AWS 白皮书

AWS 上的工作负载灾难恢复：云中的恢复

AWS 上的工作负载灾难恢复：云中的恢复: AWS 白皮书

Table of Contents

AWS 上的工作负载灾难恢复：云中的恢复

发布日期：2021 年 2 月 12 日（文档修订）

摘要

灾难恢复是指为灾难做好准备以及从灾难中恢复的过程。我们把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视为灾难。这份白皮书概括介绍了为部署到 AWS 的任何工作负载计划和测试灾难恢复的最佳实践，并提供了不同的方法来减轻风险和满足该工作负载的恢复时间目标（RTO）和恢复点目标（RPO）。

引言

您的工作负载必须正确且一致地执行其预期功能。要实现这一点，您必须构建弹性。弹性是工作负载从基础设施或服务中断中恢复、动态获取计算资源以满足需求以及减少诸如配置错误或暂时性网络问题等中断的能力。

灾难恢复（DR）是弹性策略的重要组成部分，它涉及灾难来袭时工作负载的响应方式（灾难是对您的业务造成严重负面影响的事件）。此响应必须基于贵企业的业务目标，这些目标指定了避免数据丢失的工作负载策略（称为恢复点目标（RPO）），以及在工作负载无法使用时减少停机时间的策略（称为恢复时间目标（RTO））。因此，您必须在设计云中的工作负载时实施弹性，以满足给定单次灾难事件的恢复目标（RPO 和 RTO）。作为业务连续性计划（BCP）的一部分，此方法可帮助贵企业保持业务连续性。

本白皮书重点介绍如何在 AWS 上规划、设计和实施可满足企业灾难恢复目标的架构。此处分享的信息面向担任技术角色的人员，如首席技术官（CTO）、构架师、开发人员和操作团队成员。

灾难恢复和可用性

我们可以比较一下灾难恢复与可用性，后者是弹性策略的另一个重要组成部分。灾难恢复衡量的是单次事件的目标，而可用性目标衡量的是一段时期内的平均值。

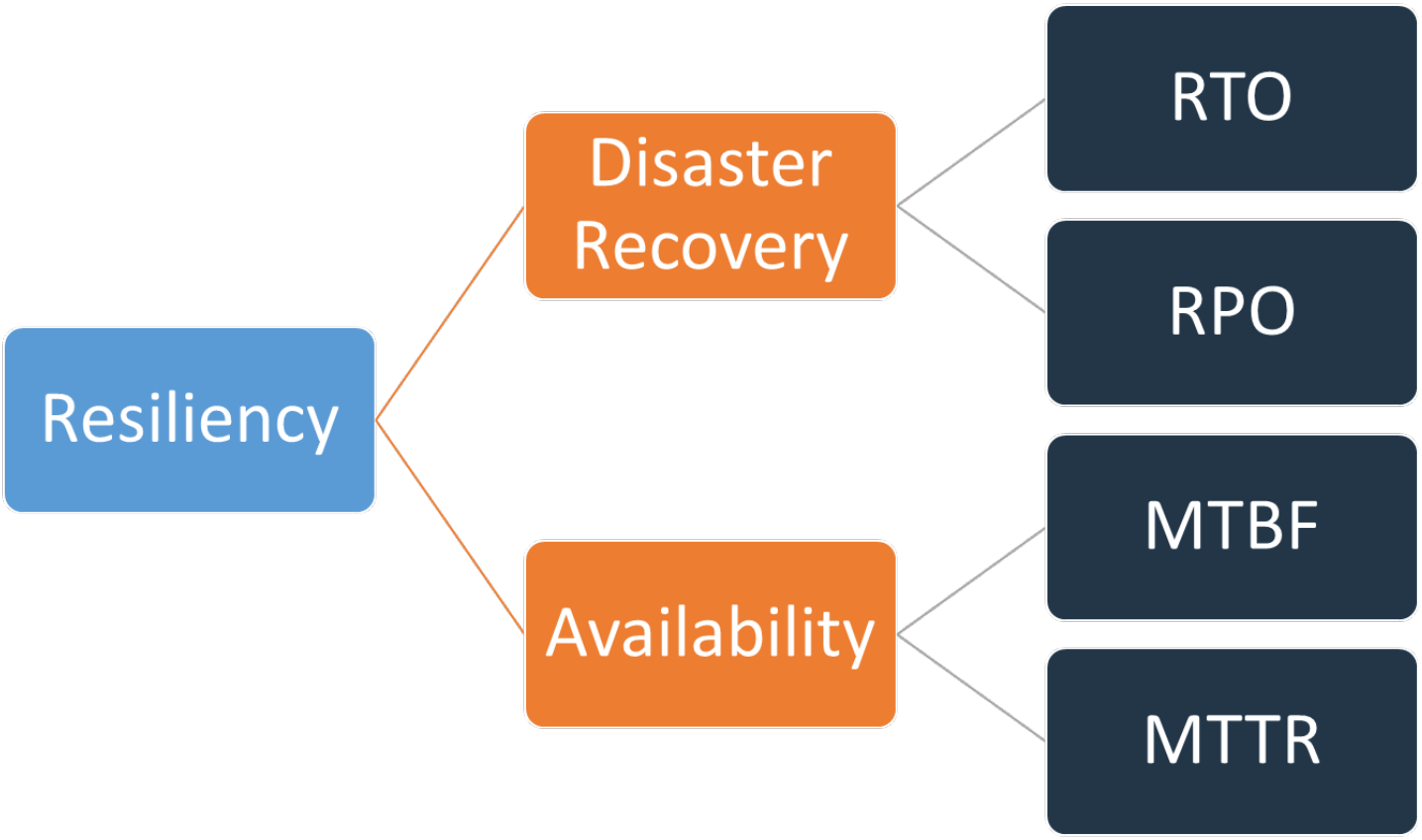

图 1 – 弹性目标

可用性是使用平均故障间隔时间（MTBF）和平均恢复时间（MTTR）计算的：

$$Availability = \frac{Available\ for\ Use\ Time}{Total\ Time} = \frac{MTBF}{MTBF + MTTR}$$

此方法通常用“几个九”来表述，例如，99.9% 的可用性目标称为“三个九”。

对于您的工作负载，与使用基于时间的方法相比，计算成功和失败的请求可能更容易。在这种情况下，可以使用以下计算方法：

$$Availability = \frac{Successful\ Responses}{Valid\ Requests}$$

灾难恢复侧重于灾难事件，而可用性则侧重于更常见的较小规模中断，例如组件故障、网络问题和负载峰值。灾难恢复的目标是业务连续性，而可用性则涉及尽可能地保证工作负载可用于执行其预期业务功能的时间。两者都应纳入您的弹性策略中。

有关确保弹性的责任共担模式

确保弹性是 AWS 和您（客户）的共同责任。了解灾难恢复和可用性（都是弹性的组成部分）在这种共担模式下如何运作非常重要。

AWS 的“云弹性”责任

AWS 负责确保运行 AWS 云中提供的所有服务的基础设施的弹性。此基础设施包含运行 AWS 云服务的硬件、软件、网络和设施。AWS 将采取商业上合理的措施使这些 AWS 云服务可用，确保服务的可用性满足或超过 AWS 服务等级协议（SLA）。

AWS 全球云基础设施旨在帮助客户构建具有高度弹性的工作负载架构。每个 AWS 区域都完全隔离，由多个可用区组成，这些可用区是基础设施的物理隔离分区。可用区可以隔离可能影响工作负载弹性的故障，防止它们影响区域中的其他可用区。与此同时，AWS 区域中的所有可用区都通过高带宽、低延迟网络互连，完全冗余的专用城域光纤为可用区之间提供了高吞吐量、低延迟的网络连接。可用区之间的所有流量都进行了加密。网络性能足以确保可用区之间的同步复制。可用区简化了对应用程序进行分区以实现高可用性的过程。

客户的“云中弹性”责任

您的责任将由您选择的 AWS 云服务决定。这决定了作为您弹性责任的一部分，您必须执行的配置工作量。例如，Amazon Elastic Compute Cloud（Amazon EC2）等服务要求客户执行所有必要的弹性配置和管理任务。部署 Amazon EC2 实例的客户负责跨多个位置（如 AWS 可用区）部署 EC2 实例，使用 AWS Auto Scaling 等服务实施自我修复，以及对安装在实例上的应用程序使用弹性工作负载架构最佳实践。对于托管式服务，例如 Amazon S3 和 Amazon DynamoDB，AWS 运营基础设施层、操作系统和平台，而客户通过访问终端节点存储和检索数据。您负责管理数据的弹性，包括备份、版本控制和复制策略。

跨一个 AWS 区域中的多个可用区部署工作负载是高可用性策略的一部分，该策略旨在通过将问题隔离在一个可用区来保护工作负载，并使用其他可用区的冗余继续为请求提供服务。多可用区架构也是灾难恢复策略的一部分，该策略旨在更好地隔离工作负载并保护其免受停电、雷击、龙卷风、地震等问题的影响。灾难恢复策略也可以利用多个 AWS 区域。例如，在主动/被动配置中，如果活动区域无法再为请求提供服务，则工作负载的服务将从其活动区域故障转移到其灾难恢复区域。

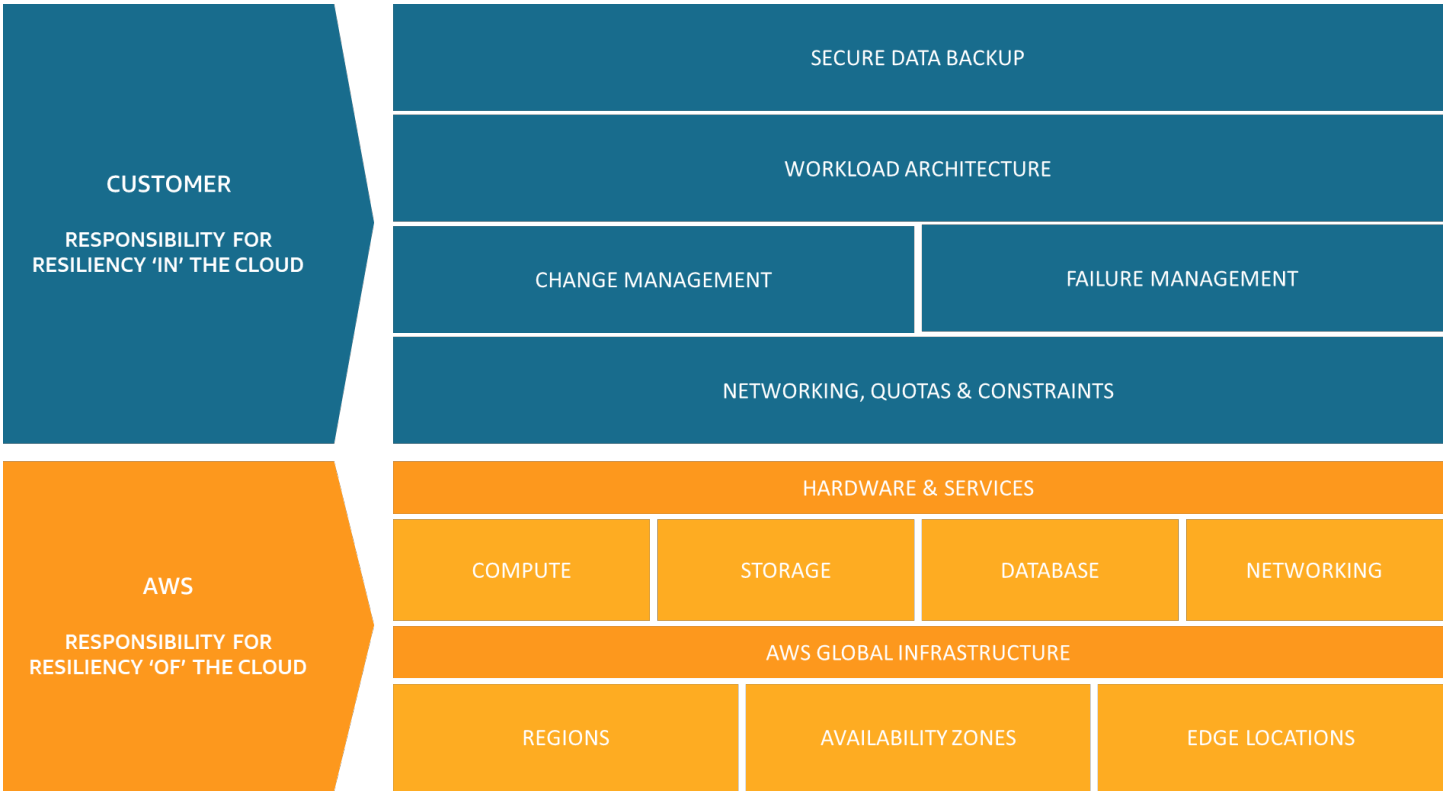

图 2 – 弹性是 AWS 和客户的共同责任

什么是灾难？

规划灾难恢复时，请评估针对以下三大类灾难的计划：

- 自然灾害，例如地震或洪水
- 技术故障，例如电源故障或网络连接
- 人为操作，例如无意的配置错误或未经授权/外部人员的访问或修改

这些潜在灾难中的每一种都会产生某种地理范围的影响，可能是地方性、区域性、全国性、大洲性，甚至全球性的。考虑灾难恢复策略时，灾难的性质和地理范围影响都很重要。例如，您可以采用多可用区策略缓解本地泛洪导致的数据中心中断问题，因为该问题不会影响多个可用区。但是，如果生产数据遭受攻击，您需要调用故障转移到另一个 AWS 区域中的备份数据的灾难恢复策略。

高可用性不是灾难恢复

可用性和灾难恢复都依赖于某些相同的最佳实践，例如监控故障、部署到多个位置以及自动故障转移。但是，可用性侧重于工作负载的组成部分，而灾难恢复则侧重于整个工作负载的分立副本。灾难恢复与可用性有着不同的目标，它衡量的是符合灾难定义的较大规模事件发生后的恢复时间。您应首先确保工作负载满足可用性目标，因为在发生影响可用性的事件时，高度可用的架构将使您能够满足客户的需求。您的灾难恢复策略需要不同于可用性策略的方法，重点是将分立系统部署到多个位置，以便在必要时可以对整个工作负载进行故障转移。

您必须在灾难恢复规划中考虑工作负载的可用性，因为这会影响您采取的方法。在一个可用区中的单个 Amazon EC2 实例上运行的工作负载没有高可用性。如果本地泛洪问题影响该可用区，则此场景需要故障转移到另一个可用区以实现灾难恢复目标。我们来将此场景与部署为多站点主动/主动模式的高可用性工作负载（工作负载部署在多个活动区域，并且所有区域都在为生产流量提供服务）进行比较。在这种情况下，即使发生了不太可能发生的大规模灾难摧毁整个区域的事件，也可通过将所有流量都路由到其余区域来实现灾难恢复策略。

可用性和灾难恢复之间处理数据的方式也有所不同。假设有一个存储解决方案，它将数据持续复制到另一站点以实现高可用性（例如多站点、主动/主动工作负载）。如果主存储设备上的一个或多个文件被删除或损坏，这些破坏性更改会被复制到辅助存储设备。在此场景中，尽管具有高可用性，但在数据删除或损坏时进行故障转移的能力将受到损害。而作为灾难恢复策略的一部分，还需要时间点备份。

业务连续性计划（BCP）

灾难恢复计划应是企业业务连续性计划（BCP）的一部分，而不应是独立的文档。如果由于灾难对工作负载以外的业务要素的影响而无法实现工作负载的业务目标，则为还原该工作负载而维护激进的灾难恢复目标就毫无意义。例如，地震可能导致无法运输客户在您的电子商务应用程序上购买的产品 – 即使有效的灾难恢复可以让工作负载正常运行，您的 BCP 也还需要满足运输需求。您的灾难恢复策略应基于业务需求、优先级和具体情况。

业务影响分析和风险评估

业务影响分析应量化工作负载中断对业务的影响。它应确定无法使用工作负载对内部和外部客户的影响，以及对您业务的影响。分析应有助于确定需要以多快的速度恢复工作负载，以及可以容忍多少数据丢失。但是，必须指出的是，不应孤立地制定恢复目标；中断的概率和恢复成本是关键因素，有助于了解为工作负载提供灾难恢复的商业价值。

业务影响可能取决于时间。您可能需要考虑将此因素纳入灾难恢复规划。例如，如果发薪工作还没处理完，薪资系统的中断可能会对业务产生很大的影响，但在所有发薪工作都完成了之后，影响可能很小。

对灾难类型和地理范围影响的风险评估以及工作负载的技术实施概况将确定每种灾难发生中断的可能性。

对于非常关键的工作负载，您可以考虑在多个区域内进行高可用性的连续备份，以尽量减少业务影响。对于不太重要的工作负载，合理的策略可能是根本不进行任何灾难恢复。而对于某些灾难场景，不制定任何灾难恢复策略也是合理的，前提是企业基于灾难发生概率较低而做出明智决定。请记住，AWS 区域内的可用区在设计时彼此之间已经有了合理的距离，并仔细规划了位置，因此大多数常见灾难只会影响一个可用区，而不会影响其他可用区。因此，AWS 区域内的多可用区架构可能已经满足了您的风险缓解需求。

应评估灾难恢复选项的成本，以确保在考虑到业务影响和风险的情况下，灾难恢复策略能够提供正确水平的商业价值。

利用所有这些信息，您可以记录不同灾难场景的威胁、风险、影响和成本，以及相关的恢复选项。应利用这些信息来确定每个工作负载的恢复目标。

恢复目标（RTO 和 RPO）

在制定灾难恢复（DR）策略时，组织通常会根据恢复时间目标（RTO）和恢复点目标（RPO）进行规划。

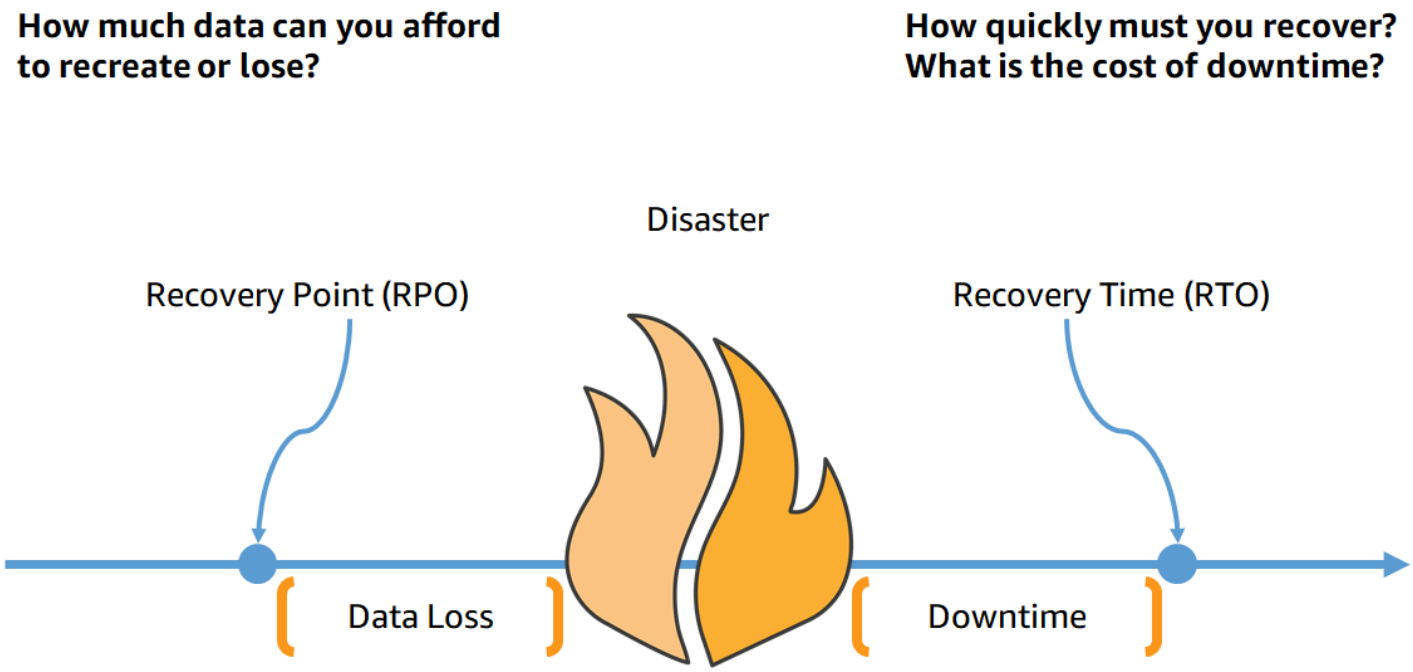

图 3 – 恢复目标

恢复时间目标（RTO）是指服务中断和服务还原之间的最大可接受延迟。此目标确定了服务不可用时，可接受的时间窗口，并由组织定义。

本白皮书大致讨论了四种灾难恢复策略：备份与还原、Pilot Light、温备用和多站点主动/主动（请参阅云中的灾难恢复选项）。在下图中，企业确定了其允许的最大 RTO，以及他们可在服务还原策略上花费金额的限制。考虑到企业的目标，Pilot Light 或温备用这两种灾难恢复策略将既符合 RTO 标准，又符合成本标准。

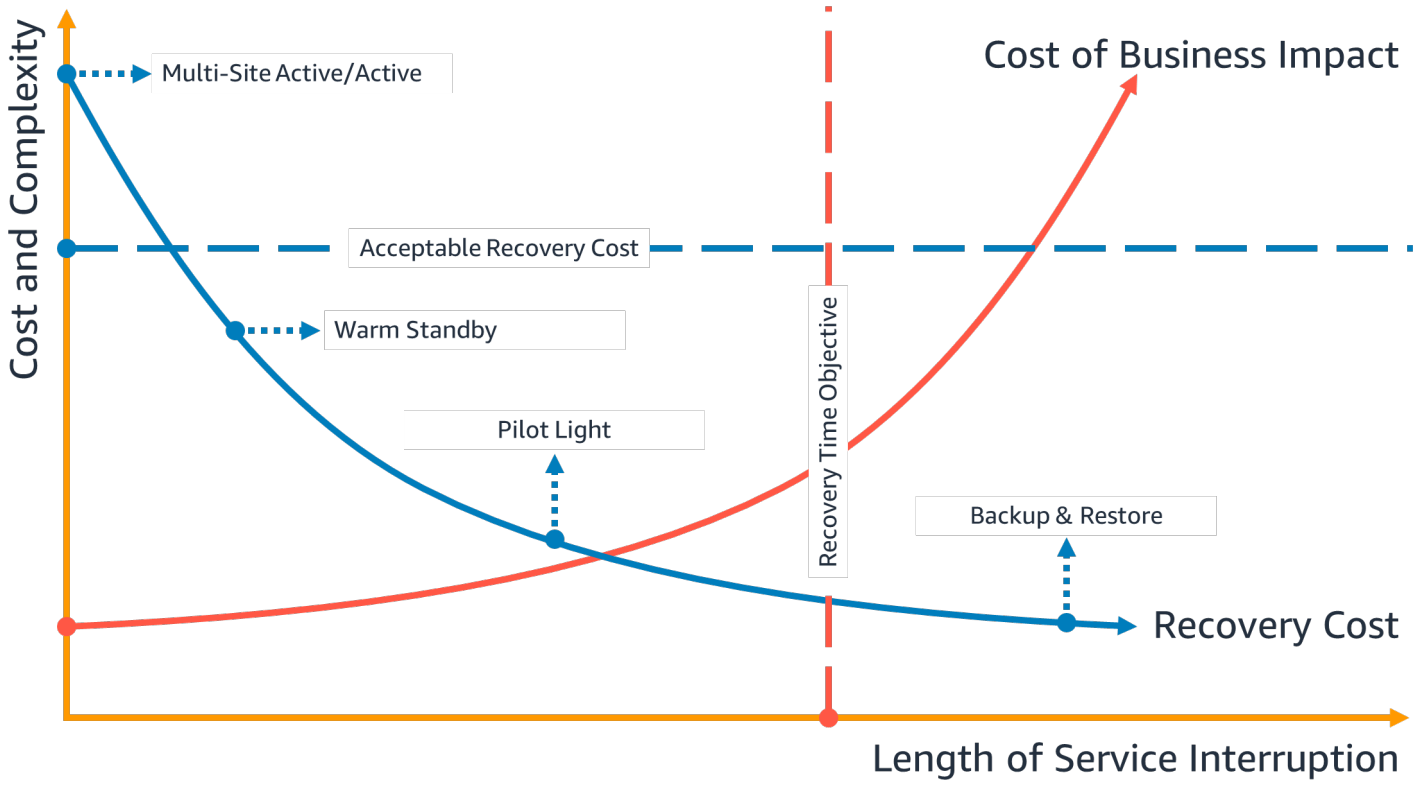

图 4 – 恢复时间目标

恢复点目标（RPO）是指自上一个数据恢复点之后的最大可接受时间。此目标确定在上一个恢复点和发生服务中断之间可接受的数据丢失量，并由组织定义。

在下图中，企业确定了其允许的最大 RPO，以及他们可在数据恢复策略上花费金额的限制。在这四种灾难恢复策略中，Pilot Light 或温备用灾难恢复策略既符合 RPO 标准，又符合成本标准。

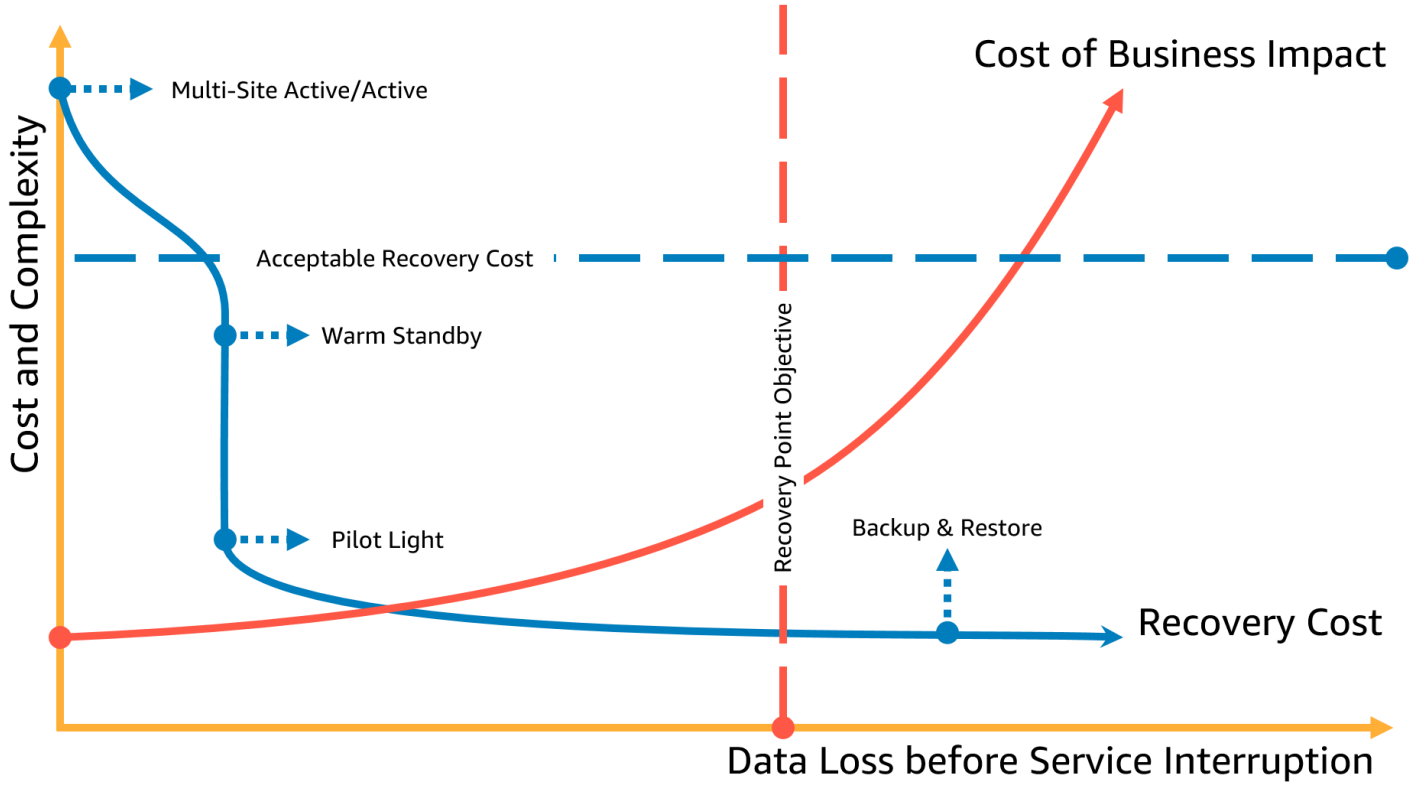

图 5 – 恢复点目标

> **Note**
>
> 如果恢复的成本高于故障或损失的成本，则除非有其他驱动因素（如监管要求），否则不应实施恢复方案。

云中的灾难恢复有所不同

灾难恢复策略随着技术创新而发展。本地灾难恢复计划可能涉及以物理方式运输磁带或将数据复制到另一站点。您的企业需要重新评估其之前灾难恢复策略的业务影响、风险和成本，以实现其在 AWS 上的灾难恢复目标。与传统环境相比，AWS 云中的灾难恢复具有以下优势：

- 迅速从灾难中恢复，并降低复杂性
- 简单且可重复的测试使您可以更轻松、更频繁地进行测试
- 更低的管理开销减轻了运营负担
- 实施自动化的机会减少了出错的几率并缩短了恢复时间

采用 AWS，您将告别物理备份数据中心的固定资本支出，转而为云中规模合适的环境支付可变营运支出，这样可以显著降低成本。

对于许多企业而言，本地灾难恢复的设计围绕着数据中心内一个或多个工作负载中断的风险，以及将备份或复制的数据恢复到辅助数据中心。当企业在 AWS 上部署工作负载时，他们可以实施架构完善的工作负载，并依靠 AWS 全球云基础设施的设计来帮助减轻此类中断的影响。有关在云中设计和运行可靠、安全、高效且具有成本效益的工作负载的架构最佳实践的更多信息，请参阅《AWS Well-Architected Framework – 可靠性支柱》白皮书。

如果您的工作负载在 AWS 上，则无需担心数据中心的连接（访问能力除外）、电力、空调、消防和硬件。所有这些均为您托管，并且您可以访问多个故障隔离可用区（每个可用区由一个或多个分立的数据中心组成）。

单个 AWS 区域

对于因一个物理数据中心中断或丢失而导致的灾难事件，在单个 AWS 区域内的多个可用区实施高可用性工作负载有助于缓解自然灾害和技术灾难，并降低人为威胁（例如可能导致数据丢失的错误或未经授权的活动）的风险。每个 AWS 区域都由多个可用区组成，每个可用区与其他可用区之间实现故障隔离。每个可用区又由多个物理数据中心组成。为了更好地隔离影响较大的问题并实现高可用性，您可以跨同一区域中的多个可用区对工作负载进行分区。可用区专为实现物理冗余而设计，具有弹性，即使在出现断电、互联网停机、洪水和其他自然灾害的情况下也能实现不间断的性能。请参阅 AWS 全球云基础设施，了解 AWS 如何做到这一点。

通过跨单个 AWS 区域中的多个可用区进行部署，可以更好地保护您的工作负载免受单个（甚至多个）数据中心故障的影响。为了对您的单区域部署提供额外的保障，您可以将数据和配置（包括基础设施定

义）备份到另一个区域。此策略将灾难恢复计划的范围缩小到仅包括数据备份和还原。与下一节所述的其他多区域选项相比，通过备份到另一个 AWS 区域来利用多区域弹性既简单又便宜。例如，通过备份到 Amazon Simple Storage Service（Amazon S3），您可以立即检索数据。但是，如果您针对部分数据的灾难恢复策略对检索时间的要求更宽松（从几分钟到几小时），那么使用 Amazon S3 Glacier 或 Amazon S3 Glacier Deep Archive 将显著降低备份和恢复策略的成本。

某些工作负载可能有监管数据驻留要求。如果您的工作负载属此情况，且其所在地点当前只有一个 AWS 区域，那么除了按照上述介绍，设计多可用区工作负载以实现高可用性之外，您还可以将该区域中的多个可用区用作分立位置，这有助于满足适用于该区域中工作负载的数据驻留要求。以下各节所述的灾难恢复策略使用多个 AWS 区域，但也可以使用多个可用区而不是区域来实施这些策略。

多个 AWS 区域

如果灾难事件涉及相距甚远的多个数据中心。且这些数据中心有丢失的风险，则您应该考虑使用能够缓解影响 AWS 中整个区域的自然灾害和技术灾难的灾难恢复选项。以下各节所述的所有选项均可作为多区域架构来实施，以防范此类灾难。

云中的灾难恢复选项

从低成本、低复杂性的制作备份到使用多个活动区域的较复杂策略，可在 AWS 中使用的灾难恢复策略大致分为四种方法。定期测试灾难恢复策略至关重要，这样您就有信心在必要时启用该策略。

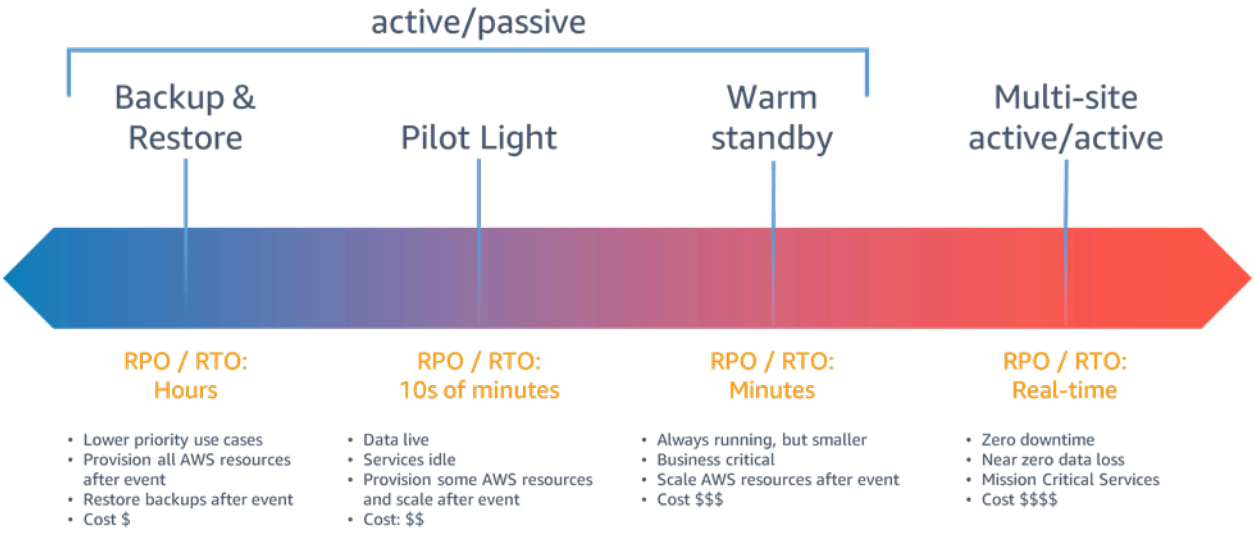

图 6 – 灾难恢复策略

对于架构完善、高度可用的工作负载，如果发生因一个物理数据中心中断或丢失而导致的灾难事件，您可能只需使用备份和还原方法进行灾难恢复。如果您对灾难的定义不仅限于物理数据中心的中断或丢失，还包括区域的中断或丢失，或者您受监管要求的约束，则应考虑 Pilot Light、温备用或多站点主动/主动方法。

备份与还原

备份与还原是缓解数据丢失或损坏后果的合适方法。此方法还可用于通过将数据复制到其他 AWS 区域来缓解区域性灾难，或者减轻部署到单个可用区的工作负载的冗余不足问题。除数据外，您还必须在恢复区域中重新部署基础设施、配置和应用程序代码。为确保快速重新部署基础设施而不出错，应始终使用基础设施即代码（IaC）进行部署，IaC 使用 AWS CloudFormation 或 AWS Cloud Development Kit (AWS CDK) 等服务。如果没有 IaC，在恢复区域中还原工作负载可能会很复杂，这将导致恢复时间延长，甚至可能超出您的 RTO。除了用户数据外，还请务必备份代码和配置，包括用于创建 Amazon EC2 实例的 Amazon Machine Image（AMI）。您可以使用 AWS CodePipeline 自动重新部署应用程序代码和配置。

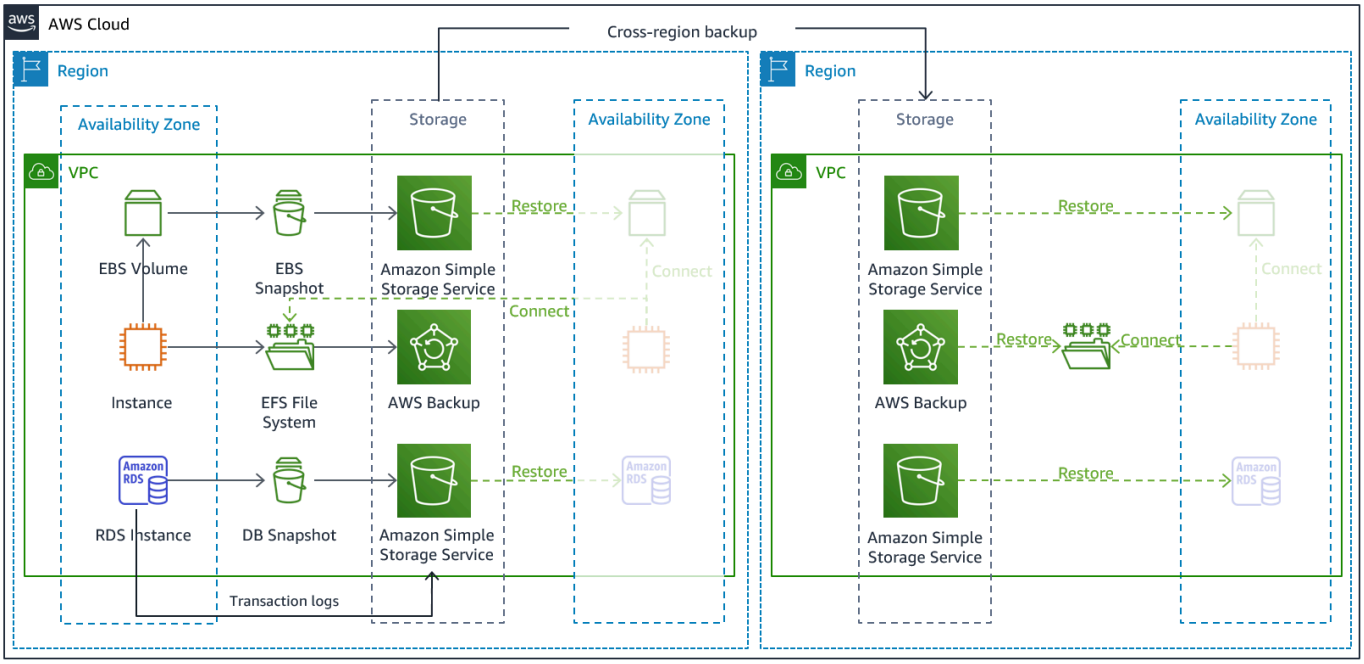

图 7 – 备份与还原架构

AWS 服务

您的工作负载数据需要定期运行或持续运行的备份策略。运行备份的频率将决定可实现的恢复点（应与您的 RPO 保持一致）。备份还应提供一种方法，以还原到制作备份的时间点。可通过以下服务和资源制作具有时间点恢复功能的备份：

- Amazon Elastic Block Store（Amazon EBS）快照
- Amazon DynamoDB 备份
- Amazon RDS 快照
- Amazon Aurora 数据库快照
- Amazon EFS 备份（使用 AWS Backup 时）
- Amazon Redshift 快照
- Amazon Neptune 快照

对于 Amazon Simple Storage Service（Amazon S3），您可以使用 Amazon S3 跨区域复制（CRR）将对象连续异步复制到灾难恢复区域中的 S3 存储桶，同时为存储的对象提供版本控制，以便您可以选择还原点。连续复制数据的优点是备份数据的时间最短（接近零），但可能无法像时间点备份

那样防范灾难事件，例如数据损坏或恶意攻击（如未经授权的数据删除）。面向 Pilot Light 的 AWS 服务一节介绍了连续复制。

AWS Backup 提供了一个集中的位置来配置、安排和监控以下服务和资源的 AWS Backup 功能：

- Amazon Elastic Block Store（Amazon EBS）卷
- Amazon EC2 实例
- Amazon Relational Database Service（Amazon RDS）数据库（包括 Amazon Aurora 数据库）
- Amazon DynamoDB 表
- Amazon Elastic File System（Amazon EFS）文件系统
- AWS Storage Gateway 卷
- Amazon FSx for Windows File Server 和 Amazon FSx for Lustre

AWS Backup 支持跨区域复制备份，例如复制到灾难恢复区域。

作为 Amazon S3 数据的额外灾难恢复策略，请启用 S3 对象版本控制。对象版本控制通过在执行删除或修改操作之前保留原始版本，来保护 S3 中的数据免受这些操作的影响。对象版本控制可以有效缓解人为错误类型的灾难。如果您使用 S3 复制将数据备份到灾难恢复区域，则默认情况下，在源存储桶中删除对象时，Amazon S3 仅在源存储桶中添加删除标记。此方法可保护灾难恢复区域中的数据不受源区域中恶意删除的影响。

除了数据之外，您还必须备份重新部署工作负载和实现恢复时间目标（RTO）所需的配置和基础设施。AWS CloudFormation 提供基础设施即代码（IaC），使您能够定义工作负载中的所有 AWS 资源，以便可靠地部署和重新部署到多个 AWS 账户和 AWS 区域。您可以将工作负载使用的 Amazon EC2 实例备份为 Amazon Machine Image（AMI）。AMI 是根据实例的根卷和附加到实例的任何其他 EBS 卷的快照创建而成。您可以使用此 AMI 启动 EC2 实例的还原版本。可在区域内或跨区域复制 AMI。或者，您可以使用 AWS Backup 跨账户复制备份或将备份复制到其他 AWS 区域。跨账户备份功能有助于防范包括内部威胁或账户泄露在内的灾难事件。AWS Backup 还为 EC2 备份添加了其他功能 – 除了实例的单个 EBS 卷之外，AWS Backup 还存储和跟踪以下元数据：实例类型、已配置的 Virtual Private Cloud（VPC）、安全组、IAM 角色、监控配置和标签。但是，只有在将 EC2 备份还原到同一 AWS 区域时才会使用此附加元数据。

故障转移时必须还原灾难恢复区域中作为备份存储的任何数据。AWS Backup 提供还原功能，但目前未启用计划还原或自动还原。您可以使用 AWS SDK 调用适用于 AWS Backup 的 API，以实施到灾难恢复区域的自动还原。您可以将其设置为定期重复的任务，也可以在每次备份完成时触发还原。下图显示了使用 Amazon Simple Notification Service（Amazon SNS）和 AWS Lambda 进行自动还原的示例。

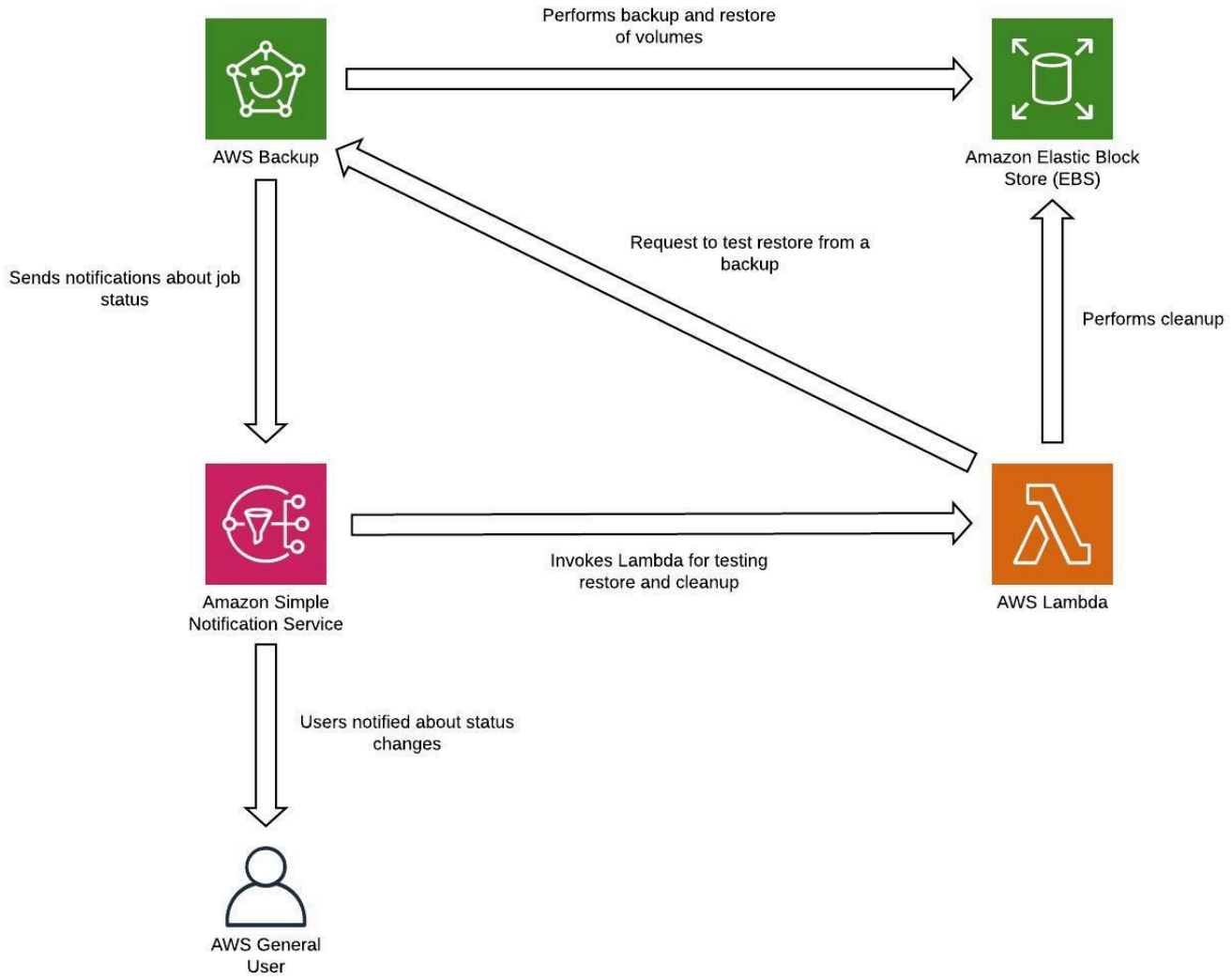

图 8 – 还原和测试备份

> **Note**
>
> 您的备份策略必须包括测试备份。有关详细信息，请参阅测试灾难恢复部分。请参阅 AWS Well-Architected Lab：测试数据的备份与还原，以了解如何实施的实践演示。

Pilot light

利用 Pilot Light 方法，您可以将数据从一个区域复制到另一个区域，并预置核心工作负载基础设施的副本。支持数据复制和备份所需的资源（如数据库和对象存储）始终处于开启状态。其他元素（例如应用程序服务器）加载了应用程序代码和配置，处于关闭状态，仅在测试期间或调用灾难恢复故障转移时使

用。不同于备份与还原方法，您的核心基础设施始终可用，而且您始终可以选择通过打开和横向扩展应用程序服务器来快速预置完整的生产环境。

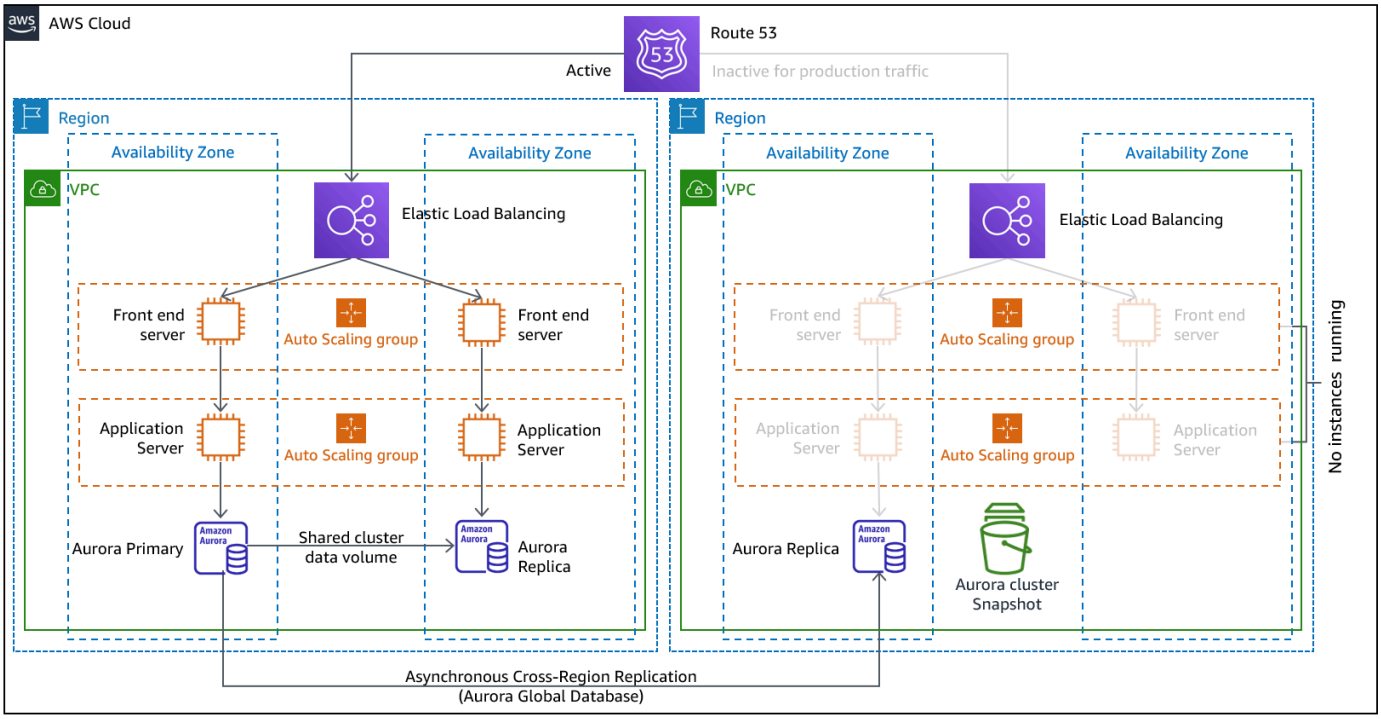

图 9 – Pilot Light 架构

Pilot Light 方法通过尽可能地减少活动资源来尽可能地降低灾难恢复的持续成本，并简化灾难发生时的恢复操作，因为核心基础设施要求均已就位。此恢复选项要求您更改部署方法。您需要对每个区域的核心基础设施进行更改，并将工作负载（配置、代码）更改同时部署到每个区域。通过自动部署以及使用基础设施即代码（IaC）跨多个账户和区域部署基础设施（在主区域完整部署基础设施，在灾难恢复区域缩减/关闭基础设施部署），可以简化此步骤。建议您在每个区域使用不同的账户，以提供最高级别的资源和安全隔离（在针对凭证被盗也制定了灾难恢复计划的情况下）。

使用这种方法，您还必须缓解数据灾难。连续数据复制可以保护您免受某些类型灾难的影响，但它可能无法防范数据损坏或销毁，除非您的策略还包括存储数据的版本控制或时间点恢复选项。您可以在灾难区域中备份复制的数据，以便在同一区域中创建时间点备份。

AWS 服务

除了使用备份与还原部分介绍的 AWS 服务创建时间点备份之外，制定 Pilot Light 策略时还要考虑以下服务。

对于 Pilot Light，将数据连续复制到灾难恢复区域中的实时数据库和数据存储是实现低 RPO 的最佳方法（与前面讨论的时间点备份一起使用时）。AWS 使用以下服务和资源为数据提供连续、跨区域的异步数据复制：

- Amazon Simple Storage Service（Amazon S3）复制
- Amazon RDS 只读副本
- Amazon Aurora Global Database
- Amazon DynamoDB 全局表

通过连续复制，您的数据版本几乎可以立即在灾难恢复区域中使用。可以使用服务功能（例如针对 S3 对象的 S3 复制时间控制（S3 RTC））和 Amazon Aurora Global Database 的管理功能监控实际复制时间。

当调用故障转移以从灾难恢复区域运行读/写负载时，必须将 RDS 只读副本提升为主实例。对于 Aurora 以外的数据库实例，该过程需要几分钟才能完成，并且需要重启。对于跨区域复制（CRR）和通过 RDS 实现故障转移，使用 Amazon Aurora Global Database 具有多项优势。Global Database 使用专用基础设施，使您的数据库完全可用于为应用程序提供服务，并且可以复制到一个辅助区域，延迟通常不到一秒（AWS 区域内的延迟远少于 100 毫秒）。借助 Amazon Aurora Global Database，如果您的主区域性能下降或中断，即使在区域完全中断的情况下，您也可以在不到 1 分钟的时间内提升其中一个辅助区域以承担读/写责任。提升可以自动进行，并且不会重启。

必须在灾难恢复区域中部署核心工作负载基础设施的缩减版本（资源较少或较小）。使用 AWS CloudFormation，您可以定义基础设施，并在 AWS 账户和 AWS 区域之间一致地进行部署。AWS CloudFormation 使用预定义的虚拟参数来标识 AWS 账户及其部署所在的 AWS 区域。因此，您可以在 CloudFormation 模板中实施条件逻辑，以便在灾难恢复区域中仅部署缩减版本的基础设施。对于 EC2 实例部署，Amazon Machine Image（AMI）提供硬件配置和已安装软件等信息。您可以实施 Image Builder 管道来创建所需的 AMI，然后将其复制到主区域和备份区域。这有助于确保在发生灾难事件时，这些黄金 AMI 拥有在新区域重新部署或横向扩展工作负载所需的一切。Amazon EC2 实例以缩减配置（实例少于主区域中的实例）进行部署。您可以使用休眠将 EC2 实例置于停止状态，在这种状态下，您无需支付 EC2 费用，只需为使用的存储空间付费。要启动 EC2 实例，您可以使用 AWS 命令行界面（CLI）或 AWS SDK 创建脚本。要横向扩展基础设施以支持生产流量，请参阅温备用部分中的 AWS Auto Scaling。

对于活动/备用配置（如 Pilot Light），所有流量最初都会流向主区域，如果主区域不再可用，则会切换到灾难恢复区域。使用 AWS 服务可以考虑两种流量管理选项。第一种选项是使用 Amazon Route 53。使用 Amazon Route 53，您可以将一个或多个 AWS 区域中的多个 IP 终端节点与一个 Route 53 域名相关联。然后，您可以将流量路由到该域名下的相应终端节点。Amazon Route 53 运行状况检

查可监控这些终端节点。使用这些运行状况检查，您可以配置 DNS 故障转移以确保将流量发送到正常运行的终端节点。

第二种选项是使用 AWS Global Accelerator。使用 AnyCast IP，您可以将一个或多个 AWS 区域中的多个终端节点与相同的静态 IP 地址相关联。然后 AWS Global Accelerator 将流量路由到与该地址关联的相应终端节点。Global Accelerator 运行状况检查可监控终端节点。使用这些运行状况检查，AWS Global Accelerator 可以自动检查应用程序的运行状况，并将用户流量仅路由到正常运行的应用程序终端节点。Global Accelerator 利用广泛的 AWS 边缘网络尽快将流量传送到 AWS 网络主干，因此应用程序终端节点的延迟较低。Global Accelerator 还可以避免 DNS 系统（如 Route 53）可能出现的缓存问题。

CloudEndure Disaster Recovery

CloudEndure Disaster Recovery（可从 AWS Marketplace 获得）使用底层服务器的块级复制功能，将服务器托管的应用程序和服务器托管的数据库从任何来源连续复制到 AWS 中。利用 CloudEndure Disaster Recovery，您可以将 AWS 云用作本地工作负载及其环境的灾难恢复区域。它还可用于 AWS 托管的工作负载的灾难恢复，前提是这些工作负载仅包含托管在 EC2 上的应用程序和数据库（即不是 RDS）。CloudEndure Disaster Recovery 使用 Pilot Light 策略，在用作暂存区的 Amazon Virtual Private Cloud（Amazon VPC）中维护数据和已关闭资源的副本。触发故障转移事件时，暂存资源将用于在目标 Amazon VPC（用作恢复位置）中自动创建全产能部署。

图 10 – CloudEndure Disaster Recovery 架构

温备用

温备用方法包括确保在另一个区域中有一个缩减但功能齐全的生产环境副本。这种方法扩展了 Pilot Light 的概念，缩短了恢复时间，因为您的工作负载在另一个区域中始终可用。此方法还使您能够更轻松地执行测试或实施连续测试，从而增强从灾难中恢复的信心。

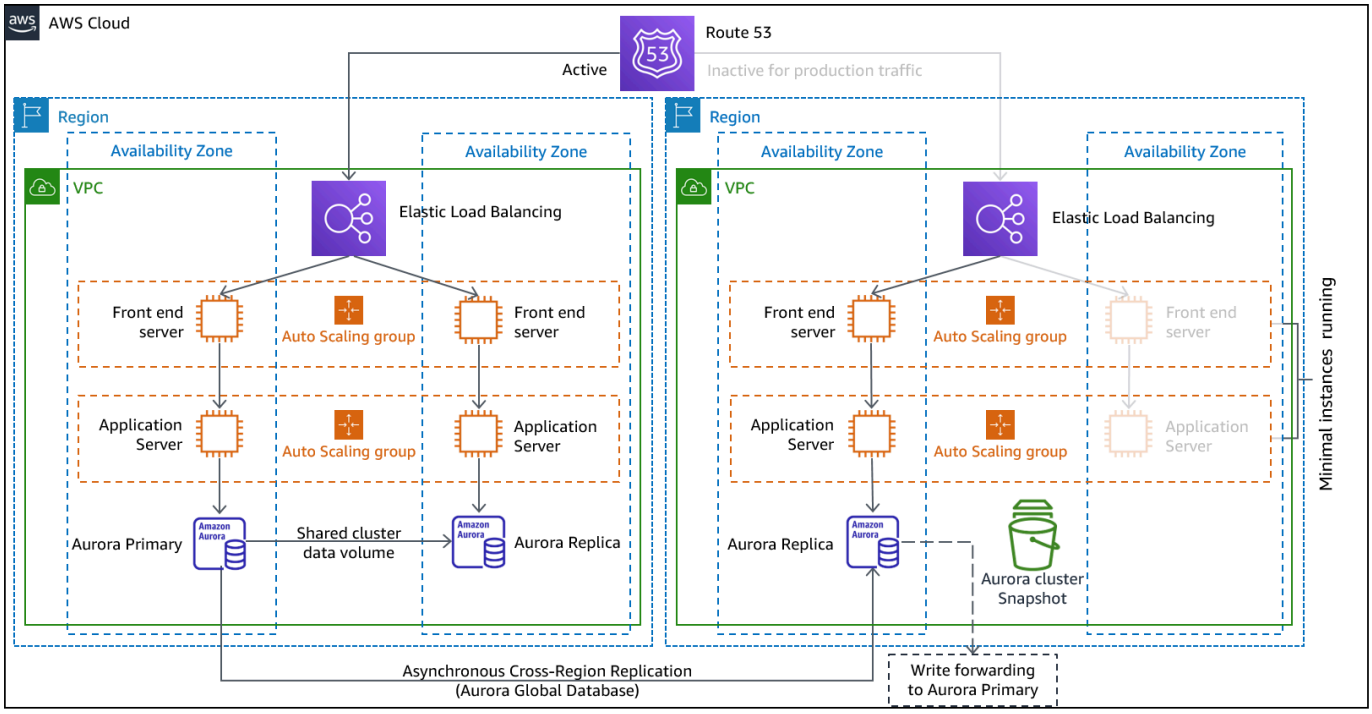

图 11 – 温备用架构

注意：Pilot Light 和温备用之间的差异有时难以区分。两者都包含灾难恢复区域中的环境，该环境包含主区域资产的副本。区别在于，如果不首先执行其他操作，Pilot Light 就无法处理请求，而温备用可以立即处理流量（在产能降低的情况下）。Pilot Light 方法要求您“打开”服务器，可能还需要部署其他（非核心）基础设施并纵向扩展；而温备用只需纵向扩展（一切均已部署并正在运行）。请结合您的 RTO 和 RPO 需求，帮助您在这些方法之间进行选择。

AWS 服务

备份与还原和 Pilot Light 涵盖的所有 AWS 服务也用于温备用，进行数据备份、数据复制、活动/备用流量路由，以及部署包括 EC2 实例在内的基础设施。

AWS Auto Scaling 用于扩展资源，包括 AWS 区域内的 Amazon EC2 实例、Amazon ECS 任务、Amazon DynamoDB 吞吐量和 Amazon Aurora 副本。Amazon EC2 Auto Scaling 可跨一个 AWS 区域内的多个可用区扩展 EC2 实例的部署，从而在该区域内提供弹性。使用 Auto Scaling 将灾难恢复区域横向扩展到全产能状态，这是 Pilot Light 或温备用策略的一部分。例如，对于 EC2，请增加 Auto Scaling 组上的 Desired Capacity（所需产能）设置。您可以通过 AWS Management Console 手动调整此设置，可以通过 AWS SDK 自动调整此设置，也可以使用新的所需产能值重新部署 AWS CloudFormation 模板。您可以使用 AWS CloudFormation 参数更轻松地重新部署 CloudFormation 模板。确保灾难恢复区域中的 Service Quotas（服务配额）设置得足够高，以免限制您纵向扩展产能。

多站点主动/主动

作为多站点主动/主动或热备用主动/被动策略的一部分，您可以在多个区域同时运行工作负载。多站点主动/主动服务于它所部署的所有区域的流量，而热备用只服务于单个区域的流量，其他区域仅用于灾难恢复。通过多站点主动/主动方法，用户可以在部署该方法的任何区域中访问工作负载。这种方法是最复杂且成本最高的灾难恢复方法，但通过正确的技术选择和实施，它可以将大多数灾难的恢复时间缩短至接近零（然而，数据损坏可能需要依赖备份，这通常会导致恢复点不为零）。热备用采用主动/被动配置，用户只定向到单个区域，并且灾难恢复区域不占用流量。大多数客户发现，如果他们要在辅助区域中建立一个完整的环境，那么采用主动/主动配置行得通。或者，如果您不想同时使用这两个区域来处理用户流量，那么可以采用温备用，这是一种更经济、操作上不那么复杂的方法。

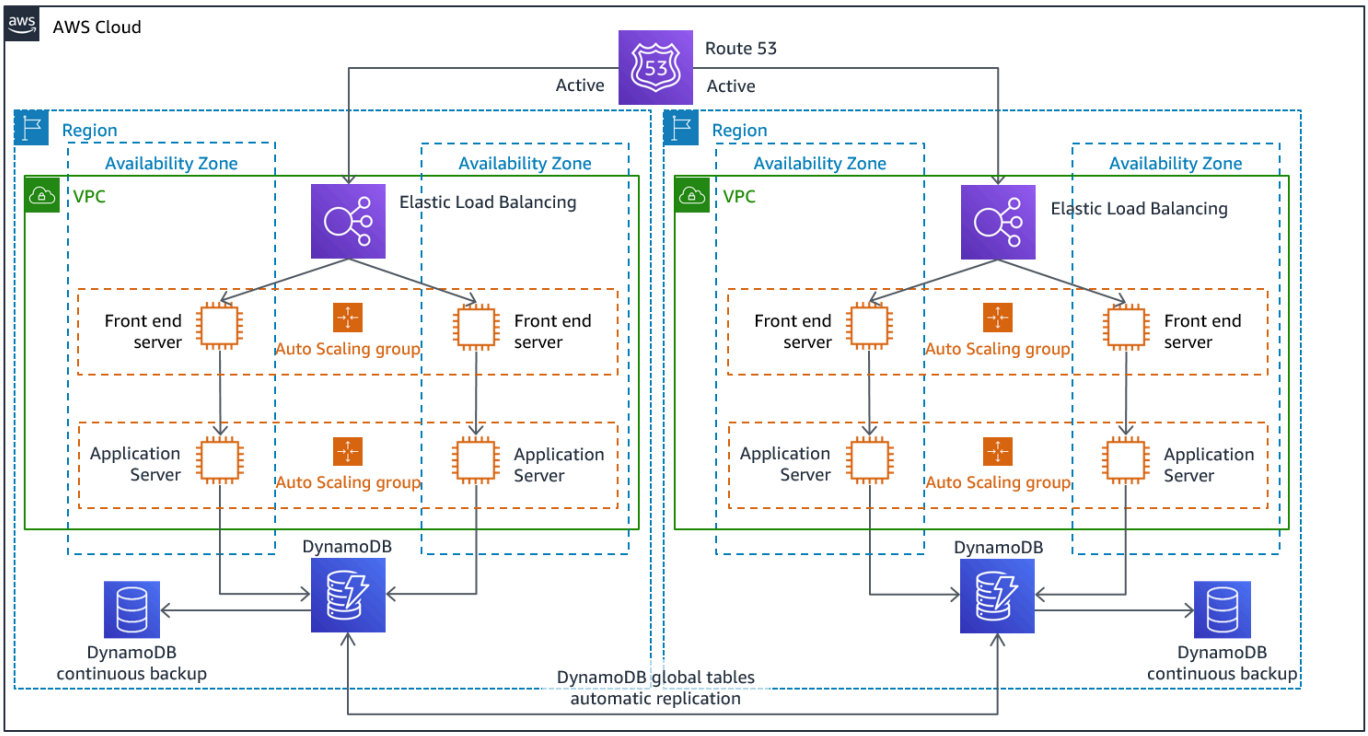

图 12 – 多站点主动/主动架构（将一条“活动”路径更改为“非活动”以实现热备用）

使用多站点主动/主动时，由于工作负载在一个以上的区域中运行，这种情况下不存在故障转移的问题。在这种情况下，灾难恢复测试将侧重于工作负载对区域损失的反应：流量是否从发生故障的区域移出？ 其他区域能否处理所有流量？ 还需要测试数据灾难。仍然需要备份和恢复，并应定期测试。还应注意的是，涉及数据损坏、删除或模糊处理的数据灾难的恢复时间将始终大于零，并且恢复点将始终位于发现灾难之前的某个时间点。如果需要增加多站点主动/主动（或热备用）方法的复杂性和成本，以保持接近零的恢复时间，则应做出更多努力来维护安全并防止人为错误，以减轻人为灾难。

AWS 服务

备份与还原、Pilot Light 和温备用涵盖的所有 AWS 服务也在此处用于时间点数据备份、数据复制、主动/主动流量路由以及基础设施（包括 EC2 实例）的部署和扩展。

对于前面讨论的主动/被动场景（Pilot Light 和温备用），Amazon Route 53 和 AWS Global Accelerator 均可用于将网络流量路由到活动区域。对于此处的主动/主动策略，这两项服务还允许定义确定哪些用户转到哪个活动区域终端节点的策略。借助 AWS Global Accelerator，您可以设置流量拨盘，以控制定向到每个应用程序终端节点的流量百分比。Amazon Route 53 支持这种百分比方法，还支持多种其他可用策略，包括地理位置临近度策略和基于延迟的策略。Global Accelerator 会自动利用广泛的 AWS 边缘服务器网络，尽快将流量引导至 AWS 网络主干，从而降低请求延迟。

使用此策略进行数据复制可实现接近零的 RPO。AWS 服务（例如 Amazon Aurora Global Database）使用专用基础设施，使您的数据库完全可用于为应用程序提供服务，并且可以复制到一个辅助区域，延迟时间通常不到一秒。对于主动/被动策略，只对主区域执行写入操作。主动/主动的区别在于设计如何处理对每个活动区域的写入。通常将用户读取设计为从离他们最近的区域提供服务，称为本地读取。对于写入，有以下几种选项：

- 全局写入策略会将所有写入操作路由到单个区域。如果该区域出现故障，将提升另一个区域以接受写入。Aurora Global Database 非常适合全局写入，因为它支持跨区域同步只读副本，而且您可以在不到 1 分钟的时间内提升其中一个辅助区域以承担读/写责任。
- 局部写入策略会将写入路由到最近的区域（就像读取操作一样）。Amazon DynamoDB 全局表支持这样的策略，允许从部署全局表的每个区域进行读取和写入。Amazon DynamoDB 全局表在并发更新之间使用以最后写入者为准原则。
- 分区写入策略根据分区键（如用户 ID）将写入操作分配到特定区域，以避免写入冲突。双向配置的 Amazon S3 复制可用于这种情况，目前支持在两个区域之间进行复制。实施此方法时，请确保在存储桶 A 和 B 上均启用副本修改同步，以复制副本元数据更改，例如对象访问控制列表（ACL）、对象标签或已复制对象上的对象锁定。您还可以配置是否在活动区域中的存储桶之间复制删除标记。除了复制之外，您的策略还必须包括时间点备份，以防止发生数据损坏或数据销毁事件。

AWS CloudFormation 是一款功能强大的工具，可在多个 AWS 区域的 AWS 账户之间强制实施一致部署的基础设施。AWS CloudFormation StackSets 扩展了此功能，您只需一次操作即可跨多个账户和区域创建、更新或删除 CloudFormation 堆栈。尽管 AWS CloudFormation 使用 YAML 或 JSON 定义基础设施即代码，但 AWS Cloud Development Kit (AWS CDK)允许您使用熟悉的编程语言定义基础设施即代码。您的代码将转换为 CloudFormation，然后用于在 AWS 中部署资源。

检测

当您的工作负载并未提供它们应提供的业务成果时，务必要尽快得知这一情况。这样一来，您就可以迅速宣布发生灾难并从事件中恢复。对于激进的恢复目标，该响应时间加上适当的信息对于实现恢复目标至关重要。如果恢复点目标为一小时，您需要检测事件，通知相关人员，执行上报流程，评估有关预期恢复时间（不执行灾难恢复计划的情况下）的信息（如有），声明发生灾难并在一小时内恢复。

> **Note**
>
> 如果利益攸关方决定即使 RTO 存在风险也不调用灾难恢复，则重新评估灾难恢复计划和目标。决定不调用灾难恢复计划可能是因为计划不够充分，或者对计划的执行缺乏信心。

在规划和目标中考虑事件检测、通知、上报、发现和声明，以提供切合实际、可实现的目标，从而提供商业价值，这一点至关重要。

AWS 会在 Service Health Dashboard 上发布最新的服务可用性信息。请随时查看以获取当前状态信息，或订阅 RSS 源以在每项服务中断时收到通知。如果您在使用我们的某项服务时遇到了实时运营问题，而该问题未显示在 Service Health Dashboard 上，您可以创建支持请求。

AWS Health Dashboard 会提供影响您账户的 AWS Health 事件的相关信息。信息会以两种方式显示：显示按类别组织的最近和未来事件的控制面板，以及显示过去 90 天内所有事件的完整事件日志。

对于最严格的 RTO 要求，您可以根据运行状况检查实施自动故障转移。 因此，建议设计代表用户体验并基于关键绩效指标的运行状况检查。深度运行状况检查可以检查工作负载的关键功能，而不仅仅是浅层的检测信号检查。建议使用基于多个信号的深度运行状况检查。使用此方法时要小心，以免触发误报，因为在不需要时进行故障转移本身会带来可用性风险。

测试灾难恢复

应测试灾难恢复实施以验证实施效果，并定期测试到工作负载灾难恢复区域的故障转移以确保满足 RTO 和 RPO。

要避免的模式是开发很少执行的恢复路径。例如，您可能有一个用于只读查询的辅助数据存储。当您写入某个数据存储，却发现主存储故障时，您可能希望将故障转移到辅助数据存储。如果您不经常测试此故障转移，可能会发现您关于辅助数据存储容量的假设是错误的。辅助数据存储容量在您上次测试时可能是足够的，但可能无法再容纳这次情况下的负载，或者辅助区域中的服务配额可能不够。

我们的经验表明，唯一有效的错误恢复是您经常测试的路径。因此，最好只开发几条恢复路径。

您可以建立恢复模式并定期对其进行测试。如果某条恢复路径比较复杂或至关重要，您仍需定期在生产环境中模拟相应故障，以验证该恢复路径有效。

管理灾难恢复区域的配置漂移。确保灾难恢复区域的基础设施、数据和配置满足需求。例如，检查 AMI 和服务配额是否为最新。

您可以利用 AWS Config 持续监控和记录 AWS 资源配置。AWS Config 可以检测漂移并触发 AWS Systems Manager Automation 来修复漂移并发出警报。AWS CloudFormation 还可以检测您已部署的堆栈中的漂移。

总结

客户应对其应用程序在云中的可用性负责。需要定义什么是灾难，并制定一项能够反映这一定义及其对业务成果可能产生的影响的灾难恢复计划，这非常重要。应根据影响分析和风险评估来创建恢复时间目标（RTO）和恢复点目标（RPO），然后选择适当的架构来减轻灾难。确保能够及时检测灾难 – 当存在无法实现目标的风险时，您需要了解这一情况，这至关重要。确保制定一项计划，并通过测试来验证该计划。如果灾难恢复计划未经验证，则可能因为缺乏信心而未实施计划，或不能实现灾难恢复目标。

贡献者

本文档的贡献者包括：

- Alex Livingstone，AWS Enterprise Support 云运维实务主管
- Seth Eliot，Amazon Web Services 首席可靠性解决方案构架师

延伸阅读

如需更多信息，请参阅：

- 可靠性支柱，AWS Well-Architected Framework
- 灾难恢复计划核对清单
- 实施运行状况检查
- AWS 解决方案实施：Multi-Region Application Architecture
- AWS re:Invent 2018：适用于多区域双活应用程序的架构模式 (ARC209-R2)

文档历史记录

变更	描述	日期
初次发布	首次发布。	2021 年 2 月 12 日

要获得有关此白皮书的更新通知，请订阅 RSS 源。

声明

客户有责任对本文档中的信息进行单独评估。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。