourcesPermissions
- BackupVaultPermissions

添加以下语句。

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

还原

从以下语句开始 AWSBackupServiceRolePolicyForRestores：

- StorageGatewayVolumePermissions
- StorageGatewayGatewayPermissions
- StorageGatewayListPermissions

虚拟机

备份

从中的BackupGatewayBackupPermissions语句开始AWSBackupServiceRolePolicyForBackup。

还原

从中的GatewayRestorePermissions语句开始AWSBackupServiceRolePolicyForRestores。

加密备份

要还原加密的备份，请执行以下操作之一：

- 将您的角色添加到 AWS KMS 密钥策略的许可名单
- 将以下语句AWSBackupServiceRolePolicyForRestores添加到您的 IAM 角色中进行恢复：
  - KMSDescribePermissions
  - KMSPermissions
  - KMSCreateGrantPermissions

的政策更新 AWS Backup

查看 AWS Backup 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 对现有策略的更新	AWS Backup 为此策略添加了权限backup:TagResource。 该权限是创建恢复点期间获得标记权限所必需的。	2024 年 5 月 17 日
AWSBackupServiceRolePolicyForS3Backup – 更新了现有策略	AWS Backup 为此策略添加了权限backup:TagResource。 该权限是创建恢复点期间获得标记权限所必需的。	2024 年 5 月 17 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	AWS Backup 为此策略添加了权限backup:TagResource。 该权限是创建恢复点期间获得标记权限所必需的。	2024 年 5 月 17 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了权限`rds:DeleteDBInstanceAutomatedBackups` 。 此权限是支持持续备份和 Amazon RDS 实例 point-in-time-restore 所必需的。 AWS Backup	2024 年 5 月 1 日
AWSBackupFullAccess – 更新了现有策略	AWS Backup 将亚马逊资源名称 (ARN) 的权限`storagegateway:ListVolumes` 从更新为，`arn:aws:storagegateway:*:*:gateway/*` 以*适应 Storage Gateway API 模型的变化。	2024 年 5 月 1 日
AWSBackupOperatorAccess – 更新了现有策略	AWS Backup 将亚马逊资源名称 (ARN) 的权限`storagegateway:ListVolumes` 从更新为，`arn:aws:storagegateway:*:*:gateway/*` 以*适应 Storage Gateway API 模型的变化。	2024 年 5 月 1 日

更改	描述	日期
AWSServiceRolePolicyForBackupRestoreTesting – 更新了现有策略	添加了以下权限，用于描述和列出恢复点和受保护的资源，以便执行恢复测试计划：backup:DescribeRecoveryPoint backup:DescribeProtectedResource 、backup:ListProtectedResources 、和backup:ListRecoveryPointsByResource 。 添加了支持 Amazon EBS 存档层存储的权限ec2:DescribeSnapshotTierStatus 。 增加了支持 Amazon Aurora 连续备份的权限rds:DescribeDBClusterAutomatedBackups 。 添加了以下权限以支持 Amazon Redshift 备份的还原测试：redshift:DescribeClusters 和。redshift:DeleteCluster 增加了支持 Amazon Timestream 备份恢复测试的权限timestream:DeleteTable 。	2024年2月14日

更改	描述	日期
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了权限`ec2:DescribeSnapshotTierStatus` 和`ec2:RestoreSnapshotTier` 。 用户需要这些权限才能选择 AWS Backup 从存档存储中恢复存储的 Amazon EBS 资源。 对于 EC2 实例还原，还必须在以下策略语句中包括所示权限才能启动 EC2 实例：	2023 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了权限`ec2:DescribeSnapshotTierStatus` 并支持`ec2:ModifySnapshotTier` 将备份的 Amazon EBS 资源过渡到存档存储层的额外存储选项。 用户需要这些权限才能选择将存储在一起的 Amazon EBS 资源转移 AWS Backup 到存档存储。	2023 年 11 月 27 日

更改	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了权限`ec2:DescribeSnapshotTierStatus` 并支持`ec2:ModifySnapshotTier` 将备份的 Amazon EBS 资源过渡到存档存储层的额外存储选项。 用户需要这些权限才能选择将存储在一起的 Amazon EBS 资源转移 AWS Backup 到存档存储。 添加了`rds:DescribeDBClusterSnapshots` 和`rds:RestoreDBClusterToPointInTime` ，这是 Aurora 集群的 PITR（point-in-time 恢复）所必需的。	
AWSServiceRolePolicyForBackupRestoreTesting：新策略	提供进行恢复测试所需的权限。权限包括适用于要在还原测试中包括的以下服务的操作 `list`, `read`, and `write`：Aurora、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS 和 Amazon S3。	2023 年 11 月 27 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	已将 `restore-testing.backup.amazonaws.com` 添加到 `IamPassRolePermissions` 和 `IamCreateServiceLinkedRolePermissions` 。为了代表客户 AWS Backup 进行恢复测试，必须添加此项。	2023 年 11 月 27 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了`rds:DescribeDBClusterSnapshots` 和`rds:RestoreDBClusterToPointInTime` ，这是 Aurora 集群的 PITR（point-in-time 恢复）所必需的。	2023 年 9 月 6 日
AWSBackupFullAccess – 更新了现有策略	添加了持续备份和 point-in-time 恢复 Aurora 集群所必需的权限`rds:DescribeDBClusterAutomatedBackups` 。	2023 年 9 月 6 日
AWSBackupOperatorAccess – 更新了现有策略	添加了持续备份和 point-in-time 恢复 Aurora 集群所必需的权限`rds:DescribeDBClusterAutomatedBackups` 。	2023 年 9 月 6 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了权限`rds:DescribeDBClusterAutomatedBackups` 。此权限是 AWS Backup 支持 Aurora 集群的持续备份和 point-in-time 恢复所必需的。 添加了`rds:DeleteDBClusterAutomatedBackups` 允许 AWS Backup 生命周期在保留期结束时删除和解除关联 Amazon Aurora 持续恢复点的权限。需要此权限才能让 Aurora 恢复点避免转换为 EXIPIRED 状态。 添加`rds:ModifyDBCluster` 了允许与 Aurora 集群 AWS Backup 进行交互的权限。此新增权限使用户能够根据所需的配置启用或禁用连续备份。	2023 年 9 月 6 日
AWSBackupFullAccess – 更新了现有策略	添加了授`ram:GetResourceShareAssociations` 予用户获取新文件库类型资源共享关联的权限的操作。	2023 年 8 月 8 日
AWSBackupOperatorAccess – 更新了现有策略	添加了授`ram:GetResourceShareAssociations` 予用户获取新文件库类型资源共享关联的权限的操作。	2023 年 8 月 8 日

更改	描述	日期
AWSBackupServiceRolePolicyForS3Backup – 更新了现有策略	添加了使用存储桶清单`s3:PutInventoryConfiguration` 来提高备份性能速度的权限。	2023 年 8 月 1 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下操作以授予用户添加标签以还原资源的权限：`storagegateway:AddTagsToResource elasticfilesystem:TagResource` ，`ec2:CreateAction` ，仅`ec2:CreateTags` 适用于包括`RunInstances` 或`CreateVolume fsx:TagResource` 、和`cloudformation:TagResource` 。	2023 年 5 月 22 日
AWSBackupAuditAccess – 更新了现有策略	将 API `config:DescribeComplianceByConfigRule` 中的资源选择替换为通配符资源，以便用户更轻松地选择资源。	2023 年 4 月 11 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下使用客户托管密钥恢复 Amazon EFS 的权限：`kms:GenerateDataKeyWithoutPlaintext` 。这有助于确保用户拥有恢复 Amazon EFS 资源所需的权限。	2023 年 3 月 27 日

更改	描述	日期
AWSServiceRolePolicyForBackupReports – 更新了现有策略	更新了config:DescribeConfigRules 和config:DescribeConfigRuleEvaluationStatus 操作以允许 Audi AWS Backup t Manager 访问 AWS Backup 审计管理器管理 AWS Config 的规则。	2023 年 3 月 9 日
AWSBackupServiceRolePolicyForS3Restore – 更新了现有策略	在策略中添加了以下权限：kms:Decrypt s3:PutBucketOwnershipControls 、和s3:GetBucketOwnershipControls AWSBackupServiceRolePolicyForS3Restore 。这些权限是支持在原始备份中使用 KMS 加密时还原对象，以及在原始存储桶而不是 ACL 上配置对象所有权时还原对象所必需的权限。	2023 年 2 月 13 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	添加了以下权限，以使用虚拟机的 VMware 标签计划备份并支持基于时间表的带宽限制：backup-gateway:GetHypervisorPropertyMappings 、、、、、backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings 、backup-gateway:GetHypervisor 和。backup-gateway:StartVirtualMachinesMetadataSync backup-gateway:GetBandwidthRateLimitSchedule backup-gateway:PutBandwidthRateLimitSchedule	2022 年 12 月 15 日
AWSBackupOperatorAccess – 更新了现有策略	添加了以下权限，以使用虚拟机的 VMware 标签计划备份并支持基于时间表的带宽限制：backup-gateway:GetHypervisorPropertyMappings 、、和。backup-gateway:GetVirtualMachine backup-gateway:GetHypervisor backup-gateway:GetBandwidthRateLimitSchedule	2022 年 12 月 15 日

更改	描述	日期
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync：新策略	允许 AWS Backup Gateway 将本地网络中虚拟机的元数据与 Backup Gateway 同步。	2022 年 12 月 15 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了以下权限以支持 Timestream 备份任务：`timestream:StartAwsBackupJob` `timestream:GetAwsBackupStatus` 、`timestream:ListTables` 、`timestream:ListDatabases` 、`timestream:ListTagsForResource` 、`timestream:DescribeTable` 、`timestream:DescribeDatabase` 、和`timestream:DescribeEndpoints` 。	2022 年 12 月 13 日

更改	描述	日期
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下权限以支持 Timestream 还原作业：timestream:StartAwsRestoreJob timestream:GetAwsRestoreStatus timestream:ListTables 、timestream:ListTagsForResource 、timestream:ListDatabases 、、timestream:DescribeTable 、timestream:DescribeDatabase 、s3:GetBucketAcl 、和timestream:DescribeEndpoints 。	2022 年 12 月 13 日
AWSBackupFullAccess – 更新了现有策略	添加了以下权限来支持 Timestream 资源：timestream:ListTables timestream:ListDatabases 、s3:ListAllMyBuckets 和。timestream:DescribeEndpoints	2022 年 12 月 13 日

更改	描述	日期
AWSBackupOperatorAccess – 更新了现有策略	添加了以下权限来支持 Timestream 资源：timestream:ListDatabases timestream:ListTables 、s3:ListAllMyBuckets 、和。timestream:DescribeEndpoints	2022 年 12 月 13 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了以下权限来支持 Timestream 资源：timestream:ListDatabases timestream:ListTables 、timestream:ListTagsForResource 、timestream:DescribeDatabase 、timestream:DescribeTable 、timestream:GetAwsBackupStatus 、timestream:GetAwsRestoreStatus 、和。timestream:DescribeEndpoints	2022 年 12 月 13 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	添加了以下权限来支持 Amazon Redshift 资源：redshift:DescribeClusters redshift:DescribeClusterSubnetGroups 、redshift:DescribeNodeConfigurationOptions 、、redshift:DescribeOrderableClusterOptions 、redshift:DescribeClusterParameterGroups 、redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules 、和。ec2:DescribeAddresses	2022 年 11 月 27 日

更改	描述	日期
AWSBackupOperatorAccess – 更新了现有策略	添加了以下权限来支持 Amazon Redshift 资源：redshift:DescribeClusters 、、redshift:DescribeClusterSubnetGroups 、redshift:DescribeNodeConfigurationOptions 、redshift:DescribeOrderableClusterOptions 、redshift:DescribeClusterParameterGroups, 。redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules ，以及ec2:DescribeAddresses 。	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下权限来支持 Amazon Redshift 恢复任务：redshift:RestoreFromClusterSnapshot、redshift:RestoreTableFromClusterSnapshot redshift:DescribeClusters 、和。redshift:DescribeTableRestoreStatus	2022 年 11 月 27 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了以下权限来支持 Amazon Redshift 备份任务：`redshift:CreateClusterSnapshot` 、`redshift:DescribeClusterSnapshots` 、`redshift:DescribeTags` 、`redshift:DeleteClusterSnapshot` `redshift:DescribeClusters` 、和。`redshift:CreateTags`	2022 年 11 月 27 日
AWSBackupFullAccess – 更新了现有策略	添加了以下权限来支持 CloudFormation 资源:`cloudformation:ListStacks` .	2022 年 11 月 27 日
AWSBackupOperatorAccess – 更新了现有策略	添加了以下权限来支持 CloudFormation 资源:`cloudformation:ListStacks` .	2022 年 11 月 27 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	为支持 CloudFormation 资源添加了以下权限：`redshift:DescribeClusterSnapshots` `redshift:DescribeTags` 、`redshift:DeleteClusterSnapshot` 、和`redshift:DescribeClusters` 。	2022 年 11 月 27 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了以下权限以支持 AWS CloudFormation 应用程序堆栈备份作业：`cloudformation:GetTemplate cloudformation:DescribeStacks` 、和`cloudformation:ListStackResources` 。	2022 年 11 月 16 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下权限以支持 AWS CloudFormation 应用程序堆栈备份作业：`cloudformation:CreateChangeSet` 和 `cloudformation:DescribeChangeSet`	2022 年 11 月 16 日
AWSBackupOrganizationAdminAccess – 更新了现有策略	为此策略添加了以下权限，以允许组织管理员使用委派管理员功能：`organizations:ListDelegatedAdministrator organizations:RegisterDelegatedAdministrator` 、和 `organizations:DeregisterDelegatedAdministrator`	2022 年 11 月 27 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了以下权限以支持 Amazon EC2 实例上的 SAP HANA：ssm-sap:GetOperation ssm-sap:ListDatabases ssm-sap:BackupDatabase 、ssm-sap:UpdateHanaBackupSettings 、ssm-sap:GetDatabase 、、和ssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupFullAccess – 更新了现有策略	添加了以下权限以支持 Amazon EC2 实例上的 SAP HANA：ssm-sap:GetOperation ssm-sap:ListDatabases ssm-sap:GetDatabase 、、和ssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupOperatorAccess – 更新了现有策略	添加了以下权限以支持 Amazon EC2 实例上的 SAP HANA：ssm-sap:GetOperation ssm-sap:ListDatabases ssm-sap:GetDatabase 、、和ssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了以下权限以支持 Amazon EC2 实例上的 SAP HANA：ssm-sap:GetOperation 。	2022 年 11 月 20 日

更改	描述	日期
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下权限以支持 Backup 网关还原任务到 EC2 实例:`ec2:CreateTags` .	2022 年 11 月 20 日
AWSBackupDataTransferAccess – 更新了现有策略	添加了以下权限以支持 SAP HANA On Amazon EC2 资源的安全存储数据传输：`backup-storage:StartObject backup-storage:PutChunk backup-storage:GetChunk 、、backup-storage:ListChunks 、backup-storage:ListObjects 、backup-storage:GetObjectMetadata 、、和backup-storage:NotifyObjectComplete 。`	2022 年 11 月 20 日

更改	描述	日期
AWSBackupRestoreAccessForSAPHANA – 更新了现有策略	为资源所有者添加了以下权限，使其能够恢复 Amazon EC2 上的 SAP HANA 资源：backup:Get* backup:List* backup:Describe* 、backup:StartBackupJob 、、backup:StartRestoreJob 、ssm-sap:GetOperation 、ssm-sap:ListDatabases 、、ssm-sap:BackupDatabase 、ssm-sap:RestoreDatabase 、、ssm-sap:UpdateHanaBackupSettings 、ssm-sap:GetDatabase 、、和ssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupServiceRolePolicyForS3Backup – 更新了现有策略	添加了支持 Amazon S3 AWS Backup 的备份操作的权限s3:GetBucketAcl 。	2022 年 8 月 24 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下操作以授予创建数据库实例的访问权限，以支持多可用区（多可用区）功能：。rds:CreateDBInstance	2022 年 7 月 20 日

更改	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了s3:GetBucketTagging 使用资源通配符授予用户选择要备份的存储桶的权限。如果没有此权限，使用资源通配符选择要备份的存储桶的用户将无法成功。	2022 年 5 月 6 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	在现有fsx:CreateBackup 和fsx:ListTagsForResource 操作范围内添加了卷资源，并添加了新操作fsx:DescribeVolumes 以支持 FSx 进行 ONTAP 卷级别备份。	2022 年 4 月 27 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了以下操作以授予用户恢复 ONTAP 卷的 FSx 的权限fsx:DescribeVolumes 、fsx:CreateVolumeFromBackup 、fsx:DeleteVolume 和。fsx:UntagResource	2022 年 4 月 27 日
AWSBackupServiceRolePolicyForS3Backup – 更新了现有策略	添加了以下操作，以授予用户在备份操作期间接收其 Amazon S3 存储桶变更通知的权限：s3:GetBucketNotification 和s3:PutBucketNotification 。	2022 年 2 月 25 日

更改	描述	日期
AWSBackupServiceRolePolicyForS3Backup：新策略	添加了以下操作以向用户授予备份其 Amazon S3 存储桶的权限：s3:GetInventoryConfiguration 、、s3:PutInventoryConfiguration 、s3:ListBucketVersions 、s3:ListBucket 、s3:GetBucketTagging 、s3:GetBucketVersioning 、、s3:GetBucketNotification s3:GetBucketLocation 、和 s3:ListAllMyBuckets 添加了以下操作以授予用户备份其 Amazon S3 对象的权限：s3:GetObject s3GetObjectAcl 、s3:GetObjectVersionTagging 、s3:GetObjectVersionAcl 、s3:GetObjectTagging 、和s3:GetObjectVersion 。 添加了以下操作以授予用户备份其加密的 Amazon S3 数据的权限：kms:Decrypt 和kms:DescribeKey 。	2022 年 2 月 17 日

更改	描述	日期
	添加了以下操作以授予用户使用 Amazon EventBridge 规则对其 Amazon S3 数据进行增量备份的权限：events:DescribeRule 、events:EnableRule 、events:PutRule 、、events:DeleteRule 、events:PutTargets 、events:RemoveTargets 、、events:ListTargetsByRule 、events:DisableRule 、cloudwatch:GetMetricData 、、和events:ListRules 。	

更改	描述	日期
AWSBackupServiceRolePolicyForS3Restore：新策略	添加了以下操作以授予用户恢复其 Amazon S3 存储桶的权限：s3:CreateBucket s3:ListBucketVersions 、s3:ListBucket 、、s3:GetBucketVersioning s3:GetBucketLocation 、和s3:PutBucketVersioning 。 添加了以下操作以授予用户恢复其 Amazon S3 存储桶的权限：s3:GetObject 、s3:GetObjectVersion 、s3:DeleteObject 、s3:PutObjectVersionAcl 、、s3:GetObjectVersionAcl 、s3:GetObjectTagging 、s3:PutObjectTagging 、s3:GetObjectAcl 、s3:PutObjectAcl 、s3:PutObject 、和s3:ListMultipartUploadParts 。 添加了以下操作以授予用户加密其恢复的 Amazon S3 数据的权限：kms:Decrypt kms:DescribeKey 、	2022 年 2 月 17 日

更改	描述	日期
	和kms:GenerateDataKey 。	
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	s3:ListAllMyBuckets 添加了授予用户查看其存储桶列表和选择要分配给备份计划的存储桶的权限。	2022 年 2 月 14 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	backup-gateway:ListVirtualMachines 添加了授予用户查看其虚拟机列表和选择要分配给备份计划的虚拟机的权限。 backup-gateway:ListTagsForResource 添加了授予用户列出其虚拟机标签的权限。	2021 年 11 月 30 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了backup-gateway:Backup 向用户授予恢复其虚拟机备份的权限。 AWS Backup 还添加了backup-gateway:ListTagsForResource 此项以授予用户列出分配给其虚拟机备份的标签的权限。	2021 年 11 月 30 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了backup-gateway:Restore 向用户授予恢复其虚拟机备份的权限。	2021 年 11 月 30 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	添加了以下操作以授予用户使用 AWS Backup Gateway 备份、还原和管理其虚拟机的权限：、、、、backup-gateway:AssociateGatewayToServer 、、、、、、backup-gateway:CreateGateway 、、backup-gateway:DeleteGateway 、backup-gateway:DeleteHypervisor 、、backup-gateway:DisassociateGatewayFromServer 、backup-gateway:ImportHypervisorConfiguration 、backup-gateway:ListGateways 、、backup-gateway:ListHypervisors 、backup-gateway:ListTagsForResource 、、backup-gateway:ListVirtualMachines 、backup-gateway:PutMaintenanceStartTime 、、backup-gateway:TagResource 、backup-gateway:TestHypervisorConfigu	2021 年 11 月 30 日

更改	描述	日期
	ration 、backup-gateway:UntagResource 、、backup-gateway:UpdateGatewayInformation 、、和backup-gateway:UpdateHypervisor 。	
AWSBackupOperatorAccess – 更新了现有策略	添加了以下操作以授予用户备份其虚拟机的权限：backup-gateway:ListGateways backup-gateway:ListHypervisors 、backup-gateway:ListTagsForResource 、和backup-gateway:ListVirtualMachines 。	2021 年 11 月 30 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加的dynamodb:ListTagsOfResource 目的是授予用户列出其 DynamoDB 表标签的权限，以便使用其高级 DynamoDB 备份 AWS Backup功能进行备份。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加dynamodb:StartAwsBackupJob 的目的是向用户授予使用高级备份功能备份其 DynamoDB 表的权限。 添加的dynamodb:ListTagsOfResource 目的是向用户授予将标签从其源 DynamoDB 表复制到备份的权限。	2021 年 11 月 23 日

更改	描述	日期
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加dynamodb:RestoreTableFromAwsBackup 此项是为了向用户授予恢复使用高级 DynamoDB 高级备份功能备份 AWS Backup的 DynamoDB 表的权限。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加dynamodb:RestoreTableFromAwsBackup 此项是为了向用户授予恢复使用高级 DynamoDB 高级备份功能备份 AWS Backup的 DynamoDB 表的权限。	2021 年 11 月 23 日
AWSBackupOperatorAccess – 更新了现有策略	删除了这些操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因为它们是多余的。 AWS Backup 不需要两者backup:GetRecoveryPointRestoreMetadata 兼backup:Get* 而有之AWSBackupOperatorAccess 。而且， AWS Backup 不需要两者rds:DescribeDBSnapshots 兼rds:describeDBSnapshots 而有之AWSBackupOperatorAccess 。	2021 年 11 月 23 日

更改	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了新的操作elasticfilesystem:DescribeFileSystems 、dynamodb:ListTables 、storagegateway:ListVolumes 、ec2:DescribeVolumes 、ec2:DescribeInstances rds:DescribeDBInstances 、rds:DescribeDBClusters 、、和fsx:DescribeFileSystems ，允许客户在选择要分配给备份计划的资源时从其AWS Backup支持的资源列表中进行查看和选择。	2021 年 11 月 10 日
AWSBackupAuditAccess：新策略	添加了授AWSBackupAuditAccess 予用户使用Audit Manag AWS Backup er的权限。权限包括配置合规框架和生成报告的能力。	2021 年 8 月 24 日
AWSServiceRolePolicyForBackupReports：新策略	添加了AWSServiceRolePolicyForBackupReports 向服务相关角色授予权限，以自动监控备份设置、作业和资源，以符合用户配置的框架。	2021 年 8 月 24 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	iam:CreateServiceLinkedRole 添加了创建服务相关角色（尽力而为），以自动为您删除过期的恢复点。如果没有此服务相关角色，AWS Backup 则无法在客户删除用于创建恢复点的原始 IAM 角色后删除过期的恢复点。	2021 年 7 月 5 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了新操作dynamodb:DeleteBackup ，DeleteRecoveryPoint 允许根据您的备份计划生命周期设置自动删除过期的 DynamoDB 恢复点。	2021 年 7 月 5 日
AWSBackupOperatorAccess – 更新了现有策略	删除了这些操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因为它们是多余的。 AWS Backup 不需要两者backup:GetRecoveryPointRestoreMetadata 兼而有之，backup:Get* 作为 AWSBackupOperatorAccess Also 的一部分，AWS Backup 不需要两者rds:DescribeDBSnapshots 兼而rds:describeDBSnapshots 有之 AWSBackupOperatorAccess	2021 年 5 月 25 日

更改	描述	日期
AWSBackupOperatorAccess – 更新了现有策略	删除了这些操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因为它们是多余的。 AWS Backup 不需要两者backup:GetRecoveryPointRestoreMetadata 兼backup:Get* 而有之AWSBackupOperatorAccess 。而且， AWS Backup 不需要两者rds:DescribeDBSnapshots 兼rds:describeDBSnapshots 而有之AWSBackupOperatorAccess 。	2021 年 5 月 25 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了授fsx:TagResource 予StartRestoreJob 权限的新操作，允许您在还原过程中向 Amazon FSx 文件系统应用标签。	2021 年 5 月 24 日
AWSBackupServiceRolePolicyForRestores – 更新了现有策略	添加了新的操作ec2:DescribeImages 和授予StartRestoreJob 权限ec2:DescribeInstances 以允许您从恢复点恢复 Amazon EC2 实例。	2021 年 5 月 24 日

更改	描述	日期
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	添加了授予StartCopyJob 权限的新操作fsx:CopyBackup ，允许您跨地区和账户复制 Amazon FSx 恢复点。	2021 年 4 月 12 日
AWSBackupServiceLinkedRolePolicyForBackup – 更新了现有策略	添加了授予StartCopyJob 权限的新操作fsx:CopyBackup ，允许您跨地区和账户复制 Amazon FSx 恢复点。	2021 年 4 月 12 日
AWSBackupServiceRolePolicyForBackup – 更新了现有策略	已更新以符合以下要求： AWS Backup 要创建加密的 DynamoDB 表的备份，您必须向用于备份的 IAM 角色添加kms:Decrypt 权限kms:GenerateDataKey 和。	2021 年 3 月 10 日

更改	描述	日期
AWSBackupFullAccess – 更新了现有策略	已更新以符合以下要求： AWS Backup 要使用为您的 Amazon RDS 数据库配置连续备份，请验证您的备份计划配置所定义的 IAM 角色中是否`rds:ModifyDBInstance` 存在 API 权限。 要还原 Amazon RDS 连续备份，您必须向为还原作业提交的 IAM 角色添加权限 `rds:RestoreDBInstanceToPointInTime` 。 在 AWS Backup 控制台中，要描述可用于 point-in-time 恢复的时间范围，您必须在 IAM 管理的`rds:DescribeDBInstanceAutomatedBackups` 策略中包含 API 权限。	2021 年 3 月 10 日
AWS Backup 开始跟踪更改	AWS Backup 开始跟踪其AWS托管策略的更改。	2021 年 3 月 10 日

将服务相关角色用于 AWS Backup

AWS Backup 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Backup服务相关角色由服务预定义 AWS Backup ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

主题

- 使用角色进行备份和复制
- 为 Audit Manag AWS Backup er 使用角色
- 使用角色进行还原测试

使用角色进行备份和复制

AWS Backup 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Backup服务相关角色由服务预定义 AWS Backup ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Backup 更加容易，因为您不必手动添加必要的权限。 AWS Backup 定义其服务相关角色的权限，除非另有定义，否则 AWS Backup 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这样可以保护您的 AWS Backup 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 AWS Backup

AWS Backup 使用名为的服务相关角色 AWSServiceRoleForBackup— 提供列出您可以备份的资源和复制备份的 AWS Backup 权限。

AWS Backup 还使用该角色删除除了 Amazon EC2 之外的所有资源类型的所有备份。

AWSServiceRoleForBackup 服务相关角色信任以下服务来代入该角色：

- `backup.amazonaws.com`

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSBackupServiceLinkedRolePolicyforBackup中的。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS Backup创建服务相关角色

您无需手动创建服务相关角色。当您列出要备份的资源、设置跨账户备份或在、或 AWS API 中执行备份时， AWS Backup 会为您创建服务相关角色。 AWS Management Console AWS CLI

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您列出要备份的资源、设置跨账户备份或执行备份时， AWS Backup 会再次为您创建服务相关角色。

为 AWS Backup编辑服务相关角色

AWS Backup 不允许您编辑 AWSServiceRoleForBackup 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AWS Backup的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。首先，您必须删除所有恢复点。然后，您必须删除所有备份保管库。

> **Note**
>
> 如果您尝试删除资源时 AWS Backup 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForBackup （控制台）使用的 AWS Backup 资源

1. 要删除所有恢复点和备份保管库（默认保管库除外），请按照删除备份保管库中的步骤操作。
2. 要删除默认保管库，请在 AWS CLI中使用以下命令：

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

删除 AWSServiceRoleForBackup (AWS CLI) 使用的 AWS Backup 资源

1. 要删除所有恢复点，请使用delete-recovery-point。
2. 要删除所有备份保管库，请使用 delete-backup-vault。

删除 AWSServiceRoleForBackup (API) 使用的 AWS Backup 资源

1. 要删除所有恢复点，请使用 DeleteRecoveryPoint。
2. 要删除所有备份保管库，请使用 DeleteBackupVault。

手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForBackup服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AWS Backup 服务相关角色的受支持区域

AWS Backup 支持在提供服务的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS Backup 支持的功能和区域。

为 Audit Manag AWS Backup er 使用角色

AWS Backup 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Backup服务相关角色由服务预定义 AWS Backup ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Backup 更加容易，因为您不必手动添加必要的权限。 AWS Backup 定义其服务相关角色的权限，除非另有定义，否则 AWS Backup 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这样可以保护您的 AWS Backup 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 AWS Backup

AWS Backup 使用名为的服务相关角色 AWSServiceRoleForBackupReports— AWS Backup 提供创建控件、框架和报告的权限。

AWSServiceRoleForBackupReports 服务相关角色信任以下服务来代入该角色：

- backup.amazonaws.com

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSServiceRolePolicyForBackupReports中的。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS Backup创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、或 AWS API 中创建框架或报告计划时， AWS Backup 会为您创建服务相关角色。 AWS CLI

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。创建框架或报告计划时， AWS Backup 会再次为您创建服务相关角色。

为 AWS Backup编辑服务相关角色

AWS Backup 不允许您编辑 AWSServiceRoleForBackupReports 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AWS Backup的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。您必须删除所有框架和报告计划。

> **Note**
>
> 如果您尝试删除资源时 AWS Backup 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForBackupReports （控制台）使用的 AWS Backup 资源

1. 要删除所有框架，请参阅删除框架。
2. 要删除所有报告计划，请参阅删除报告计划。

删除 AWSServiceRoleForBackupReports (AWS CLI) 使用的 AWS Backup 资源

1. 要删除所有框架，请使用 delete-framework。
2. 要删除所有报告计划，请使用delete-report-plan。

删除 AWSServiceRoleForBackupReports (API) 使用的 AWS Backup 资源

1. 要删除所有框架，请使用 DeleteFramework。
2. 要删除所有报告计划，请使用DeleteReportPlan。

手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForBackupReports服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AWS Backup 服务相关角色的受支持区域

AWS Backup 支持在提供服务的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS Backup 支持的功能和区域。

使用角色进行还原测试

AWS Backup 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Backup服务相关角色由服务预定义 AWS Backup ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Backup 更加容易，因为您不必手动添加必要的权限。 AWS Backup 定义其服务相关角色的权限，除非另有定义，否则 AWS Backup 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这样可以保护您的 AWS Backup 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 AWS Backup

AWS Backup 使用名为的服务相关角色 AWSServiceRolePolicyForBackupRestoreTesting— 提供备份权限以进行还原测试。

AWSServiceRolePolicyForBackupRestoreTesting 服务相关角色信任以下服务来代入该角色：

- `backup.amazonaws.com`

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSServiceRolePolicyForBackupRestoreTesting中的。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS Backup创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、或 AWS API 中进行恢复测试时， AWS Backup 会为您创建服务相关角色。 AWS CLI

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您进行恢复测试时， AWS Backup 会再次为您创建服务相关角色。

为 AWS Backup编辑服务相关角色

AWS Backup 不允许您编辑 AWSServiceRolePolicyForBackupRestoreTesting 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AWS Backup的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。您必须删除所有还原测试计划。

> **Note**
>
> 如果您尝试删除资源时 AWS Backup 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRolePolicyForBackupRestoreTesting （控制台）使用的 AWS Backup 资源

- 要删除所有还原测试计划，请参阅还原测试。

删除 AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI) 使用的 AWS Backup 资源

- 要删除还原测试计划，请使用 `delete-restore-testing-plan`。

删除 AWSServiceRolePolicyForBackupRestoreTesting (API) 使用的 AWS Backup 资源

- 要删除还原测试计划，请使用 `DeleteRestoreTestingPlan`。

手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRolePolicyForBackupRestoreTesting服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AWS Backup 服务相关角色的受支持区域

AWS Backup 支持在提供服务的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS Backup 支持的功能和区域。

防止跨服务混淆座席

混淆座席问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 AWS 中，跨服务模拟可能会导致混淆座席问题。一个服务（调用服务）调用另一项服务（被调用服务)时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键，以限制 AWS Backup 为其他服务提供的资源访问权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，`aws:SourceAccount` 值和 `aws:SourceArn` 值中的账户必须使用相同的账户 ID。

在使用 AWS Backup 代表您发布 Amazon SNS 主题时，`aws:SourceArn` 的值必须是 AWS Backup 保管库。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (*) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws::servicename::123456789012:*`。

中的基础设施安全 AWS Backup

作为一项托管服务 AWS Backup ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的更多信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用 AWS Backup 通过网络进行访问。客户端必须支持传输层安全性（TLS）1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

中的数据完整性 AWS Backup

AWS Backup 数据完整性目标

AWS Backup 力求在传输、存储和处理您的数据期间保持完整性。 AWS Backup 将存储的资源数据视为与内容无关的关键信息，因为无论您存储的数据类型如何，我们都为客户提供同样高级别的安全性。我们对客户的安全保持警惕，并且采取了先进的技术和物理措施来防止未经授权的访问。您可以完全控制数据的分类方式、存储数据的区域，以及如何控制、存档和保护您的数据免遭泄露。

AWS Backup 数据完整性实施

AWS Backup 与其他服务 AWS 和 Amazon 服务协同工作，以保持其存储和与之交互的数据的完整性。使用的工具可能会有所不同，这些工具可能包括（但不限于）：

- 根据校验和连续验证对象，以防止对象损坏
- 内部校验和，以确认传输中数据和静态数据的完整性
- 根据从主存储创建的备份中的数据计算的校验和
- 在磁盘损坏或检测到设备故障时，自动尝试还原正常级别的对象存储冗余
- 跨多个物理位置的冗余数据存储
- 在初始写入期间跨多个可用区增强对象持久性，并在设备不可用或检测到位损坏时进一步复制
- 对所有网络流量的校验和，以在存储或检索数据时检测数据包损坏

AWS Backup 原生存储具有高级功能的亚马逊 DynamoDB、亚马逊 EFS、Amazon S3、Amazon Timestream 以及通过备份网关连接的 VMware 运行的虚拟机的数据。 AWS Backup 便于备份存储在其他服务中的数据，包括亚马逊 Aurora、Amazon DocumentDB、亚马逊 DynamoDB、亚马逊 EBS、亚马逊 EC2、适用于 Windows 文件服务器的亚马逊 FSx、适用于 Lustre 的亚马逊 FSX、适用于 OpenZFS 的亚马逊 FSX、适用于 ONTAP 的亚马逊 FSX、Amazon Neptune Tune、亚马逊 RDS 和亚马逊 Redshi NetApp ft。

客观地确认和审计 AWS Backup 数据完整性

由其他 AWS 服务直接存储的数据 AWS Backup 以及与之 AWS Backup 交互的服务合作存储的数据均受亚马逊简单存储服务 (Amazon S3) 的严格流程的约束，这支撑了这种数据完整性。独立的第三方审计师通过年度 SOC 审计报告来确认这种完整性，该报告可通过 AWS Management Console 中的 AWS Artifact 获得。

合法封存和 AWS Backup

法定保留是一种管理工具，可帮助防止备份在保留状态下被删除。设置保留后，将无法删除处于保留状态的备份，并且会更改备份状态（例如转换为 Deleted 状态）的生命周期策略会延迟到法定保留被删除为止。备份可以包含多个法定保留。

AWS Backup 如果生命周期允许，可以将合法保全应用于由创建的一个或多个备份（也称为恢复点）。一种称为连续备份的备份类型拥有 35 天的最长生命周期。法律封存不会延长持续的备份生命周期。

创建法定保留后，它可以考虑特定筛选标准，例如资源类型和资源 ID。此外，您可以定义要包含在法定保留中的备份的创建日期范围。法定保留和备份具有多对多关系，这意味着一个备份可以拥有多个法定保留，并且一个法定保留可以包括多个备份。每个账户一次最多可以有 50 个法定保留处于活动状态。

法定保留仅适用于存放这些保留的原始备份。当跨区域或账户复制备份时（如果资源支持），该备份不会保留或随之带着其法定保留。与其他资源相同，法定保留有唯一的 Amazon 资源名称 (ARN) 与它关联。只有由创建的恢复点 AWS Backup 才能成为合法封存的一部分。

请注意，虽然 AWS Backup 保管库锁定为保管库提供额外的保护和不可变性，但法定保留可以提供防止删除单个备份（恢复点）的额外保护。法定保留不会过期，并且可以无限期地将数据保留在备份中。在拥有足够权限的用户解除保全之前，该保全将一直处于活动状态。

创建法定保留

在创建法定保留时，它仅包含已经创建的恢复点。状态为 EXPIRED 或 DELETING 的备份（恢复点）将不包含在法定保留中。状态为 CREATING 的恢复点（备份）可能不包含在法定保留中，具体取决于完成时间。

拥有所需 IAM 权限的用户可以添加合法保留。

使用 控制台创建法定保留

创建合法封存

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在控制台左侧的控制面板中，找到“我的账户”。选择 “合法保留”。
3. 选择 “添加合法保留”。
4. 显示了三个面板：合法封存详情、合法封存范围和合法封存标签。

a. 在法定保留详细信息下，在提供的文本框中输入法定保留名称和保留描述。

b. 在法定保留范围面板中，选择您希望如何选择要包含在法定保留中的资源。创建暂挂时，您可以选择用于选择处于合法保全状态的资源的方式。您可以选择包含以下选项之一：

- 特定的资源类型和 ID
- 选择备份存储库
- 您账户中的所有资源类型或所有备份存储库

c. 指定您的法定保留的日期范围。以 YYYY:MM:DD 格式输入日期（包括日期）。

d. 或者，您可以在 “合法封存” 标签下为保全添加标签。标签可以帮助对法定保留进行分类，以备将来参考和整理。您最多可以添加 50 个标签。

5. 当您对新法定保留的配置感到满意时，请单击添加新保留按钮。

使用创建合法封存 AWS CLI

您可以使用create-legal-hold命令创建合法保留。

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

查看法定保留

您可以在 AWS Backup 控制台中或以编程方式查看合法保留的详细信息。

使用控制台查看合法保留

要使用 Backup 控制台查看账户内的所有法定保留，请执行以下操作：

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在控制面板左侧的我的账户下，单击法定保留。
3. 法定保留表显示现有保留的标题、状态、描述、ID 和创建日期。单击表标题旁边的向下箭头，以按所选列对表进行筛选。

以编程方式查看法定保留

要以编程方式查看所有合法保留，您可以使用以下 API 调用：ListLegalHolds和。GetLegalHold

以下 JSON 模板可用于GetLegalHold。

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response

{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,

   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
   }
}
```

以下 JSON 模板可用于ListLegalHolds。

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
```

```
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response

{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

以下是可能的状态值。

Status	描述
CREATING	请求的恢复点正在保留过程中，由于保留尚未完成创建，因此对这些恢复点的删除请求可能会成功。
ACTIVE	法定保留已创建，此法定保留项下列出的所有恢复点均已保留。
CANCELLING	正在删除法定保留，关于删除该保留下的恢复点的请求可能会成功。
CANCELED	法定保留已完全释放，不再有任何效力。可以删除恢复点。

释放法定保留

在拥有足够权限的用户将其移除之前，合法保全将一直有效。删除法定保留也称为取消或释放法定保留。如果删除法定保留，会从将其附加到的所有备份中将其消除。在法定保留期间过期的所有备份都将在移除合法保留后的 24 小时内删除。

使用 控制台释放法定保留

使用控制台解除保留

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 输入您想要与该释放关联的描述。
3. 查看详细信息，然后单击释放保留。
4. 当出现“释放保留”对话框时，在文本框中键入 `confirm` 以确认您打算释放保留。
    - 选中复选框以确认您要取消保留。

在法定保留页面上，您可以看到您的所有保留。如果释放成功，则该保留状态将显示为 `Released`。

以编程方式解除法律保留

要以编程方式取消保留，请使用 API 调用CancelLegalHold。

使用以下 JSON 模板。

```
DELETE /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}


DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject to
 this date.
```

```
Response

Empty body

200 if successful
other standard codes
```

AWS PrivateLink

AWS PrivateLink 允许您通过创建接口 VPC 终端节点在您的虚拟私有云（“VPC”）和 AWS Backup 终端节点之间建立私有连接。接口终端节点由一项技术提供支持 AWS PrivateLink，通过限制您的 VPC 和 Amazon 网络之间的所有网络流量，使您 AWS Backup 能够私下访问 AWS Backup API。

AWS PrivateLink 使您无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接即可私密访问 AWS Backup 操作。您的 VPC 中的实例不需要公有 IP 地址即可与 AWS Backup API 终端节点通信。您的实例也不需要公有 IP 地址即可使用任何可用的 AWS Backup API 和 Backup 网关 API 操作。您的 VPC 和 VPC 之间的流量 AWS Backup 不会离开亚马逊网络。

有关 VPC 端点的更多信息，请参阅《Amazon VPC 用户指南》中的接口 VPC 端点 (AWS PrivateLink)。

Amazon VPC 端点注意事项

在为 AWS Backup 终端节点设置接口 VPC 终端节点之前，请查看 Amazon VPC 用户指南中的接口终端节点属性和限制。

与管理 Amazon Backup 资源相关的所有 AWS Backup 操作均可在您的 VPC 中使用 AWS PrivateLink。

Backup 端点支持 VPC 端点策略。默认情况下，允许通过端点对 Backup 操作进行完全访问。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

创建 AWS Backup VPC 终端节点

您可以使用亚马逊 VPC 控制台或 AWS Command Line Interface (AWS CLI) 创建 VPC 终端节点。AWS Backup 有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口端点。

AWS Backup 使用服务名称创建 VPC 终端节点`com.amazonaws.`*`region`*`.backup`。

在中国（北京）区域和中国（宁夏）区域，服务名称应为 `cn.com.amazonaws.`*`region`*`.backup`。

对于 Backup Gateway 端点，请使用 `com.amazonaws.region.backup-gateway`。

为 Backup Gateway 创建 VPC 端点时，必须允许在安全组中使用以下 TCP 端口：

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

协议	端口	方向	来源	目标位置	使用量
TCP	443（HTTPS）	出站	Backup Gateway	AWS	用于从 Backup Gateway 到 AWS 服务端点的通信

使用 VPC 端点

例如，如果您为终端节点启用私有 DNS，则可以使用该 AWS 区域 AWS Backup 的默认 DNS 名称向 VPC 终端节点发出 API 请求`backup.us-east-1.amazonaws.com`。

但是，对于中国（北京）区域和中国（宁夏）区域 AWS 区域，应分别使用`backup.cn-north-1.amazonaws.com.cn`和`backup.cn-northwest-1.amazonaws.com.cn`向 VPC 终端节点发出 API 请求。

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口端点访问服务。

创建 VPC 端点策略

您可以为 VPC 端点附加端点策略，以控制对 Amazon Backup API 的访问。该策略指定：

- 可执行操作的主体。
- 可执行的操作。

- 可对其执行操作的资源。

> **Important**
>
> 将非默认策略应用于的接口 VPC 终端节点时 AWS Backup，某些失败的 API 请求（例如失败的请求）可能不会记录到 AWS CloudTrail 或 Amazon CloudWatch。`RequestLimitExceeded`

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问权限。

示例：用于 AWS Backup 操作的 VPC 终端节点策略

以下是的终端节点策略示例 AWS Backup。当连接到终端节点时，此策略授予对所有资源上所有原则列出的 AWS Backup 操作的访问权限。

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

示例：拒绝来自指定 AWS 账户的所有访问的 VPC 端点策略

以下 VPC 终端节点策略拒绝 AWS 账户使用该终端节点访问123456789012所有资源。此策略允许来自其他账户的所有操作。

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
```

```
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

有关可用 API 响应的更多详细信息，请参阅 API 指南。

AWS Backup 目前可用性支持以下 AWS 区域的 VPC 终端节点：

- 美国东部（俄亥俄州）区域
- 美国东部（弗吉尼亚州北部）区域
- 美国西部（俄勒冈州）区域
- 美国西部（北加利福尼亚）区域
- 非洲（开普敦）区域
- 亚太地区（香港）区域
- 亚太地区（孟买）区域
- 亚太地区（大阪）区域
- 亚太地区（首尔）区域
- 亚太地区（新加坡）区域
- 亚太地区（悉尼）区域
- Asia Pacific（Tokyo）Region
- 加拿大（中部）区域
- 欧洲地区（法兰克福）区域
- 欧洲地区（爱尔兰）区域
- 欧洲地区（伦敦）区域
- 欧洲（巴黎）区域
- 欧洲地区（斯德哥尔摩）区域
- 欧洲地区（米兰）
- 中东（巴林）区域
- 南美洲（圣保罗）区域

- 亚太地区（雅加达）区域
- 亚太地区（大阪）区域
- 中国（北京）区域
- 中国（宁夏）区域
- AWS GovCloud （美国东部）
- AWS GovCloud （美国西部）

> **Note**
>
> AWS Backup for VMware 不适用于中国区域（中国（北京）区域和中国（宁夏）区域）或亚太地区（雅加达）区域。

韧性在 AWS Backup

AWS Backup 非常重视其弹性以及您的数据安全。

AWS Backup 存储您的备份时，其弹性和耐久性至少与资源的原始 AWS 服务所能提供的相同（如果您在那里进行备份）。

AWS Backup 旨在使用 AWS 全球基础架构跨多个可用区复制备份，在任何给定年份内持久性均可达到 99.999999999%（11 9），前提是您必须遵守当前文档。 AWS Backup

AWS Backup 对您的静态备份计划进行加密并持续对其进行备份。您还可以使用 AWS Identity and Access Management (IAM) 凭证和策略限制对备份计划的访问权限。有关更多信息，请参阅身份验证、访问控制和 IAM 中的安全最佳实践。

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。 AWS Backup 跨可用区存储您的备份。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。有关更多信息，请参阅 AWS Backup 服务水平协议 (SLA)。

此外， AWS Backup 您还可以跨区域复制备份，以获得更大的弹性。有关 AWS Backup 跨区域复制功能的更多信息，请参阅创建 Backup Copy。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS Backup 配额

使用时适用以下配额 AWS Backup。如果资源类型服务允许，许多 AWS Backup 配额是可以调整的。要请求调整配额，请向 AWS Support 描述您的使用案例。

AWS Backup 配额

资源	限额	注意
每个账户在每个区域的备份保管库数	300	您可以请求调整。
每个备份保管库的恢复点数量	1000000	您可以请求调整。
每个账户每个区域的备份计划数	300	您可以请求调整。
每个备份计划的版本数	2000	您可以请求调整。
每个备份计划的资源分配数	100	不可调整
每个账户的活动备份作业数	无限制	
每个账户出站到目的地区域的并发备份副本的数量	100	您可以请求调整某些资源（目前是虚拟机、高级 DynamoDB、Timestream、Amazon EFS 和 Amazon EC2 实例上的 SAP HANA 数据库）
达到上限（上述条目）后账户中每个目的地备份保管库的并发副本数	5	不可调整
可以将同一资源复制到同一目的地区域的并发跨账户副本数量	30	不可调整。

资源	限额	注意
每个资源的并发备份和复制作业数	1	不可调整。此配额可帮助您保持工作负载的性能。
每个备份的元数据标签的数量	50	您不能请求调整。 AWS 对所有资源施加此配额。请参阅《AWS 一般参考》中的标签命名限制和要求。
跨账户备份策略中每个资源选择的标签数	30	不可调整。通过使用多个资源分配或备份计划，可以添加其他标签。
管理程序的数量	10	不可调整
依法保留的数量	每个账户 50 个	不可调整
应用程序堆栈的最大嵌套备份层数	10	不可调整

AWS Backup 的亚马逊 Timestream 资源配额

资源	限额	注意
每个账户的并发 Timestream 备份作业数	4	您可以请求调整。
每个账户的并发 Timestream 还原作业数	1	您可以请求调整。

在单个备份规则中，单个资源分配存在配额。您可以通过多个备份规则创建备份计划。

AWS Backup Audit Manager 配额

资源	限额	注意
每个区域每个账户的框架数量	15	您可以请求调整。

资源	限额	注意
每个区域每个账户的控制数量	50	您可以请求调整。
每个账户的报告计划数量	20	您可以请求调整。
每个报告计划的框架的数量	1000	不可调整
报告计划中账户的最大数量乘以区域	300	不可调整

还原测试计划配额

资源	限额	注意
还原测试计划	100	不可调整
每个计划中的标签数	50	不可调整
每个计划的选项	30	不可调整
每个还原测试选择的 ARN	30	不可调整
每个选项的条件	30	包括 `StringEquals` 和 `StringNotEquals` 中包含的内容。
每个还原测试选择的保管库选择器	30	不可调整
选择时段的最大值（以天为单位）	365 天	
开始时段的小时数界限	最短：1 小时；最长：168 小时	
还原测试计划名称的最大字符长度	50 个字符	字母数字和下划线，没有空格

资源	限额	注意
还原测试选择名称的最大字符长度	50 个字符	字母数字和下划线，没有空格

AWS Backup gateway 配额

资源	限额	注意
每个网关的备份或还原作业数	4	您无法请求调整。相反，可以创建更多网关并将其连接到您的管理程序。

使用管理多个账户的备份时 AWS Organizations，可能会遇到 AWS Organizations 强制性的配额。有关这些配额，请参阅《AWS Organizations 用户指南》中的 AWS Organizations配额。

您可能还会遇到由 AWS Backup支持的服务施加的配额，包括：

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- 适用于 Lustre 的 Amazon FSx
- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

监控

AWS Backup 与其他 AWS 工具配合使用，使您能够监控其工作负载。这些工具包括：

- AWS Backup 控制台仪表板
  - 作业控制面板提供作业运行状况监控功能，您可以在其中查看那些显示作业成功和失败情况的指标（按原因、账户、区域和资源类型筛选）。
  - 作业控制面板可在支持 Audit M AWS Backup anager 的地区使用。有关这些区域，请参阅功能可用性来自 AWS 区域。所有其他区域都将能够访问 CloudWatch 仪表板。
- 亚马逊 CloudWatch和亚马逊 EventBridge将监控 AWS Backup 流程。
  - 您可以使用 CloudWatch 跟踪指标、创建警报和查看仪表板。
  - 您可以使用 EventBridge 来查看和监视 AWS Backup 事件。

  有关更多信息，请参阅使用 Amazon 监控 AWS Backup 事件 EventBridge。
- AWS CloudTrail监控 AWS Backup API 调用。您可以识别发出这些调用的时间、源 IP、用户和账户。有关更多信息，请参阅 使用记录 AWS Backup API 调用 CloudTrail。
- 亚马逊简单通知服务 (Amazon SNS)，用于订阅 AWS Backup相关主题，例如备份、还原和复制事件。有关更多信息，请参阅 带有的通知选项 AWS Backup。

AWS Backup 控制台仪表板

> **Note**
>
> 所有支持 Audit Manager 的 AWS Backup 区域均提供作业控制面板。有关这些区域，请参阅功能可用性来自 AWS 区域。所有其他区域都将能够访问 CloudWatch 仪表板。

主题

备份控制面板概述

AWS Backup 在控制台中提供了作业控制面板，可帮助您监控备份、复制和还原作业的运行状况。通过命令行可以检索控制台中直观显示的相同数据 AWS CLI。

使用作业控制面板可通过组织级别或成员账户监控来识别备份、复制和还原作业的问题。借助这些信息，您可以识别和诊断事件和可能的问题，以帮助确保活动的真实性。

作业控制面板可以显示两个时间范围的数据。默认情况下，会显示最近 14 天的数据，但您可以更改视图以显示最近 7 天的数据。如果您更改时间范围，数据将更新以反映新时间间隔中的情况。

请注意，控制面板会显示上个 0:00（世界标准时间）之前的数据；也就是说，不包括当天的数据。控制面板每天大约在世界标准时间 1:30-2:30 更新。

查看作业控制面板

要查看作业仪表板，请登录 AWS Backup 控制台并在左侧导航栏中选择作业仪表板。

在作业控制面板页面上，您可以从备份、复制或还原作业选项卡中进行选择。

作业控制面板概述显示指定时间范围内作业活动的汇总视图，包括已完成、已完成但存在问题、已过期和失败的作业。默认情况下，显示最近 14 天的数据，但您可以将视图更改为显示 7 天的数据。

> **Note**
>
> `Completed with issues` 是控制台中显示的作业的状态，表示已完成的作业，并带有状态消息。

作业运行状况

折线图显示一段时间内的成功和失败作业率线。成功率线显示已完成以及已完成但存在问题的作业的汇总。失败率线根据指定的时间范围显示失败和已过期作业的总和。

处于未完成或非失败状态的作业（状态为已创建、待处理、正在运行、已中止、正在中止或部分的作业）未包括在内；百分比总数可能不等于 100%。

一段时间内的作业状态

使用条形图，您可以生成自定义条形图，显示每个类别（已完成、已完成但存在问题、失败和已过期）中的作业数（按天数分布）。

在下拉菜单中，选择要在图表中看到的状态、资源类型和 AWS 区域。如果您想进一步浏览您的选项，请选择查看作业以查看作业/跨账户监控页面中预先筛选出的部分。

您可以将鼠标悬停在条形上方以显示弹出窗口，其中显示所选日期的详细作业数据。

有问题的作业

有问题的作业是指状态为“失败”、“已过期”或“已完成但存在问题”的作业。每个图表都显示相应的指标，其中包含账户、资源类型或所含有问题作业数量最多的主要原因。

默认显示屏按指定指标降序对控制面板小部件进行排序，首先列出属于该指标的有问题作业数量最多的指标。

只有具有通过 Organizations 进行访问的权限的账户（例如，管理账户和委派管理员账户）中才会显示有问题的主要账户。如果显示，您可以将鼠标悬停在账户上方以显示属于所选账户的有问题作业的数量。

您可以在图表中选择一个条形来打开弹出窗口。在此窗口中，您可以选择作业状态以打开按所选状态筛选的作业/跨账户监控表。

作业问题原因

主要问题原因小部件显示错误消息所属的消息代码类别。但是，该类别可能无法解释作业遇到的问题。展开下面的消息代码类别，查看有关您的作业可能遇到的特定消息或错误的更多详细信息。

“VSS_ERROR”

- “Windows VSS 备份尝试失败，因为实例或 SSM 代理的状态无效或权限不足。”
- “由于权限不足，无法执行此操作，Windows VSS 备份尝试失败”
- “Windows VSS 备份尝试失败，因为实例中未安装 ec2-vss-agent.exe”
- “尝试定期备份时遇到 Windows VSS 备份作业错误”
- “由于启用 VSS 的快照创建操作超时，Windows VSS 备份尝试失败”
- “由于 Windows Server 版本不受支持，Windows VSS 备份尝试失败。支持的版本为 Windows Server 2012 或更高版本。”
- “由于启用 VSS 的快照创建操作超时，Windows VSS 备份尝试失败”

“LIMIT_EXCEEDED”

- “已超过订阅者限制：您已达到最大并发备份数，即 300。等待其他作业完成，然后重试。您也可以联系 AWS Support 以申请增加配额。”
- “已超过单个卷允许的最大处理中快照数。”
- “已超过允许的最大活动快照限制。”
- “无法创建 20 个以上的用户快照”
- “生成的标签集所含用户标签数不能超过 50 个。”
- “您的账户/数据库已达到支持的最大备份数。有关更多信息，请参阅 Timestream 开发人员指南中的配额。”
- “您已达到该区域允许的公共和私有镜像数量配额，即 50,000 个。取消注册未使用的镜像，或者请求增加您的 AMI 配额。”
- “您的备份成功了，但是由于 NetworkInterfaces 元数据的大小超出了我们的内部限制，我们无法保留元数据。”
- “REGEX# 已超出订阅限制”
- “REGEX# 指定的标签超过了 50 个”
- “REGEX# 最多有”

“ACCESS_DENIED”

- “您无权执行此操作。”
- “尝试呼叫 AWS Backup 服务时访问被拒绝”
- “ AWS Marketplace 无法将来自的图像复制到其他 AWS 帐户。”
- “复制作业失败，因为使用默认的备份务托管密钥为目标备份保管库加了密。无法复制此保管库的内容。只能复制通过 AWS KMS 密钥加密的 Backup 保管库中的内容。
- 使用加密的快照 AWS 托管式密钥 无法共享。指定另一个快照。
- “无法共享使用 Amazon EBS 默认密钥加密的快照
- “复制作业失败。源和目标账户必须均是同一组织的成员。”
- “REGEX# 拒绝访问”
- “REGEX# 无权”
- “REGEX #cannot 假设为 AWS Backup
- “REGEX# 没有权限”
- “REGEX# 缺少权限”

“CONCURRENT_JOB”

- “备份作业失败，因为同一资源有正在运行的作业。”

“FEATURE_NOT_ENABLED”

- “复制作业失败。当前组织未启用跨账户复制功能。”

“JOB_EXPIRED”

- “备份作业在完成之前就已过期。”

“INVALID_LIFECYCLE”

- “复制作业失败。作业中指定的保留期不在为目标备份保管库指定的范围内。”
- “REGEX# 无法启动，因为它要么在所配置的每周维护时段之内，要么离该时段太近”
- “REGEX# 无法启动，因为它要么在所配置的自动备份时段之内，要么离该时段太近”

“INVALID_STATE”

- “REGEX# 实例未处于状态”
- “REGEX# 未处于可用状态”
- “REGEX# 未处于可用状态”
- “REGEX# 无法为卷创建快照”

“KMS_KEY_ERROR”

- “KMS 密钥已禁用或待删除，或者对 KMS 密钥的访问被拒绝”
- “无法访问给定密钥 ID”
- “AMI 快照复制失败，错误为：无法访问给定的密钥 ID。您必须拥有默认 CMK 的 DescribeKey 权限”
- “REGEX# kms 密钥”

“ACCESS_KEY_ERROR”

- “ AWS 访问密钥 ID 需要订阅服务”

“HYPERVISOR_OFFLINE”

- “此操作对指定的管理程序无效，因为它不在线”

“RESOURCE_NOT_FOUND”

- “找不到指定的卷。”
- “找不到虚拟机。”
- “给定密钥 ID 不存在”
- “REGEX# 不存在”
- “REGEX# 找不到资源”
- “REGEX# 找不到 cryopod”
- “REGEX# 找不到恢复点”
- “REGEX# 找不到资源”
- “REGEX# 不再可用”
- “REGEX# 无效”

“RESOURCE_NOT_SUPPORTED”

- “REGEX# 资源类型不受支持”
- “REGEX# 资源类型不受支持”

“TAG_COPY_ERROR”

- “由于内部故障，我们无法将资源标签复制到您的备份中。”
- “由于源或目标恢复点不可用，我们无法将资源标签复制到您的备份中”

“TOKEN_EXPIRED”

- “令牌已过期。请重试。”

“UNSUPPORTED_OPERATION”

- “创建快照期间，虚拟机管理程序不支持该CreateSnapshot 方法。备份作业已中止”

- “UnsupportedOperation : Storage Gateway 备份副本需要用户创建的备份保管库和目标位置的 CMK。”
- “REGEX# 功能不受所提供的资源类型支持。”

“FATAL_ERROR”

- “出现内部错误。”
- “复制作业遇到了致命错误。请联系 S AWS upport 寻求进一步帮助。”
- “复制作业遇到了致命错误。”
- “REGEX# 备份作业遇到了致命错误”

通过获取仪表板数据 AWS CLI

您可以使用命令行检索控制台中显示的相同数据。使用以下 CLI 命令之一：

- list-backup-job-summaries
- list-copy-job-summaries
- list-restore-job-summaries

您可以在每条命令中包含有效的参数：

```
BackupJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
```

```
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

此示例显示了一个请求示例，其中用户输入了 `list-backup-job-summaries`，请求需要返回过去 14 天内状态为 `FAILED` 的所有可用账户：

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

要获取状态为 `completed with issues` 的作业的作业计数，请从 `COMPLETED` 总数中减去 `MessageCategory` 为 `SUCCESS` 的 `COMPLETED` 作业的作业计数。

使用 Amazon 监控 AWS Backup 事件 EventBridge

AWS Backup 当备份或复印任务的状态发生变化 EventBridge 时，向 Amazon 发送事件。您可以使用 EventBridge 来监视 AWS Backup 事件。例如，当备份任务失败时，您可以收到警报。 AWS Backup 每 5 分钟以最大努力 EventBridge 的方式将事件发送到一次。

要使用跟踪事件 EventBridge，请参阅以下内容：

- 创建对事件做出反应的规则（Amazon EventBridge 用户指南）
- 的亚马逊 CloudWatch 事件和指标 AWS Backup（博客——参见配置要发送到亚马逊 AWS Backup 的事件 EventBridge）

有些事件会报告 `status: COMPLETED`，而另一些事件会报告 `state: COMPLETED`。这与 AWS Backup API 一致。有些状态是 AWS Backup 控制台所特有的：状态`Completed with issues`状态表示带有状态消息的`Completed`作业。要监控 `Completed with issues` 事件，请监控带有状态消息的 `COMPLETED` 作业。

您也可以使用 AWS Backup 通知 API 通过亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 跟踪 AWS Backup 事件。但是，EventBridge 跟踪的更改多于通知 API 的更改，包括对备份库的更改、复印任务状态、区域设置以及冷恢复点或温恢复点的数量。

事件

Backup Job 事件

以下是示例事件。

状态

状态：失败


```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
```

```
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-
west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.
\"",
    "startBy": "2020-07-30T04:13:07.392Z",
    "percentDone": 0,
    "retryCount": 3
  }
}
```

状态：已完成

```
{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-
b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
```

```
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
```

状态：正在运行

```
{
  "version": "0",
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
```

```
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```

状态：已中止

```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "ABORTED",
    "statusMessage": "\"Backup job was stopped by user.\"",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
  }
}
```

状态：已过期

```
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
```

```
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
 resource.\"",
    "completionDate": "2020-07-29T13:02:15.234Z",
    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```

状态：待定

```
{
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
```

```
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}
```


状态：已创建


```
{
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```


Backup Plan 活动

以下是示例事件。

状态

- 状态：已修改
- 状态：已删除
- 状态：已创建

状态：已修改

```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

状态：已删除

```
{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
```

```
}
```

状态：已创建

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```

Backup 保管库事件

以下是示例事件。

状态

- 状态：已创建
- 状态：已修改
- 状态：已删除

状态：已创建

```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
```

```
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

状态：已修改

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

状态：已删除

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
```

```
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-
b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```

Copy Job 事件

以下是示例事件。

状态

- 状态：失败
- 状态：正在运行
- 状态：已完成
- 状态：已创建

状态：失败

```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
```

```
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```

状态：正在运行

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
```

```
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

状态：已完成

```
{
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/
snap-0726fe70935586180",
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

状态：已创建

```
{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
  }
}
```

恢复点事件

以下是示例事件。

状态

- 状态：已完成
- 状态：已删除
- 状态：已修改

状态：已完成

```
{
    "version": "0",
    "id": "ab32977c-378d-2122-e985-fgh4596f0709",
    "detail-type": "Recovery Point State Change",
    "source": "aws.backup",
    "account": "1112233445566",
```

```
    "time": "2020-07-15T21:39:07Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
    ],
    "detail": {
        "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "creationDate": "2020-07-15T21:38:31.152Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
        "resourceType": "Aurora",
        "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
        "status": "COMPLETED",
        "isEncrypted": "false",
        "storageClass": "WARM",
        "completionDate": "2020-07-15T21:39:05.689Z",
        "createdBy": {
            "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
            "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
        },
        "lifecycle": {
            "deleteAfterDays": 100
        },
        "calculatedLifeCycle": {
            "deleteAt": "2020-10-23T21:38:31.152Z"
        }
    }
}
```

状态：已删除

```
{
  "version": "0",
  "id": "6089ee76-d856-0d7c-cee7-0a431cd43343",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T22:38:49Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:157f892e-
fe46-48da-9dbe-4154f91f8acc",
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-c1a6d40a-32d1-4d54-
bd70-bced933ef107"
  ],
  "detail": {
    "state": "DELETED",
    "lifecycle": {
      "deleteAfterDays": 300
    },
    "calculatedLifeCycle": {
      "deletedAt": "2021-05-25T22:29:02.452Z"
    }
  }
}
```

状态：已修改

```
{
  "version": "0",
  "id": "14365bb1-adef-bc00-1ee3-8fac188d7996",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-02T23:33:57Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:helo12312",
    "arn:aws:dynamodb:us-west-2:1112233445566:table/test/
backup/01593730512469-033578ce"
  ],
  "detail": {
    "calculatedLifeCycle": {
      "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
    },
    "state": "MODIFIED"
  }
}
```

区域设置事件

以下是示例事件。

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbafcfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
}
```

恢复 Job 事件

以下是示例事件。

状态

- 状态：失败
- 状态：正在运行
- 状态：已完成
- 状态：待定
- 状态：已创建

状态：失败

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
```

```
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
 EC2 instance. Please restore using the backed up instance profile."
  }
}
```

状态：正在运行

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "createdBy": [
```

```
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

状态：已完成

```
{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Restore Job State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2020-07-15T03:14:58Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:rds:us-
west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail":{
    "restoreJobId":"AB123456-78C9-0123-456D-789012E34567",
    "backupSizeInBytes":"0",
    "creationDate":"2020-07-15T03:10:01.742Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn":"arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone":0,
    "resourceType":"RDS",
    "status":"COMPLETED",
    "createdResourceArn":"arn:aws:rds:us-
west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate":"2020-07-15T03:14:53.128Z"
  }
}
```

状态：待定

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-
b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}
```

状态：已创建

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-
efgh939ij32k"
  ],
```

```
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "creationDate": "2020-06-22T18:50:46.407Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "state": "CREATED"
  }
}
```

AWS Backup 亚马逊的指标 CloudWatch

主题

- CloudWatch 仪表板
- 指标与 CloudWatch

CloudWatch 仪表板

> **Note**
>
> 控制台控制面板因访问控制台的区域而异。如需查看哪些区域有权访问作业控制面板，请参阅功能可用性来自 AWS 区域。未列出的地区将能够访问 CloudWatch控制面板。

您的 AWS Backup 控制台包括一个仪表板，用于查看已完成或失败的备份、复制和还原任务的指标。在此控制面板中，您可以按时间段查看作业状态，并根据所需的时间范围进行自定义。

访问控制面板

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在左侧导航窗格中，选择控制面板。

查看和理解控制面板

CloudWatch 仪表板显示多个小部件。每个小部件按计数显示作业指标。每个小部件显示多个折线图。每行对应一个受保护的资源（如果您没有看到显示的预期资源，请确保在设置中启用了该资源）。显示屏不显示正在进行的作业。

y 轴（垂直值）显示计数。x 轴（水平值）显示时间点。如果在所选作业状态下没有可视化的数据点，该值将设置为 0，x 轴上有一条水平线。显示资源的图例仍然可见。

这些指标显示与当前登录相关的账户特定和区域特定信息。要查看其他账户或区域，您必须使用所选账户登录。

自定义控制面板

默认情况下，显示的时间范围为一周。顶部菜单会显示多个用于重新定义所显示时间范围的选项。您可以从 1 小时、3 小时、12 小时、1 天、3 天和 1 周中进行选择。此外，您可以选择自定义来指定不同的值。自定义会暂时将当前视图更改为您的规格。

您可以将鼠标指针悬停在小部件上，该小部件的右上角会显示放大按钮。单击放大，以全屏视图打开小部件。在全屏模式下，会显示更多用于自定义图表显示的选项，例如更改时段（每个数据点之间的时间）。关闭全屏视图后，任何更改都不会保留。

要一次仅查看一种资源类型，请在图表图例中单击要查看的资源类型的标签文本。这将取消选择其他所有资源类型。要反向执行该操作，请单击图例中的资源类型颜色框。要返回所有资源类型的默认视图，并选中所有标签，请再次单击所选任何资源类型的标签文本。

单击小部件右上角的三个垂直圆点会打开一个下拉菜单，其中包含用于刷新、放大、在指标中查看和在日志中查看的选项。“在指标中查看” 会在 CloudWatch 控制台中打开控件中使用的指标。您可以在此处对控件进行任何更改，然后将该小组件添加到仪表板中的自定义仪表 CloudWatch 板中。您在 CloudWatch 控制面板中所做的任何更改都不会反映在 AWS Backup 控制台的控制面板上。“以日志形式查看” 将在 CloudWatch 控制台中打开日志查看页面。

要将显示的微件添加到您自己的自定义 CloudWatch 仪表板，请单击仪表板右上角的 “添加到控制面板” 按钮。这将打开 CloudWatch 控制台，您可以在其中选择在哪个自定义仪表板中添加所有六个小部件。

有关更多信息，请参阅使用 Amazon CloudWatch 指标。

指标与 CloudWatch

您可以使用 CloudWatch 来监控 AWS Backup 指标。`AWS/Backup`命名空间允许您跟踪以下指标。AWS Backup CloudWatch 每隔 5 分钟发布一次更新的指标。

本文档页面的目的是为您提供用于监控 CloudWatch 的参考资料 AWS Backup。要了解如何使用监控指标 CloudWatch，请参阅博客 Amazon Ev CloudWatch en ts and Metrics for “CloudWatch 用户指南” AWS Backup或 “关注单一 AWS 服务中的指标和警报”。要设置警报，请参阅CloudWatch 用户指南中的使用 Amazon CloudWatch 警报。

类别	指标	示例维度	使用案例示例
作业	每种状态下的备份、还原和复制作业数量，包括 CREATED、PENDING、F 、FAILED 和 EXPIRED。 不同的作业类型有不同的可用状态。	资源类型、保管库名称。 复制作业的保管库名称就是其目的地保管库的名称。	监控一个或多个特定备份保管库中失败的备份作业数量。如果在 1 小时内有超过五个失败的作业，请使用 Amazon SNS 发送电子邮件或短信，或者向工程团队提交工单进行调查。 报告标准：有非零值
恢复点	每个状态下的热恢复点和冷恢复点数量：MODIFIED、COMPLETE 、PARTIAL、EXPIREI	资源类型、保管库名称。	跟踪您的 Amazon EBS 卷中已删除的恢复点数量，并分别跟踪每个备份保管库中的热恢复点和冷恢复点的数量。 报告标准：有非零值

> **Note**
>
> 的任务状态`Completed with issues`仅限于 AWS Backup 控制台；无法通过进行跟踪 CloudWatch。

下表列出了您可使用的所有指标。

指标	描述
`NumberOfBackupJobsCreated`	AWS Backup 创建的备份任务数量。
`NumberOfBackupJobsPending`	即将在 AWS Backup中运行的备份作业数量。

指标	描述
NumberOfBackupJobsRunning	当前正在运行的备份任务数量 AWS Backup。
NumberOfBackupJobsAborted	用户取消的备份作业数量。
NumberOfBackupJobsCompleted	已 AWS Backup 完成的备份任务数。
NumberOfBackupJobsFailed	状态为 Failed 的备份作业数量。通常是由于将备份任务安排在数据库资源之前或之前 1 小时，或者在 Amazon FSx 维护时段或自动备份窗口之前或期间 4 小时内安排备份作业，并且不使用执行连续备份 AWS Backup 以进行恢复。 point-in-time 有关支持的服务列表以及如何使用 AWS Backup 进行连续备份或重新安排备份作业的说明，请参阅 Po int-in-Reco very。
NumberOfBackupJobsExpired	状态为的备份任务数量EXPIRED。 EXPIRED如果无法在开始窗口时间内开始备份，则备份任务的状态CREATED将从状态更改为。
NumberOfCopyJobsCreated	AWS Backup 创建的跨账户和跨区域复制作业的数量。
NumberOfCopyJobsRunning	当前正在 AWS Backup中运行的跨账户和跨区域复制作业的数量。
NumberOfCopyJobsCompleted	AWS Backup 完成的跨账户和跨区域复制作业的数量。
NumberOfCopyJobsFailed	AWS Backup 尝试但无法完成的跨账户和跨区域复印任务的数量。
NumberOfRestoreJobsPending	即将在 AWS Backup中运行的还原作业数量。
NumberOfRestoreJobsRunning	当前正在运行的还原任务数量 AWS Backup。
NumberOfRestoreJobsCompleted	已 AWS Backup 完成的还原任务数。

指标	描述
NumberOfRestoreJobsFailed	已 AWS Backup 尝试但无法完成的恢复任务数。
NumberOfRecoveryPointsCompleted	AWS Backup 创建的恢复点数量。
NumberOfRecoveryPointsPartial	已 AWS Backup 开始创建但无法完成的恢复点的数量。 AWS 稍后会重试该过程，但由于重试是在稍后进行的，因此它会保留部分恢复点。
NumberOfRecoveryPointsExpired	根据您的备份保留生命周期 AWS Backup 尝试删除但无法删除的恢复点数量。您需要为过期备份消耗的存储空间付费，您应该手动将其删除。
NumberOfRecoveryPointsDeleting	AWS Backup 正在删除的恢复点数量。
NumberOfRecoveryPointsCold	AWS Backup 分层到冷存储的恢复点数量。

除了表格中列出的维度之外，还有更多可用维度。要查看指标的所有维度，请在 CloudWatch 控制台的“指标” 部分的**AWS/Backup**命名空间中键入该指标的名称。

使用记录 AWS Backup API 调用 CloudTrail

AWS Backup 与AWS CloudTrail提供用户、角色或服务所执行操作记录的 AWS 服务 服务集成。CloudTrail 将所有 API 调用捕获 AWS Backup 为事件。捕获的调用包括来自 AWS Backup 控制台的调用和对 AWS Backup API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 AWS Backup、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

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。
- 请求是否代表 IAM Identity Center 用户发出。
- 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。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS Management Console 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许您对事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 AWS CloudTrail Lake”。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

AWS Backup 中的事件 CloudTrail

AWS Backup 在执行备份、恢复、复制或通知时生成这些 CloudTrail 事件。这些事件不一定是通过使用 AWS Backup 公共 API 生成的。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的AWS 服务 事件。

- `BackupDeleted`
- `BackupJobCompleted`

- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- ReportJobCompleted
- ReportJobStarted
- RestoreCompleted
- RestoreStarted
- PutBackupVaultNotifications

了解 AWS Backup 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 Amazon 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。

以下示例显示了一个演示StartBackupJob、StartRestoreJob、和DeleteRecoveryPoint操作以及BackupJobCompleted事件的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
```

```
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
```

```
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
```

```
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
```

```
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```

记录跨账户管理事件

使用 AWS Backup，您可以管理AWS Organizations结构 AWS 账户 内所有内容的备份。 AWS Backup 当您创建、更新或删除 AWS Organizations 备份策略（将备份计划应用于您的成员帐户）或存在无效的组织备份计划时，会生成以下 CloudTrail 事件：

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

示例：用于跨账户管理的 AWS Backup 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 Amazon 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。

以下示例显示了演示该`CreateOrganizationalBackupPlan`操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
```

```
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
        "creationDate": {
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```


以下示例显示了演示该DeleteOrganizationalBackupPlan操作的 CloudTrail 日志条目。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
```

```
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

以下示例显示了一个演示该事件的 CloudTrail 日志条目`InvalidOrganizationBackupPlan`，该条目是在 AWS Backup 收到来自 Organizations 的无效备份计划时发送的。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
```

```
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
                    "enableContinuousBackup": true
                }
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
```

```
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    },
    "eventCategory": "Management"
}
```

带有的通知选项 AWS Backup

有两种方法可以接收有关 AWS Backup以下内容的通知：

- AWS 用户通知可以发送通知，包括 Amazon CloudWatch 警报和其他服务的通知。 AWS Support
- Amazon 简单通知服务可以将 AWS Backup 事件通知您。

AWS 用户通知和 AWS Backup

AWS Backup 支持从 “AWS 用户通知” 控制台管理您的备份通知。通过 AWS 用户通知，您可以从 User Notifications Notification Center 查看备份、复制和还原作业的进度，以及对备份策略、保管库、恢复点和设置的更改。

您可以通过控制台管理其他类型的通知，包括亚马逊、亚马逊 EventBridge 警报和 AWS Support 案例更新。 CloudWatch此外，您还可以设置多个配送选项，包括电子邮件、 AWS Chatbot 通知和 AWS Console Mobile Application 推送通知。

亚马逊 SNS 和活动 AWS Backup

AWS Backup 利用了亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 提供的强大通知。您可以将 Amazon SNS 配置为通过亚马逊 SNS 控制台向您通知 AWS Backup 事件。

限制

- 虽然 Amazon SNS 服务允许跨账户通知， AWS Backup 但目前不支持此功能。您必须指定自己的 AWS 账户 ID 和主题的资源 ARN。
- AWS Backup 支持 SNS 尽力删除重复数据的标准主题，但目前 AWS Backup 不支持用于严格重复数据删除的 SNS FIFO 主题。

常见使用案例

- 按照如何获取失败任务的通知？中的步骤设置失败的备份 AWS Backup 任务的通知 来自 AWS 高级支持。
- 在下方的事件示例表格中，查看已完成、失败和已过期的备份作业的示例 Amazon SNS 通知 JSON。

有关一般 Amazon SNS 的更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的 Amazon SNS 使用入门。

AWS Backup 通知 API

使用 Amazon SNS 控制台或 AWS Command Line Interface (AWS CLI) 创建主题后，您可以使用以下 AWS Backup API 操作来管理备份通知。

- DeleteBackupVaultNotifications - 删除有关指定备份保管库的事件通知。
- GetBackupVaultNotifications - 列出指定的备份保管库的所有事件通知。
- PutBackupVaultNotifications - 打开指定主题和事件的通知。

AWS Backup 支持以下事件：

作业类型	事件
备份作业	BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | CONTINUOUS_BACKUP_INTERRUPTED
复制作业	COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED
还原作业	RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED
恢复点	RECOVERY_POINT_MODIFIED

AWS Backup for S3 支持另外两个事件：

- S3_BACKUP_OBJECT_FAILED 会通知您在备份作业期间 AWS Backup 未能备份的任何 S3 对象。
- S3_RESTORE_OBJECT_FAILED 会通知您在还原作业期间 AWS Backup 未能还原的任何 S3 对象。

事件示例

Example 示例：Backup 任务已完成

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job was completed successfully. Recovery point
 ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"COMPLETED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example 示例：Backup 任务失败

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
```

```
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"FAILED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example 示例：备份任务无法在备份窗口内完成

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes" : {
              "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
              "State" : {"Type":"String","Value":"EXPIRED"},
              "AccountId" : {"Type":"String","Value":"123456789012"},
              "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
```

```
              "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

AWS Backup 通知命令示例

您可以使用 AWS CLI 命令订阅、列出和删除与您的 AWS Backup 活动有关的 Amazon SNS 通知。

放置备份保管库通知示例

以下命令订阅指定备份保管库的 Amazon SNS 主题，该主题将在启动或完成还原作业时或修改恢复点时通知您。

```
aws backup put-backup-vault-notifications
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

获取备份保管库通知示例

以下命令列出了当前订阅指定备份保管库的 Amazon SNS 主题的所有事件。

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

示例输出如下所示：

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

删除备份保管库通知示例

以下命令取消订阅指定备份保管库的 Amazon SNS 主题。

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

指定 AWS Backup 为服务主体

> **Note**
>
> AWS Backup 要允许代表您发布 SNS 主题，您必须指定 AWS Backup 为服务委托人。

在用于跟踪 AWS Backup 事件的 Amazon SNS 主题的访问策略中加入以下 JSON。您必须指定主题的资源 Amazon 资源名称 (ARN)。

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

有关在 Amazon SNS 访问策略中指定服务主体的更多信息，请参阅《亚马逊简单通知服务开发者指南》中的 “允许任何 AWS 资源向主题发布”。

> **Note**
>
> 如果您的主题已加密，则必须在策略中包含其他权限才能 AWS Backup 向其发布内容。有关启用服务发布到加密主题的更多信息，请参阅《Amazon 简单通知服务开发者指南》中的 “启用来自 AWS 服务的事件源和加密主题之间的兼容性”。

故障排除 AWS Backup

使用时 AWS Backup，可能会遇到问题。以下部分可帮助您解决可能出现的一些常见问题。

有关的一般问题 AWS Backup，请参阅AWS Backup 常见问题解答。您还可以在 AWS Backup 论坛上搜索答案和发布问题。

主题

排查一般问题

备份和恢复资源时，您必须拥有要保护的资源的使用权限 AWS Backup 和访问权限。获得适当权限的最简单方法是在将资源分配给备份计划时选择默认角色。有关使用 AWS Identity and Access Management (IAM) 与进行访问控制的更多信息 AWS Backup，请参阅访问控制。

如果您在尝试访问某个 AWS Backup 资源（例如备份存储库）时`AccessDenied`遇到错误，则可能是该资源不存在，或者您没有访问该资源的权限。

如果在备份和还原特定资源类型时遇到问题，查看该资源的备份和还原故障排除主题会很有帮助。有关更多信息，请参阅 “AWS Backup 如何使用支持的 AWS 服务” 下的链接。

如果创建或删除资源 AWS Backup 失败，则可以通过查看错误消息或日志 AWS CloudTrail 来了解有关问题的更多信息。有关 CloudTrail与一起使用的更多信息 AWS Backup，请参阅使用记录 AWS Backup API 调用 CloudTrail。

创建资源故障排除

以下信息可帮助您排查创建备份问题。

- 通常，AWS 数据库服务在其维护时段或自动备份时段之前 1 小时或期间无法启动备份。Amazon FSx 在维护时段或自动备份时段之前 4 小时或期间无法启动备份（Amazon Aurora 不受此维护时段限制的约束）。在这段时间内安排的快照备份将失败。一个例外：当您选择 AWS Backup 为支持

的服务同时使用快照和连续备份时，您无需再担心这些窗口，因为 AWS Backup 会为您安排这些窗口。有关支持的服务列表以及如何使用 AWS Backup 进行连续备份的说明，请参阅时间点恢复。

- 正在创建 DynamoDB 表时，为这些表创建备份将失败。创建 DynamoDB 表通常需要几分钟。
- 当 Amazon EFS 文件系统非常大时，备份这些文件系统最多可能需要 7 天时间。一次只能对 Amazon EFS 文件系统的一个并发备份进行排队。如果后续备份在前一个备份仍在进行时排队，则备份窗口可能会过期，并且不会创建备份。
- Amazon EBS 的软配额为 AWS 区域 每个账户 100,000 个备份，当达到该配额时，其他备份将失败。如果达到此配额，您可以删除多余备份或请求增加配额。有关请求增加配额的更多信息，请参阅 AWS 服务限额。
- 创建 Amazon Relational Database Service (RDS) 备份时，请考虑以下几点：
  - 如果您不使用 AWS Backup 同时管理 Amazon RDS 快照和带 point-in-time 恢复功能的连续备份，则如果在用户可配置的 30 分钟每日备份窗口内按需启动备份或按需进行备份，则备份将失败。有关自动 Amazon RDS 备份的更多信息，请参阅《Amazon RDS 用户指南》中的 Working With Backups。您可以使用管理 Amazon RDS 快照和带 point-in-time 恢复功能的连续备份，AWS Backup 从而避免这种限制。
  - 如果从 Amazon RDS 控制台启动备份作业，则可能会与 Aurora 集群的备份作业发生冲突，从而导致错误 `Backup job expired before completion.`。如果发生这种情况，请在 AWS Backup中配置更长的备份时段。
  - AWS Backup 创建拷贝作业时，当前不会传递 TDE 选项组。如果您打算使用此选项组创建复制作业，则必须使用 Amazon RDS 控制台或 Amazon RDS API 而不是 AWS Backup 工具。有关更多信息，请参阅《Amazon Relational Database Service 用户指南》中的复制选项组。
  - 错误：按需备份完成，但计划备份失败，并显示错误“源快照 KMS 密钥不存在、未启用或您无权访问它”。按需作业之所以完成，是因为它使用的是 API 调用 `CopyDBSnapshot`，不需要 KMS 访问权限。

    补救措施：将 IAM 角色添加到您的 KMS 密钥。可以通过在您的 KMS 密钥策略中允许该角色来完成。

    要编辑策略，请执行以下操作：

    1. 打开 KMS 控制台。
    2. 在左侧导航栏中，选择客户托管密钥。
    3. 单击要编辑的客户托管密钥。
    4. 在密钥策略下，单击切换到策略视图。
    5. 单击编辑。

6. 添加角色。

删除资源故障排除

AWS Backup 无法在受保护资源的控制台窗口中删除由创建的恢复点。您可以在 AWS Backup 控制台上将其删除，方法是在存储它们的保管库中选择它们，然后选择删除。

要删除恢复点或备份保管库，您需要相应的权限。有关使用 IAM 和进行访问控制的更多信息 AWS Backup，请参阅访问控制。

还原资源故障排除

使用 API 进行还原

要以编程方式还原备份，请使用 StartRestoreJob API 操作。

要获取创建备份时使用的配置元数据，可以调用 GetRecoveryPointRestoreMetadata。

有关更多信息，请参阅还原备份。

使用控制台进行还原

- 还原 Amazon S3 数据
- 还原虚拟机
- 还原 Amazon FSx 文件系统
- 还原 Amazon EBS 卷
- 还原 Amazon EFS 文件系统
- 还原Amazon DynamoDB 表
- 还原 Amazon RDS 数据库
- 还原 Aurora 集群
- 还原 Amazon EC2 实例
- 还原 Storage Gateway 卷
- 还原 Amazon DocumentDB 集群
- 还原 Neptune 集群

格式化错误疑难解答

当参数中的值包含通配符 (*) 时，通配符会被处理为包括空格以外的值。包含空格的键值对中的值将不会包含在通配符中。

AWS Backup API

除使用控制台外，您还可以使用 AWS Backup API 操作和数据类型，以编程方式配置和管理 AWS Backup 及其资源。本节介绍 AWS Backup 操作和数据类型。它包含 AWS Backup 的 API 参考。

AWS Backup API

- AWS Backup 操作
- AWS Backup 数据类型

操作

AWS Backup 支持以下操作：

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework
- DeleteRecoveryPoint

- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection
- GetSupportedResourceTypes

- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob
- StartCopyJob

- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

AWS Backup gateway 支持以下操作：

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines

- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

AWS Backup 支持以下操作：

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

服务： AWS Backup

移除对恢复点的指定法律保留。只能由具有足够权限的用户执行该操作。

请求语法

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

CancelDescription

一个字符串，描述了取消合法保全的原因。

必需：是

legalHoldId

合法封存的 ID。

必需：是

RetainRecordInDays

以天为单位的整数金额，之后要取消合法保留。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 201
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 201 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidResourceStateException

AWS Backup 已在此恢复点上执行操作。在第一个操作完成之前，它无法执行您请求的操作。请稍后重试。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateBackupPlan

服务： AWS Backup

使用备份计划名称和备份规则创建备份计划。备份计划是一种文档，其中包含用于计划为资源创建恢复点的任务的信息。 AWS Backup

如果使用已存在的计划调用 `CreateBackupPlan`，您会收到 `AlreadyExistsException` 异常。

请求语法

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
```

```
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

BackupPlan

备份计划的正文。包括 BackupPlanName 和一组或多组 Rules。

类型：BackupPlanInput 对象

必需：是

BackupPlanTags

要分配给备份计划的标签。

类型：字符串到字符串映射

必需：否

CreatorRequestId

标识请求并允许重试失败的请求，而不存在两次运行操作的风险。如果请求中包含与现有备份计划匹配的 CreatorRequestId，则会返回该计划。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AdvancedBackupSettings

资源类型的设置。此选项仅适用于 Windows 卷影复制服务 (VSS) 备份作业。

类型：AdvancedBackupSetting 对象数组

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

类型：字符串

BackupPlanId

备份计划的 ID。

类型：字符串

CreationDate

备份计划的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法对其进行编辑。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateBackupSelection

服务： AWS Backup

创建 JSON 文档，指定要分配给备份计划的一组资源。有关示例，请参阅以编程方式分配资源。

请求语法

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
```

```
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

备份计划的 ID。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

BackupSelection

向备份计划分配一组资源的请求正文。

类型：BackupSelection 对象

必需：是

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanId

备份计划的 ID。

类型：字符串

CreationDate

备份选择的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

SelectionId

唯一标识要将一组资源分配给备份计划的请求正文。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateBackupVault

服务： AWS Backup

创建用于存储备份的逻辑容器。CreateBackupVault 请求包括一个名称、（可选）一个或多个资源标签、一个加密密钥和一个请求 ID。

> **Note**
>
> 不要在备份保管库的名称中包含敏感数据（如护照号码）。

请求语法

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。它们包含字母、数字和连字符。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

BackupVaultTags

要分配给备份库的标签。

类型：字符串到字符串映射

必需：否

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

EncryptionKeyArn

用于保护备份的服务器端加密密钥；例如，arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。名称包含小写字母、数字和连字符。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

CreationDate

备份保管库的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateFramework

服务： AWS Backup

创建具有一个或多个控件的框架。框架是可用于评估备份实践的控件集合。通过使用预构建的可自定义控件来定义策略，您可以评估您的备份实践是否符合您的策略以及哪些资源尚未符合要求。

请求语法

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

FrameworkControls

构成框架的控件。列表中的每个控件都有名称、输入参数和范围。

类型：FrameworkControl 对象数组

必需：是

FrameworkDescription

框架的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：`.*\S.*`

必需：否

FrameworkName

框架的唯一名称。该名称的长度必须介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必需：是

FrameworkTags

要分配给框架的标签。

类型：字符串到字符串映射

必需：否

IdempotencyToken

客户选择的字符串，可用于区分对 CreateFrameworkInput 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

FrameworkArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

FrameworkName

框架的唯一名称。该名称的长度必须介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateLegalHold

服务： AWS Backup

对恢复点（备份）创建合法保留。法定保留是在授权用户取消法定保留之前对更改或删除备份的限制。如果恢复点上有一个或多个有效的法定保留，则任何删除或解除关联恢复点的操作都将失败并出现错误。

请求语法

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

Description

对法律封存的描述。

类型：字符串

必需：是

IdempotencyToken

这是用户选择的字符串，用于区分原本相同的调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

RecoveryPointSelection

分配一组资源的标准，例如资源类型或备份存储库。

类型：RecoveryPointSelection 对象

必需：否

Tags

要包括的可选标签。标签是您可用来管理、筛选和搜索资源的键值对。允许使用的字符包括 UTF-8 字母、数字、空格以及以下字符：+ - = . _ : /。

类型：字符串到字符串映射

必需：否

Title

合法封存的标题。

类型：字符串

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
```

```
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationDate

法定封存的创建时间。

类型：时间戳

Description

对法律封存的描述。

类型：字符串

LegalHoldArn

合法封存的亚马逊资源名称 (ARN)。

类型：字符串

LegalHoldId

合法封存的 ID。

类型：字符串

RecoveryPointSelection

分配给一组资源（例如资源类型或备份存储库）的标准。

类型：RecoveryPointSelection 对象

Status

合法封存的状态。

类型：字符串

有效值：CREATING | ACTIVE | CANCELING | CANCELED

Title

合法封存的标题。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateLogicallyAirGappedBackupVault

服务： AWS Backup

创建一个可以将备份复制到的逻辑容器。

此请求包括名称、区域、最大保留天数、最小保留天数，还可以包括标签和创建者请求 ID。

> **Note**
>
> 不要在备份保管库的名称中包含敏感数据（如护照号码）。

请求语法

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。逻辑气隙备份保管库的名称在创建它们的账户和创建它们的区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

BackupVaultTags

要分配给文件库的标签。

类型：字符串到字符串映射

必需：否

CreatorRequestId

创建请求的 ID。

此参数为可选的。如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

MaxRetentionDays

存储库保留其恢复点的最长保留期。如果不指定此参数，则 AWS Backup 不会对保管库中的恢复点强制规定最长保留期（允许无限期存储）。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或小于最长保留期。如果作业的保留期长于该最长保留期，则保管库将无法执行该备份或复制作业，因此，您应该修改生命周期设置或使用其他保管库。

类型：长整型

必需：是

MinRetentionDays

此设置用于指定保管库保留其恢复点的最短保留期。如果未指定此参数，将不会强制规定最短保留期。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或大于最短保留期。如果作业的保留期短于该最短保留期，则保管库将无法执行该备份或复制作业，因此，您应该修改生命周期设置或使用其他保管库。

类型：长整型

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

文件库的 ARN（亚马逊资源名称）。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。逻辑气隙备份保管库的名称在创建它们的账户和创建它们的区域中是唯一的。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

保管库的创建日期和时间。

该值采用 Unix 格式和协调世界时 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

VaultState

文件库的当前状态。

类型：字符串

有效值：`CREATING | AVAILABLE | FAILED`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateReportPlan

服务： AWS Backup

创建报告计划。报告计划是一种文档，其中包含有关报告内容及其交付地点 AWS Backup 的信息。

如果使用已存在的计划调用 `CreateReportPlan`，您会收到 `AlreadyExistsException` 异常。

请求语法

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

IdempotencyToken

客户选择的字符串，可用于区分对 CreateReportPlanInput 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

ReportDeliveryChannel

一种结构，包含有关在何处以及如何交付报告的信息，特别是 Amazon S3 存储桶名称、S3 密钥前缀和报告格式。

类型：ReportDeliveryChannel 对象

必需：是

ReportPlanDescription

报告计划的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：.*\S.*

必需：否

ReportPlanName

报告计划的唯一名称。该名称的长度必须介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

ReportPlanTags

要分配给报告计划的标签。

类型：字符串到字符串映射

必需：否

ReportSetting

标识报告的报告模板。报告使用报告模板构建。报告模板包括：

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

如果报告模板为RESOURCE_COMPLIANCE_REPORT或CONTROL_COMPLIANCE_REPORT，则此 API 资源还描述了 AWS 区域 和框架的报告覆盖范围。

类型：ReportSetting 对象

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

备份保管库的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

ReportPlanArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

ReportPlanName

报告计划的唯一名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateRestoreTestingPlan

服务： AWS Backup

创建还原测试计划。

创建恢复测试计划的两个步骤中的第一步。此请求成功后，使用完成该过程 CreateRestoreTestingSelection。

请求语法

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

CreatorRequestId

这是唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行该操作的风险。此参数为可选的。如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

RestoreTestingPlan

还原测试计划必须包含您创建的唯一 RestoreTestingPlanName 字符串，并且必须包含一个 ScheduleExpression cron。您可以选择包括一个 StartWindowHours 整数和一个 CreatorRequestId 字符串。

RestoreTestingPlanName 是唯一字符串，即还原测试计划的名称。创建后无法对其进行更改，并且只能由字母数字字符和下划线组成。

类型：RestoreTestingPlanForCreate 对象

必需：是

Tags

要分配给还原测试计划的标签。

类型：字符串到字符串映射

必需：否

响应语法

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

服务以 JSON 格式返回的以下数据。

CreationTime

还原测试计划的创建日期和时间，以 Unix 格式和世界标准时间 (UTC) 格式表示。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

RestoreTestingPlanArn

可唯一标识已创建的还原测试计划的 Amazon 资源名称（ARN）。

类型：字符串

RestoreTestingPlanName

唯一字符串，即还原测试计划的名称。

名称一经创建便无法更改。名称只能包含字母数字字符和下划线。最大长度为 50。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateRestoreTestingSelection

服务： AWS Backup

此请求可以在请求成功返回后 CreateRestoreTestingPlan 发送。这是创建资源测试计划的第二部分，必须按顺序完成。

它包括 RestoreTestingSelectionName、ProtectedResourceType 和以下项之一：

- ProtectedResourceArns
- ProtectedResourceConditions

每种受保护的资源类型可以具有一个单一值。

还原测试选择可以包括带通配符值（“*”）的 ProtectedResourceArns 以及 ProtectedResourceConditions。或者，您最多可以在 ProtectedResourceArns 中包括 30 个特定的受保护资源 ARN。

无法同时按受保护资源类型和特定 ARN 进行选择。如果同时使用两者，则请求将失败。

请求语法

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
```

```
        ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

输入从相关 CreateRestoreTestingPlan 请求返回的还原测试计划名称。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

CreatorRequestId

这是可选的唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行该操作的风险。如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

RestoreTestingSelection

它包括 RestoreTestingSelectionName、ProtectedResourceType 和以下项之一：

- ProtectedResourceArns
- ProtectedResourceConditions

每种受保护的资源类型可以具有一个单一值。

还原测试选择可以包括带通配符值（“*”）的 ProtectedResourceArns 以及 ProtectedResourceConditions。或者，您最多可以在 ProtectedResourceArns 中包括 30 个特定的受保护资源 ARN。

类型：RestoreTestingSelectionForCreate 对象

必需：是

响应语法

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

服务以 JSON 格式返回的以下数据。

CreationTime

资源测试选择的创建时间。

类型：时间戳

RestoreTestingPlanArn

与恢复测试选择相关联的恢复测试计划的 ARN。

类型：字符串

RestoreTestingPlanName

恢复测试计划的名称。

名称一经创建便无法更改。名称只能包含字母数字字符和下划线。最大长度为 50。

类型：字符串

RestoreTestingSelectionName

相关还原测试计划的还原测试选项的名称。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteBackupPlan

服务： AWS Backup

删除备份计划。只有在删除了所有关联的资源选择之后，才能删除备份计划。删除备份计划时将删除备份计划的当前版本。以前的版本（如果有）仍将存在。

请求语法

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

类型：字符串

BackupPlanId

唯一标识备份计划。

类型：字符串

DeletionDate

备份计划的删除日期和时间，采用 Unix 格式和协调世界时 (UTC)。DeletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑版本 ID。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteBackupSelection

服务： AWS Backup

删除与由 `SelectionId` 指定的备份计划关联的资源选择。

请求语法

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

selectionId

唯一标识要将一组资源分配给备份计划的请求正文。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteBackupVault

服务： AWS Backup

删除以其名称标识的备份保管库。只有空保管库才可删除。

请求语法

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteBackupVaultAccessPolicy

服务： AWS Backup

删除管理备份保管库权限的策略文档。

请求语法

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。名称包含小写字母、数字和连字符。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteBackupVaultLockConfiguration

服务： AWS Backup

从由备份 AWS Backup 库名称指定的备份保管库中删除文件库锁。

如果保管库锁定配置不可变，则无法使用 API 操作删除保管库锁定，且您将在尝试此操作时收到 `InvalidRequestException`。有关更多信息，请参阅《 AWS Backup 开发者指南》中的文件库锁定。

请求语法

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

要从中删除文件库锁的备份 AWS Backup 存储库的名称。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

DeleteBackupVaultNotifications

服务： AWS Backup

删除有关指定备份保管库的事件通知。

请求语法

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteFramework

服务： AWS Backup

删除由框架名称指定的框架。

请求语法

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

frameworkName

框架的唯一名称。

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误信息，请参阅常见错误。

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteRecoveryPoint

服务： AWS Backup

删除由恢复点 ID 指定的恢复点。

如果恢复点 ID 属于连续备份，则调用此端点会删除现有的连续备份并停止后续的连续备份。

当 IAM 角色的权限不足以调用此 API 时，该服务会发回带有空 HTTP 正文的 HTTP 200 响应，但不会删除恢复点。相反，它进入 EXPIRED 状态。

在 IAM 角色执行 `iam:CreateServiceLinkedRole` 操作后，可以使用此 API 删除 EXPIRED 恢复点。要详细了解如何添加此角色，请参阅排查手动删除问题。

如果删除用户/角色或删除角色内的权限，则删除将失败，并将进入 EXPIRED 状态。

请求语法

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

recoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

InvalidResourceStateException

AWS Backup 已在此恢复点上执行操作。在第一个操作完成之前，它无法执行您请求的操作。请稍后重试。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteReportPlan

服务： AWS Backup

删除由报告计划名称指定的报告计划。

请求语法

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

reportPlanName

报告计划的唯一名称。

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误信息，请参阅常见错误。

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteRestoreTestingPlan

服务： AWS Backup

此请求将删除指定的还原测试计划。

只有先删除所有关联的还原测试选择，才能成功删除还原测试计划。

请求语法

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

您要删除的还原测试计划的唯一名称（必需）。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 204
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteRestoreTestingSelection

服务： AWS Backup

输入还原测试计划名称和还原测试选择名称。

必须先删除与还原测试计划关联的所有测试选项，然后才能删除还原测试计划。

请求语法

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

包含您要删除的还原测试选择的还原测试计划的唯一名称（必需）。

必需：是

RestoreTestingSelectionName

您要删除的还原测试选择的唯一名称（必需）。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 204
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

错误

有关所有操作的常见错误信息，请参阅常见错误。

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeBackupJob

服务： AWS Backup

返回指定 BackupJobId 的备份作业详细信息。

请求语法

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupJobId

唯一标识 AWS Backup 对的资源备份请求。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
    "CompletionDate": number,
    "CreatedBy": {
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "BackupPlanVersion": "string",
       "BackupRuleId": "string"
    },
    "CreationDate": number,
    "ExpectedCompletionDate": number,
    "IamRoleArn": "string",
    "InitiationDate": number,
    "IsParent": boolean,
    "MessageCategory": "string",
    "NumberOfChildJobs": number,
    "ParentJobId": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "StartBy": number,
    "State": "string",
    "StatusMessage": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AccountId

返回拥有备份作业的账户 ID。

类型：字符串

模式：^[0-9]{12}$

BackupJobId

唯一标识 AWS Backup 对的资源备份请求。

类型：字符串

BackupOptions

表示作为备份计划或按需备份作业的一部分而指定的选项。

类型：字符串到字符串映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

BackupSizeInBytes

备份的大小（以字节为单位）。

类型：长整型

BackupType

表示为备份作业选择的实际备份类型。例如，如果成功进行了 Windows 卷影复制服务 (VSS) 备份，则 BackupType 会返回 "WindowsVSS"。如果 BackupType 为空，则备份类型为常规备份。

类型：字符串

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

BytesTransferred

查询作业状态时传输到备份保管库的大小（以字节为单位）。

类型：长整型

ChildJobsInState

这将返回包含的子（嵌套）备份作业的统计信息。

类型：字符串到长整型映射

有效密钥：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

CompletionDate

创建备份作业的作业完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CreatedBy

包含有关创建备份作业的识别信息，包括用于创建该作业的备份计划的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

类型：RecoveryPointCreator 对象

CreationDate

备份作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

ExpectedCompletionDate

资源备份作业的预期完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。ExpectedCompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

InitiationDate

启动备份任务的日期。

类型：时间戳

IsParent

这将返回一个布尔值，即备份作业是父（复合）作业。

类型：布尔值

MessageCategory

指定消息类别的任务计数。

例如，字符串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 INVALIDPARAMETERS。查看 “监控”，查看可接受的 MessageCategory 字符串列表。

类型：字符串

NumberOfChildJobs

这将返回子（嵌套）备份作业的数量。

类型：长整型

ParentJobId

这将返回父（复合）资源备份作业 ID。

类型：字符串

PercentDone

包含在查询作业状态时作业已完成的估计百分比。

类型：字符串

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

ResourceArn

唯一标识所保存资源的 ARN。ARN 的格式取决于资源类型。

类型：字符串

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

ResourceType

要备份的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

采用 Unix 格式和协调世界时 (UTC)，指定备份作业必须在取消改作业之前多久启动。该值通过将启动时段与计划时间相加进行计算。因此，如果计划时间为下午 6:00，启动时段为 2 小时，则 `StartBy` 时间为指定日期的晚上 8:00。`StartBy` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

State

备份作业的当前状态。

类型：字符串

有效值：`CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

一条详细消息，解释备份资源作业的状态。

类型：字符串

错误

有关所有操作的常见错误信息，请参阅常见错误。

DependencyFailureException

依赖的 AWS 服务或资源向该 AWS Backup 服务返回了错误，操作无法完成。

HTTP 状态代码：500

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

DescribeBackupVault

服务： AWS Backup

返回由其名称指定的备份保管库的相关元数据。

请求语法

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

指定备份库的账户 ID。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
   "Locked": boolean,
   "MaxRetentionDays": number,
```

```
    "MinRetentionDays": number,
    "NumberOfRecoveryPoints": number,
    "VaultType": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。

类型：字符串

CreationDate

备份保管库的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

EncryptionKeyArn

用于保护备份的服务器端加密密钥；例如，arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

类型：字符串

LockDate

无法更改或删除 AWS Backup 文件库锁定配置的日期和时间。

如果您在未指定锁定日期的情况下对保管库应用了保管库锁定，则可以随时更改任何保管库锁定设置，或从保管库中完全删除保管库锁定。

该值采用 Unix 格式和协调世界时 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

Locked

一个布尔值，用于指示 AWS Backup Vault Lock 当前是否在保护备份存储库。 `True`意味着文件库锁定会导致对存储在保管库中的恢复点执行删除或更新操作失败。

类型：布尔值

MaxRetentionDays

AWS Backup 文件库锁定设置，用于指定文件库保留其恢复点的最大保留期。如果不指定此参数，则保管库锁定不会对保管库中的恢复点强制规定最长保留期（允许无限期存储）。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或小于最长保留期。如果作业的保留期长于该最长保留期，则保管库将无法执行该备份或复制作业，因此您应该修改生命周期设置或使用其他保管库。保管库锁定之前已存储在保管库中的恢复点不受影响。

类型：长整型

MinRetentionDays

AWS Backup 文件库锁定设置，用于指定文件库保留其恢复点的最短保留期。如果未指定此参数，保管库锁定将不会强制规定最短保留期。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或大于最短保留期。如果作业的保留期短于该最短保留期，则保管库将无法执行该备份或复制作业，因此，您应该修改生命周期设置或使用其他保管库。保管库锁定之前已存储在保管库中的恢复点不受影响。

类型：长整型

NumberOfRecoveryPoints

存储在备份保管库中的恢复点数量。

类型：长整型

VaultType

描述的保管库类型。

类型：字符串

有效值：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeCopyJob

服务： AWS Backup

返回与创建资源副本相关的元数据。

请求语法

```
GET /copy-jobs/copyJobId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

copyJobId

唯一标识复制作业。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
```

```
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "MessageCategory": "string",
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CopyJob

包含有关复制作业的详细信息。

类型：CopyJob 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeFramework

服务： AWS Backup

返回指定 FrameworkName 的框架详细信息。

请求语法

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

frameworkName

框架的唯一名称。

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
```

```
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

框架的创建日期和时间，以 ISO 8601 表示。CreationTime 的值精确到毫秒。例如，2020-07-10T15:00:00.000-08:00 表示 2020 年 7 月 10 日下午 3:00，比 UTC 晚 8 个小时。

类型：时间戳

DeploymentStatus

框架的部署状态。状态包括：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

类型：字符串

FrameworkArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

FrameworkControls

构成框架的控件。列表中的每个控件都有名称、输入参数和范围。

类型：FrameworkControl 对象数组

FrameworkDescription

框架的可选描述。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：`.*\S.*`

FrameworkName

框架的唯一名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

框架由一个或多个控件组成。每个控件都控制一种资源，例如备份计划、备份选择、备份保管库或恢复点。您也可以为每种资源开启或关闭 AWS Config 记录。状态包括：

- ACTIVE，当框架管理的所有资源都开启记录功能时。
- PARTIALLY_ACTIVE，当至少一个受框架管理的资源关闭记录时。
- INACTIVE，当框架管理的所有资源都关闭记录时。
- UNAVAILABLEwh AWS Backup en 此时无法验证录制状态。

类型：字符串

IdempotencyToken

客户选择的字符串，可用于区分对 DescribeFrameworkOutput 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeGlobalSettings

服务： AWS Backup

描述该 AWS 账户是否已选择加入跨账户备份。如果账户不是 Organizations 组织的成员，则返回错误。例如：`describe-global-settings --region us-west-2`

请求语法

```
GET /global-settings HTTP/1.1
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GlobalSettings

标志 `isCrossAccountBackupEnabled` 的状态。

类型：字符串到字符串映射

LastUpdateTime

上次更新标志 `isCrossAccountBackupEnabled` 的日期和时间。此更新采用 Unix 格式和协调世界时 (UTC)。`LastUpdateTime` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeProtectedResource

服务： AWS Backup

返回有关已保存资源的信息，包括上次备份的时间、其 Amazon 资源名称 (ARN) 以及已保存资源的 AWS 服务类型。

请求语法

```
GET /resources/resourceArn HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

resourceArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

LastBackupTime

资源的上次备份日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastBackupTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

LastBackupVaultArn

包含最新备份恢复点的备份库的 ARN（Amazon 资源名称）。

类型：字符串

LastRecoveryPointArn

最新恢复点的 ARN（亚马逊资源名称）。

类型：字符串

LatestRestoreExecutionTimeMinutes

最近一次恢复任务完成所花费的时间（以分钟为单位）。

类型：长整型

LatestRestoreJobCreationDate

最近还原任务的创建日期。

类型：时间戳

LatestRestoreRecoveryPointCreationDate

最近恢复点的创建日期。

类型：时间戳

ResourceArn

唯一标识资源的 ARN。ARN 的格式取决于资源类型。

类型：字符串

ResourceName

属于指定备份的资源的名称。

类型：字符串

ResourceType

保存为恢复点的 AWS 资源类型；例如，Amazon EBS 卷或 Amazon RDS 数据库。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeRecoveryPoint

服务： AWS Backup

返回与恢复点关联的元数据，包括 ID、状态、加密和生命周期。

请求语法

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

指定备份库的账户 ID。

模式：^[0-9]{12}$

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

recoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupSizeInBytes

备份的大小（以字节为单位）。

类型：长整型

BackupVaultArn

唯一标识备份保管库的 ARN；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

CalculatedLifecycle

包含 DeleteAt 和 MoveToColdStorageAt 时间戳的 CalculatedLifecycle 对象。

类型：CalculatedLifecycle 对象

CompletionDate

恢复点创建作业的完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CompositeMemberIdentifier

复合组中资源的标识符，例如属于复合（父）堆栈的嵌套（子）恢复点。ID 是从堆栈内的逻辑 ID 中传输的。

类型：字符串

CreatedBy

包含有关创建恢复点的识别信息，包括用于创建该恢复点的备份计划的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

类型：RecoveryPointCreator 对象

CreationDate

恢复点的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

EncryptionKeyArn

用于保护备份的服务器端加密密钥；例如，arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

类型：字符串

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

IsEncrypted

一个布尔值，如果指定的恢复点已加密，则返回 TRUE，如果恢复点未加密，则返回 FALSE。

类型：布尔值

IsParent

这将返回一个布尔值，即恢复点是父（复合）作业。

类型：布尔值

LastRestoreTime

恢复点的上次还原日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastRestoreTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

类型：Lifecycle 对象

ParentRecoveryPointArn

这是唯一标识父（复合）恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

ResourceArn

唯一标识所保存资源的 ARN。ARN 的格式取决于资源类型。

类型：字符串

ResourceName

属于指定备份的资源的名称。

类型：字符串

ResourceType

要保存为恢复点的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

SourceBackupVaultArn

唯一标识资源最初备份的源保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。如果恢复到相同的 AWS 账户或区域，则该值将为null。

类型：字符串

Status

指定恢复点状态的状态码。

PARTIAL状态表示在备份窗口关闭之前 AWS Backup 无法创建恢复点。要使用 API 延长备份计划窗口，请参阅UpdateBackupPlan。您还可以使用控制台，通过选择和编辑备份计划来延长备份计划时段。

EXPIRED状态表示恢复点已超过其保留期，但 AWS Backup 缺少权限或无法将其删除。要手动删除这些恢复点，请参阅入门章节清理资源部分中的步骤 3：删除恢复点。

当用户执行某些操作导致连续备份被禁用时，连续备份中会出现 STOPPED 状态。这可能是由于移除权限、关闭版本控制、关闭发送到 EventBridge的事件或禁用由 AWS Backup制定的 EventBridge 规则造成的。

要解决 STOPPED 状态问题，请确保请求的所有权限均已准备就绪，并且已在 S3 存储桶上启用版本控制。满足这些条件后，下一个运行的备份规则实例将导致创建新的连续恢复点。不需要删除处于 STOPPED 状态的恢复点。

对于 Amazon EC2 上的 SAP HANA，STOPPED 状态是由于用户操作、应用程序配置错误或备份失败而导致的。要确保日后连续备份成功，请参阅恢复点状态并查看 SAP HANA，以了解详细信息。

类型：字符串

有效值：COMPLETED | PARTIAL | DELETING | EXPIRED

StatusMessage

解释恢复点状态的状态消息。

类型：字符串

StorageClass

指定恢复点的存储类别。有效值为 WARM 或 COLD。

类型：字符串

有效值：`WARM | COLD | DELETED`

VaultType

存储所述恢复点的存储库的类型。

类型：字符串

有效值：`BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeRegionSettings

服务： AWS Backup

返回区域当前选择加入服务设置。如果某项服务启用了服务选择启用，则当该资源包含在按需备份或定时备份计划中时，会 AWS Backup 尝试保护该服务在该区域的资源。否则， AWS Backup 不会尝试保护该服务在该区域的资源。

请求语法

```
GET /account-settings HTTP/1.1
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ResourceTypeManagementPreference

返回是否 AWS Backup 完全管理资源类型的备份。

有关完全 AWS Backup 管理的好处，请参阅完全 AWS Backup 管理。

有关资源类型以及每种资源类型是否支持完全 AWS Backup 管理的列表，请参阅按资源划分的功能可用性表。

如果是"DynamoDB":false，则可以通过启用高级 DynamoDB 备份功能来启用 DynamoDB 备份 AWS Backup的完全 AWS Backup 管理。

类型：字符串到布尔映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

ResourceTypeOptInPreference

该地区的服务以及选择加入偏好。

类型：字符串到布尔映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包

- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeReportJob

服务： AWS Backup

返回与创建由其 ReportJobId 指定的报告相关联的详细信息。

请求语法

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

reportJobId

报告作业的标识符。唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑报告作业 ID。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
```

```
    }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ReportJob

有关报告任务的信息，包括其完成和创建时间、报告目的地、唯一的报告任务 ID、Amazon 资源名称 (ARN)、报告模板、状态和状态消息。

类型：ReportJob 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeReportPlan

服务： AWS Backup

返回 AWS 账户 和的所有报告计划的列表 AWS 区域。

请求语法

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

reportPlanName

报告计划的唯一名称。

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
```

```
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ReportPlan

返回有关由其名称指定的报告计划的详细信息。这些详细信息包括报告计划的 Amazon 资源名称 (ARN)、描述、设置、传送通道、部署状态、创建时间以及上次尝试和成功运行时间。

类型：ReportPlan 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DescribeRestoreJob

服务： AWS Backup

返回与由作业 ID 指定的还原作业关联的元数据。

请求语法

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

restoreJobId

唯一标识还原恢复点的作业。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
   "PercentDone": "string",
```

```
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AccountId

返回拥有还原作业的账户 ID。

类型：字符串

模式：^[0-9]{12}$

BackupSizeInBytes

还原资源的大小（以字节为单位）。

类型：长整型

CompletionDate

恢复点还原作业的完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CreatedBy

包含有关创建还原作业的标识信息。

类型：RestoreJobCreator 对象

CreatedResourceArn

还原任务创建的资源的亚马逊资源名称 (ARN)。

ARN 的格式取决于备份资源的资源类型。

类型：字符串

CreationDate

还原作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

DeletionStatus

还原测试生成的数据的状态。

类型：字符串

有效值：DELETING | FAILED | SUCCESSFUL

DeletionStatusMessage

这描述了还原作业的删除状态。

类型：字符串

ExpectedCompletionTimeMinutes

恢复点还原作业预计要花费的时间（以分钟为单位）。

类型：长整型

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

PercentDone

包含在查询作业状态时作业已完成的估计百分比。

类型：字符串

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

RecoveryPointCreationDate

由指定还原任务创建的恢复点的创建日期。

类型：时间戳

ResourceType

返回与按资源类型列出的还原作业关联的元数据。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

唯一标识还原恢复点的作业。

类型：字符串

Status

状态码，用于指定为恢复恢复点而启动 AWS Backup 的任务的状态。

类型：字符串

有效值：`PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

一条显示恢复点还原作业状态的消息。

类型：字符串

ValidationStatus

在指定的还原作业上运行验证的状态。

类型：字符串

有效值：`FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

状态消息。

类型：字符串

错误

有关所有操作的常见错误信息，请参阅常见错误。

DependencyFailureException

依赖的 AWS 服务或资源向该 AWS Backup 服务返回了错误，操作无法完成。

HTTP 状态代码：500

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK

- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DisassociateRecoveryPoint

服务： AWS Backup

从源服务（例如 Amazon RDS）中删除指定的连续备份恢复点， AWS Backup 并释放对该持续备份的控制权。源服务将继续使用您在原始备份计划中指定的生命周期创建和保留连续备份。

不支持快照备份恢复点。

请求语法

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

AWS Backup 文件库的唯一名称。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

recoveryPointArn

唯一标识 AWS Backup 恢复点的 Amazon 资源名称 (ARN)。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

InvalidResourceStateException

AWS Backup 已在此恢复点上执行操作。在第一个操作完成之前，它无法执行您请求的操作。请稍后重试。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DisassociateRecoveryPointFromParent

服务： AWS Backup

对特定子（嵌套）恢复点执行此操作会撤销指定恢复点与其父（复合）恢复点之间的关系。

请求语法

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

存储子（嵌套）恢复点的逻辑容器的名称。Backup 存储库由用于创建备份存储库的账户和创建备份存储库的 AWS 区域所特有的名称进行标识。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

recoveryPointArn

唯一标识子（嵌套）恢复点的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 204
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ExportBackupPlanTemplate

服务： AWS Backup

返回由计划 ID 指定的备份计划作为备份模板。

请求语法

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanTemplateJson

JSON 格式的备份计划模板的正文。

> **Note**
>
> 这是一个已签名的 JSON 文档，在将其传递给 `GetBackupPlanFromJSON`。之前无法对其进行修改

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupPlan

服务： AWS Backup

返回指定 BackupPlan 的 BackupPlanId 详细信息。详细信息包含 JSON 格式的备份计划正文以及计划元数据。

请求语法

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑版本 ID。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
```

```
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
```

```
    "CreatorRequestId": "string",
    "DeletionDate": number,
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AdvancedBackupSettings

包含每种资源的 BackupOptions 列表。仅在为备份计划设置高级选项时，才会填充该列表。

类型：AdvancedBackupSetting 对象数组

BackupPlan

指定备份计划的正文。包括 BackupPlanName 和一组或多组 Rules。

类型：BackupPlan 对象

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

类型：字符串

BackupPlanId

唯一标识备份计划。

类型：字符串

CreationDate

备份计划的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。

类型：字符串

DeletionDate

备份计划的删除日期和时间，采用 Unix 格式和协调世界时 (UTC)。DeletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

LastExecutionDate

上次运行此备份计划的时间。日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastExecutionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑版本 ID。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupPlanFromJSON

服务： AWS Backup

返回指定备份计划或错误的有效 JSON 文档。

请求语法

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

BackupPlanTemplateJson

客户提供的 JSON 格式的备份计划文档。

类型：字符串

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlan

指定备份计划的正文。包括 BackupPlanName 和一组或多组 Rules。

类型：BackupPlan 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupPlanFromTemplate

服务： AWS Backup

返回由其 templateId 指定的模板作为备份计划。

请求语法

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

templateId

唯一标识存储的备份计划模板。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanDocument

根据目标模板返回备份计划的正文，包括计划的名称、规则和备份保管库。

类型：BackupPlan 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupSelection

服务： AWS Backup

返回选择元数据和一个 JSON 格式的文档，该文档指定了与备份计划关联的资源的列表。

请求语法

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

selectionId

唯一标识要将一组资源分配给备份计划的请求正文。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanId

唯一标识备份计划。

类型：字符串

BackupSelection

指定将一组资源分配给备份计划的请求的正文。

类型：BackupSelection 对象

CreationDate

备份选择的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。

类型：字符串

SelectionId

唯一标识要将一组资源分配给备份计划的请求正文。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupVaultAccessPolicy

服务： AWS Backup

返回与指定备份保管库关联的访问策略文档。

请求语法

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

Policy

JSON 格式的备份保管库访问策略文档。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBackupVaultNotifications

服务： AWS Backup

返回有关指定备份保管库的事件通知。

请求语法

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

BackupVaultEvents

一个事件数组，指示将资源备份到备份保管库的作业状态。

类型：字符串数组

有效值：BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

SNSTopicArn

用于唯一标识 Amazon Simple Notification Service (Amazon SNS) 主题的 ARN；例如，arn:aws:sns:us-west-2:111122223333:MyTopic。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetLegalHold

服务： AWS Backup

此操作返回指定法定保留的详细信息。除元数据外，详细信息还包括 JSON 格式的法定保留的正文。

请求语法

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

legalHoldId

合法封存的 ID。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
```

```
    },
    "RetainRecordUntil": number,
    "Status": "string",
    "Title": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CancelDescription

取消法律封存的原因。

类型：字符串

CancellationDate

取消法定保留的时间。

类型：时间戳

CreationDate

法定封存的创建时间。

类型：时间戳

Description

对法律封存的描述。

类型：字符串

LegalHoldArn

特定法律封存的框架 ARN。ARN 的格式取决于资源类型。

类型：字符串

LegalHoldId

合法封存的 ID。

类型：字符串

RecoveryPointSelection

分配一组资源的标准，例如资源类型或备份存储库。

类型：RecoveryPointSelection 对象

RetainRecordUntil

保留法定保留记录的日期和时间。

类型：时间戳

Status

合法封存的状态。

类型：字符串

有效值：`CREATING | ACTIVE | CANCELING | CANCELED`

Title

合法封存的标题。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetRecoveryPointRestoreMetadata

服务： AWS Backup

返回一组用于创建备份的元数据键值对。

请求语法

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

指定备份库的账户 ID。

模式：`^[0-9]{12}$`

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

recoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 ARN；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

ResourceType

恢复点的资源类型。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

RestoreMetadata

描述备份资源原始配置的一组元数据键值对。这些值因所恢复服务的不同而异。

类型：字符串到字符串映射

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetRestoreJobMetadata

服务： AWS Backup

此请求返回指定还原作业的元数据。

请求语法

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

restoreJobId

这是其中还原任务的唯一标识符 AWS Backup。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Metadata

它包含指定备份作业的元数据。

类型：字符串到字符串映射

RestoreJobId

这是其中还原任务的唯一标识符 AWS Backup。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetRestoreTestingInferredMetadata

服务： AWS Backup

此请求返回使用安全的默认设置启动还原作业所需的最低限度元数据集。BackupVaultName 和 RecoveryPointArn 是必需参数。BackupVaultAccountId 是可选参数。

请求语法

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

指定备份库的账户 ID。

BackupVaultName

用于存储备份的逻辑容器的名称。Backup 存储库由用于创建备份存储库的账户和创建备份存储库的 AWS区域所特有的名称进行标识。它们包含字母、数字和连字符。

必需：是

RecoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

InferredMetadata

这是根据请求推断出的元数据的字符串映射。

类型：字符串到字符串映射

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetRestoreTestingPlan

服务： AWS Backup

返回指定 RestoreTestingPlan 的 RestoreTestingPlanName 详细信息。详细信息包含 JSON 格式的还原测试计划正文以及计划元数据。

请求语法

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

还原测试计划的唯一名称（必需）。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
```

```
        "RestoreTestingPlanArn": "string",
        "RestoreTestingPlanName": "string",
        "ScheduleExpression": "string",
        "ScheduleExpressionTimezone": "string",
        "StartWindowHours": number
    }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

RestoreTestingPlan

指定还原测试计划的正文。包含 RestoreTestingPlanName。

类型：RestoreTestingPlanForGet 对象

错误

有关所有操作的常见错误信息，请参阅常见错误。

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetRestoreTestingSelection

服务： AWS Backup

返回 RestoreTestingSelection，显示还原测试计划的资源和要素。

请求语法

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

还原测试计划的唯一名称（必需）。

必需：是

RestoreTestingSelectionName

还原测试选择的唯一名称（必需）。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
```

```
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

RestoreTestingSelection

还原测试选择的唯一名称。

类型：RestoreTestingSelectionForGet 对象

错误

有关所有操作的常见错误信息，请参阅常见错误。

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetSupportedResourceTypes

服务： AWS Backup

返回支持的 AWS 资源类型 AWS Backup。

请求语法

```
GET /supported-resource-types HTTP/1.1
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ResourceTypes

包含一个包含支持的 AWS 资源类型的字符串：

- 适用于 Amazon Aurora 的 `Aurora`
- `CloudFormation`对于 AWS CloudFormation
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 `DocumentDB`
- `DynamoDB`：表示 Amazon DynamoDB
- `EBS`：表示 Amazon Elastic Block Store

- EC2：表示 Amazon Elastic Compute Cloud
- EFS：表示 Amazon Elastic File System
- FSX：表示 Amazon FSx
- 适用于 Amazon Neptune 的 Neptune
- 适用于 Amazon Relational Database Service 的 RDS
- 适用于 Amazon Redshift Redshift
- SAP HANA on Amazon EC2适用于亚马逊弹性计算云实例上的 SAP HANA 数据库
- S3适用于亚马逊简单存储服务 (Amazon S3) Simple Service
- Storage Gateway对于 AWS Storage Gateway
- Timestream：表示 Amazon Timestream
- VirtualMachine适用于 VMware 虚拟机

类型：字符串数组

模式：^[a-zA-Z0-9\-_\.]{1,50}$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包

- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupJobs

服务： AWS Backup

返回过去 30 天内经过身份验证的账户的现有备份作业列表。在较长一段时间内，可以考虑使用这些监控工具。

请求语法

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByAccountId

列出作业的账户 ID。仅返回与指定账户 ID 关联的备份作业。

如果从 AWS Organizations 管理账户中使用，则传递*会返回整个组织中的所有作业。

模式：^[0-9]{12}$

ByBackupVaultName

仅返回将存储在指定备份库中的备份作业。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

ByCompleteAfter

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之后完成的备份作业。

ByCompleteBefore

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之前完成的备份作业。

ByCreatedAfter

仅返回在指定日期之后创建的备份作业。

ByCreatedBefore

仅返回在指定日期之前创建的备份作业。

ByMessageCategory

这是一个可选参数，可用于筛选出与您输入 MessageCategory 的值匹配的作业。

例如，字符串可能包括 `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL` 和 `InvalidParameters`。

查看监控

通配符 (`*`) 返回所有消息类别的计数。

`AGGREGATE_ALL` 汇总所有消息类别的作业计数并返回总和。

ByParentJobId

这是一个筛选器，用于根据父作业 ID 列出子（嵌套）作业。

ByResourceArn

仅返回与指定资源 Amazon 资源名称 (ARN) 匹配的备份作业。

ByResourceType

仅返回指定资源的备份作业：

- 适用于 Amazon Aurora 的 `Aurora`
- `CloudFormation`对于 AWS CloudFormation
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 `DocumentDB`
- `DynamoDB`：表示 Amazon DynamoDB
- `EBS`：表示 Amazon Elastic Block Store
- `EC2`：表示 Amazon Elastic Compute Cloud
- `EFS`：表示 Amazon Elastic File System
- `FSx`：表示 Amazon FSx
- `Neptune`：表示 Amazon Neptune
- `Redshift`：表示 Amazon Redshift
- `RDS`：表示 Amazon Relational Database Service
- `SAP HANA on Amazon EC2`：表示 SAP HANA 数据库
- `Storage Gateway`对于 AWS Storage Gateway
- `S3`：表示 Amazon S3
- `Timestream`：表示 Amazon Timestream

- VirtualMachine：表示虚拟机

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByState

仅返回处于指定状态的备份作业。

Completed with issues 是仅在 AWS Backup 控制台中显示的状态。对于 API 来说，此状态是指状态为 COMPLETED 和 MessageCategory 且值不是 SUCCESS 的作业，即，状态为已完成但带有状态消息的作业。

要获取 Completed with issues 的作业计数，请运行两个 GET 请求，然后减去第二个较小的数字：

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

有效值：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupJobs

包含有关以 JSON 格式返回的备份作业的元数据的结构数组。

类型：BackupJob 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 `MaxResults` 数量的项目，则 `NextToken` 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3

- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupJobSummaries

服务： AWS Backup

此请求提供最近 30 天内创建的或正在运行的备份作业的摘要。您可以添加参数 accountID、State、ResourceType、、 MessageCategory AggregationPeriod MaxResults、 NextToken 或来筛选结果。

此请求返回包含区域、账户、州、、 ResourceType MessageCategory StartTime EndTime、和包含任务数量的摘要。

请求语法

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

AccountId

返回指定账户的作业计数。

如果请求是从成员账户或不属于 Organizations 的 AWS 账户发送的，则将返回申请者账户中的职位。

根账户、管理员和委派管理员账户可以使用值 ANY 来返回组织中每个账户中的作业计数。

AGGREGATE_ALL 汇总经过身份验证的组织内所有账户中的作业计数，然后返回总和。

模式：^[0-9]{12}$

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

有效值：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

要返回的最大项目数量。

值为整数。接受的值范围为 1 到 500。

有效范围：最小值为 1。最大值为 1000。

MessageCategory

此参数返回指定消息类别的作业计数。

接受的字符串示例包括 AccessDenied、Success 和 InvalidParameters。有关可接受 MessageCategory 字符串的列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

ResourceType

返回指定资源类型的作业计数。使用请求 GetSupportedResourceTypes 获取支持的资源类型的字符串。

值 ANY 会返回所有资源类型的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

要备份的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此参数返回具有指定状态的作业的作业计数。

值 ANY 会返回所有状态的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

Completed with issues 是仅在 AWS Backup 控制台中显示的状态。对于 API 来说，此状态是指状态为 COMPLETED 和 MessageCategory 且值不是 SUCCESS 的作业，即，状态为已完成但带有状态消息的作业。要获取 Completed with issues 的作业计数，请运行两个 GET 请求，然后减去第二个较小的数字：

GET /audit/ ? backup-job-summaries AggregationPeriod=fourteen_days&state=已完成

GET /audit/ ? backup-job-summaries AggregationPeriod=FOURTEEN_DAYS& =成功&状态= MessageCategory 已完成

有效值：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

类型：字符串

BackupJobSummaries

摘要信息。

类型：BackupJobSummary 对象数组

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupPlans

服务： AWS Backup

列出该账户的有效备份计划。

请求语法

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

IncludeDeleted

默认值为的布尔值在设置FALSE为时返回已删除的备份计划TRUE。

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
```

```
                "string" : "string"
            },
            "ResourceType": "string"
        }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "DeletionDate": number,
      "LastExecutionDate": number,
      "VersionId": "string"
    }
  ],
  "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlansList

有关备份计划的信息。

类型：BackupPlansListMember 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupPlanTemplates

服务： AWS Backup

列出备份计划模板。

请求语法

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要退货的最大商品数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanTemplatesList

一系列模板列表项目，其中包含有关已保存模板的元数据。

类型：BackupPlanTemplatesListMember 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupPlanVersions

服务： AWS Backup

返回备份计划的版本元数据，其中包括 Amazon 资源名称 (ARN)、备份计划 ID、创建和删除日期、计划名称和版本 ID。

请求语法

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanVersionsList": [
```

```
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupPlanVersionsList

一系列版本列表项目，其中包含有关您的备份计划的元数据。

类型：BackupPlansListMember 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupSelections

服务： AWS Backup

返回一个数组，其中包含与目标备份计划关联的资源的元数据。

请求语法

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

唯一标识备份计划。

必需：是

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSelectionsList": [
```

```
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupSelectionsList

一系列备份选择列表项目，其中包含有关列表中每个资源的元数据。

类型：BackupSelectionsListMember 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListBackupVaults

服务： AWS Backup

返回恢复点存储容器的列表及其相关信息。

请求语法

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByShared

此参数将按共享保管库对保管库列表进行排序。

ByVaultType

此参数将按保管库类型对保管库列表进行排序。

有效值：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultList

一组备份保管库列表成员，其中包含保管库元数据，包括 Amazon 资源名称 (ARN)、显示名称、创建日期、保存的恢复点数量，以及在备份保管库中保存的资源已加密的情况下的解密信息。

类型：BackupVaultListMember 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 `MaxResults` 数量的项目，则 `NextToken` 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListCopyJobs

服务： AWS Backup

返回有关您的复制作业的元数据。

请求语法

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByAccountId

列出作业的账户 ID。仅返回与指定账户 ID 关联的复制作业。

模式：^[0-9]{12}$

ByCompleteAfter

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之后完成的复制作业。

ByCompleteBefore

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之前完成的复制作业。

ByCreatedAfter

仅返回在指定日期之后创建的复制作业。

ByCreatedBefore

仅返回在指定日期之前创建的复制作业。

ByDestinationVaultArn

唯一标识要从中复制的源备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

ByMessageCategory

这是一个可选参数，可用于筛选出与您输入 MessageCategory 的值匹配的作业。

例如，字符串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 INVALIDPARAMETERS。

查看监控以查看接受的字符串的列表。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

ByParentJobId

这是一个筛选器，用于根据父作业 ID 列出子（嵌套）作业。

ByResourceArn

仅返回与指定资源 Amazon 资源名称 (ARN) 匹配的复制作业。

ByResourceType

仅返回指定资源的备份作业：

- 适用于 Amazon Aurora 的 Aurora
- CloudFormation对于 AWS CloudFormation
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 DocumentDB
- DynamoDB：表示 Amazon DynamoDB
- EBS：表示 Amazon Elastic Block Store
- EC2：表示 Amazon Elastic Compute Cloud
- EFS：表示 Amazon Elastic File System
- FSx：表示 Amazon FSx
- Neptune：表示 Amazon Neptune
- Redshift：表示 Amazon Redshift
- RDS：表示 Amazon Relational Database Service
- SAP HANA on Amazon EC2：表示 SAP HANA 数据库
- Storage Gateway对于 AWS Storage Gateway
- S3：表示 Amazon S3
- Timestream：表示 Amazon Timestream
- VirtualMachine：表示虚拟机

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByState

仅返回处于指定状态的复制作业。

有效值：CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回商品 MaxResults 数量，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
```

```
        },
        "CreationDate": number,
        "DestinationBackupVaultArn": "string",
        "DestinationRecoveryPointArn": "string",
        "IamRoleArn": "string",
        "IsParent": boolean,
        "MessageCategory": "string",
        "NumberOfChildJobs": number,
        "ParentJobId": "string",
        "ResourceArn": "string",
        "ResourceName": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "SourceRecoveryPointArn": "string",
        "State": "string",
        "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CopyJobs

包含以 JSON 格式返回的复制作业的元数据的结构数组。

类型：CopyJob 对象数组

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回商品 MaxResults 数量，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListCopyJobSummaries

服务： AWS Backup

此请求提供最近 30 天内创建或正在运行的复制作业的摘要。您可以添加参数 accountID、State、ResourceType、、 MessageCategory AggregationPeriod MaxResults、 NextToken 或来筛选结果。

此请求返回包含区域、账户、州、、 RestourceType MessageCategory StartTime EndTime、和包含任务数量的摘要。

请求语法

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

AccountId

返回指定账户的作业计数。

如果请求是从成员账户或不属于 Organizations 的 AWS 账户发送的，则将返回申请者账户中的职位。

根账户、管理员和委派管理员账户可以使用值 ANY 来返回组织中每个账户中的作业计数。

AGGREGATE_ALL 汇总经过身份验证的组织内所有账户中的作业计数，然后返回总和。

模式：^[0-9]{12}$

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

有效值：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

此参数设置要返回的最大项目数。

值为整数。接受的值范围为 1 到 500。

有效范围：最小值为 1。最大值为 1000。

MessageCategory

此参数返回指定消息类别的作业计数。

接受的字符串示例包括 AccessDenied、Success 和 InvalidParameters。有关可接受 MessageCategory 字符串的列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

ResourceType

返回指定资源类型的作业计数。使用请求 GetSupportedResourceTypes 获取支持的资源类型的字符串。

值 ANY 会返回所有资源类型的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

要备份的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此参数返回具有指定状态的作业的作业计数。

值 ANY 会返回所有状态的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

有效值：CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

类型：字符串

CopyJobSummaries

此返回结果显示的摘要包含区域、账户、州 ResourceType MessageCategory、 StartTime、EndTime、和包含的任务数量。

类型：CopyJobSummary 对象数组

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 `MaxResults` 数量的资源，则 `NextToken` 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包

- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListFrameworks

服务： AWS Backup

返回 AWS 账户 和的所有框架的列表 AWS 区域。

请求语法

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

所需结果的数量从 1 到 1000。可选。如果未指定，则查询将返回 1 MB 的数据。

有效范围：最小值为 1。最大值为 1000。

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
         "FrameworkName": "string",
         "NumberOfControls": number
      }
   ],
```

```
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Frameworks

包含每个框架详细信息的框架，包括框架名称、Amazon 资源名称 (ARN)、描述、控件数量、创建时间和部署状态。

类型：Framework 对象数组

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListLegalHolds

服务： AWS Backup

此操作会返回有关有效和先前法定保留的元数据。

请求语法

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要返回的资源列表项的最大数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
         "LegalHoldId": "string",
         "Status": "string",
         "Title": "string"
```

```
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

LegalHolds

这是返回的法定保留（包括有效和先前保留）的数组。

类型：LegalHold 对象数组

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 `MaxResults` 数量的资源，则 `NextToken` 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListProtectedResources

服务： AWS Backup

返回成功备份的资源数组 AWS Backup，包括资源保存时间、资源的 Amazon 资源名称 (ARN) 和资源类型。

请求语法

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
```

```
            "ResourceType": "string"
        }
    ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

Results

通过 AWS Backup 包括资源保存时间、资源的 Amazon 资源名称 (ARN) 和资源类型成功备份的一系列资源。

类型：ProtectedResource 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListProtectedResourcesByBackupVault

服务： AWS Backup

此请求列出了与每个备份保管库相对应的受保护资源。

请求语法

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

按账户 ID 指定的文件库中按备份存储库列出的受保护资源列表。

模式：`^[0-9]{12}$`

backupVaultName

按名称指定的文件库中按备份存储库列出的受保护资源列表。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 `MaxResults` 数量的项目，则 `NextToken` 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

Results

这些是请求返回的结果 ListProtectedResourcesByBackupVault。

类型：ProtectedResource 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRecoveryPointsByBackupVault

服务： AWS Backup

返回有关存储在备份保管库中的恢复点的详细信息。

请求语法

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

BackupVaultAccountId

此参数将按账户 ID 对恢复点列表进行排序。

模式：^[0-9]{12}$

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

> **Note**
> 当支持的服务创建备份时，备份保管库名称可能不可用。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

ByBackupPlanId

仅返回与指定备份计划 ID 匹配的恢复点。

ByCreatedAfter

仅返回在指定时间戳之后创建的恢复点。

ByCreatedBefore

仅返回在指定时间戳之前创建的恢复点。

ByParentRecoveryPointArn

这将仅返回与指定父（复合）恢复点 Amazon 资源名称 (ARN) 匹配的恢复点。

ByResourceArn

仅返回与指定资源 Amazon 资源名称 (ARN) 匹配的恢复点。

ByResourceType

仅返回与指定资源类型匹配的恢复点。

- 适用于 Amazon Aurora 的 `Aurora`
- `CloudFormation`对于 AWS CloudFormation
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 `DocumentDB`
- `DynamoDB`：表示 Amazon DynamoDB
- `EBS`：表示 Amazon Elastic Block Store
- `EC2`：表示 Amazon Elastic Compute Cloud
- `EFS`：表示 Amazon Elastic File System
- `FSx`：表示 Amazon FSx
- `Neptune`：表示 Amazon Neptune
- `Redshift`：表示 Amazon Redshift
- `RDS`：表示 Amazon Relational Database Service
- `SAP HANA on Amazon EC2`：表示 SAP HANA 数据库
- `Storage Gateway`对于 AWS Storage Gateway
- `S3`：表示 Amazon S3
- `Timestream`：表示 Amazon Timestream
- `VirtualMachine`：表示虚拟机

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IamRoleArn": "string",
         "IsEncrypted": boolean,
         "IsParent": boolean,
         "LastRestoreTime": number,
         "Lifecycle": {
            "DeleteAfterDays": number,
```

```
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
         },
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RecoveryPoints

对象数组，其中包含有关备份保管库中保存的恢复点的详细信息。

类型：RecoveryPointByBackupVault 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRecoveryPointsByLegalHold

服务： AWS Backup

此操作将返回指定法定保留的恢复点 ARN（Amazon 资源名称）。

请求语法

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

legalHoldId

合法封存的 ID。

必需：是

MaxResults

要返回的资源列表项的最大数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
```

```
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回资源的部分列表的后续下一个项目。

类型：字符串

RecoveryPoints

恢复点。

类型：RecoveryPointMember 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRecoveryPointsByResource

服务： AWS Backup

有关资源指定类型的恢复点的信息 Amazon 资源名称 (ARN)。

> **Note**
>
> 对于 Amazon EFS 和 Amazon EC2，此操作仅列出由 AWS Backup创建的恢复点。

请求语法

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ManagedByAWSBackupOnly

此属性根据所有权筛选恢复点。

如果将其设置为TRUE，则响应将包含与由管理的选定资源关联的恢复点 AWS Backup。

如果将其设置为FALSE，则响应将包含与所选资源关联的所有恢复点。

类型：布尔值

MaxResults

要返回的最大项目数量。

> **Note**
>
> Amazon RDS 要求的值至少为 20。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

resourceArn

唯一标识资源的 ARN。ARN 的格式取决于资源类型。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RecoveryPoints

对象数组，其中包含有关指定资源类型的恢复点的详细信息。

> **Note**
>
> 只返回 Amazon EFS 和 Amazon EC2 恢复点 BackupVaultName。

类型：RecoveryPointByResource 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListReportJobs

服务： AWS Backup

返回有关您的报告作业的详细信息。

请求语法

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByCreationAfter

仅返回采用 Unix 格式和协调世界时 (UTC) 指定的日期和时间之后创建的报告作业。例如，值 1516925490 表示 2018 年 1 月 26 日星期五上午 12:11:30。

ByCreationBefore

仅返回采用 Unix 格式和协调世界时 (UTC) 指定的日期和时间之前创建的报告作业。例如，值 1516925490 表示 2018 年 1 月 26 日星期五上午 12:11:30。

ByReportPlanName

仅返回具有指定报告计划名称的报告作业。

长度约束：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

仅返回处于指定状态的报告作业。状态包括：

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

所需结果的数量从 1 到 1000。可选。如果未指定，则查询将返回 1 MB 的数据。

有效范围：最小值为 1。最大值为 1000。

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

类型：字符串

ReportJobs

JSON 格式的报告作业的相关详细信息。

类型：ReportJob 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

ListReportPlans

服务： AWS Backup

返回报告计划的列表。有关单一报告计划的详细信息，请使用 DescribeReportPlan。

请求语法

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

所需结果的数量从 1 到 1000。可选。如果未指定，则查询将返回 1 MB 的数据。

有效范围：最小值为 1。最大值为 1000。

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
```

```
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

上次调用此操作时返回的标识符，可用于返回列表中的下一组项目。

类型：字符串

ReportPlans

报告计划了每个计划的详细信息。这些信息包括 Amazon 资源名称 (ARN)、报告计划名称、描述、设置、交付渠道、部署状态、创建时间以及报告计划上次尝试并成功运行的时间。

类型：ReportPlan 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRestoreJobs

服务： AWS Backup

返回为恢复已保存资源而 AWS Backup 启动的任务列表，包括有关恢复过程的详细信息。

请求语法

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByAccountId

列出作业的账户 ID。仅返回与指定账户 ID 关联的恢复作业。

模式：`^[0-9]{12}$`

ByCompleteAfter

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之后完成的复制作业。

ByCompleteBefore

仅返回在 Unix 格式和协调世界时 (UTC) 表示的日期之前完成的复制作业。

ByCreatedAfter

仅返回在指定日期之后创建的恢复作业。

ByCreatedBefore

仅返回在指定日期之前创建的恢复作业。

ByResourceType

包含此参数可仅返回指定资源的还原作业：

- 适用于 Amazon Aurora 的 `Aurora`
- `CloudFormation`对于 AWS CloudFormation
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 `DocumentDB`
- `DynamoDB`：表示 Amazon DynamoDB
- `EBS`：表示 Amazon Elastic Block Store

- EC2：表示 Amazon Elastic Compute Cloud
- EFS：表示 Amazon Elastic File System
- FSx：表示 Amazon FSx
- Neptune：表示 Amazon Neptune
- Redshift：表示 Amazon Redshift
- RDS：表示 Amazon Relational Database Service
- SAP HANA on Amazon EC2：表示 SAP HANA 数据库
- Storage Gateway对于 AWS Storage Gateway
- S3：表示 Amazon S3
- Timestream：表示 Amazon Timestream
- VirtualMachine：表示虚拟机

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByRestoreTestingPlanArn

这仅返回与指定资源 Amazon 资源名称（ARN）匹配的还原测试作业。

ByStatus

仅返回与指定作业状态关联的恢复作业。

有效值：PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RestoreJobs

对象数组，其中包含有关用于恢复已保存资源的作业的详细信息。

类型：RestoreJobsListMember 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRestoreJobsByProtectedResource

服务： AWS Backup

这将返回包含指定受保护资源的还原作业。

必须包括 ResourceArn。您可以选择包括 NextToken、ByStatus、MaxResults、ByRecoveryPointCreationDateAfter 和 ByRecoveryPointCreationDateBefore。

请求语法

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

ByRecoveryPointCreationDateAfter

仅返回在指定日期之后创建的恢复点的还原作业。

ByRecoveryPointCreationDateBefore

仅返回在指定日期之前创建的恢复点的还原作业。

ByStatus

仅返回与指定作业状态关联的恢复作业。

有效值：PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回项目的 MaxResults 数量，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

resourceArn

仅返回与指定资源 Amazon 资源名称 (ARN) 匹配的还原作业。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RestoreJobs

对象数组，其中包含有关用于还原已保存资源的作业的详细信息。

类型：RestoreJobsListMember 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRestoreJobSummaries

服务： AWS Backup

此请求获取最近 30 天内创建的或正在运行的还原作业的摘要。您可以添加参数 accountID、State、ResourceType、 AggregationPeriod MaxResults、 NextToken 或来筛选结果。

此请求返回包含区域、账户、州、、 RestourceType MessageCategory StartTime EndTime、和包含任务数量的摘要。

请求语法

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

AccountId

返回指定账户的作业计数。

如果请求是从成员账户或不属于 Organizations 的 AWS 账户发送的，则将返回申请者账户中的职位。

根账户、管理员和委派管理员账户可以使用值 ANY 来返回组织中每个账户中的作业计数。

AGGREGATE_ALL 汇总经过身份验证的组织内所有账户中的作业计数，然后返回总和。

模式：^[0-9]{12}$

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

有效值：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

此参数设置要返回的最大项目数。

值为整数。接受的值范围为 1 到 500。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

ResourceType

返回指定资源类型的作业计数。使用请求 GetSupportedResourceTypes 获取支持的资源类型的字符串。

值 ANY 会返回所有资源类型的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

要备份的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此参数返回具有指定状态的作业的作业计数。

值 ANY 会返回所有状态的计数。

AGGREGATE_ALL 汇总所有资源类型的作业计数并返回总和。

有效值：CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AggregationPeriod

返回结果的时间段。

- ONE_DAY-过去 14 天的每日任务数。
- SEVEN_DAYS-过去 7 天的汇总任务数。
- FOURTEEN_DAYS-过去 14 天的汇总任务数。

类型：字符串

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RestoreJobSummaries

此返回包含区域、账户、州、、 ResourceType MessageCategory StartTime EndTime、和包含任务数量的摘要。

类型：RestoreJobSummary 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRestoreTestingPlans

服务： AWS Backup

返回还原测试计划的列表。

请求语法

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
         "RestoreTestingPlanName": "string",
         "ScheduleExpression": "string",
```

```
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RestoreTestingPlans

这是返回的还原测试计划列表。

类型：RestoreTestingPlanForList 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListRestoreTestingSelections

服务： AWS Backup

返回还原测试选择的列表。可以使用 MaxResults 和 RestoreTestingPlanName 对其进行筛选。

请求语法

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

RestoreTestingPlanName

按指定的还原测试计划名称返回还原测试选择。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
```

```
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

RestoreTestingSelections

返回的与还原测试计划关联的还原测试选择。

类型：RestoreTestingSelectionForList 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListTags

服务： AWS Backup

返回分配给资源的标签，例如目标恢复点、备份计划或备份存储库。

ListTags 仅适用于支持 AWS Backup 完全管理其备份的资源类型。这些资源类型列在 “按资源划分的功能可用性” 表中。

请求语法

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

MaxResults

要返回的最大项目数量。

有效范围：最小值为 1。最大值为 1000。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

resourceArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源的类型。ListTags 的有效目标是恢复点、备份计划和备份保管库。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回项目的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的项目，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

Tags

有关标签的信息。

类型：字符串到字符串映射

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutBackupVaultAccessPolicy

服务： AWS Backup

制定一项基于资源的策略，以管理对目标备份保管库的访问权限。需要备份库名称和 JSON 格式的访问策略文档。

请求语法

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

Policy

JSON 格式的备份保管库访问策略文档。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK

- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutBackupVaultLockConfiguration

服务： AWS Backup

将 AWS Backup 文件库锁定应用于备份保管库，防止尝试删除存储在备份保管库中或在备份保管库中创建的任何恢复点。保管库锁定还可以防止尝试更新生命周期策略，该策略控制当前存储在备份保管库中的任何恢复点的保留期。如果指定，保管库锁定功能将为后续针对备份保管库的备份和复制任务强制规定最小和最大保留期。

> **Note**
>
> AWS Backup Cohasset Associates已对Vault Lock进行了评估，适用于受美国证券交易委员会17a-4、美国商品期货交易委员会和美国金融监管局法规约束的环境。有关 AWS Backup Vault Lock 与这些法规的关系的更多信息，请参阅 Cohasset Associates 合规性评估。

相关详情，请参阅 AWS Backup 保管库锁定。

请求语法

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

AWS Backup 文件库锁定配置，用于指定其保护的备份存储库的名称。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

ChangeableForDays

AWS Backup 文件库锁定配置，用于指定锁定日期之前的天数。例如，在世界标准时间 2022 年 1 月 1 日晚上 8 点将 ChangeableForDays 设置为 30 会将锁定日期设置为世界标准时间 2022 年 1 月 31 日晚上 8 点。

AWS Backup 在 Vault Lock 生效并变为不可变之前，强制执行 72 小时的冷却期。因此，您必须将 ChangeableForDays 设置为 3 或更大。

在锁定日期之前，您可以使用 DeleteBackupVaultLockConfiguration 从保管库中删除保管库锁定，或使用 PutBackupVaultLockConfiguration 更改保管库锁定配置。在锁定日期及之后，保管库锁定将变为不可变且无法更改或删除。

如果未指定此参数，您可以使用 DeleteBackupVaultLockConfiguration 从保管库中删除保管库锁定，或者使用 PutBackupVaultLockConfiguration 随时更改保管库锁定配置。

类型：长整型

必需：否

MaxRetentionDays

AWS Backup 文件库锁定配置，用于指定保管库保留其恢复点的最大保留期。例如，如果贵企业的策略要求您在某些数据保留四年（1460 天）后将其销毁，则此设置非常有用。

如果不包括此参数，则保管库锁定不会对保管库中的恢复点强制规定最长保留期。如果包含此参数但没有值，保管库锁定将不会强制规定最长保留期。

如果指定了此参数，则保管库的任何备份或复制作业都必须具有生命周期策略，其保留期等于或小于最长保留期。如果作业的保留期长于该最长保留期，则保管库将无法执行该备份或复制作业，因此您应该修改生命周期设置或使用其他保管库。您可以指定的最长保留期为 36500 天（大约 100 年）。保管库锁定之前已保存在保管库中的恢复点不受影响。

类型：长整型

必需：否

MinRetentionDays

AWS Backup 文件库锁定配置，用于指定保管库保留其恢复点的最短保留期。例如，如果贵企业的策略要求您将某些数据至少保留七年（2555 天），则此设置非常有用。

通过创建文件库锁时，此参数是必需的 AWS CloudFormation；否则，此参数是可选的。如果未指定此参数，保管库锁定将不会强制规定最短保留期。

如果指定了此参数，则保管库的任何备份或复制作业都必须具有生命周期策略，其保留期等于或大于最短保留期。如果作业的保留期短于该最短保留期，则保管库将无法执行该备份或复制作业，因此您应该修改生命周期设置或使用其他保管库。您可以指定的最短保留期为 1 天。保管库锁定之前已保存在保管库中的恢复点不受影响。

类型：长整型

必需：否

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutBackupVaultNotifications

服务： AWS Backup

开启有关备份保管库的通知，以了解指定主题和事件。

请求语法

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

BackupVaultEvents

一个事件数组，指示将资源备份到备份保管库的作业状态。

有关常见用例和代码示例，请参阅使用 Amazon SNS 跟踪 AWS Backup 事件。

支持以下事件：

- BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED
- COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED

- RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED
- S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

> **Note**
>
> 以下列表包括支持的事件和不再使用的已弃用事件（供参考）。已弃用的事件不会返回状态或通知。有关支持的事件，请参阅上面的列表。

类型：字符串数组

有效值：BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

必需：是

SNSTopicArn

指定备份保管库事件主题的 Amazon 资源名称 (ARN)；例如，。arn:aws:sns:us-west-2:111122223333:MyVaultTopic

类型：字符串

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutRestoreValidationResult

服务： AWS Backup

此请求允许您发送单独的自运行还原测试验证结果。RestoreJobId 和 ValidationStatus 是必需项。或者，您可以输入 ValidationStatusMessage。

请求语法

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

restoreJobId

这是其中还原任务的唯一标识符 AWS Backup。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

ValidationStatus

您的还原验证状态。

类型：字符串

有效值：FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

必需：是

ValidationStatusMessage

这是一个可选的消息字符串，您可以输入它来描述还原测试验证的验证状态。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 204
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartBackupJob

服务： AWS Backup

针对指定资源启动按需备份作业。

请求语法

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

BackupOptions

所选资源的备份选项。此选项仅适用于 Windows 卷影复制服务 (VSS) 备份作业。

有效值：设置为 "WindowsVSS":"enabled" 以启用 WindowsVSS 备份选项并创建 Windows VSS 备份。设置为 "WindowsVSS""disabled" 可创建常规备份。此 WindowsVSS 选项默认处于启用状态。

类型：字符串到字符串映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

CompleteWindowMinutes

一个以分钟为单位的值，在此期间，成功启动的备份必须完成，否则 AWS Backup 将取消该备份作业。该值为可选项。该值从计划备份时开始倒计时。如果备份的开始时间晚于计划时间，也不会为 StartWindowMinutes 额外增加时间。

比如 StartWindowMinutes，此参数的最大值为 100 年（52,560,000 分钟）。

类型：长整型

必需：否

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

必需：是

IdempotencyToken

客户选择的字符串，可用于区分对 StartBackupJob 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

Lifecycle

生命周期定义了受保护资源何时过渡到冷存储以及何时过期。 AWS Backup 将根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

此参数的最大值为 100 年（36,500 天）。

类型：Lifecycle 对象

必需：否

RecoveryPointTags

要分配给资源的标签。

类型：字符串到字符串映射

必需：否

ResourceArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：是

StartWindowMinutes

一个时间值（以分钟为单位），用于指定在安排了备份之后，必须在多长时间内成功启动作业，否则将会被取消。这是可选值，默认值为 8 小时。如果包含此值，则必须至少为 60 分钟才能避免错误。

此参数的最大值为 100 年（52,560,000 分钟）。

在启动时段内，备份作业的状态将保持 CREATED 状态，直到成功启动或启动时段结束为止。如果在启动窗口内 AWS Backup 收到允许重试作业的错误消息， AWS Backup 则至少每 10 分钟自动重试一次以开始作业，直到备份成功开始（任务状态更改为RUNNING）或任务状态更改为EXPIRED（预计在启动窗口时间结束时发生）。

类型：长整型

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupJobId

唯一标识 AWS Backup 对的资源备份请求。

类型：字符串

CreationDate

备份作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

IsParent

这是一个返回的布尔值，表示这是父（复合）备份作业。

类型：布尔值

RecoveryPointArn

注意：此字段仅针对 Amazon EFS 和高级 DynamoDB 资源返回相应的值。

唯一标识恢复点的 ARN；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartCopyJob

服务： AWS Backup

启动任务以创建指定资源的一次性副本。

不支持连续备份。

请求语法

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

DestinationBackupVaultArn

唯一标识要复制到的目的地备份保管库的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`。

类型：字符串

必需：是

IamRoleArn

指定用于复制目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access

类型：字符串

必需：是

IdempotencyToken

客户选择的字符串，可用于区分对 StartCopyJob 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

Lifecycle

指定恢复点过渡到冷存储或被删除之前的时间段（以天为单位）。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，在主机上，保留期设置必须比在几天后过渡到冷藏设置长 90 天。将备份转换为冷备份后，无法更改天后过渡到冷的设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

要删除现有的生命周期和保留期并无限期保留恢复点，请为和指定 MoveToColdStorageAfterDays -1。DeleteAfterDays

类型：Lifecycle 对象

必需：否

RecoveryPointArn

一个唯一标识用于复制作业的恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

必需：是

SourceBackupVaultName

用于存储备份的逻辑源容器的名称。Backup 存储库由用于创建备份存储库的账户和创建备份存储库的 AWS 区域所特有的名称进行标识。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CopyJobId

唯一标识复制作业。

类型：字符串

CreationDate

复制作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

IsParent

这是一个返回的布尔值，表示这是父（复合）复制作业。

类型：布尔值

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartReportJob

服务： AWS Backup

为指定的报告计划启动按需报告作业。

请求语法

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

reportPlanName

报告计划的唯一名称。

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

IdempotencyToken

客户选择的字符串，可用于区分对 `StartReportJobInput` 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ReportJobId

报告作业的标识符。唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑报告作业 ID。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartRestoreJob

服务： AWS Backup

恢复由 Amazon 资源名称 (ARN) 标识的已保存资源。

请求语法

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

CopySourceTagsToRestoredResource

此参数为可选参数。如果此值等于 `True`，则备份中包含的标签将被复制到已还原的资源中。

这只能应用于通过创建的备份 AWS Backup。

类型：布尔值

必需：否

IamRoleArn

AWS Backup 用于创建目标资源的 IAM 角色的亚马逊资源名称 (ARN)；例如：。`arn:aws:iam::123456789012:role/S3Access`

类型：字符串

必需：否

IdempotencyToken

客户选择的字符串，可用于区分对 StartRestoreJob 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

Metadata

一组元数据键值对。

您可以通过调用 GetRecoveryPointRestoreMetadata 来获取在备份资源时有关该资源的配置元数据。但是，除了 GetRecoveryPointRestoreMetadata 提供的值之外，可能还需要其他值才能还原资源。例如，如果原始资源名称已存在，您可能需要提供一个新的资源名称。

有关每种资源的元数据的更多信息，请参阅以下内容：

- 亚马逊 Aurora 的元数据
- 亚马逊 DocumentDB 的元数据
- 的元数据 AWS CloudFormation
- 亚马逊 DynamoDB 的元数据
- 亚马逊 EBS 的元数据
- 亚马逊 EC2 的元数据
- 亚马逊 EFS 的元数据
- 亚马逊 FSx 的元数据
- 亚马逊 Neptune 的元数据
- Amazon RDS 的元数据
- 亚马逊 Redshift 的元数据
- 的元数据 AWS Storage Gateway
- 亚马逊 S3 的元数据
- 亚马逊 Timestream 的元数据

- 虚拟机的元数据

类型：字符串到字符串映射

必需：是

RecoveryPointArn

唯一标识恢复点的 ARN；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

类型：字符串

必需：是

ResourceType

启动作业，恢复以下资源之一的恢复点：

- `Aurora`-亚马逊 Aurora
- `DocumentDB`-亚马逊 DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`-亚马逊 DynamoDB
- `EBS`-亚马逊 Elastic Block
- `EC2`-Amazon 弹性计算云
- `EFS`-亚马逊 Elastic File System
- `FSx`-亚马逊 FSx
- `Neptune`-亚马逊 Neptune
- `RDS`-亚马逊 Relational Database Service
- `Redshift`-亚马逊 Redshift
- `Storage Gateway` - AWS Storage Gateway
- `S3`-Amazon 简单存储服务
- `Timestream`-亚马逊 Timestream
- `VirtualMachine`-虚拟机

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

RestoreJobId

唯一标识还原恢复点的作业。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StopBackupJob

服务： AWS Backup

尝试取消作业以创建资源的一次性备份。

以下服务不支持此操作：适用于 Windows 文件服务器的亚马逊 FSx、适用于 Lustre 的亚马逊 FSx、适用于 ONTAP 的亚马逊 FSx、适用于 OpenZFS 的亚马逊 FS NetApp x、亚马逊 DocumentDB（兼容 MongoDB）、亚马逊 RDS、亚马逊 Aurora 和亚马逊 Neptune。

请求语法

```
POST /backup-jobs/backupJobId HTTP/1.1
```

URI 请求参数

请求使用以下 URI 参数。

backupJobId

唯一标识 AWS Backup 对的资源备份请求。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

TagResource

服务： AWS Backup

将一组键值对分配给由 Amazon 资源名称 (ARN) 标识的恢复点、备份计划或备份保管库。

此 API 支持资源类型的恢复点，包括 Aurora、Amazon DocumentDB。亚马逊 EBS、亚马逊 FSx、Neptune 和亚马逊 RDS。

请求语法

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

resourceArn

唯一标识资源的 ARN。ARN 的格式取决于标记资源的类型。

不包含的 ARN 与标记backup不兼容。 TagResourceUntagResource而且 ARN 无效将导致错误。可接受的 ARN 内容可以包括。arn:aws:backup:us-east无效的 ARN 内容可能看起来像。arn:aws:ec2:us-east

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

Tags

用于帮助组织您的资源的键值对。您可以将自己的元数据分配给所创建的资源。为了清楚起见，这里提供了分配标签的结构：[{"Key":"string","Value":"string"}]。

类型：字符串到字符串映射

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UntagResource

服务： AWS Backup

从恢复点、备份计划或由 Amazon 资源名称 (ARN) 标识的备份保管库中删除一组键值对

包括 Aurora、Amazon DocumentDB 在内的资源类型的恢复点不支持此 API。亚马逊 EBS、亚马逊 FSx、Neptune 和亚马逊 RDS。

请求语法

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

URI 请求参数

请求使用以下 URI 参数。

resourceArn

唯一标识资源的 ARN。ARN 的格式取决于标记资源的类型。

不包含的 ARN 与标记backup不兼容。 TagResourceUntagResource而且 ARN 无效将导致错误。可接受的 ARN 内容可以包括。arn:aws:backup:us-east无效的 ARN 内容可能看起来像。arn:aws:ec2:us-east

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

TagKeyList

用于标识要从资源中移除哪些键值标签的密钥。

类型：字符串数组

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK

- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateBackupPlan

服务： AWS Backup

更新指定的备份计划。新版本通过其 ID 进行唯一标识。

请求语法

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
```

```
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

backupPlanId

备份计划的 ID。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

BackupPlan

备份计划的正文。包括 BackupPlanName 和一组或多组 Rules。

类型：BackupPlanInput 对象

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
```

```
        },
        "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AdvancedBackupSettings

包含每种资源的 BackupOptions 列表。

类型：AdvancedBackupSetting 对象数组

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

类型：字符串

BackupPlanId

唯一标识备份计划。

类型：字符串

CreationDate

创建备份计划的日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑版本 ID。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3

- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateFramework

服务： AWS Backup

更新指定的框架。

请求语法

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

URI 请求参数

请求使用以下 URI 参数。

frameworkName

框架的唯一名称。此名称的长度介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

长度约束：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

FrameworkControls

构成框架的控件。列表中的每个控件都有名称、输入参数和范围。

类型：FrameworkControl 对象数组

必需：否

FrameworkDescription

框架的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：.*\S.*

必需：否

IdempotencyToken

客户选择的字符串，可用于区分对 UpdateFrameworkInput 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

框架的创建日期和时间，以 ISO 8601 表示。CreationTime 的值精确到毫秒。例如，2020-07-10T15:00:00.000-08:00 表示 2020 年 7 月 10 日下午 3:00，比 UTC 晚 8 个小时。

类型：时间戳

FrameworkArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

FrameworkName

框架的唯一名称。此名称的长度介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AlreadyExistsException

所需的资源已存在。

HTTP 状态代码：400

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

LimitExceededException

已超过请求中的限制；例如，请求中允许的最大项目数。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK

- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateGlobalSettings

服务： AWS Backup

更新 AWS 账户是否已选择使用跨账户备份。如果该账户不是 Organizations 管理账户，则返回错误。使用 `DescribeGlobalSettings` API 来确定当前设置。

请求语法

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

GlobalSettings

`isCrossAccountBackupEnabled` 的值和区域。示例：`update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`。

类型：字符串到字符串映射

必需：否

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateRecoveryPointLifecycle

服务： AWS Backup

设置恢复点的转换生命周期。

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

此操作不支持连续备份。

请求语法

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

backupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：是

recoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

类型：Lifecycle 对象

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
```

```
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BackupVaultArn

唯一标识备份保管库的 ARN；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

CalculatedLifecycle

包含 DeleteAt 和 MoveToColdStorageAt 时间戳的 CalculatedLifecycle 对象。

类型：CalculatedLifecycle 对象

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

类型：Lifecycle 对象

RecoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

InvalidRequestException

表示请求的输入有问题。例如，参数的类型错误。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

UpdateRegionSettings

服务： AWS Backup

更新区域当前选择加入服务设置。

使用 `DescribeRegionSettings` API 确定支持的资源类型。

请求语法

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

ResourceTypeManagementPreference

启用或禁用对资源类型的备份的完全 AWS Backup 管理。要启用 DynamoDB 的全面 AWS Backup 管理以及AWS Backup高级 DynamoDB 备份功能，请按照程序以编程方式启用高级 DynamoDB 备份。

类型：字符串到布尔映射

密钥模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

ResourceTypeOptInPreference

更新服务列表以及该区域的选择加入偏好。

如果资源分配仅基于标签，将应用“选择加入服务”设置。如果为备份计划明确分配了资源类型，例如 Amazon S3、Amazon EC2 或 Amazon RDS，那么即使该特定服务未启用选择加入功能，该资源类型也将包含在备份中。如果在资源分配中同时指定了资源类型和标签，则备份计划中指定的资源类型优先于标签条件。在这种情况下，“选择加入服务”设置将被忽略。

类型：字符串到布尔映射

密钥模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateReportPlan

服务： AWS Backup

更新指定的报告计划。

请求语法

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

reportPlanName

报告计划的唯一名称。此名称的长度介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

长度约束：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

IdempotencyToken

客户选择的字符串，可用于区分对 UpdateReportPlanInput 的其他相同调用。使用相同的幂等性令牌重试成功的请求会生成一条成功消息，而不执行任何操作。

类型：字符串

必需：否

ReportDeliveryChannel

有关将报告投递到何处的信息，特别是您的 Amazon S3 存储桶名称、S3 key prefix 和报告格式。

类型：ReportDeliveryChannel 对象

必需：否

ReportPlanDescription

报告计划的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：.*\S.*

必需：否

ReportSetting

报告的报告模板。报告使用报告模板构建。报告模板包括：

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

如果报告模板为RESOURCE_COMPLIANCE_REPORT或CONTROL_COMPLIANCE_REPORT，则此 API 资源还描述了 AWS 区域 和框架的报告覆盖范围。

类型：ReportSetting 对象

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

报告计划的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

ReportPlanArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

ReportPlanName

报告计划的唯一名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

错误

有关所有操作的常见错误信息，请参阅常见错误。

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

UpdateRestoreTestingPlan

服务： AWS Backup

此请求将发送对您指定的还原测试计划的更改。RestoreTestingPlanName 一经创建便无法更新。

RecoveryPointSelection 可以包含：

- Algorithm
- ExcludeVaults
- IncludeVaults
- RecoveryPointTypes
- SelectionWindowDays

请求语法

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

还原测试计划名称的名称。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

RestoreTestingPlan

指定还原测试计划的正文。

类型：RestoreTestingPlanForUpdate 对象

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

资源测试计划的创建时间。

类型：时间戳

RestoreTestingPlanArn

还原测试计划的唯一 ARN（Amazon 资源名称）。

类型：字符串

RestoreTestingPlanName

名称一经创建便无法更改。名称只能包含字母数字字符和下划线。最大长度为 50。

类型：字符串

UpdateTime

还原测试计划的更新完成时间。

类型：时间戳

错误

有关所有操作的常见错误信息，请参阅常见错误。

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateRestoreTestingSelection

服务： AWS Backup

更新指定的还原测试选项。

通过此请求可以更新除 RestoreTestingSelectionName 外的大多数元素。

您可以同时使用受保护的资源 ARN 或条件，但不能同时使用两者。

请求语法

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

URI 请求参数

请求使用以下 URI 参数。

RestoreTestingPlanName

更新指定的测试计划需要使用还原测试计划名称。

必需：是

RestoreTestingSelectionName

您要更新的还原测试选择的必需恢复测试选择的名称。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

RestoreTestingSelection

要更新您的还原测试选择，您可以使用受保护的资源 ARN 或条件，但不能同时使用这两者。也就是说，如果您的选项具有 ProtectedResourceArns，则使用参数 ProtectedResourceConditions 请求更新将会失败。

类型：RestoreTestingSelectionForUpdate 对象

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

CreationTime

成功更新资源测试选择的时间。

类型：时间戳

RestoreTestingPlanArn

唯一的字符串，即还原测试计划的名称。

类型：字符串

RestoreTestingPlanName

与更新的还原测试选择相关联的恢复测试计划。

类型：字符串

RestoreTestingSelectionName

返回的恢复测试选择名称。

类型：字符串

UpdateTime

还原测试选项的更新完成时间。

类型：时间戳

错误

有关所有操作的常见错误信息，请参阅常见错误。

ConflictException

AWS Backup 在完成前一个操作之前，无法执行你请求的操作。请稍后重试。

HTTP 状态代码：400

InvalidParameterValueException

表示参数的值有问题。例如，该值超出了范围。

HTTP 状态代码：400

MissingParameterValueException

表示缺少必需的参数。

HTTP 状态代码：400

ResourceNotFoundException

该操作所需的资源不存在。

HTTP 状态代码：400

ServiceUnavailableException

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：500

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

AWS Backup gateway

AWS Backup gateway 支持以下操作：

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway

- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

服务： AWS Backup gateway

将备份网关与您的服务器关联。完成关联流程后，您可以通过网关备份和还原虚拟机。

请求语法

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用ListGateways操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必需：是

ServerArn

托管虚拟机的服务器的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CreateGateway

服务： AWS Backup gateway

创建备份网关。创建网关后，您可以通过 AssociateGatewayToServer 操作将其与服务器关联。

请求语法

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

ActivationKey

已创建网关的激活密钥。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

模式：^[0-9a-zA-Z\-]+$

必需：是

GatewayDisplayName

已创建网关的显示名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[a-zA-Z0-9-]*$

必需：是

GatewayType

已创建网关的类型。

类型：字符串

有效值：BACKUP_VM

必需：是

Tags

分配给网关的最多 50 个标签的列表。每个标签都是一个键-值对。

类型：Tag 对象数组

必需：否

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您创建的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteGateway

服务： AWS Backup gateway

删除备份网关。

请求语法

```
{
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

要删除的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您已删除的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteHypervisor

服务： AWS Backup gateway

删除管理程序。

请求语法

```
{
   "HypervisorArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

要删除的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "HypervisorArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

您已删除的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

由于您的权限不足，操作无法继续。

HTTP 状态代码：400

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DisassociateGatewayFromServer

服务： AWS Backup gateway

解除备份网关与指定服务器的关联。解除关联过程完成后，网关将无法再访问服务器上的虚拟机。

请求语法

```
{
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

要解除关联的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您已解除关联的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetBandwidthRateLimitSchedule

服务： AWS Backup gateway

检索指定网关的带宽速率限制计划。默认情况下，网关没有带宽速率限制计划，这意味着没有有效的带宽速率限制。使用该参数可获取网关的带宽速率限制计划。

请求语法

```
{
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用ListGateways操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
```

```
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

BandwidthRateLimitIntervals

包含网关带宽速率限制计划间隔的数组。如果没有安排带宽速率限制间隔，则该数组为空。

类型：BandwidthRateLimitInterval 对象数组

数组成员：最少 0 个物品。最多 20 个项目。

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用ListGateways操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetGateway

服务： AWS Backup gateway

通过提供 ARN（Amazon 资源名称），此 API 将返回网关。

请求语法

```
{
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
         "DayOfWeek": number,
```

```
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Gateway

通过提供 ARN（Amazon 资源名称），此 API 将返回网关。

类型：GatewayDetails 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetHypervisor

服务： AWS Backup gateway

此操作请求有关网关将要连接到的指定管理程序的信息。管理程序是用于创建和管理虚拟机并为其分配资源的硬件、软件或固件。

请求语法

```
{
   "HypervisorArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
      "LatestMetadataSyncStatusMessage": "string",
      "LogGroupArn": "string",
```

```
        "Name": "string",
        "State": "string"
    }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Hypervisor

有关请求的管理程序的详细信息。

类型：HypervisorDetails 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetHypervisorPropertyMappings

服务： AWS Backup gateway

此操作检索指定管理程序的属性映射。虚拟机管理程序属性映射显示虚拟机管理程序中可用的实体属性与中可用属性的关系。 AWS

请求语法

```
{
   "HypervisorArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
```

```
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

IAM 角色的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 20。最大长度为 2048。

模式：`^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

这显示了 VMware 标签与 AWS 标签的映射。

类型：VmwareToAwsTagMapping 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetVirtualMachine

服务： AWS Backup gateway

通过提供 ARN（Amazon 资源名称），此 API 将返回虚拟机。

请求语法

```
{
   "ResourceArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

ResourceArn

虚拟机的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
         {
```

```
            "VmwareCategory": "string",
            "VmwareTagDescription": "string",
            "VmwareTagName": "string"
         }
      ]
   }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

VirtualMachine

此对象包含 GetVirtualMachine 的输出所含的 VirtualMachine 的基本属性

类型：VirtualMachineDetails 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ImportHypervisorConfiguration

服务： AWS Backup gateway

通过导入管理程序的配置来连接管理程序。

请求语法

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

Host

管理程序的服务器主机。这可以是 IP 地址或完全限定域名 (FQDN)。

类型：字符串

长度约束：最小长度为 3。长度上限为 128。

模式：^.+$

必需：是

KmsKeyArn

AWS Key Management Service 适用于虚拟机管理程序。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必需：否

Name

管理程序的名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：是

Password

管理程序的密码。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[ -~]+$`

必需：否

Tags

要导入的管理程序配置的标签。

类型：Tag 对象数组

必需：否

Username

管理程序的用户名。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必需：否

响应语法

```
{
   "HypervisorArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

您已解除关联的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

由于您的权限不足，操作无法继续。

HTTP 状态代码：400

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListGateways

服务： AWS Backup gateway

列出中由拥有 AWS 账户 的备份网关 AWS 区域。返回的列表是按网关 Amazon 资源名称 (ARN) 排序的。

请求语法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

MaxResults

要列出的网关的最大数量。

类型：整数

有效范围：最小值为 1。

必需：否

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 MaxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

必需：否

响应语法

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Gateways

您的网关列表。

类型：Gateway 对象数组

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 maxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListHypervisors

服务： AWS Backup gateway

列出您的管理程序。

请求语法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

MaxResults

要列出的管理程序的最大数量。

类型：整数

有效范围：最小值为 1。

必需：否

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 maxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

必需：否

响应语法

```
{
```

```
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Hypervisors

您的 Hypervisor 对象的列表，按其 Amazon 资源名称 (ARN) 排序。

类型：Hypervisor 对象数组

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 maxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListTagsForResource

服务： AWS Backup gateway

列出应用于由其 Amazon 资源名称 (ARN) 标识的资源的标记。

请求语法

```
{
   "ResourceArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

ResourceArn

要列出的资源标记的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ResourceArn

您已列出的资源标记的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

资源标记列表。

类型：Tag 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListVirtualMachines

服务： AWS Backup gateway

列出您的虚拟机。

请求语法

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

连接到虚拟机的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

MaxResults

要列出的最大虚拟机数量。

类型：整数

有效范围：最小值为 1。

必需：否

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 maxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

必需：否

响应语法

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

所返回资源的部分列表的后续下一个项目。例如，如果请求返回 maxResults 数量的资源，则 NextToken 允许您从下一个令牌指向的位置开始返回列表中的更多项目。

类型：字符串

长度限制：长度下限为 1。最大长度为 1000。

模式：^.+$

VirtualMachines

您的 VirtualMachine 对象的列表，按其 Amazon 资源名称 (ARN) 排序。

类型：VirtualMachine 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3

- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutBandwidthRateLimitSchedule

服务： AWS Backup gateway

此操作为指定网关设置带宽速率限制计划。默认情况下，网关没有带宽速率限制计划，这意味着没有有效的带宽速率限制。使用此操作可启动网关的带宽速率限制计划。

请求语法

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

BandwidthRateLimitIntervals

包含网关带宽速率限制计划间隔的数组。如果没有安排带宽速率限制间隔，则该数组为空。

类型：BandwidthRateLimitInterval 对象数组

数组成员：最少 0 个物品。最多 20 个项目。

必需：是

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用ListGateways操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用ListGateways操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutHypervisorPropertyMappings

服务： AWS Backup gateway

此操作设置指定管理程序的属性映射。虚拟机管理程序属性映射显示虚拟机管理程序中可用的实体属性与中可用属性的关系。 AWS

请求语法

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

IamRoleArn

IAM 角色的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 20。最大长度为 2048。

模式：^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$

必需：是

VmwareToAwsTagMappings

此操作请求将 VMware 标记映射到 AWS 标记。

类型：VmwareToAwsTagMapping 对象数组

必需：是

响应语法

```
{
   "HypervisorArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

由于您的权限不足，操作无法继续。

HTTP 状态代码：400

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK

- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

PutMaintenanceStartTime

服务： AWS Backup gateway

设置网关的维护开始时间。

请求语法

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

DayOfMonth

当月的某一天开始对网关进行维护。

有效值范围为 Sunday 至 Saturday。

类型：整数

有效范围：最小值为 1。最大值为 31。

必需：否

DayOfWeek

一周中的某一天开始对网关进行维护。

类型：整数

有效范围：最小值为 0。最大值为 6。

必需：否

GatewayArn

网关的 Amazon 资源名称 (ARN)，用于指定其维护开始时间。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

HourOfDay

一天中的某个时间开始维护网关。

类型：整数

有效范围：最小值为 0。最大值为 23。

必需：是

MinuteOfHour

一小时中的某个分钟点开始对网关进行维护。

类型：整数

有效范围：最小值为 0。最大值为 59。

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您设置维护开始时间的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartVirtualMachinesMetadataSync

服务： AWS Backup gateway

此操作会发送在指定虚拟机之间同步元数据的请求。

请求语法

```
{
   "HypervisorArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "HypervisorArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

由于您的权限不足，操作无法继续。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

TagResource

服务： AWS Backup gateway

标记资源。

请求语法

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

ResourceARN

要标记的资源的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

Tags

分配给资源的标签列表。

类型：Tag 对象数组

必需：是

响应语法

```
{
   "ResourceARN": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ResourceARN

您已标记的资源的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

TestHypervisorConfiguration

服务： AWS Backup gateway

测试您的管理程序配置，以验证备份网关是否可以连接该管理程序及其资源。

请求语法

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

要测试的管理程序网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

Host

管理程序的服务器主机。这可以是 IP 地址或完全限定域名 (FQDN)。

类型：字符串

长度约束：最小长度为 3。长度上限为 128。

模式：`^.+$`

必需：是

Password

管理程序的密码。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[-~]+$

必需：否

Username

管理程序的用户名。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必需：否

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UntagResource

服务： AWS Backup gateway

删除资源标签。

请求语法

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

ResourceARN

要删除其标签的资源的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

TagKeys

指定要删除标签的标签密钥列表。

类型：字符串数组

长度约束：最小长度为 1。长度上限为 128。

模式：`^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必需：是

响应语法

```
{
   "ResourceARN": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

ResourceARN

您已删除标签的资源的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateGatewayInformation

服务： AWS Backup gateway

更新网关的名称。指定要在请求中使用网关的 Amazon 资源名称 (ARN) 更新哪个网关。

请求语法

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

要更新的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

GatewayDisplayName

更新后的网关显示名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您已更新的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateGatewaySoftwareNow

服务： AWS Backup gateway

更新网关虚拟机 (VM) 软件。该请求会立即触发软件更新。

> **Note**
>
> 您在发出此请求时会立即收到 200 OK 成功响应。但是，可能需要一段时间才能完成更新。

请求语法

```
{
   "GatewayArn": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

GatewayArn

要更新的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：是

响应语法

```
{
   "GatewayArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

GatewayArn

您已更新的网关的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateHypervisor

服务： AWS Backup gateway

更新管理程序元数据，包括其主机、用户名和密码。指定要在请求中使用管理程序的 Amazon 资源名称 (ARN) 来更新哪个管理程序。

请求语法

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

请求参数

有关所有操作的通用参数的信息，请参阅通用参数。

请求接受采用 JSON 格式的以下数据。

Host

更新后的管理程序的主机。这可以是 IP 地址或完全限定域名 (FQDN)。

类型：字符串

长度约束：最小长度为 3。长度上限为 128。

模式：^.+$

必需：否

HypervisorArn

要更新的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必需：是

LogGroupArn

请求日志中网关组的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 0。最大长度为 2048。

模式：^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:*$

必需：否

Name

更新后的管理程序名称

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[a-zA-Z0-9-]*$

必需：否

Password

更新后的管理程序密码。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[-~]+$

必需：否

Username

更新后的管理程序用户名。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

必需：否

响应语法

```
{
   "HypervisorArn": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

HypervisorArn

您已更新的管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

由于您的权限不足，操作无法继续。

HTTP 状态代码：400

ConflictException

由于不支持该操作，因此无法继续操作。

HTTP 状态代码：400

InternalServerException

由于出现内部错误，因此操作未成功。请稍后重试。

HTTP 状态代码：500

ResourceNotFoundException

未找到该操作所需的资源。

HTTP 状态代码：400

ThrottlingException

TPS 已被限制为防止故意或无意的高请求量。

HTTP 状态代码：400

ValidationException

由于出现验证错误，因此操作未成功。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go v2 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

数据类型

AWS Backup 支持以下数据类型：

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue

- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AWS Backup gateway 支持以下数据类型：

- BandwidthRateLimitInterval
- Gateway

- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

AWS Backup 支持以下数据类型：

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope

- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate

- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

服务： AWS Backup

每种资源类型的备份选项。

目录

BackupOptions

为所选资源指定备份选项。此选项仅适用于 Windows VSS 备份作业。

有效值：

设置为 "WindowsVSS":"enabled" 可启用 WindowsVSS 备份选项并创建 Windows VSS 备份。

设置为 "WindowsVSS":"disabled" 可创建常规备份。此 WindowsVSS 选项默认处于启用状态。

如果您指定的选项无效，则会出现 InvalidParameterValueException 异常。

有关 Windows VSS 备份的更多信息，请参阅创建启用 VSS 的 Windows 备份。

类型：字符串到字符串映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

ResourceType

指定包含资源类型和备份选项的对象。唯一支持的资源类型是带有 Windows 卷影复制服务 (VSS) 的 Amazon EC2 实例。有关 CloudFormation 示例，请参阅《 AWS Backup 用户指南》中启用 Windows VSS 的示例 CloudFormation 模板。

有效值：EC2。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupJob

服务： AWS Backup

包含有关备份作业的详细信息。

内容

AccountId

拥有备份作业的账户 ID。

类型：字符串

模式：^[0-9]{12}$

必需：否

BackupJobId

唯一标识 AWS Backup 对的资源备份请求。

类型：字符串

必需：否

BackupOptions

为所选资源指定备份选项。此选项仅适用于 Windows 卷影复制服务 (VSS) 备份作业。

有效值：设置为 "WindowsVSS":"enabled" 以启用 WindowsVSS 备份选项并创建 Windows VSS 备份。设置为 "WindowsVSS":"disabled" 可创建常规备份。如果您指定的选项无效，则会出现 InvalidParameterValueException 异常。

类型：字符串到字符串映射

键模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

BackupSizeInBytes

备份的大小（以字节为单位）。

类型：长整型

必需：否

BackupType

表示备份作业的备份类型。

类型：字符串

必需：否

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

必需：否

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：否

BytesTransferred

查询作业状态时传输到备份保管库的大小（以字节为单位）。

类型：长整型

必需：否

CompletionDate

创建备份作业的作业完成的日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreatedBy

包含有关创建备份作业的标识信息，包括用于创建该作业的备份计划的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

类型：RecoveryPointCreator 对象

必需：否

CreationDate

创建备份作业的日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

ExpectedCompletionDate

备份资源的作业预计完成的日期和时间，采用 Unix 格式和协调世界时 (UTC)。ExpectedCompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN。除默认角色之外的 IAM 角色必须在角色名称中包含 AWSBackup 或 AwsBackup。例如，arn:aws:iam::123456789012:role/AWSBackupRDSAccess。如果没有这些字符串，角色名称将缺少执行备份作业的权限。

类型：字符串

必需：否

InitiationDate

启动备份任务的日期。

类型：时间戳

必需：否

IsParent

这是一个布尔值，表示这是父（复合）备份作业。

类型：布尔值

必需：否

MessageCategory

此参数是指定消息类别的作业计数。

例如，字符串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 INVALIDPARAMETERS。有关 MessageCategory 字符串列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

类型：字符串

必需：否

ParentJobId

它唯一地标识向 AWS Backup 发出的备份资源请求。返回的将是父（复合）作业 ID。

类型：字符串

必需：否

PercentDone

包含查询作业状态时作业完成的估计百分比。

类型：字符串

必需：否

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

必需：否

ResourceArn

唯一标识资源的 ARN。ARN 的格式取决于资源类型。

类型：字符串

必需：否

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

必需：否

ResourceType

要备份的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。对于 Windows 卷影复制服务 (VSS) 备份，唯一支持的资源类型是 Amazon EC2。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

StartBy

采用 Unix 格式和协调世界时 (UTC)，指定备份作业必须在取消改作业之前多久启动。该值通过将启动时段与计划时间相加进行计算。因此，如果计划时间为下午 6:00，启动时段为 2 小时，则 `StartBy` 时间为指定日期的晚上 8:00。`StartBy` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

State

备份作业的当前状态。

类型：字符串

有效值：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

必需：否

StatusMessage

一条详细消息，解释备份资源作业的状态。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupJobSummary

服务： AWS Backup

此请求提供最近 30 天内创建的或正在运行的作业的摘要。

返回的摘要可能包含以下内容：区域、账户、州 RestourceType MessageCategory、 StartTime、EndTime、和包含的任务数量。

内容

AccountId

拥有摘要中作业的账户 ID。

类型：字符串

模式：`^[0-9]{12}$`

必需：否

Count

该值以作业数量的形式显示在作业摘要中。

类型：整数

必需：否

EndTime

以数字格式表示的作业结束时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

MessageCategory

此参数是指定消息类别的作业计数。

示例字符串包括 `AccessDenied`、`Success` 和 `InvalidParameters`。有关 MessageCategory 字符串列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

类型：字符串

必需：否

Region

工作摘要中的 AWS 区域。

类型：字符串

必需：否

ResourceType

此值是指定的资源类型的作业计数。请求 GetSupportedResourceTypes 返回支持的资源类型的字符串。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

StartTime

以数字格式表示的作业开始时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

State

此值是处于指定状态的作业的计数。

类型：字符串

有效值：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupPlan

服务： AWS Backup

包含可选的备份计划显示名称和 `BackupRule` 对象数组，每个对象均指定一个备份规则。备份计划中的每个规则都是一个单独的计划任务，可以备份不同的 AWS 资源选择。

内容

BackupPlanName

备份计划的显示名称。必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：是

Rules

`BackupRule` 对象的数组，其中每个对象指定用于备份所选资源的计划的任务。

类型：BackupRule 对象数组

必需：是

AdvancedBackupSettings

包含每种资源的 `BackupOptions` 列表。

类型：AdvancedBackupSetting 对象数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupPlanInput

服务： AWS Backup

包含可选的备份计划显示名称和 `BackupRule` 对象数组，每个对象均指定一个备份规则。备份计划中的每个规则都是一个单独的计划任务。

内容

BackupPlanName

备份计划的显示名称。必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：是

Rules

`BackupRule` 对象的数组，其中每个对象指定用于备份所选资源的计划的任务。

类型：BackupRuleInput 对象数组

必需：是

AdvancedBackupSettings

指定每种资源类型的 `BackupOptions` 列表。这些设置仅适用于 Windows 卷影复制服务 (VSS) 备份作业。

类型：AdvancedBackupSetting 对象数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupPlansListMember

服务： AWS Backup

包含备份计划相关的元数据。

内容

AdvancedBackupSettings

包含资源类型的 `BackupOptions` 列表。

类型：AdvancedBackupSetting 对象数组

必需：否

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`。

类型：字符串

必需：否

BackupPlanId

唯一标识备份计划。

类型：字符串

必需：否

BackupPlanName

所保存的备份计划的显示名称。

类型：字符串

必需：否

CreationDate

资源备份计划的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。`CreationDate` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

DeletionDate

备份计划的删除日期和时间，采用 Unix 格式和协调世界时 (UTC)。DeletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

LastExecutionDate

上次运行此备份计划的时间。日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastExecutionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

VersionId

唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑版本 ID。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupPlanTemplatesListMember

服务： AWS Backup

指定与备份计划模板关联的元数据的对象。

内容

BackupPlanTemplateId

唯一标识存储的备份计划模板。

类型：字符串

必需：否

BackupPlanTemplateName

备份计划模板的可选显示名称。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupRule

服务： AWS Backup

指定用于备份所选资源的安排任务。

内容

RuleName

备份规则的显示名称。必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：是

TargetBackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

CompletionWindowMinutes

一个时间值（以分钟为单位），用于指定备份作业在成功启动之后必须在多长时间内完成，否则将会被 AWS Backup取消。该值为可选项。

类型：长整型

必需：否

CopyActions

`CopyAction` 对象的数组，其中包含复制操作的详细信息。

类型：CopyAction 对象数组

必需：否

EnableContinuousBackup

指定是否 AWS Backup 创建连续备份。创建 AWS Backup 能够 point-in-time 恢复的连续备份 (PITR) 的真实原因。False（或未指定）会 AWS Backup 导致创建快照备份。

类型：布尔值

必需：否

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

类型：Lifecycle 对象

必需：否

RecoveryPointTags

从备份还原时分配给与此规则关联的资源的标签。

类型：字符串到字符串映射

必需：否

RuleId

唯一标识用于安排所选资源备份的规则。

类型：字符串

必需：否

ScheduleExpression

UTC 格式的 cron 表达式，用于指定何时 AWS Backup 启动备份作业。有关 AWS cron 表达式的更多信息，请参阅 Amazon Ev CloudWatch ents 用户指南中的规则计划表达式。 。 AWS cron 表达式的两个示例是 `15 * ? * * *`（每小时在过去 15 分钟时进行一次备份）和`0 12 * * ? *`（UTC 每天中午 12 点进行备份）。要查看示例表，请单击前面的链接并向下滚动页面。

类型：字符串

必需：否

ScheduleExpressionTimezone

设置计划表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowMinutes

一个时间值（以分钟为单位），用于指定在安排了备份之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则必须至少为 60 分钟才能避免错误。

在启动时段内，备份作业的状态将保持 CREATED 状态，直到成功启动或启动时段结束为止。如果在启动窗口内 AWS Backup 收到允许重试作业的错误消息， AWS Backup 则至少每 10 分钟自动重试一次以开始作业，直到备份成功开始（任务状态更改为RUNNING）或任务状态更改为EXPIRED（预计在启动窗口时间结束时发生）。

类型：长整型

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupRuleInput

服务： AWS Backup

指定用于备份所选资源的安排任务。

内容

RuleName

备份规则的显示名称。必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：是

TargetBackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：是

CompletionWindowMinutes

一个时间值（以分钟为单位），用于指定备份作业在成功启动之后必须在多长时间内完成，否则将会被 AWS Backup取消。该值为可选项。

类型：长整型

必需：否

CopyActions

`CopyAction` 对象的数组，其中包含复制操作的详细信息。

类型：CopyAction 对象数组

必需：否

EnableContinuousBackup

指定是否 AWS Backup 创建连续备份。创建 AWS Backup 能够 point-in-time 恢复的连续备份 (PITR) 的真实原因。False（或未指定）会 AWS Backup 导致创建快照备份。

类型：布尔值

必需：否

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 将根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。备份过渡到冷存储后，无法更改 “几天后过渡到冷存储” 设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

此参数的最大值为 100 年（36,500 天）。

类型：Lifecycle 对象

必需：否

RecoveryPointTags

要分配给资源的标签。

类型：字符串到字符串映射

必需：否

ScheduleExpression

UTC 格式的 CRON 表达式，用于指定何时 AWS Backup 启动备份作业。

类型：字符串

必需：否

ScheduleExpressionTimezone

设置计划表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowMinutes

一个时间值（以分钟为单位），用于指定在安排了备份之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则必须至少为 60 分钟才能避免错误。

此参数的最大值为 100 年（52,560,000 分钟）。

在启动时段内，备份作业的状态将保持 CREATED 状态，直到成功启动或启动时段结束为止。如果在启动窗口内 AWS Backup 收到允许重试作业的错误消息， AWS Backup 则至少每 10 分钟自动重试一次以开始作业，直到备份成功开始（任务状态更改为RUNNING）或任务状态更改为EXPIRED（预计在启动窗口时间结束时发生）。

类型：长整型

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupSelection

服务： AWS Backup

用于为备份计划指定一组资源。

我们建议您指定要包含或排除的条件、标签或资源。否则，Backup 会尝试选择所有支持和选择加入的存储资源，这可能会产生意想不到的成本影响。

有关更多信息，请参阅以编程方式分配资源。

内容

IamRoleArn

备份目标资源时 AWS Backup 用于进行身份验证的 IAM 角色的 ARN；例如，。`arn:aws:iam::123456789012:role/S3Access`

类型：字符串

必需：是

SelectionName

资源选择文档的显示名称。必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：是

Conditions

您为使用标签为备份计划分配资源而定义的条件。例如，`"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`。

`Conditions`支持`StringEquals`、`StringLike`、`StringNotEquals`、和`StringNotLike`。条件运算符区分大小写。

如果指定多个条件，则资源与所有条件非常匹配（AND 逻辑）。

类型：Conditions 对象

必需：否

ListOfTags

您为使用标签为备份计划分配资源而定义的条件。例如，`"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`。

`ListOfTags`仅支持`StringEquals`。条件运算符区分大小写。

如果您指定多个条件，则资源与任何条件（OR 逻辑）都非常匹配。

类型：Condition 对象数组

必需：否

NotResources

要从备份计划中排除的资源的 Amazon 资源名称 (ARN)。不带通配符的 ARN 的最大数量为 500 个，带通配符的 ARN 的最大数量为 30 个。

如果需要从备份计划中排除许多资源，请考虑使用不同的资源选择策略，例如仅分配一种或几种资源类型或使用标签细化资源选择。

类型：字符串数组

必需：否

Resources

要分配给备份计划的资源的 Amazon 资源名称 (ARN)。不带通配符的 ARN 的最大数量为 500 个，带通配符的 ARN 的最大数量为 30 个。

如果需要为备份计划分配许多资源，请考虑使用不同的资源选择策略，例如分配一种资源类型的所有资源或使用标签细化资源选择。

如果您指定多个 ARN，则资源与任何 ARN（或逻辑）都非常匹配。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupSelectionsListMember

服务： AWS Backup

包含有关 BackupSelection 对象的元数据。

内容

BackupPlanId

唯一标识备份计划。

类型：字符串

必需：否

CreationDate

创建备份计划的日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 Amazon 资源名称 (ARN)；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

必需：否

SelectionId

唯一标识将一组资源分配给备份计划的请求。

类型：字符串

必需：否

SelectionName

资源选择文档的显示名称。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

BackupVaultListMember

服务： AWS Backup

包含备份保管库相关的元数据。

内容

BackupVaultArn

唯一标识备份保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

必需：否

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：^[a-zA-Z0-9\-_]{2,50}$

必需：否

CreationDate

资源备份的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreatorRequestId

唯一字符串，用于标识请求并允许重试失败的请求，同时避免发生两次运行操作的风险。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

EncryptionKeyArn

您可以指定的服务器端加密密钥，用于加密来自支持完全 AWS Backup 管理的服务的备份；例如，`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。如果指定密钥，则必须指定其 ARN，而不是其别名。如果未指定密钥， AWS Backup 默认会为您创建一个 KMS 密钥。

要了解哪些 AWS Backup 服务支持完全 AWS Backup 管理以及如何 AWS Backup 处理来自尚不支持完全管理的服务的备份的加密 AWS Backup，请参阅中的备份加密 AWS Backup

类型：字符串

必需：否

LockDate

AWS Backup 文件库锁定配置变为不可变的日期和时间，这意味着无法更改或删除。

如果您在未指定锁定日期的情况下对保管库应用了保管库锁定，则可以随时更改保管库锁定设置，或从保管库中完全删除保管库锁定。

该值采用 Unix 格式和协调世界时 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

Locked

一个布尔值，用于指示 AWS Backup 文件库锁定是否适用于选定的备份存储库。如果值为 `true`，则保管库锁定会阻止对选定保管库中的恢复点执行删除和更新操作。

类型：布尔值

必需：否

MaxRetentionDays

AWS Backup 文件库锁定设置，用于指定文件库保留其恢复点的最大保留期。如果不指定此参数，则保管库锁定不会对保管库中的恢复点强制规定最长保留期（允许无限期存储）。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或小于最长保留期。如果作业的保留期长于该最长保留期，则保管库将无法执行该备份或复制作业，因此您应该修改生命周期设置或使用其他保管库。保管库锁定之前已存储在保管库中的恢复点不受影响。

类型：长整型

必需：否

MinRetentionDays

AWS Backup 文件库锁定设置，用于指定文件库保留其恢复点的最短保留期。如果未指定此参数，则保管库锁定不会强制规定最短保留期。

如果指定了此参数，则备份或复制到保管库的任何作业都必须具有生命周期策略，其保留期等于或大于最短保留期。如果作业的保留期短于该最短保留期，则保管库将无法执行该备份或复制作业，因此，您应该修改生命周期设置或使用其他保管库。保管库锁定之前已存储在保管库中的恢复点不受影响。

类型：长整型

必需：否

NumberOfRecoveryPoints

存储在备份保管库中的恢复点数量。

类型：长整型

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

CalculatedLifecycle

服务： AWS Backup

包含 `DeleteAt` 和 `MoveToColdStorageAt` 时间戳，用于指定恢复点的生命周期。

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

内容

DeleteAt

一个时间戳，用于指定何时删除恢复点。

类型：时间戳

必需：否

MoveToColdStorageAt

一个时间戳，用于指定何时将恢复点转换到冷存储。

类型：时间戳

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Condition

服务： AWS Backup

包含一个三元组数组，该数组由条件类型（如 StringEquals）、键和值组成。用于使用资源标签筛选这些资源并将其分配给备份计划。区分大小写。

内容

ConditionKey

键/值对中的键。例如，在标签 Department: Accounting 中，Department 是键。

类型：字符串

必需：是

ConditionType

一项操作，应用到用于为备份计划分配资源的键/值对。条件仅支持 StringEquals。要获得更灵活的分配选项，包括 StringLike 以及从备份计划中排除资源的功能，请针对您的 BackupSelection 使用 Conditions（末尾带有 “s”）。

类型：字符串

有效值：STRINGEQUALS

必需：是

ConditionValue

键/值对中的值。例如，在标签 Department: Accounting 中，Accounting 是值。

类型：字符串

必需：是

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ConditionParameter

服务： AWS Backup

包括有关由您定义的用于将标记的资源分配给备份计划的标签的信息。

在标签aws:ResourceTag中加入前缀。例如，"aws:ResourceTag/TagKey1": "Value1"。

内容

ConditionKey

键/值对中的键。例如，在标签 Department: Accounting 中，Department 是键。

类型：字符串

必需：否

ConditionValue

键/值对中的值。例如，在标签 Department: Accounting 中，Accounting 是值。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Conditions

服务： AWS Backup

包含有关使用资源标签从备份计划中包含或排除哪些资源的信息。条件区分大小写。

内容

StringEquals

仅针对您使用相同值进行标记的资源筛选已标记资源的值。也称为“精确匹配”。

类型：ConditionParameter 对象数组

必需：否

StringLike

通过在字符串中的任何位置使用通配符 (*)，针对匹配的标签值筛选已标记资源的值。例如，“prod*”或“*rod*”与标签值“production”相匹配。

类型：ConditionParameter 对象数组

必需：否

StringNotEquals

仅针对您标记的不具有相同值的资源筛选已标记资源的值。也称为“否定匹配”。

类型：ConditionParameter 对象数组

必需：否

StringNotLike

通过在字符串中的任何位置使用通配符 (*)，针对非匹配的标签值筛选已标记资源的值。

类型：ConditionParameter 对象数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK

- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ControlInputParameter

服务： AWS Backup

控件的参数。一个控件可以有零个、一个或多个参数。具有两个参数的控件的示例是：“备份计划频率至少为 `daily` 并且保留期至少为 `1 year`”。第一个参数是 `daily`。第二个参数是 `1 year`。

内容

ParameterName

参数的名称，例如 `BackupPlanFrequency`。

类型：字符串

必需：否

ParameterValue

参数的值，例如 `hourly`。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ControlScope

服务： AWS Backup

框架由一个或多个控件组成。每个控件都有各自的控制范围。控制范围可以包含一种或多种资源类型、标签键值组合、一种资源类型和一个资源 ID 的组合。如果没有指定范围，当记录组中的任何资源更改配置时，将触发对规则的评估。

> **Note**
>
> 要设置包含所有特定资源的控制范围，请在调用 `CreateFramework` 时将 `ControlScope` 留空或不传递。

内容

ComplianceResourceIds

您希望控制范围包含的唯一 AWS 资源的 ID。

类型：字符串数组

数组成员：最少 1 个项目。最多 100 个项目。

必需：否

ComplianceResourceTypes

描述控制范围是否包括一种或多种类型的资源，例如 `EFS` 或 `RDS`。

类型：字符串数组

必需：否

Tags

应用于要触发规则评估的 AWS 资源的标签键值对。最多可以提供一个键值对。标签值是可选的，但是如果您要从控制台创建或编辑框架，则它不能为空字符串（尽管包含在 CloudFormation 模板中时，该值可以为空字符串）。

分配给标签的结构是：`[{"Key":"string","Value":"string"}]`。

类型：字符串到字符串映射

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

CopyAction

服务： AWS Backup

复制操作的详细信息。

内容

DestinationBackupVaultArn

唯一标识复制备份的目的地备份保管库的 Amazon 资源名称 (ARN)。例如：`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`。

类型：字符串

必需：是

Lifecycle

指定恢复点过渡到冷存储或被删除之前的时间段（以天为单位）。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，在主机上，保留期设置必须比在几天后过渡到冷藏设置长 90 天。将备份转换为冷备份后，无法更改天后过渡到冷的设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

要删除现有的生命周期和保留期并无限期保留恢复点，请为和指定 -1。`MoveToColdStorageAfterDays` `DeleteAfterDays`

类型：Lifecycle 对象

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

CopyJob

服务： AWS Backup

包含有关复制作业的详细信息。

内容

AccountId

拥有复制作业的账户 ID。

类型：字符串

模式：^[0-9]{12}$

必需：否

BackupSizeInBytes

复制作业大小（以字节为单位）。

类型：长整型

必需：否

ChildJobsInState

这将返回包含的子（嵌套）复印作业的统计信息。

类型：字符串到长整型映射

有效密钥：CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

必需：否

CompletionDate

复印作业的完成日期和时间，采用 Unix 格式和世界协调时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CompositeMemberIdentifier

复合组中资源的标识符，例如属于复合（父）堆栈的嵌套（子）恢复点。ID 是从堆栈内的逻辑 ID 中传输的。

类型：字符串

必需：否

CopyJobId

唯一标识复制作业。

类型：字符串

必需：否

CreatedBy

包含有关 AWS Backup 用于启动恢复点备份的备份计划和规则的信息。

类型：RecoveryPointCreator 对象

必需：否

CreationDate

复制作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

DestinationBackupVaultArn

唯一标识目的地复制保管库的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault。

类型：字符串

必需：否

DestinationRecoveryPointArn

唯一标识目的地恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

必需：否

IamRoleArn

指定用于复制目标恢复点的 IAM 角色 ARN；例如，`arn:aws:iam::123456789012:role/S3Access`。

类型：字符串

必需：否

IsParent

这是一个布尔值，表示这是父（复合）复制作业。

类型：布尔值

必需：否

MessageCategory

此参数是指定消息类别的作业计数。

例如，字符串可能包括 `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL` 和 `InvalidParameters`。有关 MessageCategory 字符串列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

`AGGREGATE_ALL` 汇总所有消息类别的作业计数并返回总和

类型：字符串

必需：否

NumberOfChildJobs

子（嵌套）复印作业的数量。

类型：长整型

必需：否

ParentJobId

它唯一标识向 AWS Backup 发出的复制资源请求。返回的将是父（复合）作业 ID。

类型：字符串

必需：否

ResourceArn

要复制的 AWS 资源；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

类型：字符串

必需：否

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

必需：否

ResourceType

要复制的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

SourceBackupVaultArn

唯一标识源复制保管库的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`。

类型：字符串

必需：否

SourceRecoveryPointArn

唯一标识源恢复点的 ARN；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

类型：字符串

必需：否

State

复制作业的当前状态。

类型：字符串

有效值：`CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

必需：否

StatusMessage

一条详细消息，说明复制资源作业的状态。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

CopyJobSummary

服务： AWS Backup

此请求提供最近 30 天内创建的或正在运行的复制作业的摘要。

返回的摘要可能包含以下内容：区域、账户、州 RestourceType MessageCategory、 StartTime、EndTime、和包含的任务数量。

内容

AccountId

拥有摘要中作业的账户 ID。

类型：字符串

模式：`^[0-9]{12}$`

必需：否

Count

该值以作业数量的形式显示在作业摘要中。

类型：整数

必需：否

EndTime

以数字格式表示的作业结束时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

MessageCategory

此参数是指定消息类别的作业计数。

示例字符串包括 `AccessDenied`、`Success` 和 `InvalidParameters`。有关 MessageCategory 字符串列表，请参阅监控。

值 ANY 返回所有消息类别的计数。

AGGREGATE_ALL 汇总所有消息类别的作业计数并返回总和。

类型：字符串

必需：否

Region

工作摘要中的 AWS 区域。

类型：字符串

必需：否

ResourceType

此值是指定的资源类型的作业计数。请求 GetSupportedResourceTypes 返回支持的资源类型的字符串。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

StartTime

以数字格式表示的作业开始时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

State

此值是处于指定状态的作业的计数。

类型：字符串

有效值：CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

DateRange

服务： AWS Backup

这是一个包含 FromDate: DateTime 和 ToDate:的资源筛选器 DateTime。两个值都是必填项。不允许使用未来 DateTime 值。

日期和时间采用 Unix 格式和协调世界时 (UTC)，精确到毫秒（毫秒是可选项）。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

内容

FromDate

此值为起始日期（含在内）。

日期和时间采用 Unix 格式和协调世界时 (UTC)，精确到毫秒（毫秒是可选项）。

类型：时间戳

必需：是

ToDate

此值是结束日期（含在内）。

日期和时间采用 Unix 格式和协调世界时 (UTC)，精确到毫秒（毫秒是可选项）。

类型：时间戳

必需：是

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Framework

服务： AWS Backup

包含有关框架的详细信息。框架包含控件，用于评估和报告您的备份事件和资源。框架每天都会生成合规结果。

内容

CreationTime

框架的创建日期和时间，以 ISO 8601 表示。CreationTime 的值精确到毫秒。例如，2020-07-10T15:00:00.000-08:00 表示 2020 年 7 月 10 日下午 3:00，比 UTC 晚 8 个小时。

类型：时间戳

必需：否

DeploymentStatus

框架的部署状态。状态包括：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

类型：字符串

必需：否

FrameworkArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：否

FrameworkDescription

框架的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：.*\S.*

必需：否

FrameworkName

框架的唯一名称。此名称的长度介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必需：否

NumberOfControls

框架包含的控件数量。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

FrameworkControl

服务： AWS Backup

包含有关框架的所有控件的详细信息。每个框架必须至少包含一个控件。

内容

ControlName

控件的名称。此名称介于 1 到 256 个字符之间。

类型：字符串

必需：是

ControlInputParameters

名称/值对。

类型：ControlInputParameter 对象数组

必需：否

ControlScope

控件的范围。控件范围定义控件将评估的内容。控制范围的三个示例为：特定备份计划、具有特定标签的所有备份计划或所有备份计划。

有关更多信息，请参阅 `ControlScope。`

类型：ControlScope 对象

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

KeyValue

服务： AWS Backup

由两个相关字符串组成的对。允许的字符包括字母、空格、可采用 UTF-8 格式表示的数字以及下列字符： + - = . _ : /。

内容

Key

标签键（字符串）。键不能以 aws: 开头。

长度限制：长度下限为 1。长度上限为 128。

模式：^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

类型：字符串

必需：是

Value

键的值。

长度约束：最大长度为 256。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

类型：字符串

必需：是

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

LegalHold

服务： AWS Backup

法定保留是一种管理工具，可帮助防止备份在保留状态下被删除。设置保留后，将无法删除处于保留状态的备份，并且会更改备份状态（例如转换为冷存储状态）的生命周期策略会延迟到法定保留被删除为止。备份可以包含多个法定保留。法定保留适用于一个或多个备份（也称为恢复点）。可以按资源类型和资源 ID 筛选这些备份。

内容

CancellationDate

取消法定保留的时间。

类型：时间戳

必需：否

CreationDate

法定封存的创建时间。

类型：时间戳

必需：否

Description

对合法封存的描述。

类型：字符串

必需：否

LegalHoldArn

合法封存的亚马逊资源名称 (ARN)；例如，。`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

类型：字符串

必需：否

LegalHoldId

合法封存的 ID。

类型：字符串

必需：否

Status

合法封存的状态。

类型：字符串

有效值：CREATING | ACTIVE | CANCELING | CANCELED

必需：否

Title

合法封存的标题。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Lifecycle

服务： AWS Backup

指定恢复点过渡到冷存储或被删除之前的时间段（以天为单位）。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，在主机上，保留期设置必须比在几天后过渡到冷藏设置长 90 天。将备份转换为冷备份后，无法更改天后过渡到冷的设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

要删除现有的生命周期和保留期并无限期保留恢复点，请为和指定 -1。`MoveToColdStorageAfterDays` `DeleteAfterDays`

内容

DeleteAfterDays

恢复点在创建后被删除的天数。此值必须是中指定的天数后至少 90 天`MoveToColdStorageAfterDays`。

类型：长整型

必需：否

MoveToColdStorageAfterDays

恢复点在创建后移至冷存储的天数。

类型：长整型

必需：否

OptInToArchiveForSupportedResources

如果该值为 true，则您的备份计划会根据您的生命周期设置将支持的资源转换为存档（冷）存储层。

类型：布尔值

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ProtectedResource

服务： AWS Backup

一种包含有关备份资源信息的结构。

内容

LastBackupTime

资源的上次备份日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastBackupTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

LastBackupVaultArn

包含最新备份恢复点的备份库的 ARN（Amazon 资源名称）。

类型：字符串

必需：否

LastRecoveryPointArn

最新恢复点的 ARN（亚马逊资源名称）。

类型：字符串

必需：否

ResourceArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：否

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

必需：否

ResourceType

AWS 资源的类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。对于 Windows 卷影复制服务 (VSS) 备份，唯一支持的资源类型是 Amazon EC2。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ProtectedResourceConditions

服务： AWS Backup

您使用标签为还原测试计划中的资源定义的条件。

例如，`"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`。条件运算符区分大小写。

内容

StringEquals

仅针对您使用相同值进行标记的资源筛选已标记资源的值。也称为“精确匹配”。

类型：KeyValue 对象数组

必需：否

StringNotEquals

仅针对您标记的不具有相同值的资源筛选已标记资源的值。也称为“否定匹配”。

类型：KeyValue 对象数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RecoveryPointByBackupVault

服务： AWS Backup

包含有关存储在备份保管库中的恢复点的详细信息。

内容

BackupSizeInBytes

备份的大小（以字节为单位）。

类型：长整型

必需：否

BackupVaultArn

唯一标识备份保管库的 ARN；例如，`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`。

类型：字符串

必需：否

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：否

CalculatedLifecycle

包含 `DeleteAt` 和 `MoveToColdStorageAt` 时间戳的 `CalculatedLifecycle` 对象。

类型：CalculatedLifecycle 对象

必需：否

CompletionDate

恢复点还原作业的完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。`CompletionDate` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CompositeMemberIdentifier

复合组中资源的标识符，例如属于复合（父）堆栈的嵌套（子）恢复点。ID 是从堆栈内的逻辑 ID 中传输的。

类型：字符串

必需：否

CreatedBy

包含有关创建恢复点的标识信息，包括用于创建该恢复点的备份计划的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

类型：RecoveryPointCreator 对象

必需：否

CreationDate

恢复点的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

EncryptionKeyArn

用于保护备份的服务器端加密密钥；例如，arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

类型：字符串

必需：否

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

必需：否

IsEncrypted

一个布尔值，如果指定的恢复点已加密，则返回 TRUE，如果恢复点未加密，则返回 FALSE。

类型：布尔值

必需：否

IsParent

这是一个布尔值，表示这是父（复合）恢复点。

类型：布尔值

必需：否

LastRestoreTime

恢复点的上次还原日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastRestoreTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

Lifecycle

生命周期定义了受保护的资源何时过渡到冷存储以及何时过期。 AWS Backup 根据您定义的生命周期自动过渡和过期备份。

转换到冷存储的备份必须在冷存储中存储至少 90 天。因此，“保留期”设置必须比“转换为冷态前经过的天数”设置多 90 天。在备份转换为冷态后，无法更改“转换为冷态前经过的天数”设置。

按资源划分的功能可用性表中列出了可以过渡到冷存储的资源类型。 AWS Backup 对于其他资源类型，将忽略此表达式。

类型：Lifecycle 对象

必需：否

ParentRecoveryPointArn

父（复合）恢复点的亚马逊资源名称 (ARN)。

类型：字符串

必需：否

RecoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

必需：否

ResourceArn

唯一标识资源的 ARN。ARN 的格式取决于资源类型。

类型：字符串

必需：否

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

必需：否

ResourceType

保存为恢复点的 AWS 资源类型；例如，亚马逊弹性区块存储 (Amazon EBS) Block Store 卷或亚马逊关系数据库服务 (Amazon RDS) 数据库。对于 Windows 卷影复制服务 (VSS) 备份，唯一支持的资源类型是 Amazon EC2。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

SourceBackupVaultArn

最初从中复制恢复点的备份保管库。如果将恢复点还原到相同的账户，则该值将是 null。

类型：字符串

必需：否

Status

指定恢复点状态的状态码。

类型：字符串

有效值：`COMPLETED | PARTIAL | DELETING | EXPIRED`

必需：否

StatusMessage

一条说明恢复点当前状态的消息。

类型：字符串

必需：否

VaultType

存储所述恢复点的存储库的类型。

类型：字符串

有效值：`BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RecoveryPointByResource

服务： AWS Backup

包含有关已保存恢复点的详细信息。

内容

BackupSizeBytes

备份的大小（以字节为单位）。

类型：长整型

必需：否

BackupVaultName

用于存储备份的逻辑容器的名称。备份保管库的名称在创建它们的账户和创建它们的 AWS 区域中是唯一的。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：否

CreationDate

恢复点的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。`CreationDate` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

EncryptionKeyArn

用于保护备份的服务器端加密密钥；例如，`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。

类型：字符串

必需：否

IsParent

这是一个布尔值，表示这是父（复合）恢复点。

类型：布尔值

必需：否

ParentRecoveryPointArn

父（复合）恢复点的亚马逊资源名称 (ARN)。

类型：字符串

必需：否

RecoveryPointArn

唯一标识恢复点的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

类型：字符串

必需：否

ResourceName

属于指定备份的资源的非唯一名称。

类型：字符串

必需：否

Status

指定恢复点状态的状态码。

类型：字符串

有效值：`COMPLETED | PARTIAL | DELETING | EXPIRED`

必需：否

StatusMessage

一条说明恢复点当前状态的消息。

类型：字符串

必需：否

VaultType

存储所述恢复点的存储库的类型。

类型：字符串

有效值：`BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RecoveryPointCreator

服务： AWS Backup

包含有关 AWS Backup 用于启动恢复点备份的备份计划和规则的信息。

内容

BackupPlanArn

唯一标识备份计划的 Amazon 资源名称 (ARN)；例如，`arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`。

类型：字符串

必需：否

BackupPlanId

唯一标识备份计划。

类型：字符串

必需：否

BackupPlanVersion

版本 ID 是唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法对其进行编辑。

类型：字符串

必需：否

BackupRuleId

唯一标识用于安排所选资源备份的规则。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RecoveryPointMember

服务： AWS Backup

这是一个恢复点，它是父（复合）恢复点的子（嵌套）恢复点。这些恢复点可以与其父（复合）恢复点断开关联，在这种情况下，它们将不再是其成员。

内容

BackupVaultName

备份存储库（存储备份的逻辑容器）的名称。

类型：字符串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必需：否

RecoveryPointArn

父（复合）恢复点的亚马逊资源名称 (ARN)。

类型：字符串

必需：否

ResourceArn

唯一标识已保存资源的亚马逊资源名称 (ARN)。

类型：字符串

必需：否

ResourceType

保存为恢复点的 AWS 资源类型。

类型：字符串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RecoveryPointSelection

服务： AWS Backup

这会指定分配一组资源的标准，例如资源类型或备份保管库。

内容

DateRange

这是一个包含 FromDate: DateTime 和 ToDate:的资源筛选器 DateTime。两个值都是必填项。不允许使用未来 DateTime 值。

日期和时间采用 Unix 格式和协调世界时 (UTC)，精确到毫秒（毫秒是可选项）。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：DateRange 对象

必需：否

ResourceIdentifiers

这些是资源选择中包含的资源（包括资源和保管库的类型）。

类型：字符串数组

必需：否

VaultNames

这些是包含所选恢复点的保管库的名称。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ReportDeliveryChannel

服务： AWS Backup

包含您报告计划中的有关在何处交付报告的信息，特别是 Amazon S3 存储桶名称、S3 密钥前缀和报告格式。

内容

S3BucketName

接收报告的 S3 存储桶的唯一名称。

类型：字符串

必需：是

Formats

报告的格式：CSV、JSON、或两者兼而有之。如未指定，则默认格式为 CSV。

类型：字符串数组

必需：否

S3KeyPrefix

Audit Manag AWS Backup er 将您的报告发送到亚马逊 S3 的位置的前缀。前缀是以下路径的这一部分：s3: ////backup/us-west-2/year/month/day your-bucket-name prefix /report-Name。如未指定，则没有前缀。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ReportDestination

服务： AWS Backup

包含报告作业中有关报告目的地的信息。

内容

S3BucketName

接收报告的 Amazon S3 存储桶的唯一名称。

类型：字符串

必需：否

S3Keys

唯一标识 S3 存储桶中报告的对象密钥。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ReportJob

服务： AWS Backup

包含有关报告作业的详细信息。报告作业根据报告计划编译报告并将其发布到 Amazon S3。

内容

CompletionTime

报告作业的完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreationTime

报告作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

ReportDestination

报告作业发布报告的目的地的 S3 存储桶名称和 S3 密钥。

类型：ReportDestination 对象

必需：否

ReportJobId

报告作业的标识符。唯一的、随机生成的、Unicode、UTF-8 编码字符串，长度最大为 1024 个字节。无法编辑报告作业 ID。

类型：字符串

必需：否

ReportPlanArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：否

ReportTemplate

标识报告的报告模板。报告使用报告模板构建。报告模板包括：

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

类型：字符串

必需：否

Status

报告作业的状态。状态包括：

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` 表示报告可在您指定的目的地供您查看。如果状态为 `FAILED`，请查看 `StatusMessage` 以了解原因。

类型：字符串

必需：否

StatusMessage

一条说明报告作业状态的消息。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ReportPlan

服务： AWS Backup

包含有关报告计划的详细信息。

内容

CreationTime

报告计划的创建日期和时间，采用 Unix 格式和协调世界时 (UTC)。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

DeploymentStatus

报告计划的部署状态。状态包括：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED

类型：字符串

必需：否

LastAttemptedExecutionTime

与此报告计划关联的报告作业的上次尝试运行的日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastAttemptedExecutionTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

LastSuccessfulExecutionTime

与此报告计划关联的报告作业的上次成功运行日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastSuccessfulExecutionTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

ReportDeliveryChannel

包含有关在何处以及如何交付报告的信息，特别是 Amazon S3 桶名称、S3 密钥前缀和报告格式。

类型：ReportDeliveryChannel 对象

必需：否

ReportPlanArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：否

ReportPlanDescription

报告计划的可选描述，最多 1024 个字符。

类型：字符串

长度约束：最小长度为 0。最大长度为 1024。

模式：`.*\S.*`

必需：否

ReportPlanName

报告计划的唯一名称。此名称的长度介于 1 到 256 个字符之间，以字母开头，由字母（a-z、A-Z）、数字 (0-9) 和下划线 (_) 组成。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必需：否

ReportSetting

标识报告的报告模板。报告使用报告模板构建。报告模板包括：

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

如果报告模板为RESOURCE_COMPLIANCE_REPORT或CONTROL_COMPLIANCE_REPORT，则此 API 资源还描述了 AWS 区域 和框架的报告覆盖范围。

类型：ReportSetting 对象

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

ReportSetting

服务： AWS Backup

包含有关报告设置的详细信息。

内容

ReportTemplate

标识报告的报告模板。报告使用报告模板构建。报告模板包括：

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

类型：字符串

必需：是

Accounts

这些是要列入报告的账户。

使用字符串值为ROOT来包含所有组织单位。

类型：字符串数组

必需：否

FrameworkArns

报告所涵盖的框架的 Amazon 资源名称 (ARN)。

类型：字符串数组

必需：否

NumberOfFrameworks

报告涵盖的框架数量。

类型：整数

必需：否

OrganizationUnits

这些是要列入报告的组织单元。

类型：字符串数组

必需：否

Regions

这些是要列入报告的区域。

使用通配符作为包含所有区域的字符串值。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreJobCreator

服务： AWS Backup

包含有关 AWS Backup 用于启动还原作业的还原测试计划的信息。

内容

RestoreTestingPlanArn

可唯一标识还原测试计划的 Amazon 资源名称（ARN）。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreJobsListMember

服务： AWS Backup

包含还原作业相关元数据。

内容

AccountId

拥有还原作业的账户 ID。

类型：字符串

模式：^[0-9]{12}$

必需：否

BackupSizeInBytes

还原资源的大小（以字节为单位）。

类型：长整型

必需：否

CompletionDate

恢复点还原作业的完成日期和时间，采用 Unix 格式和协调世界时 (UTC)。CompletionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

CreatedBy

包含有关创建还原作业的标识信息。

类型：RestoreJobCreator 对象

必需：否

CreatedResourceArn

唯一标识资源的 Amazon 资源名称 (ARN)。ARN 的格式取决于资源类型。

类型：字符串

必需：否

CreationDate

还原作业的创建日期和时间，采用 Unix 时间格式和协调世界时 (UTC)。CreationDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

DeletionStatus

这记录了还原测试生成的数据的状态。状态可以是 Deleting、Failed 或 Successful。

类型：字符串

有效值：DELETING | FAILED | SUCCESSFUL

必需：否

DeletionStatusMessage

这描述了还原作业的删除状态。

类型：字符串

必需：否

ExpectedCompletionTimeMinutes

恢复点还原作业预计要花费的时间（以分钟为单位）。

类型：长整型

必需：否

IamRoleArn

指定用于创建目标恢复点的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

类型：字符串

必需：否

PercentDone

包含查询作业状态时作业完成的估计百分比。

类型：字符串

必需：否

RecoveryPointArn

唯一标识恢复点的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

类型：字符串

必需：否

RecoveryPointCreationDate

创建恢复点的日期。

类型：时间戳

必需：否

ResourceType

列出的还原作业的资源类型；例如 Amazon Elastic Block Store (Amazon EBS) 卷或 Amazon Relational Database Service (Amazon RDS) 数据库。对于 Windows 卷影复制服务 (VSS) 备份，唯一支持的资源类型是 Amazon EC2。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

RestoreJobId

唯一标识还原恢复点的作业。

类型：字符串

必需：否

Status

一种状态码，用于指定为恢复恢复点 AWS Backup 而启动的任务的状态。

类型：字符串

有效值：`PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

必需：否

StatusMessage

一条详细消息，说明恢复点还原作业的状态。

类型：字符串

必需：否

ValidationStatus

在指定的还原作业上运行验证的状态。

类型：字符串

有效值：`FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

必需：否

ValidationStatusMessage

这描述了针对指定的还原作业运行的验证的状态。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreJobSummary

服务： AWS Backup

此请求提供最近 30 天内创建的或正在运行的还原作业的摘要。

返回的摘要可能包含以下内容：区域、账户、州 ResourceType MessageCategory、 StartTime、EndTime、和包含的任务数量。

内容

AccountId

拥有摘要中作业的账户 ID。

类型：字符串

模式：`^[0-9]{12}$`

必需：否

Count

该值以作业数量的形式显示在作业摘要中。

类型：整数

必需：否

EndTime

以数字格式表示的作业结束时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

Region

工作摘要中的 AWS 区域。

类型：字符串

必需：否

ResourceType

此值是指定的资源类型的作业计数。请求 GetSupportedResourceTypes 返回支持的资源类型的字符串。

类型：字符串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必需：否

StartTime

以数字格式表示的作业开始时间值。

该值是采用 Unix 格式表示的时间，它是世界标准时间 (UTC)，精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

State

此值是处于指定状态的作业的计数。

类型：字符串

有效值：CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingPlanForCreate

服务： AWS Backup

其中包含有关还原测试计划的元数据。

内容

RecoveryPointSelection

RecoveryPointSelection有五个参数（三个必填参数和两个可选参数）。您指定的值决定了恢复测试中包括哪个恢复点。您必须使用指明您Algorithm是否想要最新的恢复点，SelectionWindowDays或者是否想要一个随机恢复点，并且必须指明可以IncludeVaults从哪些保管库中选择恢复点。

Algorithm（必填）有效值：“LATEST_WITHIN_WINDOW” 或 “RANDOM_WITHIN_WINDOW”。

Recovery point types（必填）有效值：“SNAPSHOT” 和/或 “CONTINUOUS”。包括SNAPSHOT仅恢复快照恢复点；包括CONTINUOUS用于恢复连续恢复点（时间点还原/PITR）；同时使用两者来恢复快照或连续恢复点。恢复点将由的值确定Algorithm。

IncludeVaults（必填）。必须包括一个或多个备份存储库。使用通配符 ["*"] 或特定的 ARN。

SelectionWindowDays（可选）值必须是介于 1 到 365 之间的整数（以天为单位）。如果未包括在内，则该值默认为30。

ExcludeVaults（可选）。您可以选择输入一个或多个特定的备份保管库 ARN，将这些文件库的内容排除在还原资格之外。或者，您可以包括选择器列表。如果不包括此参数及其值，则默认为空列表。

类型：RestoreTestingRecoveryPointSelection 对象

必需：是

RestoreTestingPlanName

RestoreTestingPlanName 是一个唯一的字符串，是还原测试计划的名称。创建后无法对其进行更改，并且只能由字母数字字符和下划线组成。

类型：字符串

必需：是

ScheduleExpression

在指定时区执行还原测试计划的 CRON 表达式。

类型：字符串

必需：是

ScheduleExpressionTimezone

可选。这是设置安排表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowHours

默认为 24 小时。

一个时间值（以小时为单位），用于指定在安排了还原测试之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则此参数的最大值为 168 小时（一周）。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingPlanForGet

服务： AWS Backup

其中包含有关还原测试计划的元数据。

内容

CreationTime

还原测试计划的创建日期和时间，以 Unix 格式和世界标准时间 (UTC) 格式表示。`CreationTime` 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：是

RecoveryPointSelection

用于分配一组资源的指定标准，例如恢复点类型或备份保管库。

类型：RestoreTestingRecoveryPointSelection 对象

必需：是

RestoreTestingPlanArn

可唯一标识还原测试计划的 Amazon 资源名称（ARN）。

类型：字符串

必需：是

RestoreTestingPlanName

恢复测试计划名称。

类型：字符串

必需：是

ScheduleExpression

在指定时区执行还原测试计划的 CRON 表达式。

类型：字符串

必需：是

CreatorRequestId

这用于标识请求并允许重试失败的请求，而不存在两次运行操作的风险。如果请求中包含与现有备份计划匹配的 CreatorRequestId，则会返回该计划。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

LastExecutionTime

上次使用指定的还原测试计划运行还原测试的时间。日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastExecutionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

LastUpdateTime

更新还原测试计划的日期和时间。此更新采用 Unix 格式和协调世界时 (UTC)。LastUpdateTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

ScheduleExpressionTimezone

可选。这是设置安排表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowHours

默认为 24 小时。

一个时间值（以小时为单位），用于指定在安排了还原测试之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则此参数的最大值为 168 小时（一周）。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingPlanForList

服务： AWS Backup

其中包含有关还原测试计划的元数据。

内容

CreationTime

还原测试计划的创建日期和时间，以 Unix 格式和世界标准时间 (UTC) 格式表示。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：是

RestoreTestingPlanArn

可唯一标识还原测试计划的 Amazon 资源名称（ARN）。

类型：字符串

必需：是

RestoreTestingPlanName

恢复测试计划名称。

类型：字符串

必需：是

ScheduleExpression

在指定时区执行还原测试计划的 CRON 表达式。

类型：字符串

必需：是

LastExecutionTime

上次使用指定的还原测试计划运行还原测试的时间。日期和时间，采用 Unix 格式和协调世界时 (UTC)。LastExecutionDate 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

LastUpdateTime

更新还原测试计划的日期和时间。此更新采用 Unix 格式和协调世界时 (UTC)。LastUpdateTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：否

ScheduleExpressionTimezone

可选。这是设置安排表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowHours

默认为 24 小时。

一个时间值（以小时为单位），用于指定在安排了还原测试之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则此参数的最大值为 168 小时（一周）。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingPlanForUpdate

服务： AWS Backup

其中包含有关还原测试计划的元数据。

内容

RecoveryPointSelection

必需：`Algorithm`；`RecoveryPointTypes`；`IncludeVaults`（一个或多个）。

可选：SelectionWindowDays（如果未指定，则为 '30'）；`ExcludeVaults`（如果未列出，则默认为空列表）。

类型：RestoreTestingRecoveryPointSelection 对象

必需：否

ScheduleExpression

在指定时区执行还原测试计划的 CRON 表达式。

类型：字符串

必需：否

ScheduleExpressionTimezone

可选。这是设置安排表达式的时区。默认情况下，以 UTC ScheduleExpressions 为单位。您可以将其修改为指定的时区。

类型：字符串

必需：否

StartWindowHours

默认为 24 小时。

一个时间值（以小时为单位），用于指定在安排了还原测试之后，必须在多长时间内成功启动作业，否则将会被取消。该值为可选项。如果包含此值，则此参数的最大值为 168 小时（一周）。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingRecoveryPointSelection

服务： AWS Backup

RecoveryPointSelection有五个参数（三个必填参数和两个可选参数）。您指定的值决定了恢复测试中包括哪个恢复点。您必须使用指明您Algorithm是否想要最新的恢复点，SelectionWindowDays或者是否想要一个随机恢复点，并且必须指明可以IncludeVaults从哪些保管库中选择恢复点。

Algorithm（必填）有效值：“LATEST_WITHIN_WINDOW” 或 “RANDOM_WITHIN_WINDOW”。

Recovery point types（必填）有效值：“SNAPSHOT” 和/或 “CONTINUOUS”。包括SNAPSHOT仅恢复快照恢复点；包括CONTINUOUS用于恢复连续恢复点（时间点还原/PITR）；同时使用两者来恢复快照或连续恢复点。恢复点将由的值确定Algorithm。

IncludeVaults（必填）。必须包括一个或多个备份存储库。使用通配符 ["*"] 或特定的 ARN。

SelectionWindowDays（可选）值必须是介于 1 到 365 之间的整数（以天为单位）。如果未包括在内，则该值默认为30。

ExcludeVaults（可选）。您可以选择输入一个或多个特定的备份保管库 ARN，将这些文件库的内容排除在还原资格之外。或者，您可以包括选择器列表。如果不包括此参数及其值，则默认为空列表。

内容

Algorithm

可接受的值包括“LATEST_WITHIN_WINDOW”或“RANDOM_WITHIN_WINDOW”

类型：字符串

有效值：LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW

必需：否

ExcludeVaults

可接受的值包括特定的 ARN 或选择器列表。如果未列出，则默认为空列表。

类型：字符串数组

必需：否

IncludeVaults

可接受的值包括通配符 ["*"]、特定 ARN 或 ARN 通配符替换值 ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

类型：字符串数组

必需：否

RecoveryPointTypes

这些是恢复点的类型。

包括SNAPSHOT仅恢复快照恢复点；包括CONTINUOUS用于恢复连续恢复点（时间点还原/PITR）；同时使用两者来恢复快照或连续恢复点。恢复点将由的值确定Algorithm。

类型：字符串数组

有效值：CONTINUOUS | SNAPSHOT

必需：否

SelectionWindowDays

可接受的值是介于 1 到 365 之间的整数。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingSelectionForCreate

服务： AWS Backup

其中包含有关特定还原测试选择的元数据。

ProtectedResourceType 是必需的，例如亚马逊 EBS 或亚马逊 EC2。

它包括 `RestoreTestingSelectionName`、`ProtectedResourceType` 和以下项之一：

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

每种受保护的资源类型可以具有一个单一值。

还原测试选择可以包括带通配符值（“*”）的 `ProtectedResourceArns` 以及 `ProtectedResourceConditions`。或者，您最多可以在 `ProtectedResourceArns` 中包括 30 个特定的受保护资源 ARN。

`ProtectedResourceConditions` 示例包括 `StringEquals` 和 `StringNotEquals`。

内容

IamRoleArn

AWS Backup 用于创建目标资源的 IAM 角色的 Amazon 资源名称 (ARN)；例如：`arn:aws:iam::123456789012:role/S3Access`

类型：字符串

必需：是

ProtectedResourceType

还原测试选项中包含的 AWS 资源类型；例如，Amazon EBS 卷或 Amazon RDS 数据库。

接受的受支持资源类型包括：

- 适用于 Amazon Aurora 的 `Aurora`
- 适用于 Amazon DocumentDB（与 MongoDB 兼容）的 `DocumentDB`
- `DynamoDB`：表示 Amazon DynamoDB
- `EBS`：表示 Amazon Elastic Block Store

- EC2：表示 Amazon Elastic Compute Cloud
- EFS：表示 Amazon Elastic File System
- FSx：表示 Amazon FSx
- 适用于 Amazon Neptune 的 Neptune
- 适用于 Amazon Relational Database Service 的 RDS
- S3：表示 Amazon S3

类型：字符串

必需：是

RestoreTestingSelectionName

属于相关还原测试计划的还原测试选择的唯一名称。

类型：字符串

必需：是

ProtectedResourceArns

每个受保护的资源都可以按其特定 ARN（例如 `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`）或按通配符（`ProtectedResourceArns: ["*"]`）进行筛选，但不能同时按这两者进行筛选。

类型：字符串数组

必需：否

ProtectedResourceConditions

如果您在中包含了通配符 ProtectedResourceArns，则可以包括资源条件，例如`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`。

类型：ProtectedResourceConditions 对象

必需：否

RestoreMetadataOverrides

您可以通过在 `RestoreTestingSelection` 的正文中添加参数 `RestoreMetadataOverrides` 来覆盖某些还原元数据键。键值不区分大小写。

请参阅还原测试推断出的元数据的完整列表。

类型：字符串到字符串映射

必需：否

ValidationWindowHours

这是可用于对数据运行验证脚本的小时数（1 到 168）。在验证脚本完成时或指定保留期结束时（以先到者为准），数据将被删除。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingSelectionForGet

服务： AWS Backup

其中包含有关特定还原测试选择的元数据。

内容

CreationTime

还原测试选择的创建日期和时间，以 Unix 格式和世界标准时间（UTC）格式表示。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：是

IamRoleArn

AWS Backup 用于创建目标资源的 IAM 角色的 Amazon 资源名称 (ARN)；例如：arn:aws:iam::123456789012:role/S3Access

类型：字符串

必需：是

ProtectedResourceType

资源测试选项中包含的 AWS 资源类型；例如，Amazon EBS 卷或 Amazon RDS 数据库。

类型：字符串

必需：是

RestoreTestingPlanName

RestoreTestingPlanName 是一个唯一的字符串，是还原测试计划的名称。

类型：字符串

必需：是

RestoreTestingSelectionName

属于相关还原测试计划的还原测试选择的唯一名称。

类型：字符串

必需：是

CreatorRequestId

这用于标识请求并允许重试失败的请求，而不存在两次运行操作的风险。如果请求中包含与现有备份计划匹配的 CreatorRequestId，则会返回该计划。此参数为可选的。

如果使用，则此参数必须包含 1 到 50 个字母数字或“-_.” 字符。

类型：字符串

必需：否

ProtectedResourceArns

您可以包括特定的 ARN（例如 ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]），也可以包括通配符（ProtectedResourceArns: ["*"]），但不能同时包括这两者。

类型：字符串数组

必需：否

ProtectedResourceConditions

在资源测试选项中，此参数按特定条件（例如 StringEquals 或 StringNotEquals）进行筛选。

类型：ProtectedResourceConditions 对象

必需：否

RestoreMetadataOverrides

您可以通过在 RestoreTestingSelection 的正文中添加参数 RestoreMetadataOverrides 来覆盖某些还原元数据键。键值不区分大小写。

请参阅还原测试推断出的元数据的完整列表。

类型：字符串到字符串映射

必需：否

ValidationWindowHours

这是可用于对数据运行验证脚本的小时数（1 到 168）。在验证脚本完成时或指定保留期结束时（以先到者为准），数据将被删除。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingSelectionForList

服务： AWS Backup

其中包含有关特定还原测试选择的元数据。

内容

CreationTime

还原测试选择的创建日期和时间，以 Unix 格式和世界标准时间（UTC）格式表示。CreationTime 的值精确到毫秒。例如，值 1516925490.087 表示 2018 年 1 月 26 日星期五上午 12:11:30.087。

类型：时间戳

必需：是

IamRoleArn

AWS Backup 用于创建目标资源的 IAM 角色的 Amazon 资源名称 (ARN)；例如：arn:aws:iam::123456789012:role/S3Access

类型：字符串

必需：是

ProtectedResourceType

还原测试选项中包含的 AWS 资源类型；例如，Amazon EBS 卷或 Amazon RDS 数据库。

类型：字符串

必需：是

RestoreTestingPlanName

唯一的字符串，即还原测试计划的名称。

名称一经创建便无法更改。名称只能包含字母数字字符和下划线。最大长度为 50。

类型：字符串

必需：是

RestoreTestingSelectionName

还原测试选择的唯一名称。

类型：字符串

必需：是

ValidationWindowHours

此值表示在还原测试之后数据会保留的时间（以小时为单位），以便可以完成可选的验证。

接受的值是 0 到 168（即七天的小时数）之间的整数。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

RestoreTestingSelectionForUpdate

服务： AWS Backup

其中包含有关特定还原测试选择的元数据。

内容

IamRoleArn

AWS Backup 用于创建目标资源的 IAM 角色的 Amazon 资源名称 (ARN)；例如：`arn:aws:iam::123456789012:role/S3Access`

类型：字符串

必需：否

ProtectedResourceArns

您可以包括特定的 ARN（例如 `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`），也可以包括通配符 `ProtectedResourceArns: ["*"]`，但不能同时包括这两者。

类型：字符串数组

必需：否

ProtectedResourceConditions

您使用标签为还原测试计划中的资源定义的条件。

例如，`"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`。条件运算符区分大小写。

类型：ProtectedResourceConditions 对象

必需：否

RestoreMetadataOverrides

您可以通过在 `RestoreTestingSelection` 的正文中添加参数 `RestoreMetadataOverrides` 来覆盖某些还原元数据键。键值不区分大小写。

请参阅还原测试推断出的元数据的完整列表。

类型：字符串到字符串映射

必需：否

ValidationWindowHours

此值表示在还原测试之后数据会保留的时间（以小时为单位），以便可以完成可选的验证。

接受的值是 0 到 168（即七天的小时数）之间的整数。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

AWS Backup gateway

AWS Backup gateway 支持以下数据类型：

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

服务： AWS Backup gateway

描述网关的带宽速率限制间隔。带宽速率限制计划由一个或多个带宽速率限制间隔组成。带宽速率限制间隔定义了一周中的一天或几天，在此期间为上传、下载（或两者）指定带宽速率限制。

内容

DaysOfWeek

带宽速率限制间隔的星期几组成部分，用从 0 到 6 的序数表示，其中 0 表示星期日，6 表示星期六。

类型：整数数组

数组成员：最少 1 个物品。最多 7 个项目。

有效范围：最小值为 0。最大值为 6。

必需：是

EndHourOfDay

一天中结束带宽速率限制间隔的小时时间。

类型：整数

有效范围：最小值为 0。最大值为 23。

必需：是

EndMinuteOfHour

一小时中结束带宽速率限制间隔的分钟时间。

> **Important**
>
> 带宽速率限制间隔在分钟结束时结束。要在小时结束时结束间隔，请使用值 59。

类型：整数

有效范围：最小值为 0。最大值为 59。

必需：是

StartHourOfDay

一天中开始带宽速率限制间隔的小时时间。

类型：整数

有效范围：最小值为 0。最大值为 23。

必需：是

StartMinuteOfHour

一小时中开始带宽速率限制间隔的分钟时间。间隔从该分钟开始时开始。要精确地在小时开始时段开始间隔，请使用值 0。

类型：整数

有效范围：最小值为 0。最大值为 59。

必需：是

AverageUploadRateLimitInBitsPerSec

带宽速率限制间隔的平均上传速率限制部分，以每秒位元数为单位。如果未设置上传速率限制，则此字段不会显示在响应中。

类型：长整型

有效范围：最小值为 51200。最大值为 8000000000000。

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Gateway

服务： AWS Backup gateway

网 AWS Backup 关是一种在客户网络上运行的网关设备，可提供与 AWS 云端备份存储的无缝连接。

内容

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用`ListGateways`操作返回您的账户的网关列表和 AWS 区域。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

GatewayDisplayName

网关的显示名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

GatewayType

网关的类型。

类型：字符串

有效值：`BACKUP_VM`

必需：否

HypervisorId

网关的管理程序 ID。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

必需：否

LastSeenTime

网关上次与 AWS Backup 网关通信的时间，采用 Unix 格式和 UTC 时间。

类型：时间戳

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

GatewayDetails

服务： AWS Backup gateway

网关的详细信息。

内容

GatewayArn

网关的 Amazon 资源名称 (ARN)。使用 `ListGateways` 操作以返回账户和 AWS 区域的网关列表。

类型：字符串

长度约束：最小长度为 50。最大长度为 180。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

GatewayDisplayName

网关的显示名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

GatewayType

网关的类型。

类型：字符串

有效值：`BACKUP_VM`

必需：否

HypervisorId

网关的管理程序 ID。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

必需：否

LastSeenTime

详细信息以 Unix 格式和 UTC 时间显示 AWS Backup 网关上次与云端通信的时间。

类型：时间戳

必需：否

MaintenanceStartTime

返回网关每周维护的起始时间信息，包括星期几以及时间。请注意，这些值采用网关时区的时间。可以是每周或每月。

类型：MaintenanceStartTime 对象

必需：否

NextUpdateAvailabilityTime

显示网关下次更新可用时间的详细信息。

类型：时间戳

必需：否

VpcEndpoint

网关用来连接到云作为备份网关的虚拟私有云 (VPC) 端点的 DNS 名称。

类型：字符串

长度限制：长度下限为 1。最大长度为 255。

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK

- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Hypervisor

服务： AWS Backup gateway

表示网关将要连接到的管理程序的权限。

管理程序是用于创建和管理虚拟机并为其分配资源的硬件、软件或固件。

内容

Host

管理程序的服务器主机。这可以是 IP 地址或完全限定域名 (FQDN)。

类型：字符串

长度约束：最小长度为 3。长度上限为 128。

模式：`^.+$`

必需：否

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

KmsKeyArn

AWS Key Management Service 用于加密虚拟机管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必需：否

Name

管理程序的名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

State

管理程序的状态。

类型：字符串

有效值：`PENDING | ONLINE | OFFLINE | ERROR`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

HypervisorDetails

服务： AWS Backup gateway

这些是指定管理程序的详细信息。管理程序是用于创建和管理虚拟机并为其分配资源的硬件、软件或固件。

内容

Host

管理程序的服务器主机。这可以是 IP 地址或完全限定域名 (FQDN)。

类型：字符串

长度约束：最小长度为 3。长度上限为 128。

模式：`^.+$`

必需：否

HypervisorArn

管理程序的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

KmsKeyArn

用于加密管理程序的 AWS KMS 的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必需：否

LastSuccessfulMetadataSyncTime

这是最近一次成功同步元数据的时间。

类型：时间戳

必需：否

LatestMetadataSyncStatus

这是指定元数据同步的最新状态。

类型：字符串

有效值：CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

必需：否

LatestMetadataSyncStatusMessage

这是指定元数据同步的最新状态。

类型：字符串

必需：否

LogGroupArn

请求日志中网关组的 Amazon 资源名称 (ARN)。

类型：字符串

长度约束：最小长度为 0。最大长度为 2048。

模式：^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:*$

必需：否

Name

这是指定管理程序的名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[a-zA-Z0-9-]*$

必需：否

State

这是指定管理程序的当前状态。

可能的状态包括 PENDING、ONLINE、OFFLINE 或 ERROR。

类型：字符串

有效值：PENDING | ONLINE | OFFLINE | ERROR

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

MaintenanceStartTime

服务： AWS Backup gateway

这是网关的每周维护开始时间，包括一周中的星期几以及时间。请注意，这些值采用网关时区的时间。可以是每周或每月。

内容

HourOfDay

维护开始时间的小时部分以 hh 表示，其中 hh 是小时数（0 到 23）。一天中的时间以网关所在的时区为准。

类型：整数

有效范围：最小值为 0。最大值为 23。

必需：是

MinuteOfHour

维护开始时间的分钟部分以 mm 表示，其中 mm 是分钟数（0 到 59）。小时中的分钟以网关所在的时区为准。

类型：整数

有效范围：最小值为 0。最大值为 59。

必需：是

DayOfMonth

维护开始时间的日期的组成部分表示为从 1 到 28 的序数，其中 1 表示该月的第一天，28 表示该月的最后一天。

类型：整数

有效范围：最小值为 1。最大值为 31。

必需：否

DayOfWeek

介于 0 和 6 之间的序数，代表一周中的某一天，其中 0 代表星期日，6 代表星期六。星期数以网关所在的时区为准。

类型：整数

有效范围：最小值为 0。最大值为 6。

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

Tag

服务： AWS Backup gateway

一个用于管理、筛选和搜索资源的键值对。允许使用的字符包括 UTF-8 字母、数字、空格以及以下字符：+ - = . _ : /。

内容

Key

标签键值对中的键部分。键不能以 aws: 开头。

类型：字符串

长度限制：长度下限为 1。长度上限为 128。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

必需：是

Value

标签键值对中的值部分。

类型：字符串

长度约束：最小长度为 0。最大长度为 256。

模式：^[^\x00]*$

必需：是

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

VirtualMachine

服务： AWS Backup gateway

位于管理程序上的虚拟机。

内容

HostName

虚拟机的主机名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[a-zA-Z0-9-]*$

必需：否

HypervisorId

虚拟机的管理程序的 ID。

类型：字符串

必需：否

LastBackupDate

虚拟机的最新备份日期，采用 Unix 格式和 UTC 时间。

类型：时间戳

必需：否

Name

虚拟机的名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：^[a-zA-Z0-9-]*$

必需：否

Path

虚拟机的路径。

类型：字符串

长度限制：长度下限为 1。最大长度为 4096。

模式：`^[^\x00]+$`

必需：否

ResourceArn

虚拟机的 Amazon 资源名称 (ARN)。例如：`arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

VirtualMachineDetails

服务： AWS Backup gateway

您的 `VirtualMachine` 对象，按其 Amazon 资源名称 (ARN) 排序。

内容

HostName

虚拟机的主机名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

HypervisorId

虚拟机的管理程序的 ID。

类型：字符串

必需：否

LastBackupDate

虚拟机的最新备份日期，采用 Unix 格式和 UTC 时间。

类型：时间戳

必需：否

Name

虚拟机的名称。

类型：字符串

长度约束：最小长度为 1。最大长度为 100。

模式：`^[a-zA-Z0-9-]*$`

必需：否

Path

虚拟机的路径。

类型：字符串

长度限制：长度下限为 1。最大长度为 4096。

模式：`^[^\x00]+$`

必需：否

ResourceArn

虚拟机的 Amazon 资源名称 (ARN)。例如：`arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`。

类型：字符串

长度约束：最小长度为 50。最大长度为 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必需：否

VmwareTags

这些是与指定虚拟机关联的 VMware 标签的详细信息。

类型：VmwareTag 对象数组

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

VmwareTag

服务： AWS Backup gateway

VMware 标签是附加到特定虚拟机的标签。标签是您可用来管理、筛选和搜索资源的键值对。

VMware 标签的内容可以与 AWS 标签进行匹配。

内容

VmwareCategory

这是 VMware 的类别。

类型：字符串

长度限制：长度下限为 1。最大长度为 80。

必需：否

VmwareTagDescription

这是用户定义的 VMware 标签描述。

类型：字符串

必需：否

VmwareTagName

这是用户定义的 VMware 标签名称。

类型：字符串

长度限制：长度下限为 1。最大长度为 80。

必需：否

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS 适用于 Ruby V3 的 SDK

VmwareToAwsTagMapping

服务： AWS Backup gateway

这将显示 VMware 标签与相应 AWS 标签的映射。

内容

AwsTagKey

AWS 标签键值对的关键部分。

类型：字符串

长度限制：长度下限为 1。长度上限为 128。

模式：`^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必需：是

AwsTagValue

AWS 标签键值对的值部分。

类型：字符串

长度约束：最小长度为 0。最大长度为 256。

模式：`^[^\x00]*$`

必需：是

VmwareCategory

这是 VMware 的类别。

类型：字符串

长度限制：长度下限为 1。最大长度为 80。

必需：是

VmwareTagName

这是用户定义的 VMware 标签名称。

类型：字符串

长度限制：长度下限为 1。最大长度为 80。

必需：是

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS 适用于 Ruby V3 的 SDK

常见参数

以下列表包含所有操作用于使用查询字符串对 Signature Version 4 请求进行签名的参数。任何特定于操作的参数都列在该操作的主题中。有关 Signature Version 4 的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

Action

要执行的操作。

类型：字符串

必需：是

Version

编写请求所针对的 API 版本，格式为 YYYY-MM-DD。

类型：字符串

必需：是

X-Amz-Algorithm

您用于创建请求签名的哈希算法。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

有效值：AWS4-HMAC-SHA256

必需：条件

X-Amz-Credential

凭证范围值，该值是一个字符串，其中包含您的访问密钥、日期、您要定位的区域、您请求的服务以及终止字符串（“aws4_request”）。值采用以下格式表示：access_key/YYYYMMDD/region/service/aws4_request。

有关更多信息，请参阅《IAM 用户指南》中的创建已签名的 AWS API 请求。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-Date

用于创建签名的日期。格式必须为 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期时间是有效的 X-Amz-Date 值：20120325T120000Z。

条件：X-Amz-Date 对于所有请求都是可选的；它可以用于覆盖对请求签名所使用的日期。如果以 ISO 8601 基本格式指定 Date 标头，则不需要 X-Amz-Date。使用 X-Amz-Date 时，它始终会覆盖 Date 标头的值。有关更多信息，请参阅《IAM 用户指南》中的 AWS API 请求签名的元素。

类型：字符串

必需：条件

X-Amz-Security-Token

通过调用 AWS Security Token Service（AWS STS）获得的临时安全令牌。有关支持来自 AWS STS 的临时安全凭证的服务列表，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。

条件：如果您使用来自 AWS STS 的临时安全凭证，则必须包含安全令牌。

类型：字符串

必需：条件

X-Amz-Signature

指定从要签名的字符串和派生的签名密钥计算的十六进制编码签名。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-SignedHeaders

指定作为规范请求的一部分包含的所有 HTTP 标头。有关指定已签名标头的更多信息，请参阅《IAM 用户指南》中的创建已签名的 AWS API 请求。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

常见错误

本部分列出了所有 AWS 服务的常见 API 操作错误。对于特定于此服务的 API 操作的错误，请参阅该 API 操作的主题。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：400

IncompleteSignature

请求签名不符合 AWS 标准。

HTTP 状态代码：400

InternalFailure

由于未知错误、异常或故障，请求处理失败。

HTTP 状态代码：500

InvalidAction

所请求的操作无效。验证操作是否已正确键入。

HTTP 状态代码：400

InvalidClientTokenId

在我们的记录中没有所提供的 X.509 证书或 AWS 访问密钥 ID。

HTTP 状态代码：403

NotAuthorized

您无权执行此操作。

HTTP 状态代码：400

OptInRequired

AWS 访问密钥 ID 需要订阅服务。

HTTP 状态代码：403

RequestExpired

请求到达服务的时间超过请求上的日期戳或请求到期日期 (如针对预签名 URL) 15 分钟，或者请求上的日期戳离到期还有 15 分钟以上。

HTTP 状态代码：400

ServiceUnavailable

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：503

ThrottlingException

由于请求限制而导致请求被拒绝。

HTTP 状态代码：400

ValidationError

输入未能满足 AWS 服务指定的约束。

HTTP 状态代码：400

的文档历史记录 AWS Backup

- API 版本：2023 年 12 月 6 日
- 最新文档更新：2024 年 6 月 3 日

下表列出了自 2019 年 1 月推出该服务以来至今的所有 AWS Backup 发布情况。如需对此文档更新的通知，您可以在上方订阅 RSS 源。

更改	描述	日期
AWS Backup 功能区域扩张	AWS Backup Amazon EBS 快照存档层的支持现已在以下区域提供： • 中国（北京） • 中国（宁夏） • AWS GovCloud （美国西部） • AWS GovCloud （美国东部）	2024年6月3日
更新了 AWS 托管策略	AWS Backup `backup:TagResource` 为以下托管策略添加了权限： • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup 有关更多信息，请参阅政策更新。	2024 年 5 月 17 日

更改	描述	日期
AWS Backup 现已在加拿大西部（卡尔加里）地区推出	AWS 区域 加拿大西部（卡尔加里）现已提供多种资源类型的备份和恢复。 有关兼容的备份功能，请参阅功能可用性 AWS 区域。 有关支持的资源类型，请参阅支持的服务 AWS 区域。	2024 年 3 月 14 日
为托管策略添加了权限	AWS Backup 更新AWSServiceRolePolicyForBackupRestoreTesting了策略，在还原测试功能中添加了支持其他资源类型的权限。 有关添加的特定权限的更多信息，请参阅策略更新。	2024年2月14日
ONTAP 卷对 FSx 的备份和还原支持 FlexGroup	AWS Backup 现在大多数都支持 ONTAP FlexGroup 卷的 FSx 备份和恢复。 AWS 区域 有关更多信息，请参阅还原 Amazon FSx 文件系统。 .	2024 年 1 月 10 日
支持 SAP HANA HA 备份和还原	AWS Backup 现在在 Amazon EC2 备份和恢复上支持 SAP HANA 高可用性数据库。 有关更多信息，请参阅 Amazon EC2 上的 SAP HANA 备份和还原 SAP HANA 高可用性系统	2023 年 12 月 21 日

更改	描述	日期
AWS Backup 用于恢复测试的 Audit Manager 控制	AWS Backup Audit Manager 现在可以控制资源达到目标的恢复时间，以帮助监控恢复时间。此控制功能可检查某资源的还原时间是否符合目标持续时间。 有关更多信息，请参阅 控制和修复 和 审核还原测试。	2023 年 12 月 18 日
支持 Amazon EBS 冷存储	AWS Backup 现在支持将 EBS 备份从温存储过渡到冷存储。有关更多信息，请参阅 • 适用于冷存储的 Amazon EBS 归档层 • 生命周期和存储层 • 创建备份计划	2023 年 11 月 27 日
还原测试简介	AWS Backup 引入了恢复测试，它可以自动定期评估恢复的可行性，并能够监控恢复作业的持续时间。 有关更多信息，请参阅还原测试。	2023 年 11 月 27 日

更改	描述	日期
更新了 AWS 托管策略	AWS Backup 已将权限`ec2:DescribeSnapshotTierStatus` 和`ec2:ModifySnapshotTier` 添加到托管策略`AWSBackupServiceRolePolicyForBackups` 和`AWSBackupServiceLinkedRolePolicyForBackup` 。AWS Backup 还`ec2:RestoreSnapshotTier` 向托管策略添加了权限`ec2:DescribeSnapshotTierStatus` 和`AWSBackupServiceRolePolicyForRestores` 。 用户必须拥有这些权限，才能选择将存储在一起的 Amazon EBS 资源转移 AWS Backup 到存档存储以及从存档存储层恢复资源。 有关更多信息，请参阅策略更新。	2023 年 11 月 27 日

更改	描述	日期
添加了传递角色权限以支持还原测试。	AWS Backup 已`restore-testing.backup.amazonaws.com` 添加到`IamPassRolePermissions` 和`IamCreateServiceLinkedRolePermissions` 。为了代表客户 AWS Backup 进行恢复测试，必须添加此项。	2023 年 11 月 27 日
添加了新的服务相关角色	AWS Backup 添加了名为的新服务相关角色 `AWSServiceRoleForBackupRestoreTesting` ，该角色为执行还原测试提供了备份权限。 这个新的服务相关角色 AWS Backup 提供了执行还原测试所需的权限。权限包括适用于要在还原测试中包括的以下服务的操作 `list, read, and write` ：Aurora、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS 和 Amazon S3。	2023 年 11 月 27 日

更改	描述	日期
控制台中的新工作指标 AWS Backup 控制面板	AWS Backup 控制台现在显示作业仪表板，通过新的可视用户界面以及支持的服务的汇总备份、复制和还原指标，简化了大规模的备份运行状况监控 AWS Backup。 工作控制面板可在所有可用 Audit M AWS Backup anager 的地区使用。 未列出的地区仍然可以访问CloudWatch 控制面板。 有关更多信息，请参阅 AWS Backup 控制台控制面板。	2023 年 11 月 15 日
对嵌套堆栈备份的支持	AWS Backup 已扩展其对 AWS CloudFormation 资源备份的支持。您的 CloudFormation 应用程序堆栈中包含嵌套堆栈，可以包含在备份中。 有关更多信息，请参阅 CloudFormation 堆栈备份。	2023 年 11 月 8 日
支持中国（北京）和中国（宁夏）区域中的 Amazon S3。	AWS Backup 中国（北京）和中国（宁夏）地区现已提供对 Amazon S3 的支持。 相关详情，请参阅按区域划分的特征可用性。	2023 年 10 月 26 日

更改	描述	日期
支持 Amazon Aurora 连续备份和 P oint-in-time 恢复	AWS Backup 现在支持 Aurora 资源的连续备份和 point-in-time 恢复 (PITR)。 有关更多信息，请参阅连续备份和 P oint-in-time 恢复。	2023 年 9 月 7 日
AWS CloudFormation 堆栈支持排除资源	AWS Backup 现在支持从 AWS CloudFormation 堆栈中排除所选资源的选项。 有关更多信息，请参阅 AWS CloudFormation 堆栈备份。	2023 年 9 月 6 日
备份计划规则引入了时区灵活性	AWS Backup 计划规则现在可以为备份窗口指定时区。 有关更多信息，请参阅管理备份计划。	2023 年 8 月 28 日
AWS Backup 现已在以色列（特拉维夫）地区推出	现在，在新的以色列（特拉维夫）地区提供了许多 AWS Backup 功能。 要查看支持哪些资源，请访问按 AWS 区域划分的特征可用性。	2023 年 8 月 22 日
AWS Backup Audit Manager 现在支持委派的管理员帐户	AWS Backup 现在，授权的管理员帐户可以访问 Audit Manager 报告的生成。有关更多信息，请参阅 • 使用 Audit Manager AWS Backup 审核备份并创建报告 • 使用审计报告 • 委托管理员	2023 年 8 月 16 日

更改	描述	日期
预览逻辑气隙备份保管库	AWS Backup 现在提供了一种新型备份保管库的预览，以帮助补充数据保护操作。 有关更多信息，请参阅逻辑气隙保管库（预览版）。	2023 年 8 月 8 日
AWS Backup 增强 Amazon S3 备份	AWS Backup 提高了 S3 存储桶备份的性能、大小和速度。 有关更多信息，请参阅 Amazon S3 备份。	2023 年 8 月 1 日
还原标签功能现已在中国区域推出	现在，在中国（北京）或中国（宁夏）区域中创建还原作业时，可以复制作为备份一部分的标签。 有关更多信息，请参阅在还原期间复制标签。	2023 年 7 月 17 日
AWS Backup 现在在其他区域支持 Amazon S3	AWS Backup 欧洲（西班牙）、欧洲（苏黎世）、亚太地区（海得拉巴）和亚太地区（墨尔本）地区现已提供对 Amazon S3 的支持。 相关详情，请参阅按区域划分的特征可用性。	2023 年 7 月 6 日

更改	描述	日期
跨账户复制扩展到其他区域	AWS Backup 现在支持以下地区大多数资源的跨账户备份副本：亚太地区（雅加达）、中东（巴林）、亚太地区（香港）、非洲（开普敦）、欧洲（米兰）、亚太地区（大阪）、中东（阿联酋）、欧洲（西班牙）、欧洲（苏黎世）、亚太地区（海得拉巴）和亚太地区（墨尔本）。 相关详情，请参阅按区域划分的特征可用性。	2023 年 7 月 5 日
Backup Audit Manager 在 GovCloud 各地区可用	AWS Backup 已将 Au AWS Backup dit Manager 扩展到 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）。 相关详情，请参阅按区域划分的特征可用性。	2023 年 6 月 29 日
跨账户管理现已在区域中 GovCloud 推出	AWS Backup 现在支持跨账户管理 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）中的资源。 有关更多信息，请参阅跨多个 AWS 账户管理 AWS Backup 资源。	2023 年 6 月 29 日

更改	描述	日期
在其他区域支持 Amazon Aurora 的跨区域复制	AWS Backup 现在支持 Aurora 集群往返以下地区的跨区域备份副本：亚太地区（雅加达）、中东（巴林）、亚太地区（香港）、非洲（开普敦）、欧洲（米兰）、中东（阿联酋）、欧洲（西班牙）、欧洲（苏黎世）、亚太地区（海得拉巴）和亚太地区（墨尔本）。	2023 年 6 月 5 日
还原时复制标签	现在，创建还原作业时，可以复制作为备份一部分的标签。 有关更多信息，请参阅在还原期间复制标签。	2023 年 5 月 22 日
AWS Backup 与 AWS 用户通知集成	现在，您可以选择通过 AWS 用户通知控制台接收与备份、复制和还原事件相关的通知。 有关更多信息，请参阅AWS 用户通知入门。	2023 年 5 月 10 日
在四个新的区域中提供跨区域备份	AWS Backup 现在支持中东（阿联酋）地区、欧洲（西班牙）地区、欧洲（苏黎世）地区和亚太地区（海得拉巴）地区的跨区域备份。	2023 年 4 月 28 日

更改	描述	日期
扩展了跨区域 AWS Backup 复制支持	现在，可以在以下区域中对 Amazon EFS、VMware 和 DynamoDB 资源进行跨区域备份：亚太地区（雅加达）、中东（巴林）、亚太地区（香港）、非洲（开普敦）和欧洲地区（米兰）。	2023 年 4 月 28 日
南美洲（圣保罗）区域中的 Amazon S3 备份和还原	AWS Backup 南美洲（圣保罗）地区现已提供对 Amazon S3（亚马逊简单存储服务）的支持。 有关更多信息，请参阅 Amazon S3 备份。	2023 年 4 月 20 日
AWS Backup 扩展到亚太地区（墨尔本）地区	AWS Backup 现已在亚太地区（墨尔本）地区推出。 有关更多信息，请参阅按 AWS 地区划分的功能可用性。	2023 年 4 月 20 日
扩展了对 Amazon S3 的区域支持	AWS Backup （美国东部）和（美国西部）地区现已提供对 Amazon S3 AWS GovCloud（亚马逊简单存储服务）的支持 AWS GovCloud 有关更多信息，请参阅 Amazon S3 备份。	2023 年 4 月 19 日

更改	描述	日期
备份和还原 Amazon EC2 实例上的 SAP HANA 数据库	AWS Backup 现在可以备份和恢复在大多数地区的 Amazon EC2 实例上运行的 SAP HANA 数据库。 有关更多信息，请参阅 Amazon EC2 实例上的 SAP HANA 数据库备份。	2023 年 4 月 17 日
AWS Backup 现已在欧洲（西班牙）、欧洲（苏黎世）和亚太地区（海得拉巴）地区推出	AWS Backup 支持已扩展到新的区域，包括欧洲（西班牙）、欧洲（苏黎世）和亚太地区（海得拉巴）。可以在这些区域中备份和还原支持的资源。 有关更多信息，请参阅按 AWS 地区划分的功能可用性。	2023 年 4 月 13 日
更新了 AWS 托管策略 AWSBackupAuditAccess	更新了 AWS 托管策略AWSBackupAuditAccess。 AWS Backup 将 API config:DescribeComplianceByConfigRule 中的资源选择替换为通配符资源。 有关更多信息，请参阅 AWS Backup的策略更新。	2023 年 4 月 11 日
带有 Amazon 日志的虚拟机管理程序 CloudWatch	AWS Backup 网关用户现在可以将虚拟机管理程序与 CloudWatch 日志集成以维护日志。有关更多信息，请参阅编辑虚拟机管理程序配置和 CloudWatch 日志。	2023 年 3 月 29 日

更改	描述	日期
扩展了对 Amazon S3 的区域支持	AWS Backup 亚太地区（雅加达）和中东（阿联酋）地区现已提供对 Amazon S3 的支持。	2023 年 3 月 22 日
虚拟机增量备份改进	遇到 CBT（更改块跟踪）数据问题的 VMware VM（虚拟机）备份现在包含其他信息，有助于进行补救和故障排除。 有关更多信息，请参阅增量虚拟机备份和对虚拟机进行故障排除。	2023 年 3 月 15 日
AWS Backup 支持多个网络适配器	AWS Backup 网关现在支持配置多个网络适配器 有关配置网络适配器的更多信息，请参阅《AWS Backup 开发人员指南》中的在 VMware 中为多个 NIC 配置网关。	2023 年 3 月 8 日
AWS Backup 支持 vSphere 8	AWS Backup 现在支持备份和还原在 VMware vSphere 8 上运行的虚拟机。 有关支持的 VMware 选项的更多信息，请参阅《AWS Backup 开发人员指南》中的支持的虚拟机。	2023 年 3 月 8 日

更改	描述	日期
AWS Backup Audit Manager 支持 Amazon RDS 多可用区备份	Backup Audit Manager 现在支持 Amazon Relational Database Service 多可用区备份。 有关更多信息，请参阅如何使用 Audit Manager AWS Backup 审计备份和创建报告。	2023 年 2 月 1 日
AWS Backup 为 Amazon Timestream 表提供增量备份	AWS Backup 现在为 Timestream 备份提供了扩展的备份功能。备份计划现在可以进行增量备份，以缩短备份 Timestream 资源所需的时间并降低存储成本。 有关更多信息，请参阅 Amazon Timestream 备份。	2023 年 1 月 23 日
AWS Backup 现已在迪拜上市	AWS Backup 已扩展到中东（阿联酋）地区。可以在此区域中备份和还原支持的资源。	2023 年 1 月 17 日
跨区域复制在其他区域提供	AWS Backup 现在在亚太地区（雅加达）地区、中东（巴林）地区、亚太地区（香港）地区、非洲（开普敦）地区和欧洲（米兰）地区为大多数资源提供跨区域备份。 有关更多信息，请参阅跨 AWS 区域创建备份副本。	2022 年 12 月 21 日

更改	描述	日期
Backup Gateway 带宽限制和节流	AWS Backup 网关现在允许限制从网关 AWS Backup 到的上传吞吐量，以控制网关使用的网络带宽量。 为了支持此功能， AWS Backup 已创建并更新了托管策略，包括`AWSBackupFullAccess` 和`AWSBackupOperatorAccess` 。 有关更多信息，请参阅 Backup Gateway 带宽限制。	2022 年 12 月 15 日
Backup Gateway VMware 标签支持	AWS Backup 网关现在支持 VMware 标签。用户可以更加灵活地创建与用于虚拟机的 AWS 标签相匹配的标签。 为了支持此功能， AWS Backup 已创建并更新了托管策略`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` ，包括`AWSBackupFullAccess` 、和`AWSBackupOperatorAccess` 。 有关更多信息，请参阅 VMware 标签。	2022 年 12 月 15 日
AWS Backup 支持 Amazon Timestream	AWS Backup 现在支持备份和恢复 Amazon Timestream 表。有关更多信息，请参阅 Amazon Timestream 备份。	2022 年 12 月 13 日

更改	描述	日期
AWS Backup 提供合法保留	AWS Backup 引入了一种新工具，可通过法律封存来帮助保护恢复点。有关更多信息，请参阅依法保留。	2022 年 11 月 27 日
AWS Backup Audit Manager 跨区域和跨账户报告	AWS Backup Audit Manager 为合规和工作报告带来了更多功能。用户可以生成报告，其中包含多个区域和多个账户。 有关更多信息，请参阅使用审计报告。	2022 年 11 月 27 日
AWS Backup 支持 Amazon Redshift	AWS Backup 现在支持备份 Amazon Redshift 集群和恢复亚马逊 Redshift 集群和表。有关更多信息，请参阅 Amazon Redshift 备份。	2022 年 11 月 27 日
AWS Backup 为备份 AWS CloudFormation 应用程序堆栈提供支持	AWS Backup 通过备份堆栈 CloudFormation 并恢复其中的资源，提供备份和恢复包含多个资源的应用程序的功能。 有关更多信息，请参阅应用程序堆栈备份。	2022 年 11 月 27 日
AWS Backup 提供委托管理员帐户和备份策略授权	AWS Backup 注册的帐户 AWS Organizations 可以将成员帐户指定为委派管理员帐户。 有关更多信息，请参阅使用管理多个账户 AWS Organizations。	2022 年 11 月 27 日

更改	描述	日期
Amazon EC2 实例上的 SAP HANA 备份和还原（公开预览版）	AWS Backup 而且 AWS Backint 提供了在 EC2 实例上备份和恢复 SAP HANA 数据库的功能的集成公开预览。 有关更多信息，请参阅 Amazon EC2 实例上的 SAP HANA 公开预览版。 为了支持此预览版， AWS Backup 为这些功能提供了策略更新和新的AWS 托管策略。	2022 年 11 月 20 日
将 VMware 还原到 Amazon EC2 实例	AWS Backup 除了能够将虚拟机还原到 EBS、VMware、VMware Cloud on 和 VMware Cloud 开启 VMware Cloud 之外，现在还能够将虚拟机还原到 Amazon EC2 实例。 AWS AWS Outposts 有关更多信息，请参阅有关如何使用 AWS Backup 控制台恢复虚拟机恢复点的文档。	2022 年 11 月 9 日
扩展了 AWS Backup 文件库锁定功能	AWS Backup 现在可以在治理模式下创建文件库锁以获得额外的 IAM 保护，也可以在合规模式下创建文件库锁以确保不可变性。 相关详情，请参阅 AWS Backup 保管库锁定。	2022 年 10 月 4 日

更改	描述	日期
AWS Backup Audit Manager 现已在非洲（开普敦）地区和欧洲（米兰）地区推出	AWS Backup Audit Manager 已扩展到非洲（开普敦）地区和欧洲（米兰）地区。有关 Backup Audit Manager 的更多信息，请参阅使用 Audit Manager AWS Backup 审核备份和创建报告。	2022 年 9 月 14 日
AWS Backup 将 Amazon CloudWatch 指标引入 Backup 控制台控制面板	AWS Backup 增强了其 Backup 控制台控制台控制面板，以显示备份和还原任务的集成 Amazon CloudWatch 指标，从而提高了监控能力和灵活性。	2022 年 9 月 8 日
支持还原期间的额外 Amazon EBS 加密灵活性	AWS Backup 现在在恢复 Amazon EBS 快照期间提供了额外的加密选择。	2022 年 9 月 1 日
AWS Backup 支持 Amazon S3 跨账户和跨区域备份复制	AWS Backup 现在为 Amazon S3 备份提供跨区域和跨账户备份复制。 有关更多信息，请参阅 Amazon S3 备份。	2022 年 7 月 28 日
AWS Backup Audit Manager 为适用于 ONTAP 的 FSx 提供了额外的控制支持	AWS Backup Audit Manager 现在提供了其他控件来支持监控和审计 FSx 的 ONTAP 卷，包括受备份计划保护的备份资源和上次创建的恢复点。 有关更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施。	2022 年 7 月 22 日

更改	描述	日期
AWS Backup 增加了对备份和恢复 PostgreSQL 和 MySQL 集群的 Amazon RDS 多可用区集群的支持	AWS Backup 添加了多可用区集群备份和还原选项，其中包含一个主数据库实例和两个可读备用数据库实例。 要了解更多信息，请参阅 Amazon RDS Multi-AZ 备份。	2022 年 7 月 20 日
AWS Backup Audit Manager 为恢复点的创建添加了新的控件	AWS Backup Audit Manager 提供了一种新的审计控制，以增强合规支持。 `Last recovery point created` 是一个可选附加控件，用于确保在指定时间范围内创建恢复点。 要了解更多信息，请参阅上次创建的恢复点控件。	2022 年 6 月 29 日
添加了 AWS Backup 网关终端节点示例	AWS Backup Gateway 提供了一个示例端点来帮助用户连接 VPN（虚拟专用网络）。有关更多信息，请参阅创建 AWS Backup VPC 终端节点。	2022 年 6 月 14 日
AWS Backup 现在提供适用于 VMware 的亚马逊 VPC 终端节点	AWS Backup 现在支持适用于 VMware 的 Amazon VPC 终端节点，使您能够在 VMware 环境和 AWS 使用之间使用虚拟专用网络 AWS PrivateLink。 有关更多信息，请参阅创建网关以及 AWS Backup 和 AWS PrivateLink。	2022 年 6 月 1 日

更改	描述	日期
AWS Backup Audit Manager 为亚马逊 S3 提供额外的控制支持	Backup Audit Manager 现在为 S3 资源类型提供合规性控件受备份计划保护的备份资源支持。 有关更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施。	2022 年 5 月 25 日
AWS Backup Audit Manager 为 Storage Gateway 提供了额外的控制支持	Backup Audit Manager 现在为 Storage Gateway 资源类型提供合规性控件受备份计划保护的备份资源支持。 有关更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施。	2022 年 5 月 25 日
支持适用于 OpenZFS 的 Amazon FSx	AWS Backup 现在为备份和恢复到 FSX 的 OpenZFS 文件系统提供了额外的数据保护管理。	2022 年 5 月 18 日
AWS Backup Audit Manager 支持 VMware	AWS Backup 现在在 Backup Audit Manager 控制和修复中为虚拟机提供支持。有关更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施。	2022 年 5 月 11 日
Amazon FSx 现已在亚太地区（大阪）区域提供支持	AWS Backup 现在提供在亚太地区（大阪）地区备份 Amazon FSx 以及往返亚太地区（大阪）地区的跨区域副本。	2022 年 4 月 26 日

更改	描述	日期
支持适用于 Lustre 的 Amazon FSx Persistent_2	AWS Backup 现已全面提供对 Amazon FSx for Lustre 的支持，与 Persistent_1 文件系统相比，它支持的每个存储单元的吞吐量更高。	2022 年 4 月 5 日
VMware 增强功能	AWS Backup 现在提供还原到 Amazon EBS 卷、磁盘级别恢复以及对 VMware on AWS Outposts的支持。有关更多信息，请参阅还原虚拟机。	2022 年 3 月 31 日
AWS Backup 亚太地区（雅加达）上市	AWS Backup 现已向亚太地区（雅加达）地区的客户开放。	2022 年 3 月 17 日
Audit Manager AWS Backup 的新控件	AWS Backup Audit Manager 引入了三种新的审计控制措施：跨区域复制、跨账户复制和备份文件库锁定。有关更多信息，请参阅 AWS Backup Audit Manager 控件和补救措施。	2022 年 3 月 17 日
Support AWS PrivateLink	AWS Backup 使用 f AWS PrivateLink o AWS Backup r，您可以使用您的 VPC 中的接口终端节点直接连接，而不必通过公共互联网进行连接。接口端点可以直接从本地或其他 AWS 区域的应用程序访问。有关更多信息，请参阅 AWS Backup 和 AWS PrivateLink。	2022 年 2 月 28 日

更改	描述	日期
支持 Amazon Simple Storage Service (Amazon S3)	除中国（北京）区域、中国（宁夏）区域、（美国西部）和 AWS GovCloud AWS GovCloud （美国东部）区域外，Amazon S3 已在所有 AWS 区域 区域正式上市。AWS Backup 有关更多信息，请参阅使用 Amazon S3 数据。	2022 年 2 月 14 日
支持中国区域的高级 DynamoDB 备份 AWS	中国（北京）和中国（宁夏）区域现已推出高级 DynamoDB 备份。有关更多信息，请参阅高级 DynamoDB 备份。	2022 年 1 月 18 日
Amazon S3 支持的公开预览版	AWS Backup 提供了 Amazon S3 备份的公开预览。有关更多信息，请参阅 使用 Amazon S3 数据。	2021 年 11 月 30 日
对 VMware 虚拟机 (VM) 的支持	现在，您可以使用 AWS Backup 自动备份 VMware 虚拟机。有关更多信息，请参阅虚拟机备份。	2021 年 11 月 30 日

更改	描述	日期
支持高级 DynamoDB 备份	现在，您可以使用 AWS Backup 对您创建的所有新 DynamoDB 表备份执行以下功能：冷存储分层、成本分配标记、跨区域复制、跨账户复制、独立加密以及从源 DynamoDB 表复制标签。有关更多信息，请参阅高级 DynamoDB 备份亚马逊 DynamoDB 开发者指南和使用 AWS Backup DynamoDB。	2021 年 11 月 23 日
Support 支持增强 AWS 中国地区的 AWS Backup 资源分配	AWS Backup 资源分配增强功能现已在中国（北京）区域和中国（宁夏）区域推出。有关更多信息，请参阅将资源分配给备份计划。	2021 年 11 月 16 日
推出 AWS Backup 资源分配增强功能	Backup 资源分配增强功能为您提供了额外的精细控制和新的简化流程，用于部署保护成千上万资源的 AWS 备份计划。借助此功能，可以在使用 AWS Backup保护数据时提高速度、灵活性和精度。有关更多信息，请参阅将资源分配给备份计划。	2021 年 11 月 10 日
支持 Amazon Neptune	现在，您可以使用 AWS Backup 来备份 Amazon Neptune 集群。要了解更多信息，请参阅什么是 AWS Backup？	2021 年 11 月 5 日

更改	描述	日期
支持 Amazon DocumentDB	现在，您可以使用 AWS Backup 备份亚马逊文档数据库集群。要了解更多信息，请参阅什么是 AWS Backup？	2021 年 11 月 5 日
Support 支持 AWS 中国地区的 AWS Backup 文件库锁	AWS Backup 文件库锁现已在中国（北京）区域和中国（宁夏）区域推出。相关详情，请参阅 AWS Backup 保管库锁定。	2021 年 11 月 3 日
推出 AWS Backup 文件库锁	使用 AWS Backup Vault Lock，您可以防止删除存储在 AWS Backup 备份保管库中的备份。相关详情，请参阅 AWS Backup 保管库锁定。	2021 年 10 月 7 日
发布 Audi AWS Backup t Manager 合规报告	借助合规性报告，您可以根据在 Audit Manager 框架中定义的控制措施，生成有关备份活动和资源合 AWS Backup 规性的每日报告。有关更多信息，请参阅合规性报告模板。	2021 年 10 月 5 日
AWS CloudFormation 支持 Audit AWS Backup Manager	借 AWS CloudFormation助，您现在可以以安全、 AWS Backup 可重复的方式大规模部署 Audit Manager 框架、控件和报告计划。有关更多信息，请参阅使用 Audit Manager 备份 AWS Backup 审计和报告。	2021 年 10 月 4 日

更改	描述	日期
Audit Man AWS Backup ager 上线	借 AWS Backup 助 Audit Manager，您现在可以为备份活动和资源定义控制措施，并识别不符合您的控制措施的活动和资源。您还可以使用 Audi AWS Backup t Manager 生成每日报告和按需报告，这些报告可作为在一段时间内遵守您定义的控制措施的证据。有关更多信息，请参阅使用 Audit Manager 备份 AWS Backup 审计和报告。	2021 年 8 月 24 日
支持新的异步恢复点操作	AWS Backup 现在，如果您修改或删除了原始 IAM 角色，则会担任服务相关角色来管理您的备份生命周期规则。相关详情，请参阅删除备份。	2021 年 8 月 23 日
支持 Amazon EBS 多卷、崩溃一致性备份	现在，当您使用保护您的 Amazon EC2 实例时，默认情况下， AWS Backup 会对附加 AWS Backup 到每个 Amazon EC2 实例的所有 Amazon EBS 卷进行多卷、崩溃一致性备份。有关更多信息，请参阅创建 Amazon EBS 多卷、崩溃一致性备份。	2021 年 6 月 14 日

更改	描述	日期
额外支持 Amazon FSx AWS 区域	现在，您可以使用 AWS Backup 在以下区域保护您的 Amazon FSx 文件系统： AWS GovCloud (US)、欧洲（米兰）区域、非洲（开普敦）地区和中东（巴林）区域。有关更多信息，请参阅《AWS 一般参考》中的 AWS Backup 端点和限额。	2021 年 4 月 15 日
支持 Amazon FSx 跨区域和跨账户备份	现在，您可以使用跨账户 AWS Backup 复制 Amazon FSx 备份 AWS 区域 。有关更多信息，请参阅创建备份副本。 如果您使用客户托管策略，则应添加新权限 `fsx:CopyBackup` 以防止现有备份作业失败。有关该权限，请参阅客户托管策略中 Amazon FSx 备份策略的最后一个语句。	2021 年 4 月 12 日
支持 Amazon EFS 备份的成本分配标签	现在，您可以使用成本分配标签来详细跟踪 Amazon EFS 备份的成本，并使用查看和筛选这些标签 AWS Cost Explorer。有关更多信息，请参阅使用成本分配标签。	2021 年 4 月 7 日
FedRAMP 高影响授权	AWS Backup 现已获得支持 FedRAMP 高工作负载的授权。有关更多信息，请参阅合规性计划范围内的AWS 服务。	2021 年 3 月 25 日

更改	描述	日期
全新 AWS 区域	AWS Backup 现已在亚太地区（大阪）地区推出。在该区域， AWS Backup 目前不支持该区域的 Storage Gateway、Amazon FSx 和跨账户备份。有关更多信息，请参阅《AWS 一般参考》中的 AWS Backup 端点和限额。	2021 年 3 月 25 日
支持恢复点批量操作	现在，您可以使用 AWS Backup 控制台自动执行批量操作，以清理备份存储库中的恢复点。相关详情，请参阅删除备份。	2021 年 3 月 23 日
支持还原到 Amazon EFS 单区存储类	现在，您可以将 Amazon EFS 备份还原到 Amazon EFS 单区存储类。相关详情，请参阅还原 Amazon EFS 文件系统。	2021 年 3 月 12 日
支持 Amazon Relational Database Service point-in-time 还原和持续备份	现在，除了编排快 AWS Backup 照备份外，您还可以使用自动执行 Amazon RDS 连续备份和执行 point-in-time 恢复 (PITR)。有关更多信息，请参阅使用 point-in-time 恢复功能还原到指定时间。	2021 年 3 月 10 日
对 Amazon 的支持 CloudWatch	现在，您可以使用 CloudWatch 来监控 AWS Backup 指标。有关更多信息，请参阅使用 Amazon 和 Amazon 监控事件 CloudWatch 和指标 EventBridge。	2021 年 2 月 3 日

更改	描述	日期
对 Amazon 的支持 EventBridge	现在，您可以使用 EventBridge 来监视 AWS Backup 事件。有关更多信息，请参阅使用 Amazon 和 Amazon 监控事件 CloudWatch 和指标 EventBridge。	2021 年 2 月 3 日
支持跨账户备份	现在 AWS Backup ，您可以使用跨多个备份资源 AWS 账户。有关更多信息，请参阅跨 AWS 账户创建备份副本。	2020 年 11 月 18 日
支持 Amazon FSx 文件系统的备份和还原	现在，您可以使用 AWS Backup 来备份 Amazon FSx 文件系统。有关更多信息，请参阅使用 Amazon FSx 文件系统。	2020 年 11 月 9 日
全新 AWS 区域	AWS Backup 现已在非洲（开普敦）和欧洲（米兰）上市 AWS 区域。有关更多信息，请参阅《AWS 一般参考》中的 AWS Backup 端点和限额。	2020 年 10 月 21 日
对启用 VSS 的 Windows 备份的支持	现在，您可以备份和还原在 Amazon EC2 实例上运行且启用 VSS（卷影复制服务）的 Windows 应用程序。有关更多信息，请参阅创建 Windows VSS 备份。	2020 年 9 月 22 日
支持 Amazon EFS 自动备份	现在，您可以使用 AWS Backup 自动备份 Amazon EFS 文件系统。有关更多信息，请参阅入门 4：创建 Amazon EFS 自动备份。	2020 年 7 月 16 日

更改	描述	日期
全新 AWS 区域	AWS Backup 现已在 AWS GovCloud (US) Region。有关更多信息，请参阅《AWS 一般参考》中的 AWS Backup 端点和限额。	2020 年 6 月 24 日
Support 支持管理多个备份 AWS 账户	现在，您可以使用管理多个 AWS 账户 备份AWS Organizations。有关更多信息，请参阅跨账户管理的工作原理。	2020 年 6 月 24 日
已将对亚马逊 Aurora 的支持添加到 AWS Backup	现在，您可以配置 AWS Backup 为为 Amazon Aurora 备份资源。有关更多信息，请参阅《Amazon Aurora 用户指南》中的备份和还原 Aurora DB 集群概述。	2020 年 6 月 10 日
Support 支持配置要使用的服务 AWS Backup	现在，您可以配置 AWS Backup 为备份特定 AWS 服务的资源。有关更多信息，请参阅选择使用管理服务 AWS Backup。	2020 年 5 月 20 日
支持备份 Amazon EC2 实例，还增加了对跨区域备份的支持	现在，您可以备份整个 Amazon EC2 实例，也可以跨 AWS 区域复制资源。有关更多信息，请参阅跨 AWS 区域创建备份副本。	2020 年 1 月 13 日
新指南	AWS 启动 AWS Backup 和《AWS Backup 开发人员指南》。	2019 年 1 月 15 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。