aws

上的 Backup 和恢复方法 AWS

AWS 规范性指导

AWS 规范性指导: 上的 Backup 和恢复方法 AWS

Table of Contents

简介 1
为什么要将 AWS 用作数据保护平台？ 2
目标业务成果 3
选择 AWS 服务 4
设计备份与恢复解决方案 6
AWS Backup 7
Amazon S3 和 Amazon S3 Glacier 9
Amazon S3 9
标准 S3 存储桶 10
维护回滚历史记录 11
自定义的配置文件 11
自定义备份和还原 11
Amazon S3 Glacier 11
使用 Amazon S3 生命周期对象转换 12
保护备份数据 13
具有 EBS 卷的 Amazon EC2 15
Amazon EC2 备份和恢复 16
AMI 或快照 16
服务器卷 17
单独的服务器卷 18
实例存储卷 18
标记和执行标准 19
创建 EBS 卷备份 19
准备 EBS 卷 20
从控制台创建快照 21
创建 AMI 21
Amazon Data Lifecycle Manager 22
AWS Backup 22
多卷备份 23
保护备份 24
归档快照 25
自动化快照和 AMI 创建 25
恢复卷或实例 26
从 EBS 快照恢复文件和目录 26

从Amazon EBS 快照还原 EBS 卷 26
从 EBS 快照创建或恢复 EC2 实例 28
从 AMI 还原正在运行的实例 28
从本地备份和恢复 30
文件网关 30
卷网关 31
磁带网关 31
备份和恢复应用程序 33
云原生 AWS 服务 34
Amazon RDS 34
使用 DNS CNAME 35
DynamoDB 36
混合架构 37
移动集中化备份管理解决方案 37
灾难恢复 39
本地灾难恢复到 AWS 39
云原生工作负载的灾难恢复 41
单个可用区中的灾难恢复 41
区域故障中的灾难恢复 42
清理备份 43
常见问题 44
我应该选择什么备份计划？ 44
我需要在我的开发账户中创建备份吗？ 44
我能否在创建快照的同时升级应用程序并继续使用 EBS 卷而不产生任何影响？ 44
后续步骤 45
资源 46
文档历史记录 48
术语表 50
..... 50
A 50
B 53
C 54
D 56
E 59
F 61
G 62

H 63
I 64
L 66
M 66
O 69
P 71
Q 73
R 73
S 76
T 78
U 80
V 80
W 80
Z 81
..... lxxxii

AWS 上的备份和恢复方法

Khurram Nizami, Amazon Web Services (AWS)

2023 年 4 月（文档历史记录）

本指南讨论如何使用适用于本地、云原生和混合架构的 Amazon Web Services (AWS) 服务实施备份和恢复方法。这些方法提供了更低的成本、更高的可扩展性和更高的持久性，满足恢复时间目标（RTO）、恢复点目标（RPO）和合规要求。

本指南面相负责保护企业 IT 和云环境中数据的技术领导者。

本指南涵盖不同的备份架构（云原生应用程序、混合环境和本地环境）。它还涵盖了相关的 Amazon Web Services (AWS) 服务，这些服务可用于为架构的不可变组件构建可扩展且可靠的数据保护解决方案。

另一种方法是对工作负载进行现代化改造，使用不可变的架构，从而减少对组件备份和恢复的需求。AWS 提供了多种服务来实现不可变的体系结构并减少对备份和恢复的需求，包括：

- 使用 AWS Lambda 的无服务器
- 使用 Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 AWS Fargate 的容器
- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 的 Amazon 机器映像 (AMI)

随着企业数据的加速增长，保护数据的任务变得更具挑战性。关于备份方法的持久性和可扩展性的问题屡见不鲜，包括以下问题：云如何帮助满足我的备份和恢复需求？

本指南包括以下主题：

- 选择数据保护 AWS 服务
- 设计备份与恢复解决方案
- 使用 AWS Backup 备份和恢复
- 使用 Amazon S3 和 Amazon S3 Glacier 进行备份和恢复
- 具有 EBS 卷的 Amazon EC2 备份和恢复
- 从本地基础设施备份和恢复到 AWS
- 将应用程序从 AWS 到您的数据中心进行备份和恢复
- 云原生的 AWS 服务的备份和恢复

- 混合架构的备份和恢复
- 使用 AWS 进行灾难恢复
- 清理备份

为什么要将 AWS 用作数据保护平台？

AWS 是一个安全、高性能、灵活、省钱且易于使用的云计算平台。AWS 负责创建、实施和管理可扩展的备份和恢复解决方案所需的无差别繁重工作。

作为数据保护策略的一部分使用 AWS 有许多优点：

- 持久性：Amazon Simple Storage Service (Amazon S3)、Amazon S3 Glacier 和 S3 Glacier Deep Archive 的设计持久性高达 99.999999999%（11 个 9）。这两个平台都提供可靠的数据备份，并且可以跨至少三个地理位置分散的可用区进行对象复制。许多 AWS 服务使用 Amazon S3 进行存储和导出/导入操作。例如，Amazon Elastic Block Store (Amazon EBS) 使用 Amazon S3 进行快照存储。
- 安全：AWS 为传输中和静态时的访问控制和数据加密提供了多种选项。
- 全球基础设施：AWS 服务遍布全球，因此您可以在符合您的合规性和工作负载要求的区域备份和存储数据。
- 合规性：AWS 基础设施已通过认证，符合以下标准，因此您可以轻松地将备份解决方案纳入现有的合规方案：
  - 服务组织控制（SOC）
  - 审核业务标准声明 (SSAE) 16 号
  - 国际标准化组织 (ISO) 27001
  - 支付卡行业数据安全标准 (PCI DSS)
  - 健康保险流通与责任法案 (HIPAA)
  - SEC1
  - 联邦风险与授权管理项目 (FedRAMP)
- 可扩展性：有了 AWS，您就不必担心容量问题。随着需求的变化，您可以向上或向下扩展消费，而无需管理开销。
- 降低总拥有成本（TCO）：AWS 运营规模降低了服务成本，有助于降低 AWS 服务的 TCO。AWS 通过降价将节省的成本转嫁给客户。
- 即用即付定价模式：根据需要购买 AWS 服务，且仅在计划使用期限内购买。AWS 定价没有预付费用、终止罚款或长期合同。

目标业务成果

本指南旨在概述可用于支持以下备份和恢复方法的 AWS 服务：

- 本地架构
- 云原生架构
- 混合架构
- AWS 原生服务
- 灾难恢复 (DR)

其中涵盖了最佳实践和注意事项以及服务概述。本指南还为您提供选择使用何种方法进行备份和恢复的权衡。

选择数据保护 AWS 服务

AWS 提供了许多存储和补充服务，可用作备份和恢复方法的一部分。这些服务可以支持云原生架构和混合架构。针对不同用例的不同服务更有效。

- Amazon S3、Amazon S3 Glacier 和 S3 Glacier 深度档案适用于混合用例和云原生用例。这些服务提供高度耐用的通用对象存储解决方案，适用于备份单个文件、服务器或整个数据中心。
- AWS Storage Gateway 非常适合混合用例。Storage Gateway 使用 Amazon S3 的强大功能来满足常见的本地备份和存储需求。您的应用程序使用以下标准存储协议通过虚拟机 (VM) 或硬件网关设备连接到服务：
  - 网络文件系统 (NFS)
  - 服务器消息块 (SMB)
  - 互联网小型计算机系统接口 (iSCSI)

  网关将这些常见的本地协议与 AWS 存储服务连接起来，例如：
  - Amazon S3
  - Amazon S3 Glacier
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway 可以更轻松地为中的文件、卷、快照和虚拟磁带提供弹性、高性能的存储 AWS。
- AWS Backup是一项完全托管的备份服务，用于集中和自动化跨 AWS 服务备份数据。通过 AWS Backup，您可以集中配置备份策略并监控 AWS 资源的备份活动，如下所示：
  - EBS 卷
  - EC2 实例（包括 Windows 应用程序）
  - Amazon RDS 和 Amazon Aurora 数据库
  - DynamoDB 表
  - Amazon Neptune 数据库
  - Amazon DocumentDB(与 MongoDB 兼容）数据库
  - Amazon EFS 文件系统
  - 适用于 Lustre 的 Amazon FSx 文件系统和适用于 Windows File Server 的 Amazon FSx 文件系统
  - 本地和 VMware 云端的 VMware 工作负载 AWS
  - Storage Gateway 卷

AWS Backup 的成本取决于您在一个月内消耗、恢复和传输的存储空间。有关更多信息，请参阅 AWS Backup 定价。

- AWS Elastic Disaster Recovery持续将您的计算机复制到目标 AWS 账户和首选区域的低成本暂存区。您可以将 Elastic 灾难恢复用于灾难恢复和跨区域 premises-to-cloud 灾难恢复
- AWS Config提供了您 AWS 账户中 AWS 资源配置的详细视图。这些信息包括资源之间的关联方式以及资源以前的配置方式。在此视图中，您可以看到资源配置和关系如何随着时间的推移而发生变化。

  当您为 AWS 资源开启AWS Config 配置记录功能时，您可以保留一段时间内的资源关系历史记录。这有助于识别和跟踪长达七年的 AWS 资源关系（包括已删除的资源）。例如， AWS Config 可以跟踪 Amazon EBS 快照卷与该卷所连接的 EC2 实例之间的关系。
- AWS Lambda 可用于以编程方式定义和自动执行工作负载的备份和恢复程序。您可以使用 AWS 软件开发工具包与 AWS 服务及其数据进行交互。您也可以使用 Amazon E CloudWatch ven ts 按计划运行您的 Lambda 函数。

AWS 服务为备份和恢复提供特定的功能。对于您正在使用的每项 AWS 服务，请查阅 AWS 文档，以确定该服务提供的备份、还原和数据保护功能。您可以使用 AWS Command Line Interface (AWS CLI)、 AWS SDK 和 API 操作自动执行 AWS 特定于服务的数据备份和恢复功能。

设计备份与恢复解决方案

在制定全面的数据备份和恢复策略时，您必须首先确定可能的故障或灾难性情况及其潜在的业务影响。在某些行业中，您必须考虑数据安全、隐私和记录保留方面的监管规定。

备份和恢复过程应包括适当的粒度级别，以达到工作负载及其支持业务流程的恢复时间目标（RTO）和恢复点目标（RPO），包括：

- 文件级恢复（例如，应用程序的配置文件）
- 应用程序数据级恢复（例如，MySQL 中的特定数据库）
- 应用程序级恢复（例如，特定的 Web 服务器应用程序版本）
- Amazon EC2 卷级恢复（例如，EBS 卷）
- EC2 实例级恢复。（例如，EC2 实例）
- 托管服务恢复（例如，DynamoDB 表）

请务必考虑解决方案的所有恢复要求以及架构中各个组件之间的数据依赖关系。为了促进恢复过程的成功，请协调架构中各个组件之间的备份和恢复。

以下主题描述了基于基础设施组织的备份和恢复方法。IT 基础设施可以大致分为本地、混合或云原生。

使用 AWS Backup 备份和恢复

AWS Backup 是一项完全托管的备份服务，可集中管理和自动执行跨 AWS 服务的数据备份。AWS Backup 提供了一个集成 Amazon CloudWatch AWS CloudTrail、AWS Identity and Access Management (IAM)、AWS Organizations 和其他服务的编排层。这种集中的 AWS 云原生解决方案提供全局备份功能，可帮助您实现灾难恢复和合规性要求。使用 AWS Backup，您可以集中配置备份策略并监控 AWS 资源的备份活动。

AWS Backup 是为跨 AWS 账户和地区的 AWS 资源实施标准备份计划的理想解决方案。由于 AWS Backup 支持多种 AWS 资源类型，因此可以更轻松地维护和实施使用需要集体备份的多个 AWS 资源的工作负载备份策略。AWS Backup 还允许您集体监视涉及多个 AWS 资源的备份和还原操作。

如果您有合规和审计要求，则可以使用 AWS BackupAudit Manager 功能创建审计框架和报告，以支持您的合规性要求。AWS BackupVault Lock 功能还支持合规性要求，它对存储在 AWS Backup 中备份保管库中的所有备份强制执行一次写入多次读取 (WORM) 配置。

AWS Backup 的一个关键差异化因素是对 Organizations 的支持。使用此支持，您可以在组织或组织单位级别定义和管理备份策略，并自动为每个相关 AWS 账户和地区实施这些策略。当您注册新 AWS 账户和区域时，您不必单独定义和管理备份计划。

AWS Backup 可以让您更轻松地使用标签实施组织范围的备份策略。您可以创建单独的备份计划，每个计划都有独特的频率和保留期设置，然后创建唯一的键值对标签来选择要包含的备份资源。

例如，您可以创建一个每日备份计划，该计划每天 05:00 UTC 开始备份，并有 35 天的保留策略。此备份计划可以包括备份资源分配，该分配指定将根据该计划备份任何具有标签键 backup 和标签值 daily 的受支持 AWS 资源。此外，您可以创建一个月度备份计划，该计划从每个月的第一天 05:00 UTC 开始，并拥有 366 天的保留政策。此备份计划可以包括备份资源分配，该分配指定将根据该计划备份任何具有标签键 backup 和标签值 monthly 的受支持 AWS 资源。

然后，您可以使用标签策略和 required-tags AWS Config 规则来确保所有 AWS 支持的资源都具有此标签键和其中一个标签值。这种方法可以帮助您在 AWS 中始终如一地为受支持的 AWS Backup 资源实施和维护标准备份方法。您可以扩展此方法，以标准化具有不同恢复点目标 (RPO) 要求的应用程序和架构层的备份。

我们建议采取措施保护您的备份保管库。例如，您可以实施 Organizations 服务控制策略 (SCP)，防止您的备份库被删除或与非预期 AWS 账户共享。有关更多详细信息和其他重要的安全注意事项，请查看博客文章中的AWS 中保护备份的十大安全最佳实践。

AWS Backup 可以简化 AWS 灾难恢复 (DR) 计划的实施，因为它支持多种可以集中处理的 AWS 资源。例如，您可以为 AWS Backup 支持的大多数 AWS 资源类型实施跨区域和跨账户备份。跨账户备

份可提高备份安全性，因为副本可在单独的账户中使用。跨区域备份提高了可用性，因为备份可在多个区域中使用。有关受支持的 AWS 资源类型的详细信息，请参阅按资源划分的功能可用性表。

您可以使用带有 AWS Backup 开源解决方案的 Backup and Recovery（备份与恢复）示例，实施基础设施即代码 (IaC) 以及持续集成和持续交付 (CI/CD) 方法来管理 AWS Organizations 组织的备份。此解决方案包括自定义功能，例如在已恢复的 AWS 资源上自动重新应用 AWS 标签，以及在单独的账户和区域中建立辅助备份存储库以用于灾难恢复。

使用 Amazon S3 和 Amazon S3 Glacier 进行备份和恢复

Amazon S3 和 Amazon S3 Glacier 是用于本地、混合和云原生架构的理想存储服务。这些服务提供耐用、低成本的存储平台，可提供可扩展的容量，并且随着备份数据集的增长，无需进行卷或媒体管理。pay-for-what-you-use 模式和每 GB/月的低成本使这些服务适合各种数据保护用例。

> **Note**
>
> 某些存储类别收取最低持续时间费用。有关详情，请参阅 Amazon S3 定价，然后使用网页搜索进行查找`duration`。

主题

- Amazon S3
- Simple Storage Service (Amazon S3) Glacier
- 保护 Amazon S3 和 Amazon S3 Glacier 中的备份数据

Amazon S3

您可以通过 Amazon S3 随时存储和检索的任意数量的数据。您可以将 Amazon S3 用作应用程序数据以及文件级备份和还原过程的持久存储。例如，您可以使用 AWS CLI 或软件开发工具包使用备份脚本将数据库备份从数据库实例复制到 Amazon S3。

AWS 服务使用 Amazon S3 实现高度耐用和可靠的存储，如以下示例所示：

- Amazon EC2 使用 Amazon S3 来存储 EBS 卷和 EC2 实例存储的 Amazon EBS 快照。
- Storage Gateway 与 Amazon S3 集成，为本地环境提供由 Amazon S3 支持的文件共享、卷和磁带库。
- Amazon RDS 使用 Amazon S3 来生成数据库快照。

许多第三方备份解决方案也使用 Amazon S3。例如，Arcserve 统一数据保护支持 Amazon S3 对本地和云原生服务器进行持久备份。

您可以使用这些服务的 Amazon S3 集成功能来简化备份和恢复方法。同时，您可以从 Amazon S3 提供的高耐久性和可用性中受益。

Amazon S3 将数据作为对象存储在名为存储桶中的资源。您可将任意数量的对象存储在存储桶。您可以通过精细访问控制来写入、读取和删除存储桶中的对象。单个对象大小最多为 5 TB。

Amazon S3 提供一系列适合不同使用案例的存储类，包括以下类别：

- S3 标准用于存储经常访问的数据（例如，配置文件、计划外备份、每日备份）的通用存储。
- S3 标准-IA 用于存放时间较长但访问频率较低的数据（例如，每月备份）。IA 表示不经常访问。

Amazon S3 提供生命周期策略，您可以配置这些策略以在整个生命周期中对您的数据进行管理。设置策略后，您的数据将迁移到相应的存储类，而无需对应用程序进行任何更改。有关更多信息，请参阅《Amazon S3 对象生命周期管理》文档。

为降低备份成本，可根据您的恢复时间目标 (RTO) 和恢复点目标 (RPO) 使用分层存储类方法，如以下示例所示：

- 使用 S3 标准进行过去 2 周的每日备份
- 使用 S3 标准-IA 进行过去 3 个月的每周备份
- 对 S3 Glacier Flexible Retrieval 进行过去一年的季度备份
- 对 S3 Glacier Deep Archive 进行过去 5 年的年度备份
- 5 年后从 S3 Glacier Deep Archive 中删除备份

您可以使用对象生命周期管理自动过渡备份。

> **Note**
>
> 某些存储类别收取最低持续时间费用。有关详情，请参阅 Amazon S3 定价，然后使用网页搜索进行查找`duration`。

创建用于备份和存档的标准 S3 存储桶

您可以使用 S3 生命周期策略实施公司的备份和保留策略，创建用于备份和存档的标准 S3 存储桶。AWS 计费的成本分配标记和报告基于在存储桶级别分配的标签。如果成本分配很重要，请为每个项目或业务单元创建单独的备份和存档 S3 存储桶，以便您可以相应地分配成本。

您的备份脚本和应用程序可以使用您创建的备份和存档 S3 存储桶来存储应用程序和工作负载数据的 point-in-time 快照。您可以创建标准 s3 前缀来帮助您整理 point-in-time 数据快照。例如，如果您创建

每小时备份，请考虑使用备份前缀，例如 YYYY/MM/DD/HH/<WorkloadName>/<files...>。通过这样做，您可以手动或以编程方式快速检索 point-in-time 备份。

使用 Amazon S3 版本控制来自动维护回滚历史记录

您可以启用 S3 对象版本控制来维护对象更改的历史记录，包括恢复到先前版本的功能。这对于可能比 point-in-time 备份计划更频繁地更改的配置文件和其他对象很有用。对于必须单独还原的文件，它也很有用。

使用 Amazon S3 备份和恢复 AMI 的自定义配置文件

具有对象版本控制功能的 Amazon S3 可以成为您的工作负载配置和选项文件的记录系统。例如，您可以使用由 ISV 维护的标准 AWS Marketplace Amazon EC2 映像。此映像可能包含其配置保存在多个配置文件中的软件。您可以在 Amazon S3 中维护您的自定义配置文件。当您的实例启动时，您可以将这些配置文件作为实例用户数据的一部分复制到您的实例。应用此方法时，您无需自定义和重新创建 AMI 即可使用更新的版本。

在自定义备份和还原过程中使用 Amazon S3

Amazon S3 提供了一个通用备份存储，您可以将其快速集成到现有的自定义备份流程中。您可以使用 AWS CLI、 AWS 软件开发工具包和 API 操作来集成使用 Amazon S3 的备份和还原脚本和流程。例如，您可能有一个执行夜间数据库导出的数据库备份脚本。您可以自定义此脚本，将夜间备份复制到 Amazon S3 以进行异地存储。有关如何执行此操作的概述，请参阅分批将文件上传到云教程。

您可以采用类似的方法根据不同应用程序的 RPO 为其导出和备份数据。此外，您可以使用 AWS Systems Manager 在托管实例上运行备份脚本。Systems Manager 为您的各个备份过程提供自动化、访问控制、计划、记录和通知。

Simple Storage Service (Amazon S3) Glacier

Amazon S3 Glacier 是一种低成本、云存档的存储服务，用于为数据存档和在线备份提供安全而持久的存储。为了保持低成本，S3 Glacier 提供了三种存储类别，从几毫秒到几小时不等。S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 根据您恢复数据所需的速度提供了其他选项。借助 S3 Glacier，您能安全地存储大量或少量数据，与本地解决方案相比，显著降低了成本。S3 Glacier 非常适合存储具有长期或无限期保留要求的备份数据以及长期数据存档。S3 Glacier 提供以下存储类别：

- S3 Glacier Instant Retrieval，用于存档每季度可能需要一次且需要快速恢复（毫秒）的数据
- S3 Glacier Flexible Retrieval，用于存档可能很少需要在几小时内恢复的数据，每年恢复一两次

- S3 Glacier Deep Archive，用于存档可能很少需要在 12 小时内恢复的长期备份周期数据

下表总结了归档检索选项。

存储类	加速	标准	批量
S3 Glacier Instant Retrieval	不适用	不适用	不适用
S3 Glacier Flexible Retrieval	1–5 分钟	3–5 小时	5–12 小时
S3 Glacier Deep Archive	不可用	12 小时内	48 小时内

使用 Amazon S3，您可以在创建 S3 存储桶时为其中的每个对象设置存储类别。创建对象后，您可以通过将对象复制到具有不同存储类别的新对象来更改存储类别。或者，您可以启用生命周期配置，该配置将根据您指定的规则自动更改对象的存储类别。

要自动执行备份和还原流程，您可以通过、和软件开发工具包访问 Amazon S3 Glacier 和 S3 Glacier AWS Deep Archive。 AWS Management Console AWS CLI有关更多信息，请参阅 Amazon S3 Glacier。

> **Note**
>
> S3 Glacier 存储类收取最低持续时间费用。有关详情，请参阅 Amazon S3 定价，然后使用网页搜索进行查找`duration`。

与管理 Amazon S3 Glacier 档案相比，使用 Amazon S3 生命周期对象过渡到 Amazon S3 Glacier

Amazon S3 可以方便地将 S3 对象过渡到 Amazon S3 Glacier 存储类别，这样您就可以管理备份的生命周期和成本。但是，根据对象的大小以及是否必须恢复架构中不同组件的对象集合，您可能需要自己管理此过程。

如果您有大量必须集体恢复的小型对象，请考虑以下选项的成本影响：

- 使用生命周期策略自动将对象单独过渡到 Amazon S3 Glacier
- 将对象压缩到单个文件中并将其存储在 Amazon S3 Glacier 中

Amazon S3 Glacier 对每个对象收取最低容量费用，具体取决于您使用的存储类别。例如，S3 Glacier Instant Retrieval 的每个对象的最低容量费用为 128 KB。有关更多信息，请参阅性能图表。 up-to-date

对于您存档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的每个对象，Amazon S3 将 8 KB 存储用于对象的名称和其他元数据。Amazon S3 将存储此元数据，以便您可以使用 Amazon S3 API 获取已存档对象的实时列表。将按照 S3 Standard 标准费率对此附加存储收费。

对于归档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类的每个对象的索引和相关元数据，Amazon S3 还为此增加了 32 KB 的存储空间。标识和还原对象需要此额外数据。按照 Amazon S3 Glacier 或 S3 Glacier Deep Archive 费率对此附加存储收费。

通过将对象压缩到单个文件中，您可以减少 Amazon S3 Glacier 使用的额外存储空间，并避免对许多小对象收取最低容量费用。

另一个重要的考虑因素是，生命周期策略是单独应用于对象的。如果必须从某个具体时间点集中恢复一组对象，这可能会影响备份的完整性。即使跨对象设置了相同的过期时间和生命周期转换时间，也无法保证所有对象都能同时过渡。从满足生命周期规则到规则操作完成之间可能会有延迟。有关更多信息，请参阅 AWS Knowledge Center。

最后，考虑一下使用生命周期策略中的存档和管理您创建的单独存档之间的恢复工作。您必须分别从 Amazon S3 Glacier 为每个对象启动恢复。这需要您编写脚本或使用工具来启动多个对象的恢复。您可以使用 S3 Batch Operations 来帮助减少单个请求的数量，也可以使用 Amazon S3 控制台。

保护 Amazon S3 和 Amazon S3 Glacier 中的备份数据

数据安全是一个普遍关注的问题，并且非常 AWS 重视安全性。安全是每项 AWS 服务的基础。诸如 Amazon S3 之类的存储服务为静态和传输中的访问控制和加密提供了强大的功能。所有 Amazon S3 和 Amazon S3 Glacier API 端点都支持安全套接字层/传输层安全性 (SSL/TLS)，以加密传输中数据。默认情况下，Amazon S3 Glacier 会加密所有静态数据。使用 Amazon S3，您可以通过执行以下操作为静态对象选择服务器端加密：

- 使用具有 Amazon S3 托管式加密密钥的服务器端加密
- 使用服务器端加密， AWS Key Management Service (AWS KMS) 密钥存储在 AWS KMS

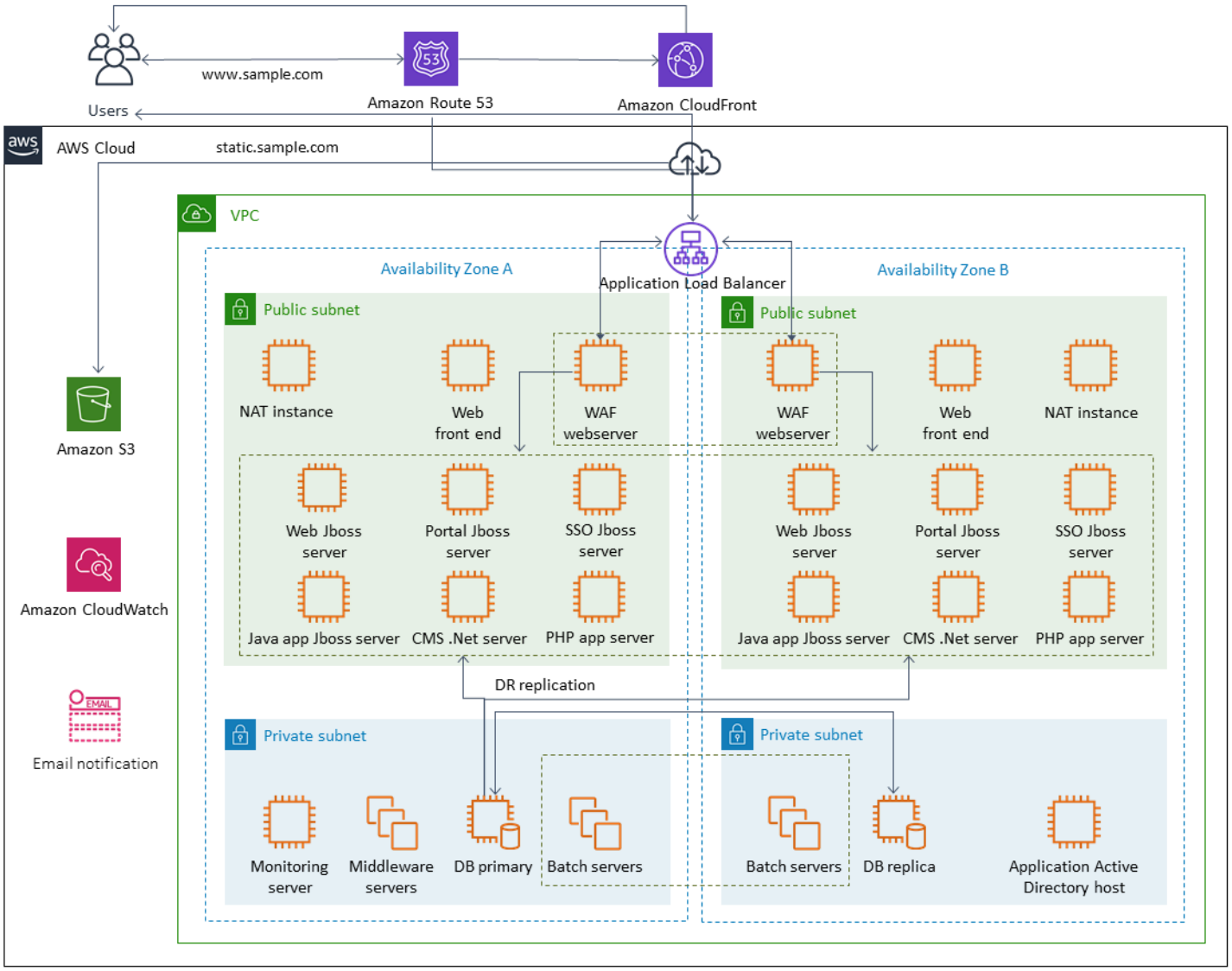
或者，您可以在将数据上传到之前对其进行加密 AWS。有关更多信息，请参阅客户端加密文档。

您可以使用 AWS Identity and Access Management (IAM) 来控制对 S3 对象的访问权限。IAM 可让您控制 S3 存储桶中单个对象和特定前缀路径的权限。您可以通过 AWS CloudTrail使用对象级日志记录来审核对 S3 对象的访问权限。

具有 EBS 卷的 Amazon EC2 备份和恢复

AWS 提供了多种备份您的 Amazon EC2 实例的方法。本节介绍为存储而备份 Amazon Elastic Block Store (Amazon EBS) 卷或实例存储卷的不同方面。 AWS 如果备份符合您的要求，请考虑将其 AWS Backup 作为管理备份的首选。请记住，只有当备份可以恢复到预期功能时，备份才是合格的。应定期测试复原和恢复功能以确认这一点。

下图中的解决方案架构描述了一个完全存在的工作负载环境，其中大部分架构都基于 Amazon EC2。AWS 如下图所示，该场景包括 Web 服务器、应用程序服务器、监控服务器、数据库和 Active Directory。



AWS 为该架构中代表的许多 Amazon EC2 服务器提供了许多功能齐全的服务，用于执行创建、预配置、备份、还原和优化实例和存储的无差别工作。考虑这些服务在您的架构中是否有意义，以减少复

杂性和管理。 AWS 还提供服务以提高基于 Amazon EC2 的架构的可用性。特别是 Amazon EC2 Auto Scaling 和 Elastic Load Balancing 来补充您在 Amazon EC2 上的工作负载。使用这些服务可以提高架构的可用性和容错能力，并帮助您恢复受损的实例，同时最大限度减少对用户的影响。

EC2 实例主要将 Amazon EBS 卷用于持久性存储。Amazon EBS 提供了许多备份和恢复功能，本节将详细介绍这些功能。

主题

- 使用快照和 AMI 进行的 Amazon EC2 备份和恢复
- 使用 AMI 和 EBS 快照创建 EBS 卷备份
- 还原 Amazon EBS 卷或 EC2 实例

使用快照和 AMI 进行的 Amazon EC2 备份和恢复

考虑是否需要使用 Amazon 机器映像 (AMI) 创建 EC2 实例的完整备份或拍摄单个卷的快照。

使用 AMI 或 Amazon EBS 快照进行备份

AMI 包括以下内容：

- 一个或多个快照。I nstance-store-backed AMI 包含实例根卷的模板（例如，操作系统、应用程序服务器和应用程序）。
- 启动权限，用于控制哪些 AWS 账户可以使用 AMI 启动实例。
- 数据块设备映射，指定在实例启动时要附加到实例的卷。

您可以使用 AMI 启动置有预配置软件和数据的新实例。当您想要建立基准时，您可以创建 AMI，这是一种用于启动更多实例、可重复使用的配置。当您创建现有 EC2 实例的 AMI 时，将为附加到该实例的所有卷拍摄快照。快照包括设备映射。

您不能使用快照启动新实例，但您可以使用快照来替换现有实例上的卷。如果您遇到数据损坏或卷故障，则可以根据拍摄的快照创建卷并替换旧卷。您还可以使用快照来配置新卷并在新实例启动期间连接它们。

如果您使用的是由维护和发布的平台和应用程序 AM AWS I AWS Marketplace，请考虑为数据保留单独的卷。您可以将数据卷备份为独立于操作系统和应用程序卷的快照。然后将数据卷快照与发布 AWS 或从发布的最新更新的 AMI 一起使用。 AWS Marketplace这种方法需要仔细测试和规划，以备份和恢复新发布的 AMI 上的所有自定义数据，包括配置信息。

您在 AMI 备份或快照备份之间做出选择会影响还原过程。如果您创建 AMI 作为实例备份，则必须在还原过程中从 AMI 启动 EC2 实例。您可能还需要关闭现有实例以避免潜在冲突。可能发生冲突的一个例子是加入域的 Windows 实例的安全标识符 (SID)。快照的恢复过程可能需要您分离现有卷并连接新恢复的卷。或者，您可能需要更改配置，将应用程序指向新连接的卷。

AWS Backup 支持将实例级备份作为 AMI，也支持将卷级备份作为单独的快照：

- 要对实例上的所有 EBS 卷进行完整备份，请创建在 Linux 或 Windows 上运行的 EC2 实例的 AMI。当您想要回滚时，请使用启动实例向导创建实例。在实例启动向导中，选择我的 AMI。
- 要备份单个卷，请创建快照。要恢复快照，请参阅从快照创建卷。你可以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI)。

实例 AMI 的成本是实例上所有卷的存储空间，而不是元数据。EBS 快照的成本是单个卷的存储空间。有关卷存储成本的更多信息，请参阅 Amazon EBS 定价页面。

服务器卷

EBS 卷是 Amazon EC2 的主要永久存储选项。您可以将此块存储用于存储结构化数据（例如数据库）或非结构化数据（例如卷上文件系统中的文件）。

EBS 卷放置在特定的可用性区域中。这些卷在多个服务器间进行复制，以防止由于任何单个组件发生故障而丢失数据。故障是指卷完全或部分丢失，具体取决于卷的大小和性能。

EBS 卷的设计年故障率（AFR）为 0.1-0.2%。这使得 EBS 卷的可靠程度比普通磁盘高 20 倍，后者通常在 AFR 约为 4% 时出现故障。例如，如果 1,000 个 EBS 卷运行 1 年，则应该会有一两个卷出现故障。

Amazon EBS 还支持快照功能，用于对您的数据进行 point-in-time 备份。所有 EBS 卷类型都提供持久的快照功能，旨在实现 99.999% 的可用性。有关更多信息，请参阅 Amazon 计算服务等级协议。

Amazon EBS 允许创建任何 EBS 卷的快照（备份）。快照是创建 EBS 卷备份的基本功能。快照为 EBS 卷拍摄副本并将其放入 Amazon S3 中，其中数据以冗余方式存储在多个可用区中。初始快照是卷的完整副本；正在进行的快照仅存储增量块级别的更改。有关如何创建Amazon EBS 快照的详细信息，请参阅 Amazon EC2 文档。

在拍摄快照的同一区域，您可以从 Amazon EC2 控制台执行还原操作、删除快照或更新与快照关联的快照元数据（例如标签）。

恢复快照会创建一个包含完整卷数据的新 Amazon EBS 卷。如果您只需要部分恢复，则可以使用不同的设备名称将卷连接到正在运行的实例。然后将其装载，并使用操作系统复制命令将数据从备份卷拷贝到制作卷。

如亚马逊 EC2 文档中所述，也可以使用 Amazon EBS 快照复制功能在 AWS 区域之间复制 Amazon EBS 快照。您可以使用此功能将备份存储在另一区域，而不必管理底层复制技术。

建立单独的服务器卷

您可能已经为操作系统、日志、应用程序和数据使用了一组标准的独立卷。通过建立单独的服务器卷，可以缩小因磁盘空间耗尽而导致应用程序或平台故障时的影响范围。使用物理硬盘时，这种风险通常更大，因为您无法灵活地快速扩展存储量。对于物理驱动器，您必须购买新的驱动器，备份数据，然后在新驱动器上恢复数据。有了它 AWS，这种风险就会大大降低，因为您可以使用 Amazon EBS 来扩展您的预配置卷。有关更多信息，请参阅 AWS 文档。

为应用程序数据、用户数据、日志和交换文件保留单独的卷，以便您可以对这些资源使用不同的备份和还原策略。通过为数据分隔卷，您还可以根据数据的性能和存储要求使用不同类型的卷。然后，您可以针对不同工作负载优化和微调成本。

实例存储卷注意事项

实例存储 为您的实例提供临时性块级存储。此存储位于已物理附加到主机的磁盘上。实例存储非常适合临时存储频繁更改的信息，例如缓冲区、缓存、暂存数据和其他临时内容。对于在一组实例集中复制的数据，例如负载均衡的 Web 服务器池，它们也更可取。

实例存储内的数据仅在与关联的实例的生命周期内保留。如果实例重启 (无论是故意还是意外)，实例存储内的数据都会保留下来。然而，在以下任一情况下，实例存储中的数据会丢失。

- 底层驱动器故障。
- 实例停止。
- 实例终止。

因此，切勿依赖实例存储来存储珍贵且需要长期保存的数据。应使用更持久的数据存储，如 Amazon S3、Amazon EBS 或 Amazon EFS。

实例存储卷的常见策略是，基于恢复点目标 (RPO) 和恢复时间目标 (RTO)，根据需要定期将必要的数据保存到 Amazon S3。然后，当启动新实例时，您可以将数据从 Amazon S3 下载到您的实例存储。您也可以在实例停止之前将数据上传到 Amazon S3。为了保持持久性，请创建一个 EBS 卷，将其连接

到您的实例，然后定期将数据从实例存储卷复制到 EBS 卷。有关更多信息，请参阅 AWS Knowledge Center。

为 EBS 快照和 AMI 标记并强制执行标准

标记所有 AWS 资源是成本分配、审计、故障排除和通知的重要做法。标记对于 EBS 卷很重要，这样才能提供管理和恢复卷所需的相关信息。标签不会自动从 EC2 实例复制到 AMI 或从源卷复制到快照。确保您的备份过程包含来自这些来源的相关标签。这将帮助您设置快照元数据（如访问策略、附件信息和成本分配），以便将来使用这些备份。有关为 AWS 资源添加标签的更多信息，请参阅标记最佳实践技术论文。

除了用于所有 AWS 资源的标签外，还可使用以下特定于备份的标签：

- 源实例 ID
- 源卷 ID（用于快照）
- 恢复点描述

您可以使用 AWS Config 规则和 IAM 权限强制执行标签策略。IAM 支持强制使用标签，因此您可以编写 IAM policies，强制在处理 Amazon EBS 快照时使用特定标签。如果尝试 `CreateSnapshot` 操作时未使用 IAM 权限策略中定义的标签授予权限，则快照创建失败，访问被拒绝。有关更多信息，请参阅关于在创建时标记 Amazon EBS 快照和实施更严格安全策略的博客文章。

您可以使用 AWS Config 规则自动评估 AWS 资源的配置设置。为了帮助您入门， AWS Config 提供了名为托管规则的可自定义的预定义规则。您还可以创建自己的自定义规则。在 AWS Config 持续跟踪资源之间的配置更改的同时，它会检查这些更改是否违反了规则中的任何条件。如果某个资源违反了规则，则会将该资源和规则 AWS Config 标记为不合规。请注意，必填标签托管规则目前不支持快照和 AMI。

使用 AMI 和 EBS 快照创建 EBS 卷备份

AWS 为创建和管理 AMI 和快照提供了大量选项。您可以使用满足您需求的方法。许多客户面临的一个常见问题是管理快照生命周期，并根据目的、保留策略等明确调整快照。如果没有适当的标记，快照可能会被意外删除或作为自动清理过程的一部分删除。您最终还可能要为保留的过时快照付费，因为不清楚是否还需要这些快照。

在创建快照或 AMI 之前准备 EBS 卷

在拍摄快照或创建 AMI 之前，请对 EBS 卷进行必要的准备。创建 AMI 会为连接到实例的每个 EBS 卷生成一个新的快照，因此这些准备工作也适用于 AMI。

您可以通过启动 EC2 实例制作正在使用的已附加 EBS 卷的快照。但是，快照只能捕获发出快照命令时已经写入您的 EBS 卷的数据。其中可能不包括已由应用程序或操作系统缓存的任何数据。最佳做法是让系统处于不执行任何 I/O 的状态。理想情况下，计算机不接受流量并处于停止状态，但这种情况很少见，因为全天候的 IT 运营已成为常态。如果可以将系统内存中的任何数据刷新到应用程序正在使用的磁盘上，并且可以暂停对卷的任何文件写入操作，时间长到可以创建快照，那么快照就是完整的。

要进行干净的备份，必须暂停数据库或文件系统。执行此操作的方式取决于数据库或文件系统。

数据库的过程如下所示：

1. 如果可能，请将数据库置于热备份模式。
2. 运行 Amazon EBS 快照命令。
3. 使数据库退出热备份模式，或者，如果使用只读副本，则终止只读副本实例。

文件系统的过程类似，但它取决于操作系统或文件系统的功能。例如，XFS 是一个可以刷新其数据以实现一致备份的文件系统。有关更多信息，请参阅 xfs_freeze。或者，您可以使用支持冻结 I/O 的逻辑卷管理器简化此过程。

但是，如果您无法刷新或暂停向该卷写入所有文件，请执行以下操作：

1. 从操作系统中卸载卷。
2. 发出快照命令。
3. 重新装载卷以获得一致且完整的快照。当快照状态为“待处理”时，您可以重新挂载并使用卷。

快照过程在后台继续，快照创建速度很快，可以及时捕获某个点。您正在备份的卷将在几秒钟内卸载。您可以安排一个较小的备份窗口，在该窗口中客户端可以正常地处理中断。

当您为充当根设备的 EBS 卷创建快照时，应在拍摄快照之前停止实例。Windows 提供了卷影复制服务 (VSS) 来帮助创建应用程序一致的快照。 AWS 提供了一个 Systems Manager 文档，您可以运行该文档对支持 VSS 的应用程序进行映像级备份。这些快照包括这些应用程序和磁盘之间的挂起事务中的数据。在备份所有已附加的卷时，您无需关闭实例或将其断开连接。有关更多信息，请参阅 AWS 文档。

> **Note**
>
> 如果您正在创建 Windows AMI 以便可以部署另一个类似实例，请使用 EC2Config 或 EC2Launch 对您的实例进行 Sysprep。然后，从已停止的实例创建一个 AMI。Sysprep 会从 Amazon EC2 Windows 实例中删除唯一信息，包括 SID、计算机名称和驱动程序。重复的 SID 可能会导致 Active Directory、Windows 服务器更新服务 (WSUS)、登录问题、Windows 卷密钥激活、Microsoft Office 和第三方产品出现问题。如果您的 AMI 用于备份目的，并且您想要在所有唯一信息完好无损的情况下还原同一实例，请不要将 Sysprep 用于您的实例。

从控制台手动创建 EBS 卷快照

在进行任何尚未在实例上全面测试的重大更改之前，请创建相应卷或整个实例的快照。例如，您可能需要在实例上升级或修补应用程序或系统软件之前创建快照。

您可以从控制台手动创建快照。在 Amazon EC2 控制台的 Elastic Block Store Volumes（弹性块存储卷）页面上，选择要备份的卷。在 Actions（操作）菜单上，选择 Create snapshot（创建快照）。您可以通过在筛选框中输入实例 ID 来搜索连接到特定实例的卷。

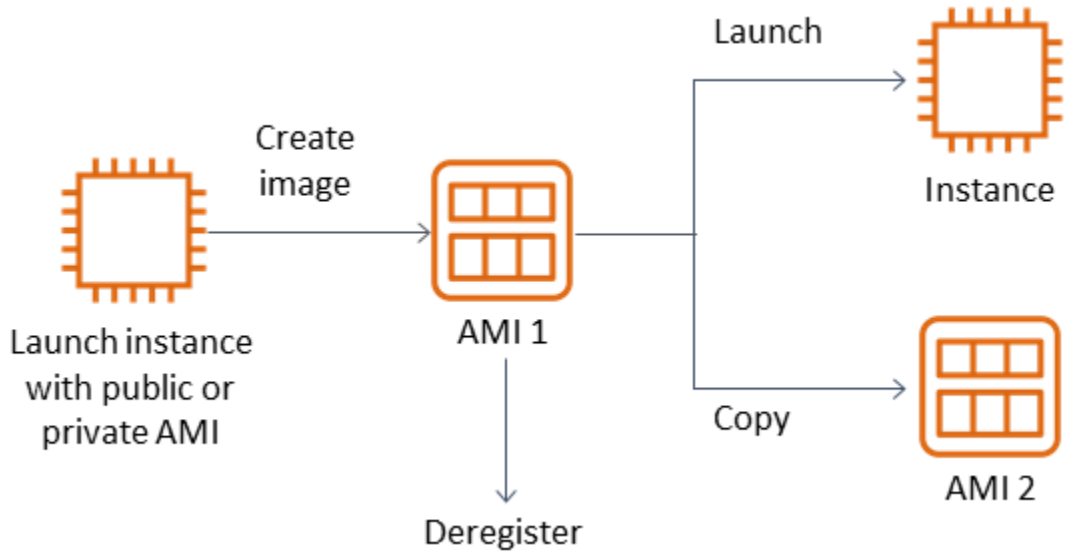
输入描述并添加相应的标签。添加 Name 标签以便日后更容易找到该卷。根据您的标记策略添加任何其他合适的标签。

创建 AMI

AMI 提供启动实例所需的信息。AMI 包括根卷和创建映像时附加到实例的 EBS 卷的快照。您不能仅从 EBS 快照启动新实例；必须从 AMI 启动新实例。

创建 AMI 时，将在您使用的账户和区域中创建。AMI 创建过程会为连接到实例的每个卷创建 Amazon EBS 快照，AMI 指的是这些 Amazon EBS 快照。这些快照存储在 Amazon S3 中，并且非常耐用。

创建 EC2 实例的 AMI 后，您可以使用 AMI 重新创建实例或启动实例的更多副本。您也可以将 AMI 从一个区域复制到另一区域以进行应用程序迁移或 DR。



除非您将虚拟机（例如 VMWARE 虚拟机）迁移到，否则必须从 EC2 实例创建 AMI AWS。要从 Amazon EC2 控制台创建 AMI，请选择实例，然后依次选择 操作、映像、创建映像。

Amazon Data Lifecycle Manager

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除 EBS 快照。自动化快照管理可以帮助您完成以下工作：

- 通过实施定期备份计划来保护重要数据。
- 按照审核员的要求或内部合规性保留备份。
- 通过删除过时的备份来降低存储成本。

使用 Amazon Data Lifecycle Manager，您可以自动执行 EC2 实例（及其附加的 EBS 卷）或单独 EBS 卷的快照管理流程。它支持跨区域复制等选项，因此您可以自动将快照复制到其他 AWS 区域。将快照复制到备选区域是支持备选区域中灾难恢复工作和恢复选项的一种方法。您也可以使用 Amazon Data Lifecycle Manager 创建支持快速快照还原的快照生命周期策略。

Amazon Data Lifecycle Manager 是 Amazon EC2 和 Amazon EBS 的内含功能。Amazon Data Lifecycle Manager 不收取任何费用。

AWS Backup

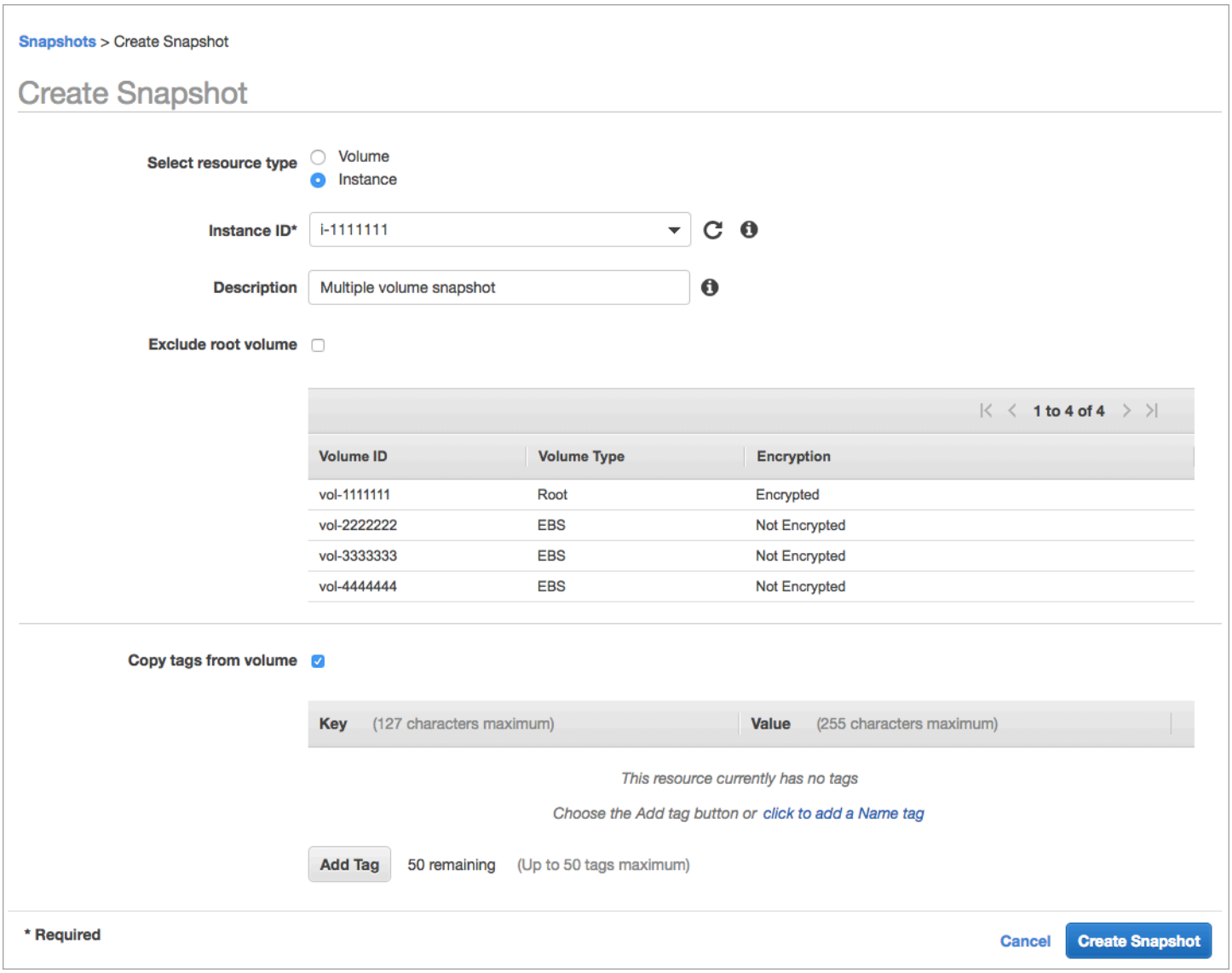
AWS Backup 与 Amazon Data Lifecycle Manager 截然不同，因为您可以创建包含多项 AWS 服务的资源的备份计划。您可以协调备份以覆盖正在一起使用的资源，而不必单独协调资源的备份。

AWS Backup 还包括备份存储库的概念，它可以限制对已完成备份的恢复点的访问。恢复操作可以从每个资源启动， AWS Backup 而不是继续执行每个单独的资源并恢复创建的备份。 AWS Backup 还包括许多其他功能，例如审计管理和报告。有关更多信息，请参见本指南的 使用 AWS Backup 备份和恢复 部分。

执行多卷备份

如果要使用快照备份 RAID 阵列中 EBS 卷上的数据，则快照必须保持一致。原因在于这些卷的快照是独立创建的。从不同步的快照恢复 RAID 阵列中的 EBS 卷会降低阵列的完整性。

要为您的 RAID 阵列创建一组一致的快照，请使用 CreateSnapshotsAPI 操作，或者登录 Amazon EC2 控制台并选择 “弹性块存储”、“快照”、“创建快照”。



在 RAID 配置中连接了多个卷的实例快照将合并为多卷快照。多卷快照可在连接 point-in-time到 EC2 实例的多个 EBS 卷之间提供数据协调且崩溃一致的快照。您不需要停止实例以在多个卷之间协调来实现一致性，因为快照将跨多个 EBS 卷自动拍摄。启动卷的快照后（通常是一两秒钟），文件系统可以继续其操作。

创建快照后，每个快照将视为单个快照。您可以执行与单卷快照相同的所有快照操作，例如恢复、删除、跨区域和帐户复制。您还可以标记多卷快照，就像您使用单卷快照执行的操作一样。我们建议您标记多卷快照以在恢复、复制或保留操作期间集中管理它们。有关更多信息，请参阅 AWS 文档。

您也可以从逻辑卷管理器或文件系统级别的备份中执行这些备份。在这些情况下，使用传统的备份代理可通过网络备份数据。互联网和 AWS Marketplace 中提供了许多基于代理的备份解决方案。

另一种方法是创建存在于单个大卷上的主系统卷的副本。这简化了备份过程，因为只需要备份一个大卷，而且备份不在主系统上进行。但是，首先要确定单个卷在备份期间能否充分发挥作用，以及最大卷大小是否适合应用程序。

保护您的 Amazon EC2 备份

重要的是要考虑备份的安全性，并防止意外或恶意删除备份。您可以综合使用多种方法来实现此目的。为防止由于安全漏洞而丢失重要备份，我们建议您将备份复制到其他 AWS 帐户。如果您有多个 Amazon Web Services account，则可以指定一个单独的账户作为存档账户，所有其他账户都可以将备份复制到该账户。例如，您可以使用 AWS Backup 中的跨账户备份完成此操作。

您的灾难恢复计划可能还要求您能够在另一个 Amazon Web Services Region 重现 EC2 实例，以防出现区域故障。您可以通过将备份复制到同一账户内的其他区域来实现这一目标。这可以提供额外的意外删除保护层，并支持灾难恢复 (DR) 目标。AWS Backup 为跨区域备份提供支持。

考虑阻止 IAM 对 ec2: DeleteSnapshot 和 ec2: DeregisterImage 操作的权限。相反，您可以让您的保留策略和方法管理 EBS 快照和 Amazon EC2 AMI 的生命周期。阻止删除操作是为 EBS 快照实施一次写入多次读取 (WORM) 策略的一种方法。您还可以使用AWS Backup 文件库锁定，它为 EBS 快照和其他 AWS 资源提供支持。

此外，可以考虑通过阻止 ec2: 和 ec2: ModifySnapshotAttribute IAM 操作来阻止用户共享 AMI ModifyImageAttribute 和 EBS 快照。这将防止您的 AMI 和快照与组织外部的 AWS 账户共享。如果您正在使用 AWS Backup，请限制用户对备份存储库执行类似的操作。有关更多信息，请参见本指南的 AWS Backup 部分。

Amazon EC2 包含回收站功能，可帮助您恢复意外删除的 EBS 快照。如果您允许用户删除快照，请开启此功能，这样所需的快照就不会被永久删除。用户在删除多个快照时应特别小心，因为 Amazon

EC2 控制台允许您在一次操作中选择多个快照并将其删除。此外，在使用清理脚本和自动化时要小心，以免无意中删除所需快照。回收站功能有助于提供保护，使其免受此类情况的侵害。

归档 EBS 快照

如果您不打算保留在 90 天或更长时间内恢复的卷副本以供参考，归档 EBS 快照是一种经济实惠的方法。在永久删除 EBS 卷的所有相关快照之前，这可能是一个不错的中间步骤。例如，对于不再使用的 EBS 卷，您可以考虑将存档快照作为一个 end-of-lifecycle 步骤。存档而不是删除也是一种更具成本效益的删除保留方法，而不是使用回收站。

使用 Systems Manager、和软件开发工具包自动创建快照和 AMI AWS CLIAWS

您的备份方法可能需要在创建快照或 AMI 之前或之后进行操作。例如，您可能需要停止和启动服务以停止文件系统。或者，您可能需要在 AMI 创建期间停止并启动您的实例。您可能还需要共同创建架构中多个组件的备份，每个组件都有自己的创建前和创建后步骤。

通过自动化备份过程并验证备份过程是否得到一致应用，可以缩短备份的维护时段时间。要自动执行自定义的创建前和创建后操作，请使用 AWS CLI 和 SDK 编写备份过程脚本。

您的自动化可以在 Systems Manager 运行手册中定义，该运行手册可以按需运行，也可以在 Systems Manager 维护时段内运行。您可以向用户授予运行 Systems Manager 运行手册的权限，而无需向他们授予对 Amazon EC2 破坏性命令的权限。这还可以帮助您验证您的用户是否一致地应用了您的备份过程和标记。您可以使用 AWS CreateSnapshot 和 A WS CreateImage 运行手册来创建快照和 AMI，也可以向其他用户授予使用它们的权限。Systems Manager 还包括 AWS UpdateLinuxAmi 和 AWS UpdateWindowsAmi 运行手册，用于自动执行 AMI 修补和 AMI 创建。

您还可以使用 AWS CLI 和AWS Tools for Windows PowerShell自动创建快照和 AMI。您可以使用 aws ec2 create-sn apsho AWS CLI t 命令创建 EBS 卷的快照，这是自动化的一个步骤。您可以使用 aws ec2 create-snapshots 命令为连接到 EC2 实例的所有卷创建崩溃一致的同步快照。

您可以使用 AWS CLI 创建新的 AMI。您可以使用 aws ec2 register-image 命令为 EC2 实例创建新映像。要自动关闭实例、创建映像和重启实例，请将此命令与 aws ec2 stop-instances 和 aws ec2 start-instances 命令结合使用。

还原 Amazon EBS 卷或 EC2 实例

如果您只需要恢复连接到 EC2 实例的单个卷，则可以单独恢复该卷，分离现有卷，然后将恢复的卷连接到 EC2 实例。如果您需要恢复整个 EC2 实例，包括其所有关联卷，则必须使用实例的 Amazon 机器映像 (AMI) 备份。

为了减少恢复时间和对相关应用程序和进程的影响，您的恢复过程必须考虑它所取代的资源。为了获得最佳结果，请定期在较低环境（例如非生产环境）中测试恢复过程，以验证您的过程是否符合恢复点目标 (RPO) 和恢复时间目标 (RTO)，以及恢复过程是否按预期运行。考虑恢复过程将如何影响依赖于您要恢复实例的应用程序和服务，然后根据需要协调恢复。尽量自动化并测试恢复过程，以降低恢复过程失败或实施不一致的风险。

如果您使用 Elastic Load Balancing，并且有多个实例为流量提供服务，则可能会使出现故障或受损的实例停止服务。然后，您可以恢复一个新实例来替换它，同时其他实例继续为流量提供服务，而不会对用户造成干扰。

描述的以下还原过程适用于未使用 Elastic Load Balancing 的实例：

- 从 EBS 快照恢复单个文件和目录
- 从Amazon EBS 快照还原 EBS 卷
- 从 EBS 快照创建或恢复 EC2 实例
- 从 AMI 还原正在运行的实例

从 EBS 快照恢复文件和目录

EBS 快照提供了用于创建快照的原始卷的 point-in-time 精确副本。要还原单个文件或目录，必须执行以下操作：

1. 首先，从 EBS 快照中恢复卷，该快照包含文件或目录。
2. 将卷附加到要将文件还原到的 EC2 实例。
3. 将文件从还原卷复制到 EC2 实例卷。
4. 分离并删除已恢复的卷。

从Amazon EBS 快照还原 EBS 卷

您可以恢复连接到现有 EC2 实例的卷，方法是根据其快照创建卷并将其附加到您的实例。您可以使用控制台 AWS CLI、或 API 操作根据现有快照创建卷。然后，您可以使用操作系统将卷挂载到实例。

请注意，来自 Amazon EBS 快照的数据会异步加载到 EBS 卷中。如果应用程序访问未加载数据的卷，则从 Amazon S3 加载数据时，延迟将比正常情况更高。为避免对延迟敏感的应用程序造成这种影响，您有两种选择：

- 您可以初始化 EBS 卷。
- Amazon EBS 支持 快速快照恢复，无需初始化您的卷，但需额外付费。

如果要更换必须使用相同装入点的卷，请卸载该卷，以便可以将新卷装入原处。要卸载该卷，请先停止所有正在使用该卷的进程。如果要替换根卷，则在分离根卷之前必须先停止实例。

例如，按照以下步骤使用控制台将卷恢复到之前的 point-in-time 备份：

1. 在 Amazon EC2 控制台的 弹性块存储 菜单上，选择 快照。
2. 搜索要还原的快照，然后将其选中。
3. 选择 Actions （操作），然后选择 Create Volume （创建卷）。
4. 在与 EC2 实例相同的可用区中创建新卷。
5. 在 Amazon EC2 控制台选择实例。
6. 在实例详细信息中，在根设备条目或块设备条目中记下要替换的设备名称。
7. 附加卷。根卷和非根卷的过程有所不同。

   根卷：

   a. 请停止 EC2 实例。

   b. 在 EC2 弹性块存储卷菜单上，选择要替换的根卷。

   c. 依次选择 操作 和 分离卷。

   d. 在 EC2 弹性块存储卷菜单上，选择新卷。

   e. 依次选择 操作 和 附加卷。

   f. 选择要将卷连接到的实例，并使用您之前记下的相同设备名称。

   非根卷：

   a. 在 EC2 Elastic Block Store Volumes （EC2 弹性块存储卷）菜单上，选择要替换的非根卷。

   b. 依次选择 操作 和 分离卷。

c. 在 EC2 弹性块存储卷菜单上选择新卷，然后依次选择 操作、附加卷，即可连接新卷。选择要将其附加到的实例，然后选择可用的设备名称。

d. 使用实例的操作系统，卸载现有卷，然后将新卷装入原处。

   在 Linux 操作系统下，您可以使用 umount 命令。在 Windows 中，您可以使用逻辑卷管理器 (LVM)，例如磁盘管理系统实用程序。

e. 在 EC2 弹性块存储卷 菜单上选择该卷，然后依次选择操作、分离卷，即可分离之前可能要替换的任何卷。

您也可以将 AWS CLI 与操作系统命令结合使用来自动执行这些步骤。

从 EBS 快照创建或恢复 EC2 实例

要创建用于还原整个 EC2 实例的备份，我们建议创建 Amazon 机器映像 (AMI)。AMI 会捕获虚拟化类型等计算机信息。他们还为连接到 EC2 实例的每个卷创建快照，包括其设备映射，以便可以在相同的配置下恢复快照。

但是，如果您必须使用 EBS 快照来恢复实例，请先从 EBS 快照创建 AMI，该快照将成为新 EC2 实例的根卷：

1. 在 Amazon EC2 控制台的 弹性块存储 菜单上，选择 快照。
2. 搜索将用于为您的新 EC2 实例创建根卷的快照，然后将其选中。
3. 依次选择 Actions （操作） 和 Create Image from Snapshot （从快照创建映像）。
4. 输入映像名称（例如 YYYYMMDD-restore-for-i-012345678998765de），然后为新映像选择相应的选项。

映像创建并可用后，您可以启动一个新的 EC2 实例，该实例将使用 EBS 快照作为根卷。

从 AMI 还原正在运行的实例

您可以从 AMI 备份中启动新实例，以替换现有正在运行的实例。一种方法是停止现有实例，在从 AMI 启动新实例时将其保持离线状态，然后执行所有必要的更新。这种方法降低了两个实例同时运行时发生冲突的风险。如果您的实例提供的服务出现故障，或者您在维护时段内执行恢复，则这是一种可以接受的方法。测试新实例后，您可以重新指定分配给旧实例的任何弹性 IP 地址。然后，您可以更新任何域名服务 (DNS) 记录以指向新实例。

但是，如果在还原期间必须最大限度地减少服务中实例的停机时间，请考虑从 AMI 备份启动和测试新实例。然后将现有实例替换为新实例。

当两个实例都在运行时，您必须防止新实例造成任何平台级或应用程序级冲突。例如，使用相同的 SID 和计算机名称运行的加入域的 Windows 实例可能会遇到问题。对于需要唯一标识符的网络应用程序和服务，您可能会遇到类似问题。

为防止其他服务器和服务在新实例准备就绪之前连接到该实例，请使用安全组暂时阻止新实例的所有入站连接，但您自己用于访问和测试的 IP 地址除外。您也可以暂时阻止新实例的出站连接，以防止服务和应用程序启动对其他资源的任何连接或更新。新实例准备就绪后，停止现有实例，在新实例上启动服务和进程，然后解除对您实现的所有入站或出站网络连接的封锁。

从本地基础设施备份和恢复到 AWS

您可以将 AWS 用于本地基础设施备份的持久异地存储。在这种情况下使用 AWS 存储服务，您可以专注于备份和存档任务。您不必为备份任务担心存储基础架构的配置、扩展或基础架构容量。

Amazon S3 和 Amazon S3 Glacier 提供广泛的 API 操作和软件开发工具包，用于将这些服务集成到新的和现有备份和恢复方法中。这也为备份软件供应商提供了直接将其应用程序与 AWS 存储解决方案集成的方法。

在这种情况下，您在本地基础架构中使用的备份和存档软件通过 API 操作直接与 AWS 交互。由于备份软件具有 AWS 感知能力，因此它会将本地服务器中的数据直接备份到 Amazon S3 或 Amazon S3 Glacier。

如果您现有的备份软件本身不支持 AWS Cloud，则可以使用 Storage Gateway。Storage Gateway 是一项云存储服务，可让您的本地系统访问可扩展的云存储。它支持开放标准存储协议，可与您的现有应用程序配合使用，同时将加密后的数据安全地存储在 Amazon S3 或 Amazon S3 Glacier 中。您可以将 Storage Gateway 用作本地基于数据块的存储工作负载备份和恢复方法的一部分。

Storage Gateway 在混合场景中非常有用，在这种场景中，您需要过渡到基于云的存储来进行备份。Storage Gateway 还可以帮助您减少对本地存储的资本投资。您可以将 Storage Gateway 部署为虚拟机或专用硬件设备。本指南重点介绍 Storage Gateway 如何应用于备份和恢复。

Storage Gateway 提供了三个不同的选项来满足不同的需求：

- 用于使用基于 SMB 或基于 NFS 的访问将应用程序数据文件和备份映像作为耐用对象存储在 Amazon S3 云存储上的文件网关。
- 用于向本地应用程序提供基于云的 iSCSI 块存储卷的卷网关。卷网关在本地提供本地缓存或完整卷，同时还将卷的完整副本存储在 AWS Cloud 中。
- 用于将可信的备份软件指向本地存储网关的一种磁带网关，该网关反过来又连接到 Amazon S3 和 Amazon S3 Glacier。此选项提供了云扩展和耐用性，可在不中断现有投资或流程的情况下实现安全、长期的保留。

文件网关

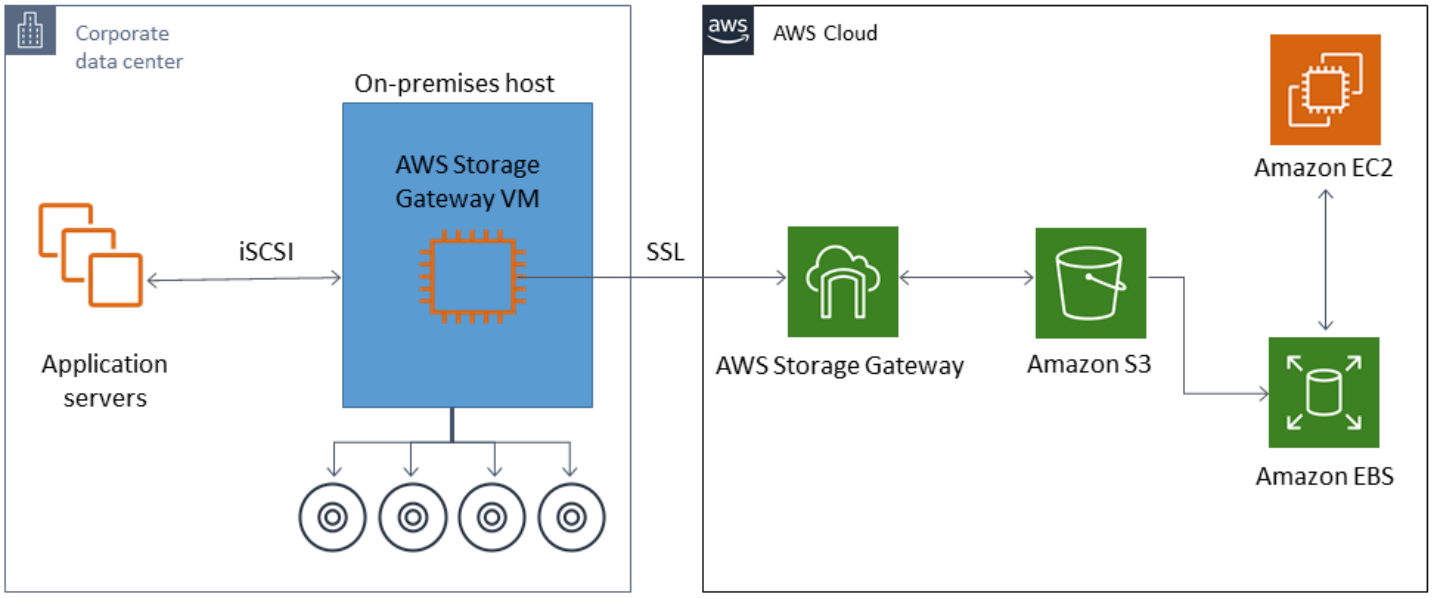
许多组织通过将二级和三级数据（例如备份）迁移到云端来开始他们的云之旅。文件网关的 SMB 和 NFS 接口支持为 IT 组提供了一种将备份任务从现有本地备份系统过渡到云端的方法。可以写入 SMB 或 NFS 的备份应用程序、本机数据库工具或脚本可以写入文件网关。文件网关将备份存储为大小不超过 5 TiB 的 Amazon S3 对象。使用适当大小的本地缓存，可以使用最近的备份进行快速现场恢复。通

过将备份分层到低成本的 S3 标准 - Infrequent Access 和 Amazon S3 Glacier 存储层，可以满足长期保留需求。

文件网关为您基于块的 Amazon S3 存储提供了一个快速通道，以实现高度持久的异地备份。对于必须快速恢复最近备份文件的情况特别有用。由于文件网关支持 SMB 和 NFS 协议，因此用户可以像访问网络文件共享一样访问文件。您还可以利用 Amazon S3 对象版本控制功能。使用对象版本控制，您可以恢复文件以前的对象版本，然后使用 SMB 或 NFS 轻松访问这些版本。

卷网关

卷网关允许您为本地服务器配置基于云的 iSCSI 块存储卷。卷网关将您的卷数据存储到 Amazon S3，以实现持久、可扩展、基于云的异地存储。卷网关便于拍摄卷的完整时间点快照，并将其作为 Amazon EBS 快照存储在云中。将它们存储为快照后，可以将整个卷恢复为 EBS 卷并连接到 EC2 实例，从而加快实现基于云的灾难恢复解决方案。也可以将卷恢复到 Storage Gateway，从而使您的本地应用程序能够恢复到以前的状态。



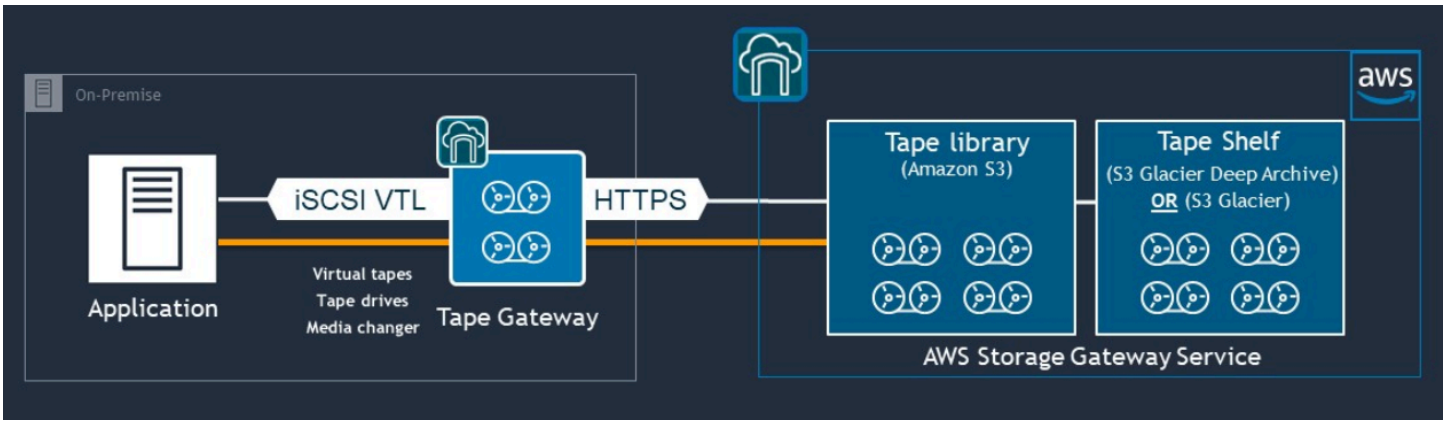
由于卷网关与 Amazon EC2 的 Amazon EBS 卷功能集成，因此您可以使用 AWS Backup 自动执行和安排快照流程。卷网关为您提供了由 Amazon S3 支持的耐用 Amazon EBS 快照和标记功能的额外优势。有关更多信息，请参阅 Amazon EBS 快照文档。

磁带网关

磁带网关为您的异地虚拟磁带备份存储提供 Amazon S3 和 Amazon S3 Glacier 的高耐久性、低成本的分层存储以及丰富的功能。您存储在 Amazon S3 和 Amazon S3 Glacier 中的所有虚拟磁带都将在至少三个地理上分散的可用区进行复制和存储。您的虚拟磁带受到 11 个九分耐久性保护。

AWS 还会定期执行固定性检查，以确认您的数据可以读取并且没有引入错误。存储在 Amazon S3 中的所有磁带都使用默认密钥或您的 AWS KMS 密钥进行服务器端加密保护。此外，您还可以避免与磁带便携性相关的物理安全风险。与异地存储磁带相比，使用磁带网关可以获得正确的数据，在恢复过程中，您可能会收到不正确或损坏的磁带。

将数据存储在 Amazon S3 中时，您可以节省每月的存储成本。使用 S3 Glacier Deep Archive，您可以为长期存档需求节省更多资金。



磁带网关充当虚拟磁带库 (VTL)，涵盖从您的本地环境到高度可扩展、冗余和耐用的存储服务：Amazon S3、S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive。

磁带网关将 Storage Gateway 作为基于 iSCSI 的开放标准虚拟磁带库 (VTL) 提供给您的现有备份应用程序，带有虚拟媒体更换器和虚拟磁带驱动器。您可以继续使用现有备份应用程序和工作流程，同时写入存储在可大规模扩展的 Amazon S3 上的一组虚拟磁带。当您不再需要立即或频繁访问虚拟磁带上的数据时，您的备份应用程序可以将其存档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中，从而进一步降低存储成本。

您通常可以在 3 - 5 小时或 12 小时内取回归档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中的磁带。磁带网关可以和与基于 iSCSI 的磁带库接口兼容的备份应用程序一起使用，用于访问虚拟磁带。还要考虑每个磁带的最低 100-GB 存储大小。有关更多信息，请查看支持磁带网关的第三方备份应用程序列表。

将应用程序从 AWS 到您的数据中心进行备份和恢复

您可能有一项政策，要求您为基于云的工作负载和本地基础设施实施灾难恢复或业务连续性等方案。如果您的本地服务器已经有了数据备份框架，则可以通过 VPN 连接或通过 AWS Direct Connect 将其扩展到您的 AWS 资源。您可以在 EC2 实例上安装备份代理，并根据您的数据保护策略备份您的数据和应用程序。您也可以使用 Amazon S3 作为中间服务来存储应用程序级备份。然后，您可以使用 API 操作、软件开发工具包或 AWS CLI 将数据恢复到您的本地环境。

要在 Amazon EC2 以外的 AWS 服务中备份数据，请使用 AWS CLI、软件开发工具包和 API 操作将数据提取为所需的格式。然后将数据复制到 Amazon S3，从 Amazon S3 复制到您的本地环境。有些服务可以直接导出到 Amazon S3。例如，Amazon RDS 支持将微软 SQL Server 数据库原生备份到 Amazon S3。

云原生的 AWS 服务的备份和恢复

您的备份和恢复方法应涵盖工作负载中使用的AWS服务。AWS提供特定于服务的功能和选项，用于管理和与您的数据交互。您可以使用控制台、AWS CLI、软件开发工具包和 API 操作为您正在使用的AWS服务实现备份和恢复。本指南以 Amazon RDS 和 Amazon DynamoDB 为例。AWS Backup同时支持 DynamoDB 和 Amazon RDS，如果它满足您的要求，则应使用。

Amazon RDS 的备份和恢复

Amazon RDS 包含用于自动备份数据库的功能。Amazon RDS 创建数据库实例的存储卷快照，并备份整个数据库实例，而不仅仅是单个数据库。使用 Amazon RDS，您可以为自动备份建立备份窗口、创建数据库实例快照以及跨区域和账户共享和复制快照。

Amazon RDS 为备份和恢复数据库实例提供了两种不同的选项：

- 自动备份可实现数据库实例的时间点故障恢复 (PITR)。创建新的数据库实例时，默认开启自动备份。

  Amazon RDS 在创建数据库实例时定义的备份窗口内对您的数据执行每日完整备份。您可以为自动备份配置最长 35 天的保留期。Amazon RDS 每隔 5 分钟也将数据库实例的事务日志上传到 Amazon S3 一次。Amazon RDS 使用您的每日备份以及数据库事务日志来恢复您的数据库实例。您可以将实例恢复到保留期内的任意一秒钟，最长可达`LatestRestorableTime`（通常为最后五分钟）。

  要查找数据库实例的最新可恢复时间，请使用 `DescribeDBInstances` API 调用。或者在 Amazon RDS 控制台上查看数据库的描述选项卡。

  启动 PITR 时，会将事务日志与最合适的每日备份相结合，将数据库实例恢复到请求的时间。
- 数据库快照是用户启动的备份，可用于随心所欲地将数据库实例还原到已知状态。然后，您可以随时恢复到该状态。您可以使用 Amazon RDS 控制台或 `CreateDBSnapshot` API 调用来创建数据库快照。这些快照会一直保留，直到您使用控制台或 `DeleteDBSnapshot` API 调用将其明确删除。

AWS Backup中的 Amazon RDS 支持这两个备份选项，它还提供其他功能。考虑使用AWS Backup为您的 Amazon RDS 数据库设置标准备份计划，如果特定数据库的备份计划是唯一的，则使用用户启动的实例备份选项。

Amazon RDS 禁止直接访问数据库实例使用的底层存储。这还可以防止您将 RDS 数据库实例上的数据库直接导出到其本地磁盘。在某些情况下，您可以使用客户端实用程序使用本机备份和还原功能。

例如，您可以将 mysqldump 命令与 Amazon RDS MySQL 数据库配合使用，将数据库导出到本地客户端计算机。在某些情况下，Amazon RDS 还提供了用于执行数据库原生备份和还原的增强选项。例如，Amazon RDS 提供了用于导出和导入 SQL Server 数据库的 RDS 数据库备份的存储过程。

作为整体备份和还原方法的一部分，请务必彻底测试数据库恢复过程及其对数据库客户端的影响。

使用 DNS CNAME 记录减少数据库恢复期间对客户端的影响

使用 PITR 或 RDS 数据库实例快照还原数据库时，会创建一个带有新端点的新数据库实例。通过这种方式，您可以根据特定的数据库快照或时间点创建多个数据库实例。在恢复 RDS 数据库实例以替换实时的 RDS 数据库实例时，需要注意一些特殊事项。例如，您必须确定如何将现有数据库客户端重定向到新实例，同时尽量减少中断和修改。您还必须考虑恢复数据的时间和新实例开始接收写入时的恢复时间，从而确保数据库内数据的连续性和一致性。

您可以创建指向您的数据库实例端点的单独 DNS CNAME 记录，并让您的客户端使用此 DNS 名称。然后，您可以更新 CNAME 以指向已恢复的新端点，而无需更新数据库客户端。

将 CNAME 记录的有效时间 (TTL) 设置为适当的值。您指定的 TTL 决定了在发出另一个请求之前用 DNS 解析器缓存记录的时间。值得注意的是，某些 DNS 解析器或应用程序可能不支持 TTL，并且它们缓存记录的时间可能会超过 TTL。对于 Amazon Route 53，如果您指定较长的值（例如，172,800 秒，即 2 天），则可以减少 DNS 递归解析器为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并降低您的 Route 53 服务账单。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

应用程序和客户端操作系统也可能缓存 DNS 信息，您必须刷新或重新启动这些信息，才能发起新的 DNS 解析请求并检索更新后的 CNAME 记录。

当您启动数据库还原并将流量转移到还原的实例时，请确认您的所有客户端都在写入还原的实例，而不是之前的实例。您的数据架构可能支持恢复数据库、更新 DNS 以将流量转移到已还原的实例，然后修复可能仍写入先前实例的所有数据。如果不是这种情况，则可以在更新 DNS CNAME 记录之前停止现有实例。然后，所有访问权限都来自您新恢复的实例。这可能会暂时导致某些可以单独处理的数据库客户端出现连接问题。为了减少对客户端的影响，可以在维护窗口内执行数据库还原。

通过使用指数回退进行重试，编写应用程序以优雅地处理数据库连接故障。这使您的应用程序能够在还原期间数据库连接不可用时进行恢复，而不会导致应用程序意外崩溃。

完成还原过程后，您可以将先前的实例保持在停止状态。或者，您可以使用安全组规则限制之前实例的流量，直到您确信不再需要该实例为止。对于逐步停用的方法，首先要限制安全组对运行中数据库的访问权限。如果不再需要实例，则可以最终将其停止。最后，拍摄数据库实例的快照并将其删除。

DynamoDB 的备份和恢复

DynamoDB 提供 PITR，它可以对 DynamoDB 表数据进行几乎持续的备份。启用后，DynamoDB 会在过去 35 天内保留您的表的增量备份，直到您明确将其关闭。

您还可以使用 DynamoDB 控制台、AWS CLI或 DynamoDB API 创建 DynamoDB 表的按需备份。有关更多信息，请参阅备份 DynamoDB 表。您可以使用AWS Backup来安排定期或未来的备份，也可以使用 Lambda 函数自定义和自动执行备份方法。有关使用 Lambda 函数备份 DynamoDB 的更多信息，请参阅博客文章用于计划 Amazon DynamoDB 按需备份的无服务器解决方案。如果您不想创建计划脚本和清理作业，则可以使用AWS Backup来创建备份计划。备份计划包括 DynamoDB 表的计划和保留策略。AWS Backup根据您的保留计划创建备份并删除之前的备份。AWS Backup还包括 DynamoDB 服务中没有的高级 DynamoDB 备份选项，包括成本较低的分层存储以及跨账户和跨区域复制。有关更多信息，请参阅高级 DynamoDB 备份。

必须在还原的 DynamoDB 表上手动设置以下各项：

- 自动扩展策略
- IAM policy
- Amazon CloudWatch 指标和警报
- 标签
- 流设置
- TTL 设置

只能从一个备份将整个表数据还原到一个新表。只能在还原的表变为活动状态后，才能向其中写入内容。

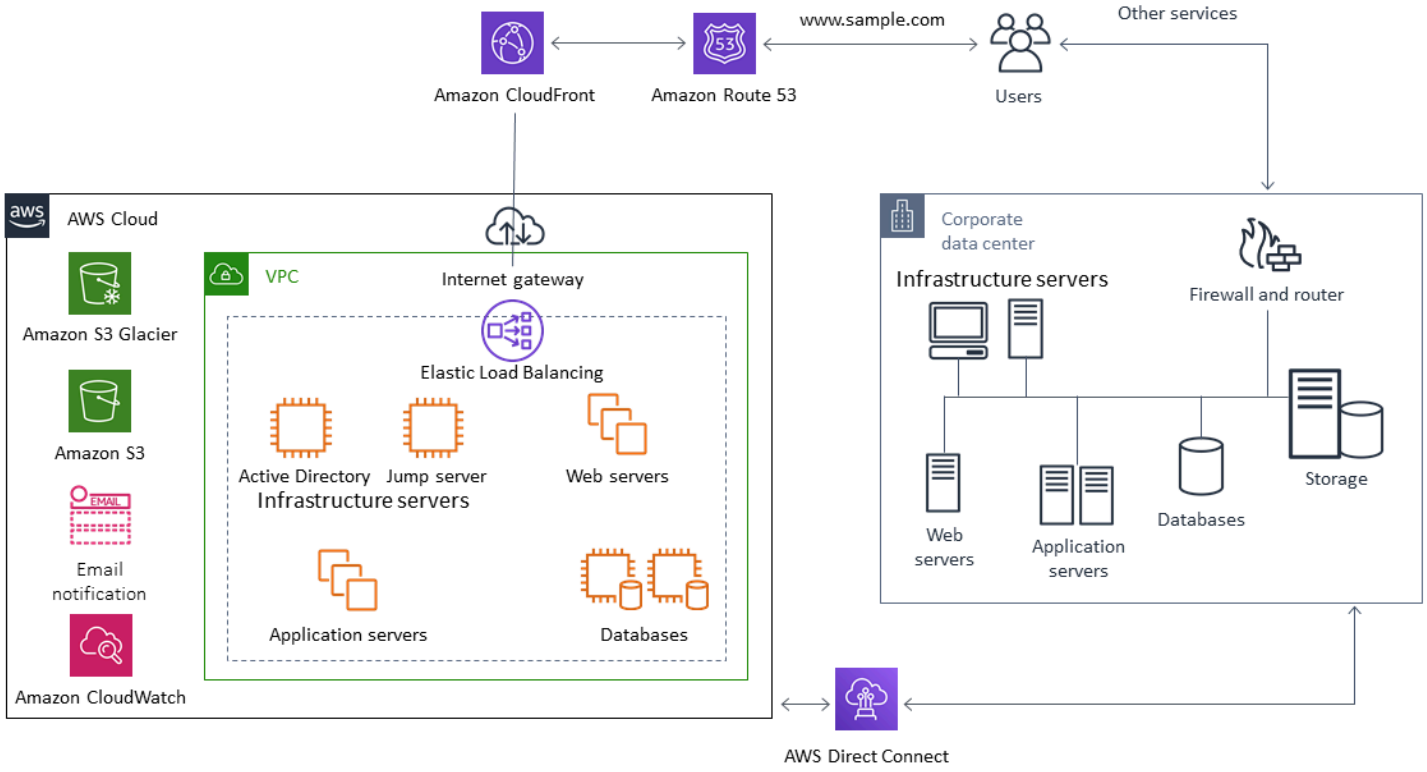
您的还原过程必须考虑如何引导客户端使用新恢复的表名。您可以将应用程序和客户端配置为从配置文件、AWS Systems Manager、Parameter Store 值或其他可以动态更新以反映客户端应使用的表名的引用中检索 DynamoDB 表名。

作为恢复过程的一部分，您应该仔细考虑切换过程。您可以选择拒绝通过 IAM 权限访问您的现有 DynamoDB 表，并允许访问您的新表。然后，您可以更新应用程序和客户端配置以使用新表。您可能还需要协调现有 DynamoDB 表和新恢复的 DynamoDB 表之间的差异。

混合架构的备份和恢复

本指南中讨论的云原生部署和本地部署可以组合成混合场景，在这种场景中，工作负载环境包含本地和 AWS 基础设施组件。资源（包括 Web 服务器、应用程序服务器、监控服务器、数据库和 Microsoft Active Directory）托管在客户数据中心或 AWS。在 AWS Cloud 运行的应用程序与本地运行的应用程序相连。

这已成为企业工作负载的常见场景。许多企业都有自己的数据中心，并且使用 AWS 来增加容量。这些客户数据中心通常通过高容量网络链路连接到 AWS 网络。例如，使用 AWS Direct Connect，您可以建立从本地数据中心到 AWS 的私有专用连接。这为出于数据保护目的将数据上传到云端提供了带宽和一致的延迟。它还为混合工作负载提供稳定的性能和延迟。下图提供了混合环境方法的一个示例。



精心设计的数据保护解决方案通常使用本指南中云原生解决方案和本地解决方案中描述的选项组合。许多 ISV 为本地基础设施提供市场领先的备份和恢复解决方案，并已扩展其解决方案以支持混合方法。

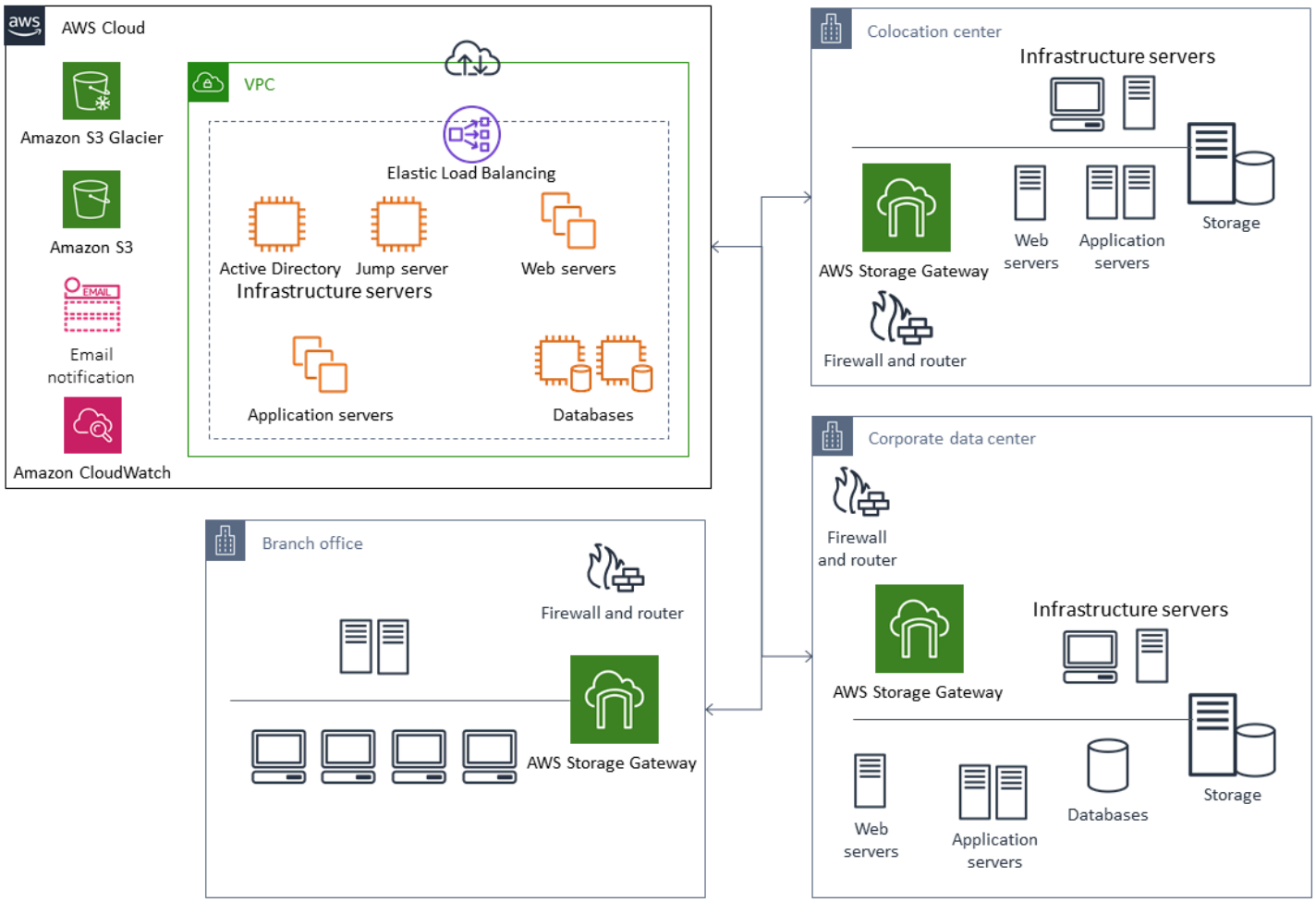
将集中式备份管理解决方案迁移到云端以提高可用性

通过将现有的备份管理解决方案投资与 AWS 一起使用，您可以改善方法的弹性和体系架构。您可能有一台主备份服务器和一台或多台位于本地的媒体或存储服务器，这些媒体或存储服务器位于靠近它们所

保护的服务器和服务的多个位置。在这种情况下，可以考虑将主备份服务器移至 EC2 实例，以保护其免受本地灾难的影响并实现高可用性。

要管理备份数据流，您可以在 EC2 实例上创建一个或多个媒体服务器，这些服务器与它们要保护的服务器位于同一区域。EC2 实例附近的媒体服务器可为您节省互联网传输费用。当您备份到 Amazon S3 或 Amazon S3 Glacier 时，媒体服务器可以提高整体备份和恢复性能。

您还可以使用 Storage Gateway（存储网关）为来自地理分散的数据中心和办公室的数据提供集中云端访问。例如，文件网关允许您按需、低延迟地访问存储在 AWS 中的数据，以实现跨越全球的应用程序工作流程。您可以使用诸如缓存刷新之类的功能来刷新地理位置分散的数据，以便可以轻松地在办公室之间共享内容。



使用 AWS 进行灾难恢复

备份和恢复方法以及支持服务和技术可用于实施灾难恢复 (DR) 解决方案。许多企业都在使用 AWS 云进行备份和恢复，并用作灾难恢复站点。AWS 提供了许多支持灾难恢复和业务连续性的服务和功能。

主题

- 本地灾难恢复到 AWS
- 云原生工作负载的灾难恢复

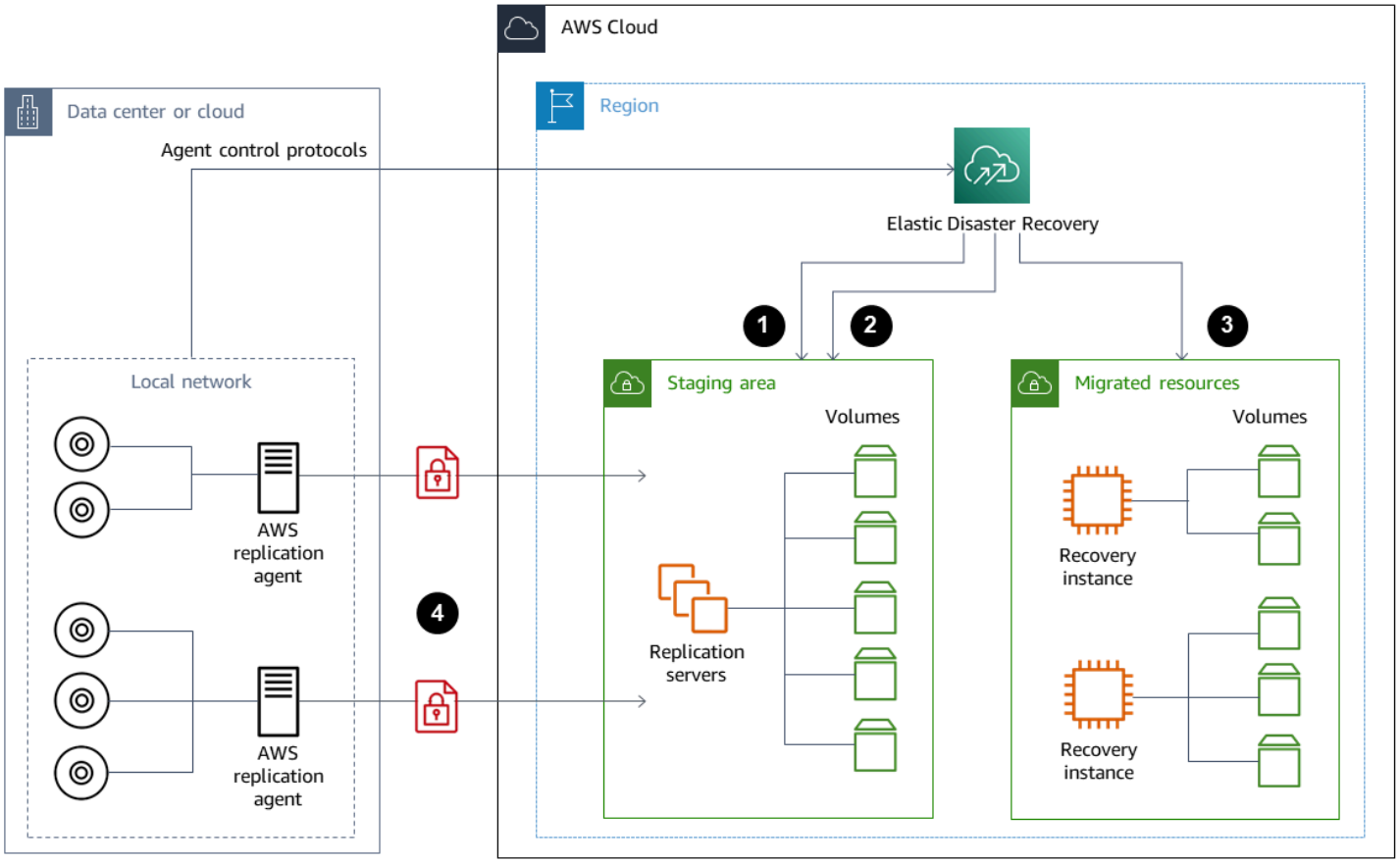
本地灾难恢复到 AWS

AWS 用作本地工作负载的异地灾难恢复 (DR) 环境是一种常见的混合方案。在选择要使用的技术之前，请定义您的灾难恢复目标，包括所需的恢复时间和恢复点目标。为帮助这项定义问题，您可以使用灾难恢复计划清单。

有许多选项可帮助您快速在 AWS 上设置和配置灾难恢复环境。请务必考虑所有工作负载依赖关系，并定期全面测试灾难恢复计划和解决方案，以验证其完整性。

AWS 提供 AWS Elastic Disaster Recovery 用于在 AWS 上创建本地服务器（包括根卷和操作系统）的完整副本。弹性灾难恢复会持续将您的计算机复制到目标 Amazon Web Services account 中的低成本暂存区域，并首选AWS 区域。块级复制是服务器存储的精确副本，包括操作系统、系统状态配置、数据库、应用程序和文件。如果发生灾难，您可以指示弹性灾难恢复在几分钟内快速启动数千台处于完全配置状态的计算机。

弹性灾难恢复使用安装在您的每台本地服务器上的代理。这些代理会将本地服务器的状态与 AWS 上运行的功率较低的 Amazon EC2 等效服务器同步。您还可以使用弹性灾难恢复功能自动执行灾难恢复故障转移和故障恢复流程。自动化故障转移和故障恢复过程可以帮助您实现更低、更稳定的恢复时间目标 (RTO)。



1. 复制服务器状态报告
2. 自动创建和终止暂存区域资源
3. 启动恢复实例时的 RTO 为分钟，RPO 为秒
4. 连续块级复制（压缩和加密）

测试灾难恢复流程并验证实时暂存环境不会与本地环境发生冲突非常重要。例如，确认适当的许可证在您的本地、暂存和已启动的灾难恢复环境中可用且可以正常运行。还要确认是否已正确配置任何可能从中央数据库进行轮询和提取工作的工作器类型的进程，以避免重叠或冲突。在灾难恢复过程中，包括恢复服务器实例上线之前必须执行的所有必要步骤。还包括恢复服务器实例联机且可用后要执行的步骤。您可以使用诸如AWS Elastic Disaster Recovery 计划自动化解决方案之类的解决方案或其他方法来帮助您实现灾难恢复计划的自动化。

您可以使用 Storage Gateway 卷网关为本地服务器提供基于云的卷。也可以使用 Amazon EBS 快照快速配置这些卷，以便与 Amazon EC2 配合使用。尤其，存储卷网关为您的本地应用程序提供对整个数据集的低延迟访问。卷网关还提供基于快照的持久备份，可以将其恢复以供本地使用或与 Amazon EC2 一起使用。您可以根据工作负载的恢复点目标 (RPO) 安排时间点快照。

> **Important**
>
> 卷网关卷旨在用作数据卷，而不是用作启动卷。

您可以使用 Amazon EC2 Amazon 机器映像 (AMI)，其配置与您的本地服务器相匹配并单独指定您的数据量。配置和测试 AMI 后，从 AMI 预配置 EC2 实例以及基于卷网关快照的数据卷。这种方法要求您对环境进行全面测试，以验证您的 EC2 实例是否正常运行，尤其是对于 Windows 工作负载。

云原生工作负载的灾难恢复

考虑您的云原生工作负载如何与灾难恢复目标保持一致。AWS 在全球区域中提供多个可用区。许多使用 AWS 云的企业会调整其工作负载架构和灾难恢复目标，以抵御可用区的损失。Well-Architected AWS ed 框架中的可靠性支柱支持这一最佳实践。您可以设计工作负载及其服务和应用程序依赖关系，以使用多个可用区。然后，您可以自动执行灾难恢复，只需极少干预甚至无需干预即可实现灾难恢复目标。

但是，实际上，您可能会发现无法为所有组件建立冗余、主动和自动化的架构。检查架构的每一层，确定实现目标所需的灾难恢复流程。这可能因工作负载而异，架构和服务要求也不同。本指南涵盖适用于 Amazon EC2 的注意事项和选项。对于其他 AWS 服务，您可以参考 AWS文档 以确定高可用性和灾难恢复选项。

单个可用区中的 Amazon EC2 灾难恢复

尝试设计您的工作负载，以积极支持和服务来自多个可用区的客户。您可以使用 Amazon EC2 Auto Scaling 和 Elastic Load Balancing 为 Amazon EC2 和其他服务实现多可用区服务器架构。

如果您的架构中有无法进行负载平衡的 EC2 实例，并且在任何给定时刻只能运行一个实例，则可以使用以下任一选项。

- 创建一个自动扩缩组，其最小、最大和所需大小均为 1，并针对多个可用区进行配置。创建一个 AMI，用于在实例出现故障时替换实例。请务必定义正确的自动化和配置，以便可以自动配置来自 AMI 的新配置实例并提供服务。创建一个指向 Auto Scaling 组并为多个可用区配置的负载均衡器。或者，创建一个指向负载均衡器终端节点的 Amazon Route 53 别名。
- 为您的活动实例创建 Route 53 记录，并使用此记录让您的客户端进行连接。创建一个脚本，该脚本为您的活动实例创建新 AMI，并使用该 AMI 在单独的可用区中配置处于停止状态的新 EC2 实例。将脚本配置为定期运行并终止先前已停止的实例。如果可用区出现故障，请在备用可用区启动备份实例。然后更新 Route 53 记录以指向这个新实例。

通过模拟解决方案旨在防范的故障，对解决方案进行全面测试。另外，请考虑您的灾难恢复解决方案在工作负载架构变化时需要的更新。

Amazon EC2 区域故障中的灾难恢复

尽管 AWS 区域故障很少见，但某个AWS 地区有可能在未来的某个时候发生故障。客户必须仔细权衡制定和维护多区域灾难恢复计划所需的复杂性、成本和精力与好处。 AWS 提供支持多区域架构的功能，以实现全球可用性、故障转移和灾难恢复。本指南涵盖了一些特定于 Amazon EC2 备份和恢复的可用功能。

AWS AMI 和 Amazon EBS 快照是区域资源，可用于在单个区域内配置新实例。但是，您可以将快照和 AMI 复制到另一个区域，然后使用它们在该区域配置新实例。为了支持区域故障灾难恢复计划，您可以自动将 AMI 和快照复制到其他区域。 AWS Backup 及 Amazon Data Lifecycle Manager 支持将跨区域复制作为备份配置的一部分。

AWS Elastic Disaster Recovery 可用于自动将一个区域中的 Amazon EC2 服务器持续复制到另一个灾难恢复区域。弹性灾难恢复可以简化您的多区域灾难恢复方法，并通过演练帮助您定期测试跨区域 Amazon EC2 灾难恢复计划。当备份和恢复无法实现您的 RTO 和 RPO 目标时，弹性灾难恢复可以提供帮助。弹性灾难恢复可以帮助您将 RTO 降低到几分钟，将 RPO 降低到亚秒级。

无论使用哪种解决方案，都必须确定在停机时要使用的配置、故障转移和故障恢复流程。您可以将 Route 53 与运行状况检查和域名系统故障转移配合使用，以帮助支持您的解决方案。

清理备份

为了降低成本，请清理不再需要用于恢复或保留目的的备份。您可以使用 AWS Backup 和 Amazon 数据生命周期管理器来自动执行部分备份的保留策略。但是，即使有了这些工具，您仍然需要一种清理方法来清理单独进行的备份。

标记策略是清理策略的先决条件。使用标记来识别应清理的资源，适当地通知所有者，并自动执行清理过程。由 AWS 创建的备份的创建日期与其一致，但是标记对于将备份与您的工作负载、保留要求和恢复点识别关联起来非常重要。

您可以使用自动化来实现快照的清理流程。例如，您可以扫描您的账户以获取快照，并确定相应的卷是处于已连接状态还是可用状态。您可以根据您指定的时间阈值进一步筛选结果。使用附加到卷上的标签，您可以自动向快照所有者发送电子邮件，并警告他们已安排删除快照。这种自动修复可以通过使用AWS Config规则、使用AWS CLI的脚本或使用AWS软件开发工具包的 Lambda 函数来实现。

Systems Manager 提供 AWS-DeleteEBSVolumeSnapshots 和 AWS-DeleteSnapshots 文档，以帮助您启动和自动清理 Amazon EBS 快照。您还可以使用AWS CLI和AWS软件开发工具包自动清理其他AWS资源，例如 Amazon RDS 快照。

备份和恢复常见问题

我应该选择什么备份计划？

定义与恢复点目标（RPO）保持一致的备份计划频率。定义一个备份时间，即您的工作负载最小且可以减少对用户的影响。每当您要对工作负载进行重大更改时，都要创建时间点快照。

我需要在我的开发账户中创建备份吗？

测试开发账户中针对工作负载可能发生的重大更改，并在执行重大更改之前创建备份。您的开发和非生产账户中可能还有更多来自开发和测试活动的时间点故障恢复（PITR）备份。

我能否在创建快照的同时升级应用程序并继续使用 EBS 卷而不产生任何影响？

快照是异步制作的；时间点快照是立即创建的，但在所有已修改数据块都已转移到 Amazon S3 之前，其状态为待处理。对于大型初始快照或后续快照（其中许多区块发生了变化），传输可能需要几个小时。传输期间，正在进行的快照不会受到同时发生的卷读写操作的影响。有关更多信息，请参阅 AWS 文档。

后续步骤

首先在非生产环境中评估、实施和测试您的备份和恢复方法。请务必全面测试恢复过程并验证恢复的工作负载是否按预期运行。

除了架构中的所有组件外，还要测试架构中单个组件的恢复过程。验证每个恢复时间。还要验证备份和恢复过程对上游和下游依赖关系的影响。确认任何服务中断对上游依赖关系的影响，并确认下游对备份的影响。

其他资源

AWS 资源

- AWS Prescriptive Guidance
- AWS 文档
- AWS 一般参考
- AWS 术语表

Amazon Web Services

- AWS Backup
- Amazon CloudWatch
- Amazon CloudWatch Events
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Amazon S3 Glacier
- Storage Gateway
- AWS Systems Manager

其他资源

- AWS Backup 备份和恢复（解决方案）
- AWS 工作负载的灾难恢复：云端恢复（白皮书）
- 灾难恢复系列（AWS 架构博客文章）
- 灾难恢复计划清单
- 使用 AWS 备份和恢复方法（技术论文 – 已存档）

- AWS Backup 入门
- AWS 市场 – 备份和恢复

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
已更新信息	更新了本地灾难恢复到 AWS一节中的信息。	2023 年 4 月 13 日
添加一个章节	添加了从快照创建或恢复实例的指导和步骤。	2023 年 3 月 7 日
添加了有关弹性灾难恢复的信息，并增加了澄清说明	在“使用AWS灾难恢复和选择AWS数据保护服务”一节中，添加了有关的 AWS Elastic Disaster Recovery 相关信息。在“使用快照和 AMI 进行的 Amazon EC2 备份和恢复”、“在创建快照或 AMI 之前准备 EBS 卷”和“从 Amazon EBS 快照或 AMI 恢复”章节中，添加了澄清说明。已添加到备份和恢复常见问题解答中。	2023 年 1 月 19 日
添加了一个链接	在 Amazon Data Lifecycle Manager 一节添加了指向 Amazon Data Lifecycle Manager 文档的链接。	2022 年 10 月 31 日
已更新信息	更新了有关恢复卷的信息。	2022 年 8 月 30 日
更新了信息并新增一节	在选择用于数据保护的AWS服务一节中，添加了服务。添加了使用 AWS Backup 进行备份和恢复一节。在使用 Amazon S3 和 Amazon S3 Glacier 进行备份和恢复一节中，添加了有	2022 年 1 月 28 日

	关新的 Amazon S3 Glacier 存储类的信息。在带有 EBS 卷的 Amazon EC2 的备份和恢复一节中，添加了指向文档和其他信息的链接。在云原生AWS服务的备份和恢复一节中，添加了使用AWS Backup的建议。在其他资源一节中，添加了资源。	
已更新信息	在 S3 Glacier Flexible Retrieval 一节中添加了有关设置存储类的信息。在使用快照和 AMI 的 Amazon EC2 备份和恢复一节中添加了有关检索快照的信息。	2021 年 9 月 9 日
已更新信息	在AWS Backup一节中，添加了有关AWS Backup支持的AWS服务的信息。	2021 年 6 月 1 日
初次发布	—	2020 年 7 月 29 日

AWS Prescriptive Guidance 术语表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构 - 充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台 - 将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中的 Amazon Relational Database Service（Amazon RDS）for Oracle。
- 重新购买 - 转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 更换主机（直接迁移）- 将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- 重新定位（虚拟机监控器级直接迁移）- 将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。此迁移场景特定于 VMware Cloud on AWS，它支持本地环境和 AWS 之间的虚拟机兼容性和工作负载可移植性。在将基础设施迁移到 VMware Cloud on AWS 时，您可以在本地数据中心使用 VMware Cloud Foundation 技术。示例：将托管 Oracle 数据库的管理程序重新定位到 VMware Cloud on AWS。
- 保留（重访）- 将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用 - 停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

酸

参见原子性、一致性、隔离性、耐久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。与主动-被动迁移相比，它更灵活，但需要更多的工作。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一个 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括SUM和MAX。

AI

参见人工智能。

AIOps

参见人工智能运营。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能运营（AIOps）

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AWS 迁移策略中使用 AIOps 的更多信息，请参阅运营集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management（IAM）文档中的有关 AWS 的 ABAC。

权威数据源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

一个 AWS 区域 中的不同位置，用于与其他可用区的故障隔离，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架（AWS CAF）

AWS 的指导原则和最佳实践框架，旨在帮助组织制定高效且有效的计划来成功迁移到云。AWSCAF 将指导原则分为六个重点领域（角度）：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS Workload Qualification Framework（AWS WQF）

一种评估数据库迁移工作负载、推荐迁移策略并提供工作量估算的工具。AWSWQF 包含在 AWS Schema Conversion Tool（AWS SCT）中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

BCP

参见业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参见字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

破碎的玻璃通道

在特殊情况下，通过批准的流程，用户AWS 账户可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 Well -Architected 指南中的“实施破碎玻璃程序”指示AWS器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS 上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

参见AWS云采用框架。

CCoE

参见云卓越中心。

CDC

参见变更数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的弹性。您可以使用 AWS Fault Injection Service(AWS FIS) 来执行实验，对您的AWS工作负载施加压力并评估其响应。

CI/CD

查看持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 接收数据之前，在本地对数据进行加密。

云卓越中心（CCoE）

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS 云企业战略博客上的 CCoE 帖子。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常与边缘计算技术相关。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS 云中时通常会经历四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 - 进行基础投资以扩大云采用率（例如，创建登录区、定义 CCoE、建立运营模型）
- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

Stephen Orban 在 AWS 云企业战略博客上发表的博客文章云优先之旅和采用阶段中对这些阶段进行了定义。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

参见配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或AWS CodeCommit。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管道可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉

机器用来在图像中以比肩或高于人类水平的精度辨识人、地点和事物的 AI 领域。它往往用深度学习模型构建，使得可自动从单幅图像或一系列图像提取、分析、分类和理解有用信息。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和修复操作，您可以将其组合起来以自定义合规性和安全性检查。您可以使用 YAML 模板，将合规性包作为单个实体部署到 AWS 账户 区域中，或者跨组织部署。有关更多信息，请参阅 AWS Config 文档中的合规性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。CI/CD 通常被描述为管道。CI/CD 可以帮助您实现流程自动化、提高工作效率、改善代码质量并加快交付速度。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 AWS Well-Architected Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据最少化

仅收集并处理绝对必要数据的原则。在 AWS Cloud 中践行数据最少化可以降低隐私风险、成本和您的分析碳足迹。

数据边界

AWS环境中的一组预防性防护措施，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在上构建数据边界。AWS

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当您在 AWS 上采用此策略时，您可以在 AWS Organizations 结构的不同层添加多种控制措施，来保护资源。例如，一种 defense-in-depth 方法可以结合多因素身份验证、网络分段和加密。

委托管理员

在 AWS Organizations 中，兼容服务可以注册 AWS 成员账户来管理组织的账户，并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations 的服务。

部署

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

参见环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出警报。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS 上实施安全控制中的侦测性控制。

开发价值流映射 (DVSM)

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

在星型架构中，一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复 (DR)

您用来最大限度地减少灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 AWS 上工作负载的灾难恢复：AWS Well-Architected Framework 中的云中恢复。

DML

参见数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

跟踪与基准配置的偏差。例如，您可以使用AWS CloudFormation来检测系统资源中的偏差，也可以使用AWS Control Tower来检测着陆区中可能影响监管要求合规性的变化。

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算相比，边缘计算可以减少通信延迟并缩短响应时间。

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

参见服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用 AWS PrivateLink 创建端点服务，并将权限授予其他 AWS 账户 或 AWS Identity and Access Management（IAM）主体。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service（AWS KMS）文档中的信封加密。

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。
- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如，AWS CAF security epics 包括身份和访问管理、侦测性控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

F

事实表

星形架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在中AWS Cloud，诸如可用区AWS 区域、控制平面或数据平面之类的边界，它限制了故障的影响并有助于提高工作负载的弹性。有关更多信息，请参阅AWS故障隔离边界。

功能分支

参见分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅机器学习模型的可解释性：AWS。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，它使用连续的数据复制，通过更改数据捕获在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

在 Amazon 中 CloudFront，一种阻止特定国家/地区的用户访问内容分发的选项。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分布。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的，而基于主干的工作流程是现代的首选方法。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

防护机制

一种高级规则，用于跨组织单位（OU）管理资源、策略和合规性。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用AWS Config、、Amazon、AWS Security Hub GuardDutyAWS Trusted Advisor、Amazon Inspector 和自定义AWS Lambda支票来实现。

H

HA

参见高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性 (HA)

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术 (OT) 系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常是在典型的 DevOps 发布工作流程之外进行的。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

I

IaC

参见基础架构即代码。

基于身份的策略

附加到一个或多个 IAM 主体的策略，用于定义它们在 AWS Cloud 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

参见工业物联网。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测。有关更多信息，请参阅 Well-Architected Framework 中的使用不可变基础架构AWS部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种用于接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预置和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网（IIoT）

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网（IIoT）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，一种用于管理 VPC（相同或不同的 AWS 区域）、互联网和本地网络之间的网络流量检查的集中式 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用 AWS 实现机器学习模型的可解释性。

IoT

参见物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制 (LBAC)

强制访问控制 (MAC) 的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

登录区是一个架构完善、可扩展且安全的多账户 AWS 环境。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

参见分支。

托管服务

AWS 服务它AWS运行基础设施层、操作系统和平台，您可以访问端点来存储和检索数据。亚马逊简单存储服务 (Amazon S3) Service 和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

MAP

参见迁移加速计划。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

除管理账户外，属于 AWS Organizations 中的组织的所有 AWS 账户。一个账户一次只能是一个组织的成员。

微服务

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级 API 通过明确定义的接口进行通信。该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在 AWS 上实现微服务。

迁移加速计划（MAP）

一项提供咨询支持、培训和服务的 AWS 计划，旨在帮助组织为迁移到云奠定坚实的运营基础，并抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发 DevOps 人员和冲刺专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS Application Migration Service 将主机迁移到 Amazon EC2。

迁移组合评测（MPA）

一种在线工具，提供了用于验证迁移到 AWS 云的业务用例的信息。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据收集、应用程序分组、迁移优先级排序和波次规划）。MPA 工具（需要登录）向所有 AWS 顾问和 APN 合作伙伴顾问免费提供。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态，找出优势和劣势，并制定行动计划来弥补发现的差距。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

将工作负载迁移到 AWS 云中的方法。有关更多信息，请参阅此词汇表中的 7 R 条目和动员组织以加快大规模迁移。

ML

参见机器学习。

MPA

参见迁移组合评估。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关详细信息，请参阅在 AWS 云中实现应用程序现代化的策略。

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关详细信息，请参阅在 AWS 云中评估应用程序的现代化准备情况。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础架构

一种用于更新和修改现有生产工作负载基础架构的模型。为了提高一致性、可靠性和可预测性，Well-Architect AWS ed Framework 建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查 (ORR)

一份问题清单和相关的最佳实践，可帮助您理解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 Well-Architecte AWS d Frame work 中的运营准备情况评估 (ORR)。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 创建的跟踪，用于记录 AWS Organizations 中的组织的所有 AWS 账户 事件。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，这个框架称为人员加速，因为云采用项目需要快速的变革。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

在中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 支持所有 AWS 区域 中的 S3 存储桶、使用 AWS KMS 的服务器端加密（SSE-KMS）以及对 S3 存储桶的动态 PUT 和 DELETE 请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

或者

参见运营准备情况审查。

出站（出口）VPC

在 AWS 多账户架构中，一种用于处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息 (PII)

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

查看个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

策略

一个对象，可以在中定义权限（参见基于身份的策略）、指定访问条件（参见基于资源的策略）或定义组织中所有账户的最大权限AWS Organizations（参见服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。有关更多信息，请参阅在微服务中实现数据持久性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

一种数据库查询优化技术，可在传输前筛选查询中的数据。这减少了必须从关系数据库检索和处理的数据量，并提高了查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS 上实施安全控制中的预防性控制。

主体

AWS 中可执行操作并访问资源的实体。该实体通常是 AWS 账户、IAM 角色或用户的根用户。有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制措施，旨在防止部署不合规的资源。这些控件会在资源置备之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。有关更多信息，请参阅AWS Control Tower文档中的控制参考指南，并参见在上实施安全控制中的主动控制AWS。

生产环境

参见环境。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

R

RACI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新设计架构

见 7 R。

恢复点目标 (RPO)

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

地理区域中的 AWS 资源集合。每个 AWS 区域 是孤立的，独立于其他的区域，以提供容错能力、稳定性和弹性。有关更多信息，请参阅在 AWS 一般参考 中管理 AWS 区域。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责 (R)、问责 (A)、咨询 (C) 和知情 (I)。支持 (S) 类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在 AWS 上实施安全控制中的响应性控制。

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行列访问控制 (RCAC)

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

S

SAML 2.0

许多身份提供商 (IdPs) 使用的开放标准。此功能可实现联合单点登录（SSO），因此用户可以登录 AWS Management Console 或调用 AWS API 操作，而无需在 IAM 中为组织中的每个人都创建用户。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCP

参见服务控制政策。

secret

在中AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Sec rets Manager 文档中的密钥。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制主要有四种类型：预防性、侦测、响应式和主动式。

安全加固

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义和编程的操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施AWS安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换证书。

服务器端加密

由接收数据的 AWS 服务 在目的地对数据进行加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations 的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

AWS 服务 的入口点的 URL。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

一种描述您在云安全性和合规性方面与 AWS 共担的责任模型。AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

暹粒

参见安全信息和事件管理系统。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见服务级别协议。

SLI

参见服务级别指标。

SLO

参见服务级别目标。

split-and-seed 模型

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅中的分阶段实现应用程序现代化的方法。AWS Cloud

恶作剧

参见单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储交易数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。你可以使用 Amazon S CloudWatch ynthetics 来创建这些测试。

T

tags

充当元数据的键值对，用于组织 AWS 资源。标签可帮助您管理、识别、组织、搜索和筛选资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

参见环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是中转网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

为您指定的服务授予权限，让其代表您在 AWS Organizations 的组织中及其账户中执行任务。当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的将 AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小 DevOps 团队，你可以用两个披萨来喂食。双披萨团队的规模可确保在软件开发过程中充分协作。

U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

参见环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两个 VPC 之间的连接，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一个 SQL 函数，用于对一组以某种方式与当前记录相关的行进行计算。窗口函数对于处理任务很有用，例如计算移动平均线或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

蠕虫

参见一次写入，多读。

WQF

请参阅 AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

一种存储模型，它可以一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但他们无法对其进行更改。这种数据存储基础架构被认为是不可变的。

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。

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。