AWS Well-Architected 框架

# 工作负载的灾难恢复 AWS：云端恢复

# 工作负载的灾难恢复 AWS：云端恢复: AWS Well-Architected 框架

# Table of Contents

摘要 ..... 1
简介 ..... 2
灾难恢复和可用性 ..... 2
您使用 Well-Architected 了吗？ ..... 4
韧性的责任共担模式 ..... 5
AWS 责任 “云的弹性” ..... 5
客户责任 “云端弹性” ..... 5
什么是灾难？ ..... 7
高可用性不是灾难恢复 ..... 8
业务连续性计划 (BCP) ..... 9
业务影响分析和风险评估 ..... 9
恢复目标（RTO 和 RPO） ..... 9
云中的灾难恢复不相同 ..... 13
单个 AWS 区域 ..... 13
多个 AWS 区域 ..... 14
云中的灾难恢复选项 ..... 15
备份和还原 ..... 15
Amazon Web Services ..... 16
指示灯 ..... 19
Amazon Web Services ..... 20
AWS 弹性灾难恢复 ..... 22
温备用 ..... 22
Amazon Web Services ..... 23
多站点主动/主动 ..... 24
Amazon Web Services ..... 25
检测 ..... 27
测试灾难恢复 ..... 28
结论 ..... 29
贡献者 ..... 30
延伸阅读 ..... 31
文档历史记录 ..... 32
版权声明 ..... 33
AWS 词汇表 ..... 34
..... xxxv

# 工作负载的灾难恢复 AWS：云端恢复

发布日期：2021 年 2 月 12 日 (文档历史记录)

灾难恢复是为灾难做好准备和从灾难中恢复的过程。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被视为灾难。这篇论文概述了为部署到的任何工作负载规划和测试灾难恢复的最佳实践 AWS，并提供了不同的方法来降低风险并满足该工作负载的恢复时间目标 (RTO) 和恢复点目标 (RPO)。

本白皮书介绍了如何对上的 AWS工作负载实施灾难恢复。有关 AWS 用作本地工作负载灾难恢复站点的信息，请参阅本地应用程序的灾难恢复。 AWS

# 简介

您的工作负载必须正确、一致地执行其预期功能。要实现这一目标，您必须为弹性进行架构设计。弹性是指工作负载能够从基础架构、服务或应用程序中断中恢复，动态获取计算资源以满足需求，并缓解中断（例如配置错误或临时网络问题）的能力。

灾难恢复 (DR) 是您的弹性策略的重要组成部分，它涉及灾难来袭时您的工作负载如何响应（灾难是对您的业务造成严重负面影响的事件）。这种响应必须基于贵组织的业务目标，这些目标指定了工作负载的策略，以避免数据丢失，即恢复点目标 (RPO)，并在工作负载无法使用时缩短停机时间，即恢复时间目标 (RTO)。因此，您必须在云端工作负载的设计中实现弹性，以满足给定的一次性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，这种方法可以帮助您的组织保持业务连续性。

本 paper 重点介绍如何规划、设计和实施 AWS 能够满足企业灾难恢复目标的架构。此处共享的信息适用于担任技术职务的人，例如首席技术官 (CTOs)、架构师、开发人员、运营团队成员以及负责评估和缓解风险的人。

## 灾难恢复和可用性

可以将灾难恢复与可用性进行比较，后者是您的弹性策略的另一个重要组成部分。灾难恢复衡量一次性事件的目标，而可用性目标则衡量一段时间内的平均值。

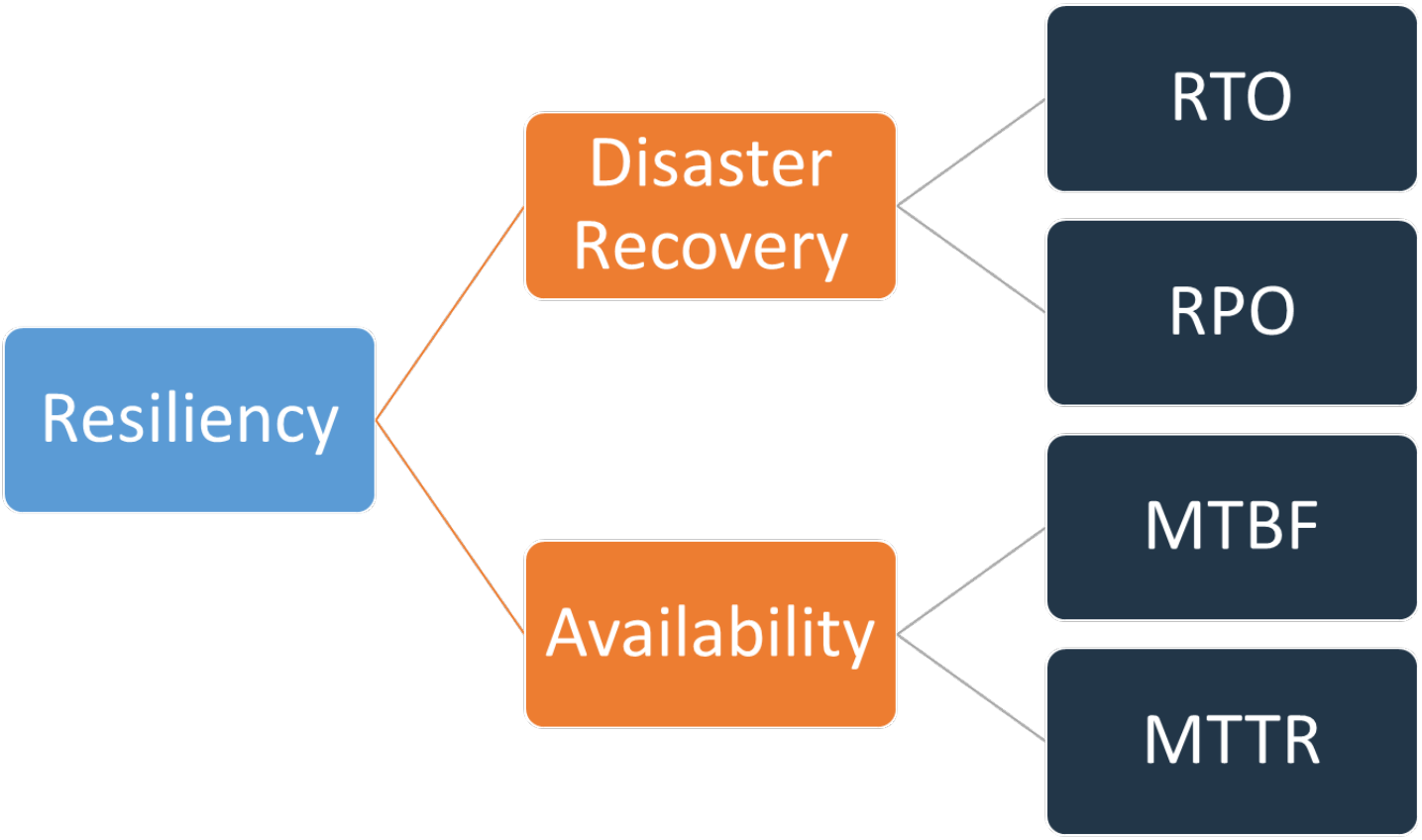


图 1-弹性目标

可用性是使用平均故障间隔时间 (MTBF) 和平均恢复时间 (MTTR) 计算得出的：

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

这种方法通常被称为 “九”，其中 99.9% 的可用性目标被称为 “三九”。

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

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

灾难恢复侧重于灾难事件，而可用性则侧重于更常见的小规模中断，例如组件故障、网络问题、软件错误和负载峰值。灾难恢复的目标是业务连续性，而可用性则涉及最大限度地延长工作负载可用来执行其预期业务功能的时间。两者都应该成为您的弹性战略的一部分。

# 您使用 Well-Architected 了吗？

AWS Well-Architected Fram ework 可帮助您了解在云中构建系统时所做决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。使用 AWS 管理控制台中免费提供的 AWS Well-Architected 工具，您可以通过回答每个支柱的一组问题，根据这些最佳实践来审查您的工作负载。

本白皮书中涵盖的概念扩展了可靠性支柱白皮书中包含的最佳实践，特别是问题 REL 13 “您如何规划灾难恢复 (DR)？”。实施本白皮书中的实践后，请务必使用 AWS Well-Architected Tool 审查（或重新审核）您的工作负载。

# 韧性的责任共担模式

弹性是 AWS 与您（客户）共同承担的责任。了解作为弹性一部分的灾难恢复和可用性在这一共享模式下是如何运作的，这一点很重要。

## AWS 责任 “云的弹性”

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。该基础设施包括运行 AWS 云服务的硬件、软件、网络和设施。AWS 采取商业上合理的努力来提供这些 AWS 云服务，确保服务可用性达到或超过 AWS 服务等级协议 (SLAs)。

A WS 全球云基础设施旨在让客户能够构建高度弹性的工作负载架构。每个 AWS 区域都是完全隔离的，由多个可用区组成，这些可用区是物理隔离的基础设施分区。可用区会隔离可能影响工作负载韧性的故障，防止这些故障影响区域内的其他可用区。但同时，AWS 区域中的所有区域都通过完全冗余的专用城域光纤通过高带宽、低延迟的网络互连，在区域之间提供高吞吐量、低延迟的联网。可用区之间的所有流量都经过加密。网络性能足以完成可用区之间的同步复制。将应用程序划分为多个部门时 AZs，可以更好地隔离并保护公司免受停电、雷击、龙卷风、飓风等问题的侵害。

## 客户责任 “云端弹性”

您的责任将由您选择的 AWS 云服务决定。这决定了您承担韧性责任时必须执行的配置工作量。例如，诸如亚马逊弹性计算云 (Amazon EC2) 之类的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 实例的客户负责在多个位置（例如 AWS 可用区）部署 EC2 实例，使用 Amazon A EC2 uto Scaling 等服务实现自我修复，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。对于托管服务，例如 Amazon S3 和 Amazon DynamoDB，AWS 负责基础设施层、操作系统和平台，客户可以访问终端节点来存储和检索数据。您负责管理数据的韧性，包括备份、版本控制和复制策略。

跨一个 AWS 区域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到一个可用区来保护工作负载，并利用其他可用区的冗余来继续处理请求。多可用区架构也是灾难恢复策略的一部分，旨在更好地隔离工作负载，防止受到停电、雷击、龙卷风、地震等事故和灾害的影响。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，如果主动区域无法再处理请求，则工作负载的服务将从其主动区域故障转移到其灾难恢复区域。

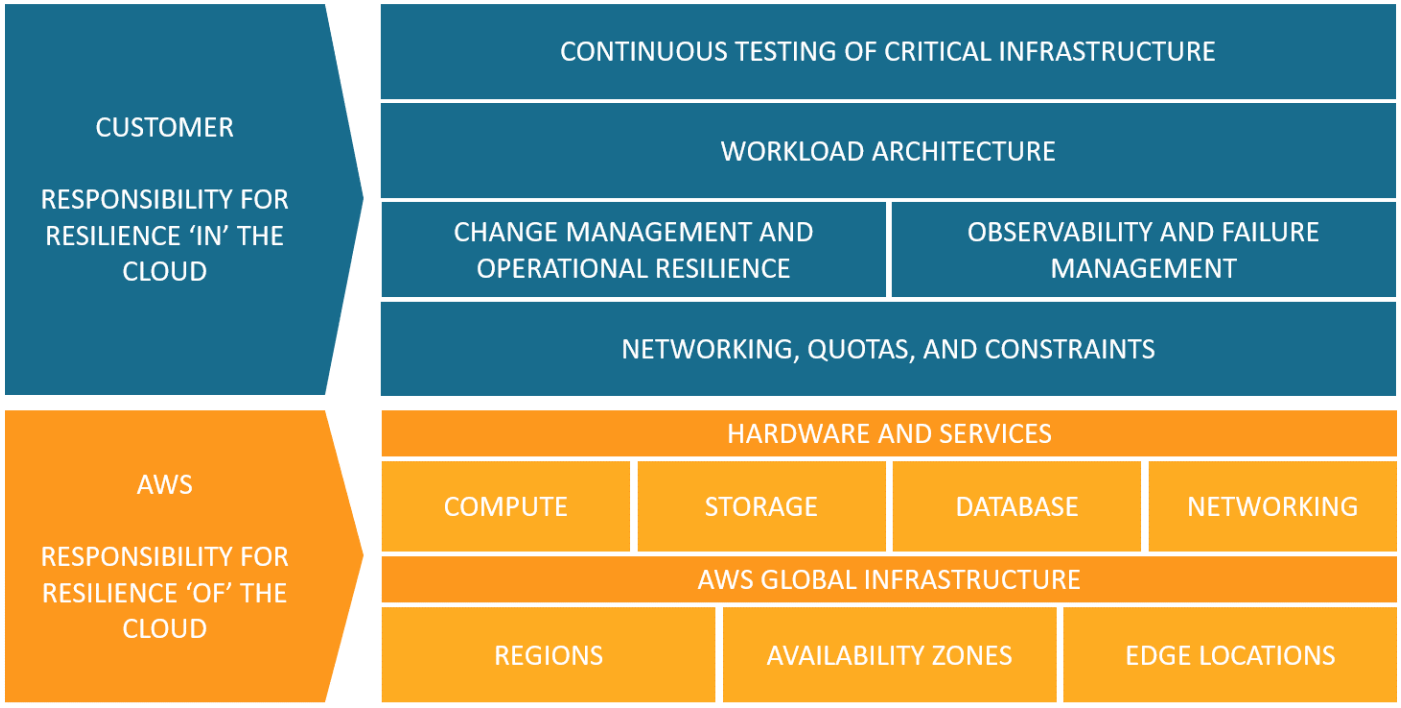


图 2-弹性是 AWS 和客户共同承担的责任

# 什么是灾难？

在规划灾难恢复时，请评估您针对以下三种主要灾难类别的计划：

- 自然灾害，例如地震或洪水
- 技术故障，例如停电或网络连接
- 人为行为，例如无意中配置错误或 unauthorized/outside 派对访问或修改

这些潜在灾害中的每一个都将产生地域影响，影响可能是地方、区域、全国、大陆或全球。在考虑灾难恢复策略时，灾难的性质和地理影响都很重要。例如，您可以通过采用多可用区策略来缓解导致数据中心中断的局部洪水问题，因为它不会影响多个可用区。但是，对生产数据的攻击需要您调用灾难恢复策略，该策略会故障转移到另一个 AWS 区域中备份数据。

# 高可用性不是灾难恢复

可用性和灾难恢复都依赖于一些相同的最佳实践，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离散副本。灾难恢复的目标与可用性不同，即衡量符合灾难条件的大规模事件发生后的恢复时间。您应该首先确保您的工作负载符合可用性目标，因为高可用性架构将使您能够在可用性受到影响的事件发生时满足客户的需求。您的灾难恢复策略需要的方法与可用性方法不同，重点是将离散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切换。

在灾难恢复计划中，您必须考虑工作负载的可用性，因为它会影响您采取的方法。在一个可用区的单个 Amazon EC2 实例上运行的工作负载没有高可用性。如果本地洪水问题影响了该可用区，则这种情况需要故障转移到另一个可用区以实现灾难恢复目标。将此场景与部署多站点主动/主动的高可用性工作负载进行比较，在这种工作负载中，工作负载部署在多个活动区域，所有区域都为生产流量提供服务。在这种情况下，即使万一发生大规模灾难使某个区域无法使用，灾难恢复策略也是通过将所有流量路由到其余区域来实现的。

可用性和灾难恢复之间的数据处理方式也有所不同。考虑一种能够持续复制到另一个站点以实现高可用性的存储解决方案（例如多站点、 active/active 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，则这些破坏性更改可以复制到辅助存储设备。在这种情况下，尽管可用性很高，但在数据删除或损坏时进行故障转移的能力仍将受到影响。相反，作为灾难恢复策略的一部分，还需要进行point-in-time备份。

# 业务连续性计划 (BCP)

您的灾难恢复计划应该是组织业务连续性计划 (BCP) 的子集，而不应该是独立的文档。如果由于灾难对工作负载以外的业务要素造成影响而无法实现该工作负载的业务目标，则为恢复工作负载而保持激进的灾难恢复目标就没有意义了。例如，地震可能会使您无法运输在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使您的工作负载正常运行，您的业务运营中心也需要满足运输需求。您的灾难恢复策略应基于业务需求、优先级和背景。

## 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。它应该确定无法使用您的工作负载对内部和外部客户的影响以及对您的业务的影响。分析应有助于确定需要以多快的速度提供工作负载以及可以容忍多少数据丢失。但是，必须注意的是，不应孤立地制定恢复目标；中断的可能性和恢复成本是有助于了解为工作负载提供灾难恢复的业务价值的关键因素。

业务影响可能取决于时间。您可能需要考虑在灾难恢复计划中考虑这一点。例如，在每个人都获得报酬之前，薪资系统的中断可能会对业务产生非常大的影响，但是在每个人都已经获得报酬之后，其影响可能很小。

对灾难类型和地理影响的风险评估以及工作负载的技术实施概述，将确定每种类型的灾难发生中断的可能性。

对于高度关键的工作负载，您可以考虑在多个区域部署基础架构，同时进行数据复制和持续备份，以最大限度地减少对业务的影响。对于不太重要的工作负载，有效的策略可能是根本不进行任何灾难恢复。而且，对于某些灾难情景，不制定任何灾难恢复策略作为基于灾难发生概率较低的明智决策也是有效的。请记住，AWS 区域内的可用区已经在设计时设置了它们之间有意义的距离，并仔细规划了位置，因此最常见的灾难只能影响一个区域，而不会影响其他区域。因此，AWS 区域内的多可用区架构可能已经可以满足您的大部分风险缓解需求。

应评估灾难恢复选项的成本，以确保考虑到业务影响和风险，灾难恢复战略能够提供正确的业务价值水平。

利用所有这些信息，您可以记录不同灾难情景的威胁、风险、影响和成本以及相关的恢复选项。应使用此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，组织通常会规划恢复时间目标 (RTO) 和恢复点目标 (RPO)。

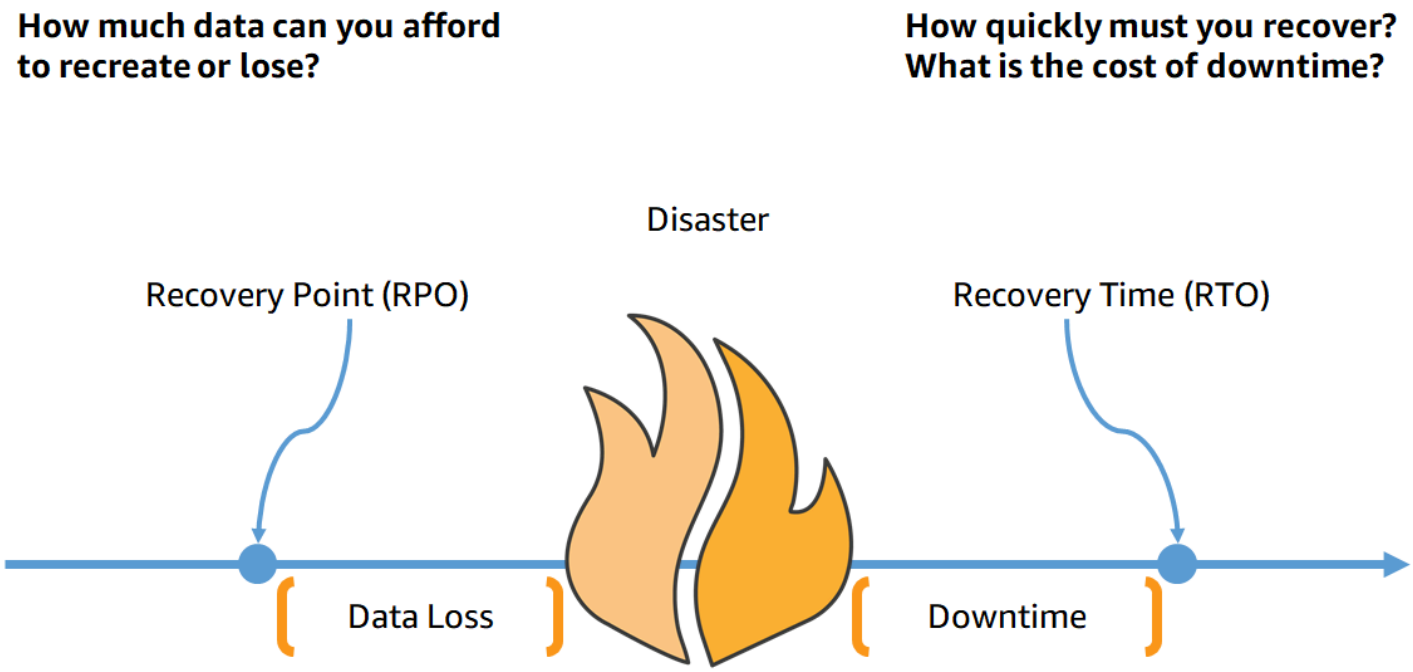


图 3-恢复目标

恢复时间目标 (RTO) 是服务中断和恢复服务之间可接受的最大延迟。该目标决定了当服务不可用时，什么时间段被视为可接受的时间窗口，并由组织定义。

本 paper 中主要讨论了四种灾难恢复策略：备份和恢复、指示灯、热待机和多站点 active/active（参见云中的灾难恢复选项）。在下图中，企业已经确定了允许的最大RTO以及他们在服务恢复策略上可以花费的限额。考虑到企业的目标，灾难恢复策略 Pilot Light 或 Warm Standby 将同时满足 RTO 和成本标准。

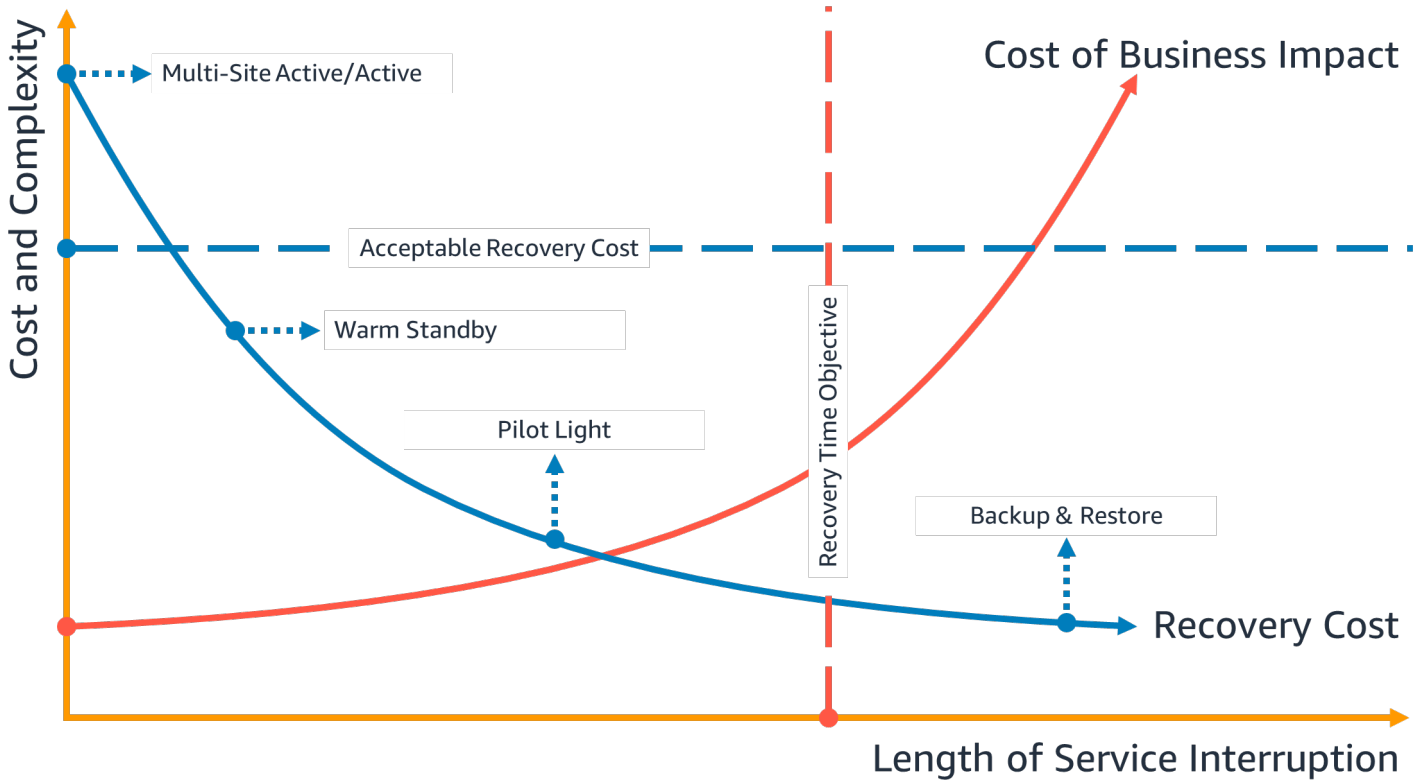


图 4-恢复时间目标

恢复点目标 (RPO) 是自上次数据恢复点以来的最大可接受时间。该目标确定了在最后一个恢复点和服务中断之间可接受的数据丢失情况，并由组织定义。

在下图中，企业已经确定了允许的最大 RPO 以及他们可以在数据恢复策略上花费的限额。在这四种灾难恢复策略中，指示灯或热待机灾难恢复策略都符合 RPO 和成本两个标准。

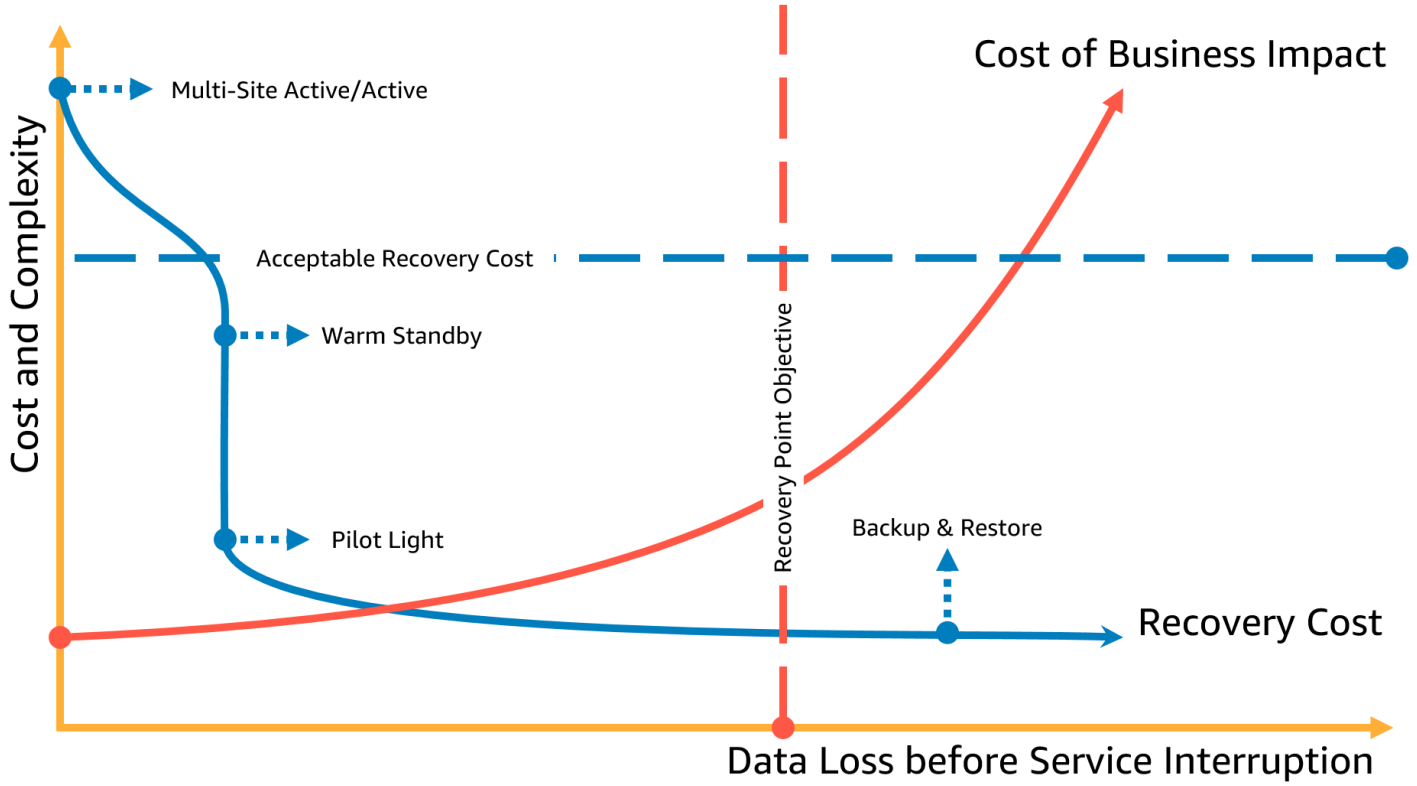


图 5-恢复点目标

> **Note**
>
> 如果恢复策略的成本高于失败或损失的成本，则除非有次要驱动因素，例如监管要求，否则不应制定恢复方案。进行此评估时，请考虑成本各异的恢复策略。

# 云中的灾难恢复不相同

灾难恢复策略随着技术创新而演变。本地灾难恢复计划可能涉及物理传输磁带或将数据复制到另一个站点。您的组织需要重新评估其先前灾难恢复策略的业务影响、风险和成本，以便在 AWS 上实现其灾难恢复目标。与传统环境相比，AWS 云中的灾难恢复具有以下优势：

- 以更低的复杂性从灾难中快速恢复
- 简单且可重复的测试使您可以更轻松、更频繁地进行测试
- 降低管理开销可减轻运营负担
- 自动化的机会减少了出错的几率并缩短了恢复时间

AWS 允许您将物理备份数据中心的固定资本支出与云中适当规模的环境的可变运营费用进行交易，这样可以显著降低成本。

对于许多组织而言，本地灾难恢复是基于数据中心的工作负载或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的风险。当组织在 AWS 上部署工作负载时，他们可以实施架构良好的工作负载，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。使用定期检查您的工作负载，确保它们遵循了 Well-Architected Framework 的最佳实践和指导。AWS Well-Architected Tool该工具可在中免费获得AWS 管理控制台。

如果您的工作负载在 AWS 上，则无需担心数据中心连接（您能否访问数据中心除外）、电源、空调、灭火装置和硬件。所有这些都由您管理，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独立的数据中心组成）。

# 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中实施高可用性工作负载有助于缓解自然和技术灾难。在单个区域内持续备份数据可以降低人为威胁的风险，例如可能导致数据丢失的错误或未经授权的活动。每个 AWS 区域都由多个可用区组成，每个可用区都与其他区域的故障隔离。每个可用区依次由一个或多个离散的物理数据中心组成。为了更好地隔离有影响的问题并实现高可用性，您可以将工作负载分成同一区域的多个区域。可用区域专为物理冗余而设计，可提供弹性，即使在停电、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。查看 AWS 全球云基础设施，了解 AWS 是如何做到这一点的。

通过跨单个 AWS 区域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。为了进一步保障您的单区域部署，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恢复。与下一节中描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，通过备份到亚马逊简单存储服务 (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（从几分钟到几小时）有更宽松的要求，那么使用 Amazon Glacier 或 Amazon Glacier 深度存档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。如果这适用于您在当前只有一个 AWS 区域的地区的工作负载，那么除了如上所述设计多可用区工作负载以实现高可用性外，您还可以将该区域 AZs 内的工作负载用作离散位置，这有助于满足适用于该区域内工作负载的数据驻留要求。以下各节中描述的灾难恢复策略使用多个 AWS 区域，但也可以使用可用区代替区域来实现。

# 多个 AWS 区域

对于包括失去彼此相距很远的多个数据中心的风险的灾难事件，您应该考虑灾难恢复选项，以缓解影响 AWS 中整个区域的自然和技术灾难。以下各节中描述的所有选项都可以作为多区域架构来实现，以防范此类灾难。

# 云中的灾难恢复选项

AWS 中可供您使用的灾难恢复策略可以大致分为四种方法，从备份的低成本和低复杂性到使用多个活动区域的更复杂的策略。 Active/passive 策略使用活动站点（例如 AWS 区域）来托管工作负载和提供流量。被动站点（例如不同的 AWS 区域）用于恢复。在触发故障转移事件之前，被动站点不会主动提供流量。

定期评估和测试您的灾难恢复策略至关重要，这样您就有信心在必要时调用该策略。使用 AWS Resilience Hub 持续验证和跟踪 AWS 工作负载的弹性，包括您是否有可能实现 RTO 和 RPO 目标。

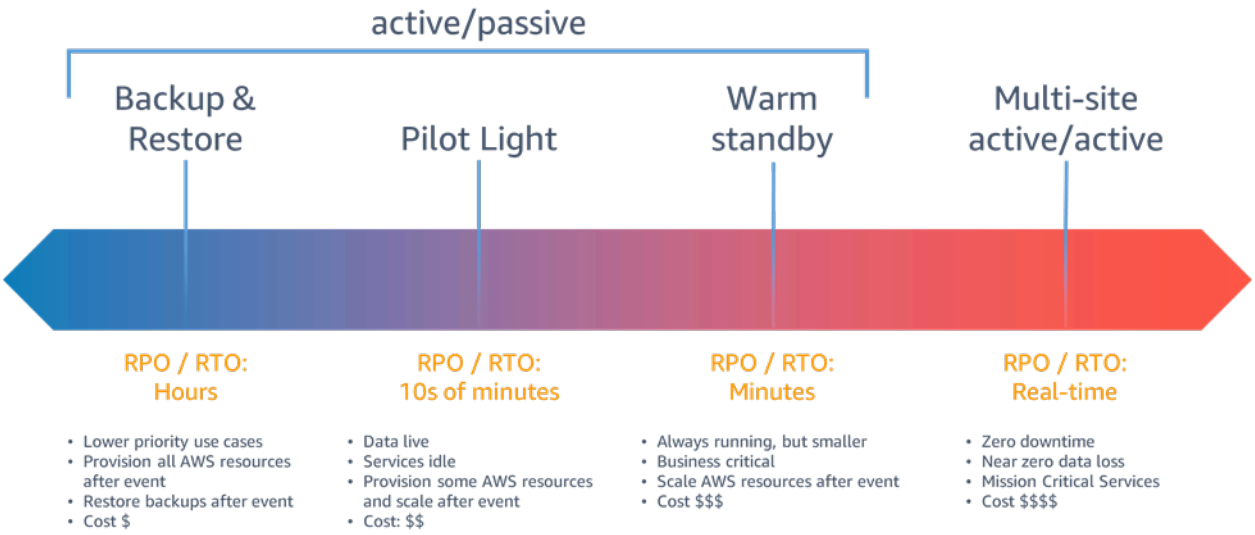


图 6-灾难恢复策略

对于因一个物理数据中心中断或丢失而导致架构良好、高度可用的工作负载而发生的灾难事件，您可能只需要使用备份和恢复方法进行灾难恢复。如果您对灾难的定义超出了物理数据中心的中断或丢失，而不仅仅是某个地区的物理数据中心中断或丢失，或者您受到要求的监管要求的约束，那么您应该考虑指示灯、热待机或多站点主动/主动。

在选择策略以及实施策略的 AWS 资源时，请记住，在 AWS 中，我们通常将服务分为数据平面和控制平面。数据面板负责交付实时服务，控制面板则用于配置环境。为了获得最大的弹性，您应仅使用数据平面操作作为故障转移操作的一部分。这是因为数据平面通常比控制平面具有更高的可用性设计目标。

# 备份与还原

Backup and Restore 是缓解数据丢失或损坏的合适方法。这种方法还可用于通过将数据复制到其他 AWS 区域来缓解区域灾难，或者缓解部署到单个可用区的工作负载的冗余不足。除数据外，您还必须

在恢复区域中重新部署基础架构、配置和应用程序代码。为了能够在没有错误的情况下快速重新部署基础架构，您应始终使用基础设施即代码 (IaC) 进行部署，并使用诸如AWS CloudFormation或之类的服务。AWS Cloud Development Kit (AWS CDK)如果没有 IaC，恢复区域中的工作负载可能会很复杂，这将导致恢复时间延长，并可能超过您的 RTO。除用户数据外，请务必备份代码和配置，包括您用于创建亚马逊 EC2 实例的亚马逊系统映像 (AMIs)。您可以使用自动AWS CodePipeline重新部署应用程序代码和配置。

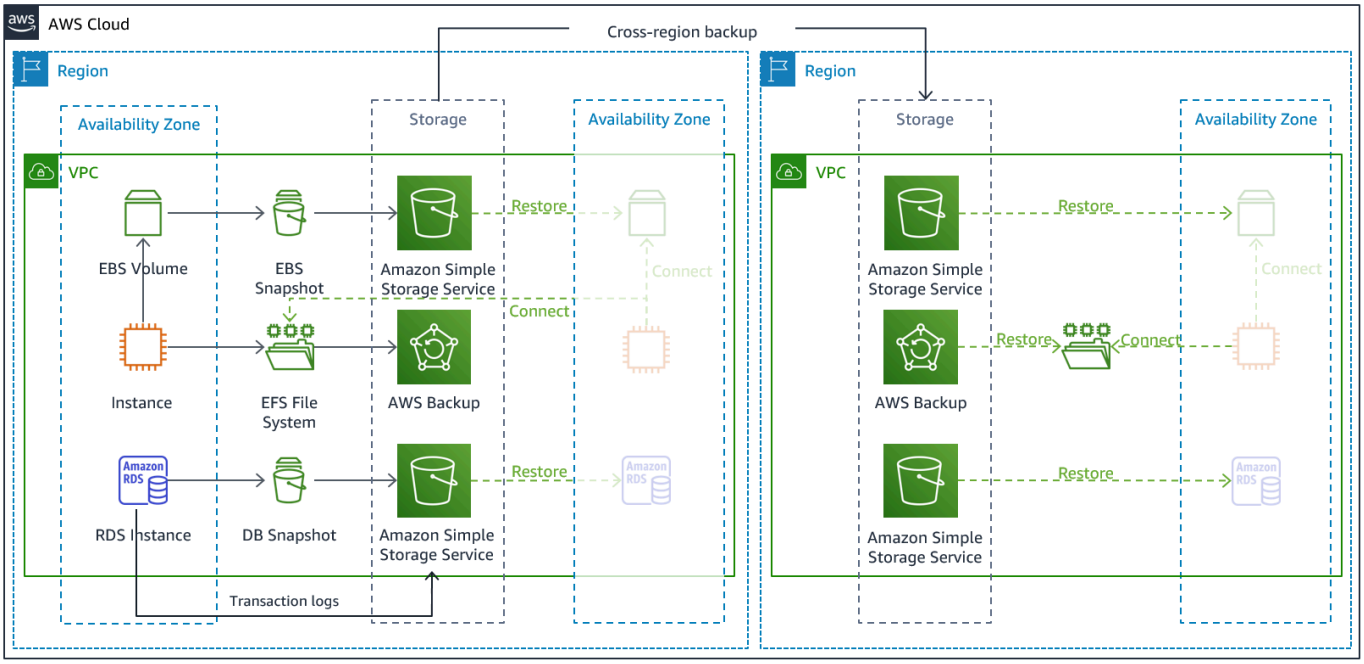


图 7-Backup 和恢复架构

## Amazon Web Services

您的工作负载数据需要定期运行或连续运行的备份策略。您运行备份的频率将决定您可实现的恢复点（恢复点应与您的 RPO 保持一致）。备份还应提供一种将其恢复到拍摄时间点的方法。Backup point-in-time with Recovery 可通过以下服务和资源获得：

- 亚马逊 Elastic Block Store (亚马逊 EBS) Block Store 快照
- 亚马逊 DynamoDB 备份
- 亚马逊 RDS 快照
- 亚马逊 Aurora 数据库快照
- 亚马逊 EFS 备份（使用时 AWS Backup）
- 亚马逊 Redshift 快照

- 亚马逊 Neptune 快照
- Amazon DocumentDB
- FSx 适用于 Windows 文件服务器的亚马逊、Lustre FSx 的亚马逊、 NetApp ONTAP FSx 的亚马逊、OpenZFS 的亚马逊 FSx

对于亚马逊简单存储服务 (Amazon S3) Simple Service，您可以使用 Amazon S3 跨区域复制 (CRR) 将对象持续异步复制到灾难恢复区域的 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），但可能无法抵御灾难事件，例如数据损坏或恶意攻击（例如未经授权的数据删除）以及 point-in-time备份。AWS Pilot Light 服务部分介绍了持续复制。

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

- Amazon Elastic Block Store（Amazon EBS）卷
- 亚马逊 EC2实例
- 亚马逊关系数据库服务 (Amazon RDS) 数据库（包括亚马逊 Aurora 数据库）
- 亚马逊 DynamoDB 表
- 亚马逊 Elastic File System（亚马逊 EFS）文件系统
- AWS Storage Gateway 卷
- FSx 适用于 Windows 文件服务器的亚马逊、Lustre FSx 的亚马逊、 NetApp ONTAP FSx 的亚马逊、OpenZFS 的亚马逊 FSx

AWS Backup 支持跨区域复制备份，例如复制到灾难恢复区域。

作为针对您的 Amazon S3 数据的其他灾难恢复策略，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，从而保护您在 S3 中的数据免受删除或修改操作的影响。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，当删除源存储桶中的对象时，Amazon S3 仅在源存储桶中添加删除标记。这种方法可以保护灾难恢复区域中的数据免遭源区域的恶意删除。

除数据外，您还必须备份必要的配置和基础架构，以重新部署工作负载并满足恢复时间目标 (RTO)。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，以便您可以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 实例作为亚马逊系统映像 (AMIs) 进行备份。AMI 是根据您的实例的根卷和连接到您的实例的任何其他 EBS 卷的快照创建的。您可以使用此 AMI 启动 EC2 实例的还原版本。AMI 可以在区域内复制，也可

以跨区域复制。或者，您可以使用AWS Backup跨账户复制备份并复制到其他 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 还增加了额外的 EC2备份功能——除了实例的单个 EBS 卷外， AWS Backup 还可以存储和跟踪以下元数据：实例类型、已配置的虚拟私有云 (VPC)、安全组、IAM 角色、监控配置和标签。但是，这些额外的元数据仅在将 EC2 备份还原到同一 AWS 区域时使用。

作为备份存储在灾难恢复区域中的任何数据都必须在故障转移时恢复。 AWS Backup 提供恢复功能，但目前不支持定时或自动恢复。您可以使用 AWS 软件开发工具包实现灾难恢复区域 APIs 的自动恢复 AWS Backup。您可以将其设置为定期重复的任务，也可以在备份完成时触发恢复。下图显示了使用亚马逊简单通知服务 (Amazon SNS) 进行自动恢复的示例，以及。AWS Lambda实施定期数据恢复是个好主意，因为从备份中恢复数据是一项控制平面操作。如果在灾难期间无法使用此操作，您仍然可以从最近的备份中创建可操作的数据存储。

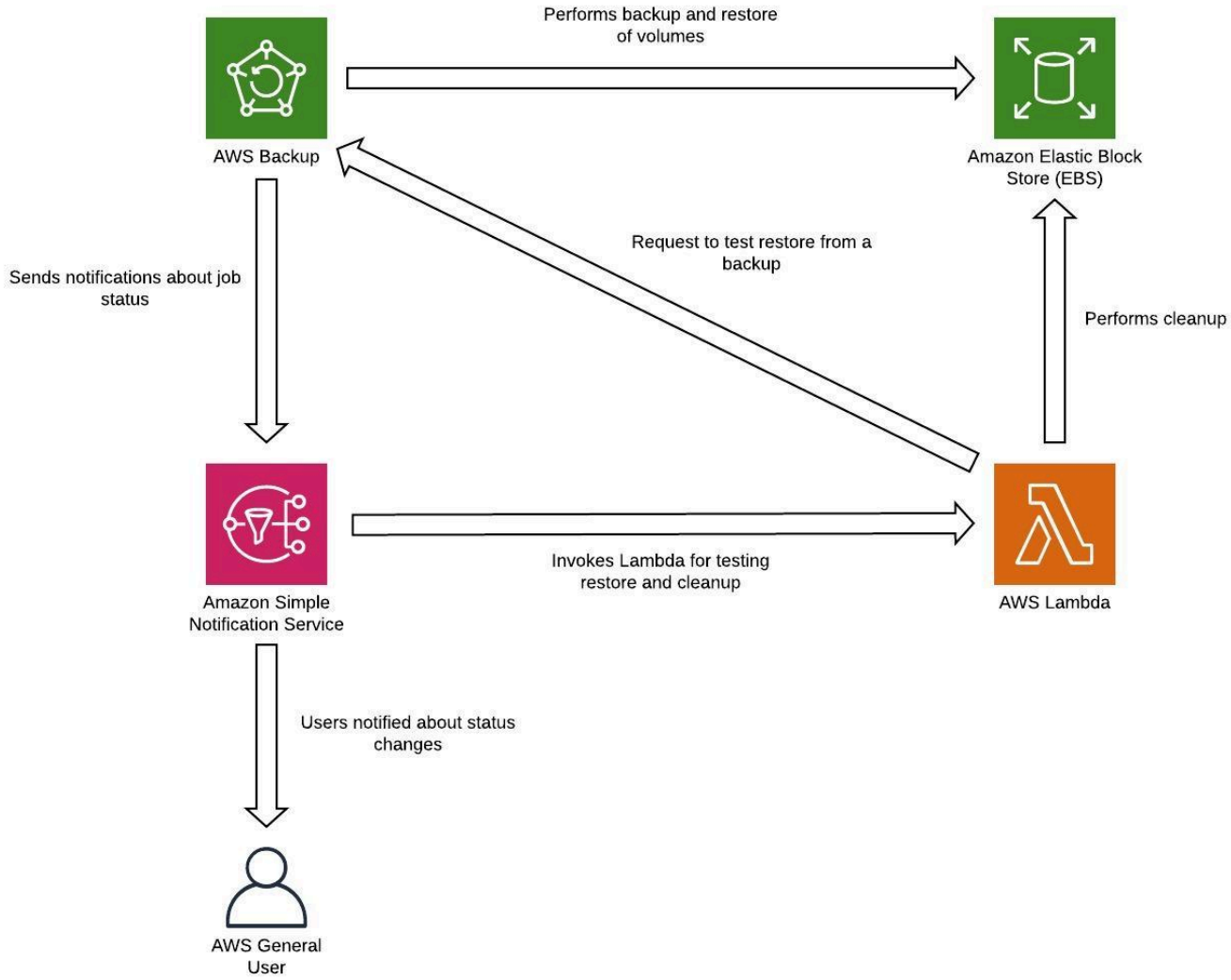


图 8-恢复和测试备份

> **Note**
>
> 您的备份策略必须包括测试备份。有关更多信息，请参阅 “测试灾难恢复” 部分。有关实施的实际演示，请参阅 AWS Well-Architected 实验室：测试数据的备份和恢复。

# 指示灯

使用试点方法，您可以将数据从一个区域复制到另一个区域，并配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）始终处于启用状态。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，但是 “已关闭”，仅在测试期间或调用灾难恢复故障转移时使用。在云中，您可以灵活地在不需要资源时取消配置资源，并在需要时对其进行配置。“关闭” 的最佳做法是不部署资源，然后创建配置和功能以在需要时进行部署（“开启”）。与备份和恢复方法不同，您的核心基础架构始终可用，并且您始终可以选择通过打开和扩展应用程序服务器来快速配置全面的生产环境。

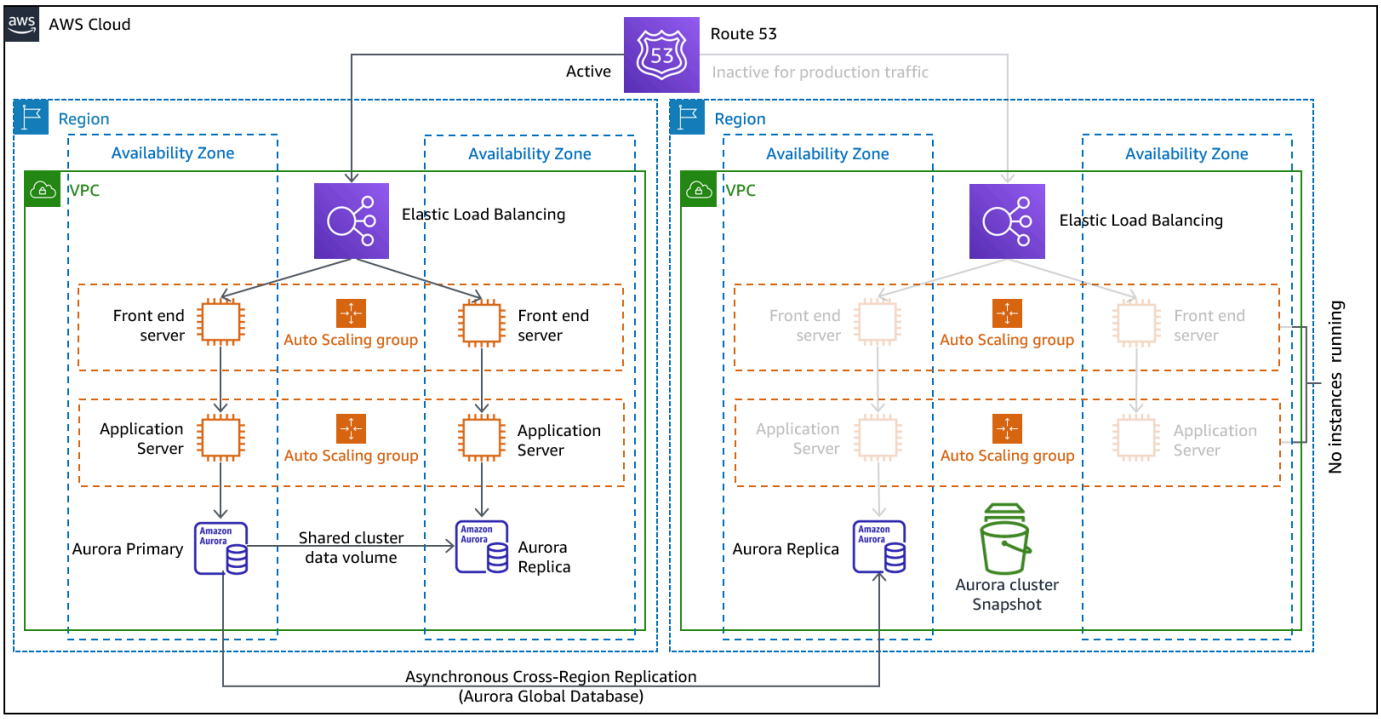


图 9-指示灯架构

指示灯方法通过最大限度地减少活跃资源来最大限度地降低灾难恢复的持续成本，并且由于核心基础设施要求都已到位，因此可以简化灾难发生时的恢复。此恢复选项要求您更改部署方法。您需要对每个区域进行核心基础设施更改，并将工作负载（配置、代码）更改同时部署到每个区域。通过自动化部署并使用基础设施即代码 (IaC) 跨多个账户和地区部署基础架构（将基础设施全面部署到主区域，缩小/关

闭基础设施部署到灾难恢复区域），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（在这种情况下，您的灾难恢复计划中也会包含泄露的凭证）。

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的灾难的侵害，但除非您的策略还包括存储数据的版本控制或 point-in-time恢复选项，否则它可能无法保护您免受数据损坏或破坏的影响。您可以备份灾难区域中复制的数据，以便在同一区域中创建 point-in-time备份。

## Amazon Web Services

除了使用 Backup and Re store 部分中介绍的 AWS 服务来创建 point-in-time备份外，还要考虑将以下服务作为试点策略。

首先，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（除了前面讨论的 point-in-time备份之外还使用时）。AWS 使用以下服务和资源为数据提供持续、跨区域、异步的数据复制：

- 亚马逊简单存储服务 (Amazon S3) Semple Service 复制
- 亚马逊 RDS 只读副本
- 亚马逊 Aurora 全球数据库
- Amazon DynamoDB 全局表
- Amazon DocumentDB 全局集群
- 适用于亚马逊的全球数据存储 ElastiCache (Redis OSS)

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 S3 对象的 S3 复制时间控制 (S3 RTC) 和 Amazon A urora 全球数据库的管理功能等服务功能来监控实际的复制时间。

在故障转移以从灾难恢复区域运行 read/write 工作负载时，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，重启是该过程的一部分。对于跨区域复制 (CRR) 和使用 RDS 进行故障转移，使用 Amazon Aurora 全球数据库具有多种优势。全球数据库使用专用的基础设施，使您的数据库完全可用于您的应用程序，并且可以复制到辅助区域，延迟通常不到一秒（AWS 区域内的延迟远小于 100 毫秒）。借助 Amazon Aurora 全球数据库，如果您的主要区域出现性能下降或中断，即使在区域完全中断的情况下，您也可以在不到一分钟的时间内将其中一个次要区域提升为承担读/写责任。您还可以将 Aurora 配置为监控所有辅助集群的 RPO 延迟时间，以确保至少有一个辅助集群保持在目标 RPO 窗口内。

必须在灾难恢复区域中部署资源较少或更少的核心工作负载基础架构的缩小版本。使用 AWS CloudFormation，您可以定义您的基础设施，并将其一致地部署在 AWS 账户和 AWS 区域中。 AWS

CloudFormation 使用预定义的虚拟参数来识别 AWS 账户及其部署的 AWS 区域。因此，您可以在 CloudFormation 模板中实现条件逻辑，以便在灾难恢复区域中仅部署缩小版本的基础架构。 EC2 例如部署，Amazon 系统映像 (AMI) 提供诸如硬件配置和已安装软件之类的信息。您可以实施一个 Image Builder 管道来创建所需的内容，然后将其复制到您的主区域和备份区域。 AMIs 这有助于确保这些黄金 AMIs拥有在发生灾难事件时在新区域重新部署或扩展工作负载所需的一切。Amazon EC2 实例以缩小配置进行部署（实例数少于您的主区域中的实例）。要扩展基础设施以支持生产流量，请参阅 “热待机” 部分中的 A mazon A EC2 uto Scaling。

对于诸如指示灯之类的 active/passive 配置，所有流量最初都会流向主区域，如果主区域不再可用，则切换到灾难恢复区域。此失效转移操作可以自动或手动启动。应谨慎使用基于运行状况检查或警报自动启动的故障转移。即使使用此处讨论的最佳实践，恢复时间和恢复点也将大于零，从而导致一些可用性和数据丢失。如果你在不需要的时候进行故障转移（误报），那么你就会蒙受这些损失。因此，通常会使用手动启动的失效转移。在这种情况下，您仍然应该自动执行失效转移步骤，这样手动启动就像按一下按钮一样简单。

使用 AWS 服务时，需要考虑多种流量管理选项。

一个选项是使用 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 Route 53 域名关联起来。然后，您可以将流量路由到该域名下的相应终端节点。在故障转移时，您需要将流量切换到恢复终端节点，使其远离主端点。亚马逊 Route 53 运行状况检查会监控这些终端节点。使用这些运行状况检查，您可以配置自动启动的 DNS 故障转移，以确保流量仅发送到健康的终端节点，这是在数据平面上完成的高度可靠的操作。要使用手动启动的故障转移来实现这一点，您可以使用 Amazon 应用程序恢复控制器 (ARC)。使用 ARC，您可以创建 Route 53 运行状况检查，这些检查实际上并不检查运行状况，而是充当您可以完全控制的开/关开关。使用 AWS CLI 或 AWS 开发工具包，您可以使用此高度可用的数据平面 API 编写故障转移脚本。您的脚本会切换这些开关（Route 53 运行状况检查），告诉 Route 53 将流量发送到恢复区域而不是主区域。有些人使用的手动启动故障转移的另一种选择是使用加权路由策略并更改主区域和恢复区域的权重，以便所有流量都流向恢复区域。但是，请注意，这是控制平面操作，因此不如使用 Amazon 应用程序恢复控制器 (ARC) 的数据平面方法具有弹性。

另一种选择是使用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公有 IP 地址相关联。 AWS Global Accelerator 然后将流量路由到与该地址关联的相应终端节点。全球加速器运行状况检查监控终端节点。使用这些运行状况 AWS Global Accelerator 检查，检查应用程序的运行状况，并将用户流量自动路由到健康的应用程序终端节点。对于手动启动的故障转移，您可以使用流量拨号调整哪个端点接收流量，但请注意，这是控制平面操作。Global Accelerator 利用广泛的 AWS 边缘网络将流量尽快转移到 AWS 网络主干上，因此它为应用程序终端节点提供了更低的延迟。全球加速器还可以避免 DNS 系统（如 Route 53）可能出现的缓存问题。

Amazon CloudFront 提供源站故障转移，如果对主终端节点的给定请求失败，则会将请求 CloudFront 路由到辅助终端节点。与前面描述的故障转移操作不同，所有后续请求仍会发送到主终端节点，并且每个请求都会进行故障转移。

## AWS 弹性灾难恢复

AWS Elastic Daser Recovery (DRS) AWS 使用底层服务器的块级复制，持续将来自任何来源的服务器托管应用程序和服务器托管的数据库复制复制到底层服务器的块级复制中。Elastic 灾难恢复允许您使用中的区域 AWS 云 作为本地或其他云提供商上托管的工作负载及其环境的灾难恢复目标。如果 AWS 托管的工作负载仅包含托管在上的应用程序和数据库 EC2（即不是 RDS），则它也可以用于对托管的工作负载进行灾难恢复。Elastic 灾难恢复使用 Pilot Light 策略，在用作暂存区的亚马逊虚拟私有云（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，将使用暂存的资源在用作恢复位置的目标 Amazon VPC 中自动创建满容量部署。

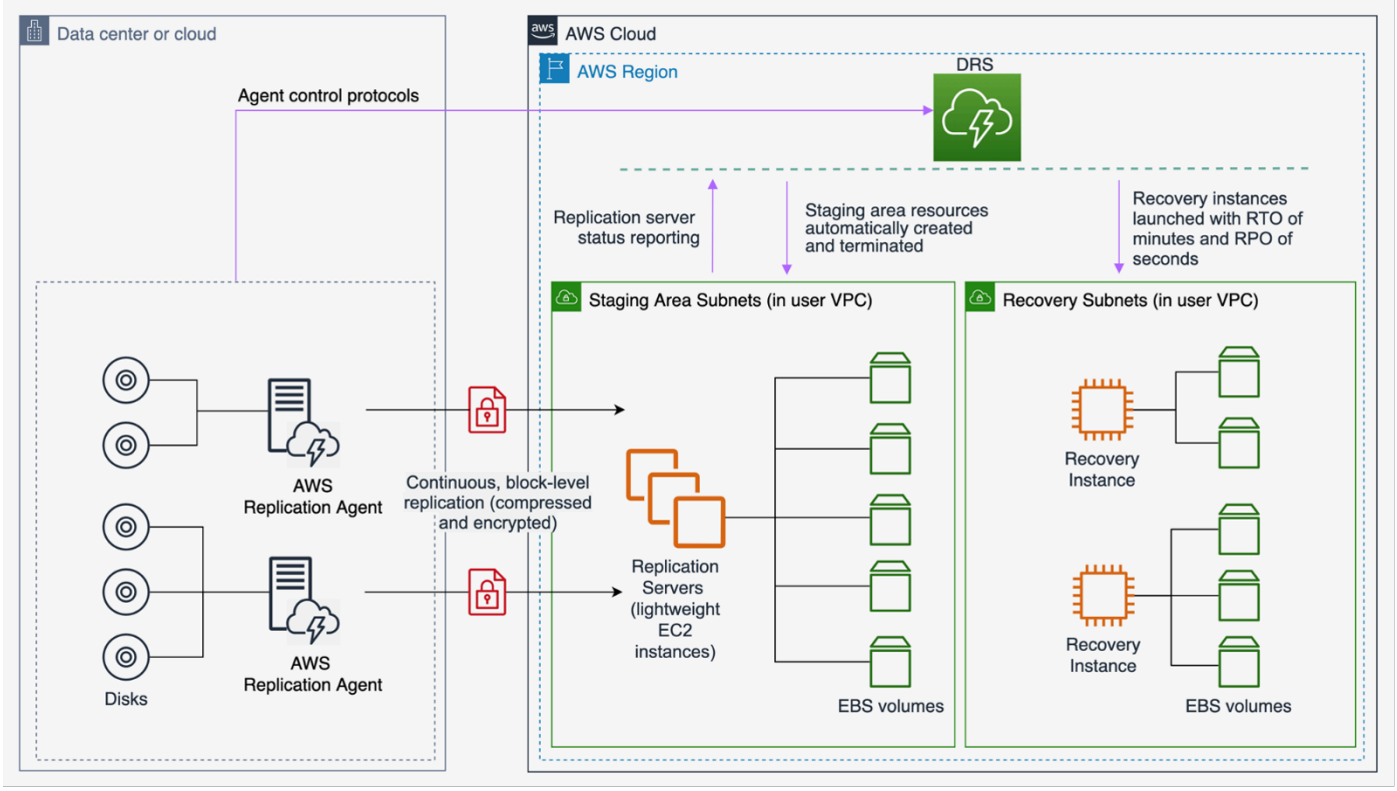


图 10- AWS 弹性灾难恢复架构

# 温备用

温备用方法涉及到确保在另一个区域中存在生产环境的规模缩减但功能齐全的副本。这种方法扩展了指示灯概念并减少了恢复时间，因为工作负载始终在另一个区域中运行。这种方法还允许您更轻松地执行测试或实施持续测试，从而增强您对灾难中恢复能力的信心。

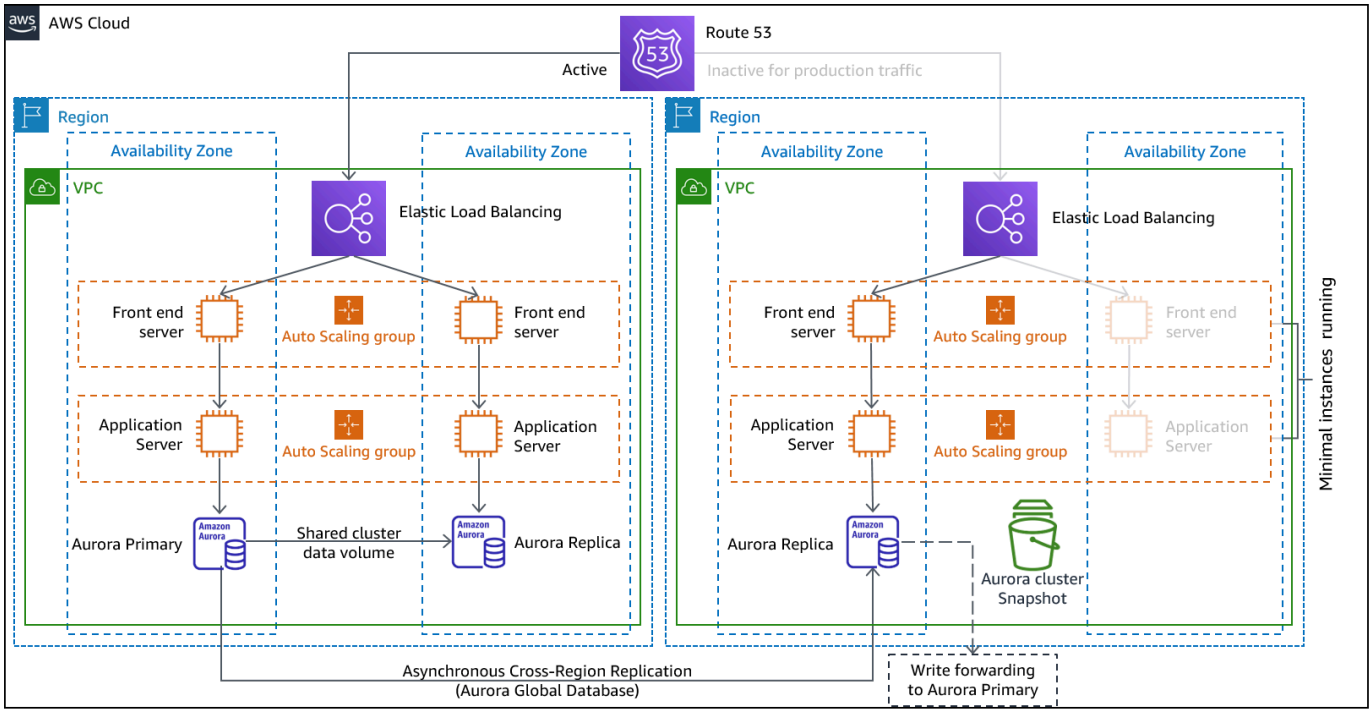


图 11-热备用架构

注意：指示灯和热待机之间的区别有时可能很难理解。两者都包含灾难恢复区域中的一个环境，其中包含您的主要区域资产的副本。区别在于，如果不先采取额外措施，指示灯就无法处理请求，而热备用模式可以立即处理流量（在降低的容量水平下）。指示灯方法要求您“开启”服务器，可能部署其他（非核心）基础架构，然后向上扩展，而热待机只需要您向上扩展（所有内容都已部署并正在运行）。使用您的 RTO 和 RPO 需求来帮助您在这些方法之间做出选择。

## Amazon Web Services

备份和还原以及指示灯下涵盖的所有 AWS 服务也用于热备用状态，用于数据备份、数据复制、 active/passive 流量路由和基础设施（包括 EC2 实例）的部署。

Amazon A EC2 uto Scaling 用于在 AWS 区域内扩展资源，包括亚马逊 EC2 实例、亚马逊 ECS 任务、亚马逊 DynamoDB 吞吐量和 Amazon Aurora 副本。Amazon A EC2 uto Scaling 在一个 AWS 区域内跨可用区域扩展 EC2 实例部署，从而在该区域内提供弹性。作为指示灯或热待机策略的一部分，使用 Auto Scaling 将灾难恢复区域扩展到完全的生产能力。例如，对于 EC2，增加 Auto Scaling 组的所需容量设置。您可以通过手动调整此设置 AWS 管理控制台，也可以通过 AWS SDK 自动调整此设置，也可以使用新的所需容量值重新部署 AWS CloudFormation 模板。您可以使用 AWS CloudFormation 参数来简化 CloudFormation 模板的重新部署。确保灾难恢复区域的服务配额设置得足够高，以免限制您向上扩展到生产容量。

由于 Auto Scaling 是一项控制平面活动，因此依赖它会降低整体恢复策略的弹性。这是一种权衡取舍。您可以选择预置足够的容量，以便恢复区域能够在部署时处理全部生产负载。这种静态稳定的配置称为热待机（参见下一节）。或者，您可以选择配置更少的资源，这样成本会更低，但要依赖于 Auto Scaling。某些 DR 实现会部署足够的资源来处理初始流量，从而确保低 RTO，然后依靠 Auto Scaling 来增加后续流量。

## 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 active/active 提供来自其部署到的所有区域的流量，而热备用仅为来自单个区域的流量提供服务，而其他区域仅用于灾难恢复。使用多站点 active/active 方法，用户可以在部署工作负载的任何区域访问您的工作负载。这种方法是最复杂、成本最高的灾难恢复方法，但是如果选择正确的技术和实施，它可以将大多数灾难的恢复时间缩短到接近零（但是，数据损坏可能需要依赖于备份，这通常会导致恢复点不为零）。热备用使用的 active/passive 配置仅将用户定向到单个区域，灾难恢复区域不占用流量。大多数客户发现，如果他们要在第二个区域建立完整的环境，那么主动/主动使用它是有意义的。或者，如果您不想同时使用两个区域来处理用户流量，那么 Warm Standby 提供了一种更经济、操作上不那么复杂的方法。

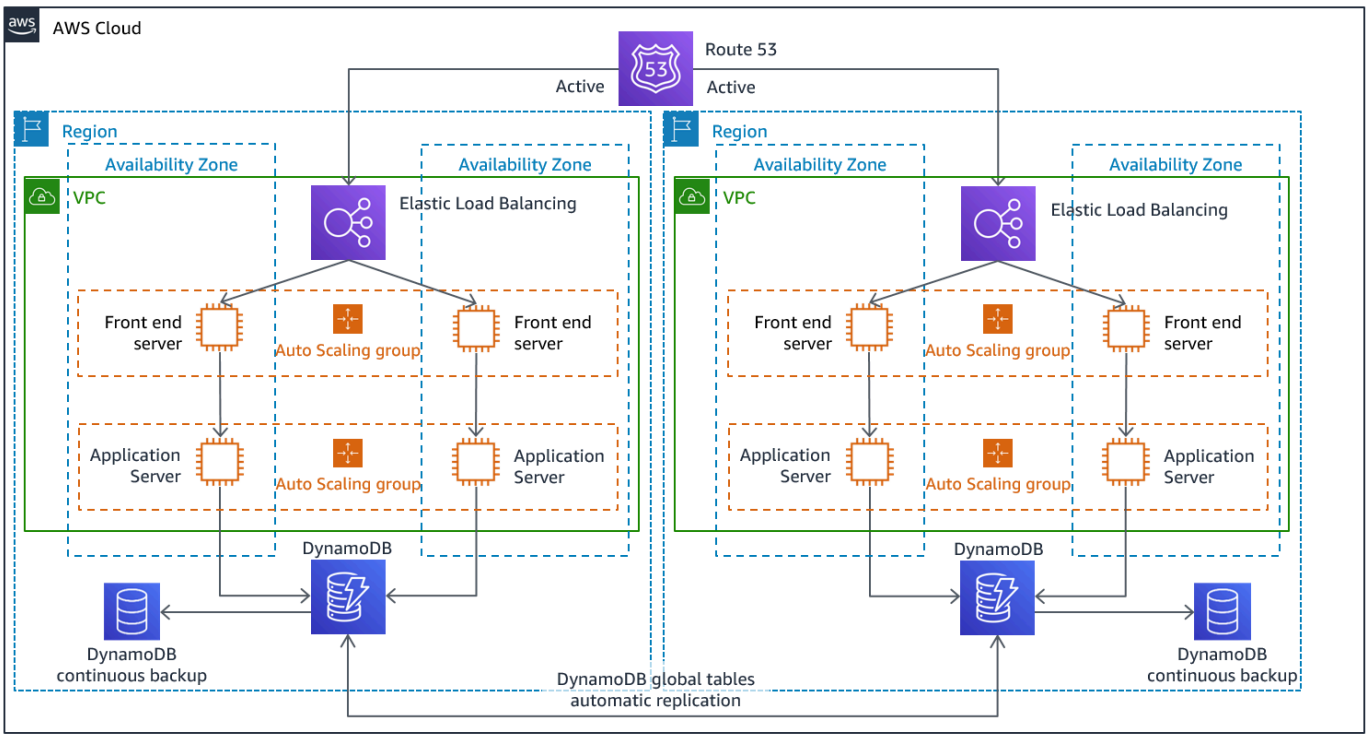


图 12-多站点 active/active 架构（对于热备用，将一条活动路径更改为 “非活动”）

由于需要采用多站点active/active, because the workload is running in more than one Region, there is no such thing as failover in this scenario. Disaster recovery testing in this case would focus on how the workload reacts to loss of a Region: Is traffic routed away from the failed Region? Can the other Region(s) handle all the traffic? Testing for a data disaster is also required. Backup and recovery are still required and should be tested regularly. It should also be noted that recovery times for a data disaster involving data corruption, deletion, or obfuscation will always be greater than zero and the recovery point will always be at some point before the disaster was discovered. If the additional complexity and cost of a multi-site active/active（或热备用）方法来保持接近零的恢复时间，因此应付出更多努力来维护安全并防止人为错误，以缓解人为灾难。

## Amazon Web Services

备份和恢复、指示灯和热备用中涵盖的所有 AWS 服务也用于数据备份、 point-in-time数据复制、active/active 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 active/passive 场景（指示灯和热待机），Amazon Route 53 和 Amazon Route 53 都 AWS Global Accelerator 可用于将网络流量路由到活动区域。对于此处的 active/active 策略，这两项服务还允许定义政策，以确定哪些用户访问哪个活跃的区域端点。通过 AWS Global Accelerator 设置流量拨号来控制定向到每个应用程序端点的流量百分比。Amazon Route 53 支持这种百分比方法以及其他多种可用策略，包括基于地理位置和延迟的策略。Global Accelerator 会自动利用广泛的 AWS 边缘服务器网络，尽快将流量载入 AWS 网络主干，从而降低请求延迟。

使用此策略进行异步数据复制可实现接近零的 RPO。像 A mazon Aurora 全球数据库这样的 AWS 服务使用专用的基础设施，使您的数据库完全可用于您的应用程序，并且可以复制到多达五个次要区域，典型延迟不到一秒。active/passive strategies, writes occur only to the primary Region. The difference with active/active正在设计如何处理向每个活动区域写入数据时的数据一致性。通常将用户读取设计为从离他们最近的区域（称为本地读取）提供读取。对于写入，您有几种选择：

- 写入全局策略将所有写入路由到单个区域。如果该区域失败，则另一个区域将被提升为接受写入。Aurora 全球数据库非常适合全局写入，因为它支持跨区域的只读副本同步，而且您可以在不到一分钟的时间内将其中一个辅助区域提升为承担 read/write 责任。Aurora 还支持写入转发，它允许 Aurora 全局数据库中的辅助集群将执行写入操作的 SQL 语句转发到主集群。
- 写入本地策略路由写入最近的区域（就像读取一样）。Amazon DynamoDB 全局表支持这样的策略，允许从您的全局表部署到的每个区域进行读取和写入。Amazon DynamoDB 全局表使用最后一个写入器赢得并发更新之间的协调。
- 写入分区策略根据分区键（如用户 ID）将写入分配给特定区域，以避免写入冲突。在这种情况下，可以使用双向配置的 Amazon S3 复制，并且目前支持在两个区域之间进行复制。实现此方法时，请确保在存储桶 A 和 B 上启用副本修改同步，以复制副本元数据更改，例如对象访问控制列表

(ACLs)、对象标签或复制对象上的对象锁。您还可以配置是否在活动区域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 point-in-time备份，以防止数据损坏或破坏事件。

AWS CloudFormation 是一款强大的工具，用于在多个 AWS 区域的 AWS 账户之间强制部署一致的基础设施。 AWS CloudFormation StackSets扩展了此功能，使您能够通过一次操作在多个账户和地区创建、更新或删除 CloudFormation 堆栈。尽管 AWS CloudFormation 使用 YAML 或 JSON 将基础设施定义为代码，但AWS Cloud Development Kit (AWS CDK)允许您使用熟悉的编程语言将基础设施定义为代码。您的代码将转换为 CloudFormation 该代码，然后用于在 AWS 中部署资源。

# 检测

请务必尽快了解您的工作负载并未实现应有的业务成果。通过这种方式，您可以快速宣布灾难并从事件中恢复。对于积极的恢复目标，这种响应时间加上适当的信息对于实现恢复目标至关重要。如果您的恢复时间目标为一小时，则需要检测事件，通知相关人员，参与上报流程，评估有关预计恢复时间的信息（如果有的话）（不执行灾难恢复计划），宣布灾难并在一小时内恢复。

> **Note**
>
> 如果利益相关者决定不调用 DR，即使 RTO 会面临风险，请重新评估灾难恢复计划和目标。之所以决定不援引灾难恢复计划，可能是因为计划不够充分，或者对执行缺乏信心。

至关重要的是，要将事件检测、通知、上报、发现和申报纳入您的计划和目标，以提供具有商业价值的切合实际、可实现的目标。

AWS 在 Service Healt h Dashboard 上发布了我们最多的服务可用性 up-to-the-minute信息。随时查看以获取当前状态信息，或订阅 RSS feed 以获得每项服务中断的通知。如果您遇到我们的一项服务的实时操作问题，但该问题未显示在 Service Health Dashboard 上，则可以创建支持请求。

AWS Health Dashboard提供有关可能影响您账户 AWS Health 的事件的信息。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现自动故障转移。设计能够代表用户体验并基于关键绩效指标的健康检查。深度运行状况检查可以发挥工作负载的关键功能，而不仅仅是浅层的心跳检查。使用基于多个信号的深度健康检查。谨慎使用这种方法，以免触发虚假警报，因为在不需要时进行故障转移本身就会带来可用性风险。

# 测试灾难恢复

测试灾难恢复实施以验证实施情况，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。

要避免的一种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。在写入某个数据存储，却发现主存储故障时，您可能希望失效转移到辅助数据存储。如果不经常测试此失效转移，您可能会发现自己关于辅助数据存储容量的假设是错误的。在这种情况下，辅助区域的容量（在您上次测试时可能已经足够了）可能无法再承受负载，或者辅助区域的服务配额可能不足。

根据我们的经验，唯一有效的错误恢复路径是您经常测试的路径。这就是为什么最好使用少量恢复路径的原因。

您可以建立恢复模式并定期对其进行测试。如果您的恢复路径复杂或关键，则仍需要定期在生产环境中执行该故障，以验证恢复路径是否有效。

管理灾难恢复区域的配置偏差。确保您的基础架构、数据和配置符合灾难恢复区域的需求。例如，检查一下 AMIs ，服务配额是 up-to-date。

您可以利用AWS Config来持续监控和记录您的 AWS 资源配置。 AWS Config 可以检测漂移并触发 AWS Systems Manager Automation 以修复漂移并发出警报。 AWS CloudFormation此外，还可以检测您部署的堆栈中的偏差。

# 结论

客户应对其云端应用程序的可用性负责。重要的是要定义什么是灾难，并制定反映这一定义及其对业务结果可能产生的影响的灾难恢复计划。根据影响分析和风险评估创建恢复时间目标 (RTO) 和恢复点目标 (RPO)，然后选择适当的架构来缓解灾难。确保能够及时发现灾难——了解目标何时处于危险之中至关重要。确保您有计划并通过测试验证计划。由于缺乏信心或未能实现灾难恢复目标，未经验证的灾难恢复计划有可能无法实施。

# 贡献者

本文档的贡献者包括：

- Alex Livingstone，AWS 企业支持云运营业务主管
- Seth Eliot，Amazon Web Services 首席可靠性解决方案架构师

# 延伸阅读

有关更多信息，请参阅：

- AWS 建筑中心
- 可靠性支柱，AWS Well-Architected Framework
- 灾难恢复计划清单
- 实施健康检查
- AWS 上的灾难恢复 (DR) 架构，第一部分：云端恢复策略
- AWS 上的灾难恢复 (DR) 架构，第二部分：使用快速恢复功能进行备份和恢复
- AWS 上的灾难恢复 (DR) 架构，第三部分：指示灯和热待机
- AWS 上的灾难恢复 (DR) 架构，第 IV 部分：多站点主动/主动
- 使用 Amazon Route 53 创建灾难恢复机制
- Minimizing Dependencies in a Disaster Recovery Plan
- 亲身体验 Well-A AWS rchitected 灾难恢复实验室
- AWS 解决方案实施：多区域应用程序架构
- AWS re: Invent 2018：多区域主动-主动应用程序的架构模式 (09-R2) ARC2

# 文档历史记录

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

| 变更 | 说明 | 日期 |
| --- | --- | --- |
| 次要更新 | 自始至终都修复了错误并进行了许多细微的更改。 | 2022 年 4 月 1 日 |
| 已更新白皮书 | 较小的编辑更新。 | 2022 年 3 月 21 日 |
| 已更新白皮书 | 添加了有关数据平面和控制平面的信息。添加了有关如何实现 active/passive 故障转移的更多详细信息。将 CloudEndure 灾难恢复替换为 AWS 弹性灾难恢复。 | 2022 年 2 月 17 日 |
| 次要更新 | AWS Well-Architected Tool 信息已添加。 | 2022 年 2 月 11 日 |
| 初次发布 | 白皮书首次发布。 | 2021 年 2 月 12 日 |

# 版权声明

# AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

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。