AWS 白皮书

AWS故障隔离边界

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS故障隔离边界: AWS 白皮书

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

摘象、简介 1
- 摘要 1
- 你Well-Architected 1
- 介绍 1

AWS 基础设施 2
- 可用区 2
- 区域 3
- AWSLocal Zones 4
- AWS Outposts 4
- 存在点 4
- 分区 5
- 控制面板和数据面板 6
- 静态稳定性 6
- Summary 7

AWS 服务类型 8
- 区域服务 8
- 区域服务 10
- 全球服务 11
  - 按分区划分的唯一全球服务 11
  - 边缘网络中的全球服务 13
  - 全球单一区域运营 14
  - 使用默认全局端点的服务 17
  - 全球服务摘要 19

结论 21

附录 A-分区服务指南 22
- AWSIAM 22
- AWS Organizations 22
- AWS 账户管理 23
- Route 53 应用程序恢复控制器 23
- AWS 网络管理器 23
- 53 号路由私有 DNS 24

附录 B-边缘网络全球服务指南 25
- Route 53 25
- Amazon CloudFront 25

亚马逊Certificate Manager 26
AWSWeb 应用程序防火墙 (WAF) 和 WAF 经典版 26
AWS Global Accelerator 26
亚马逊Shield 26
附录 C-单区域服务 27
贡献者 28
文档修订 29
AWS 术语表 30
版权声明 31
..... xxxii

AWS Faul

发布日期：2022 年 11 月 16 日 (文档修订)

摘要

Amazon Web Services (AWS) 提供不同的隔离边界，例如可用区 (AZ)、区域、控制平面和数据平面。paper 详细介绍了如何AWS使用这些边界创建区域、区域和全球服务。它还包括关于如何考虑对这些不同服务的依赖关系以及如何提高使用它们构建的工作负载的弹性的规范性指导。

你Well-Architected

Wel AWSI-Architec ted Framework 可帮助您了解在云中构建系统时所做决策的利弊。该框架的六大支柱使您可以学习设计和运行可靠、安全、高效、具有成本效益和可持续系统的架构最佳实践。使用中免费提供的 AWS Well-Architected Tool，您可以根据AWS 管理控制台这些最佳实践对工作负载进行审查，为每个支柱回答一系列问题。

有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅架构中心。AWS

介绍

AWS运营全球基础架构，提供云服务，帮助客户以灵活、安全、可扩展和高度可用的方式部署工作负载。该AWS基础架构使用多种故障隔离结构来帮助客户实现其弹性目标。这些故障隔离边界使客户能够设计工作负载，以利用它们提供的可预测的影响控制范围。了解如何使用这些边界设计AWS服务也很重要，这样您就可以针对工作负载选择的依赖关系做出有针对性的选择。

paper 将首先总结AWS全球基础架构及其提供的故障隔离边界，以及用于设计我们服务的一些模式。根据这一理解基线，paper 接下来将概述所AWS提供的不同服务范围：区域、区域和全球。它还将提供构建架构的最佳实践，这些架构使用这些隔离边界和不同的服务范围来提高您运行的工作负载的弹性AWS。特别是，它为如何依赖全球服务，同时最大限度地减少单点故障提供了规范性指导。这将帮助您就AWS依赖关系以及如何设计高可用性 (HA) 和灾难恢复 (DR) 的工作负载做出明智的选择。

AWS 基础设施

本节概述了AWS全球基础架构及其提供的故障隔离边界。此外，本节将概述控制平面和数据平面的概念，它们是其服务AWS设计方式的关键区别。这些信息为了解故障隔离边界以及服务的控制平面和数据平面如何应用于我们在下一节中讨论的AWS服务类型提供了基准。

主题

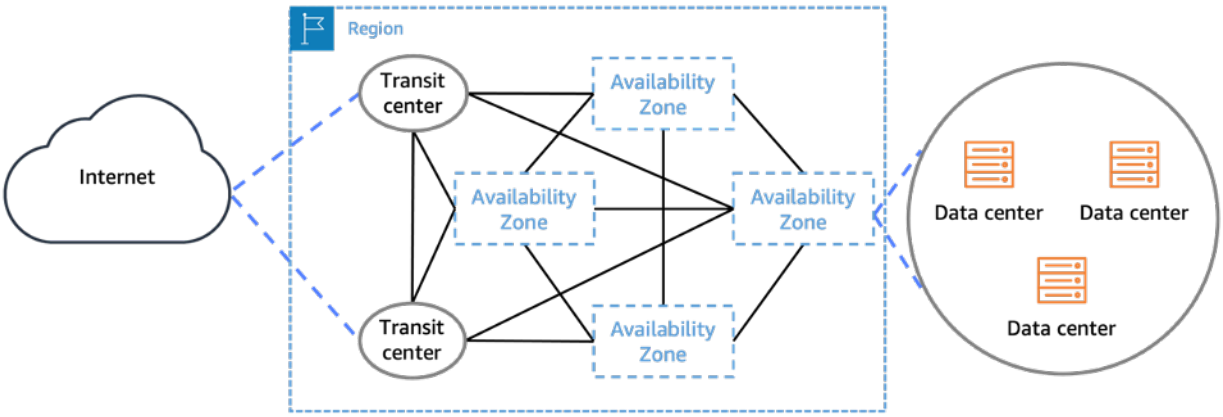
- 可用区
- 区域
- AWSLocal Zones
- AWS Outposts
- 存在点
- 分区
- 控制面板和数据面板
- 静态稳定性
- Summary

可用区

AWS在全球多个地区运营着 100 多个可用区（当前数字可在此处找到：AWS全球基础设施）。可用区是一个或多个独立的数据中心，其中包含独立和冗余的电源基础架构、网络和连接AWS 区域。一个区域中的可用区域彼此之间的距离相当大，最远可达 60 英里（约 100 km），以防止相关故障，但距离足够近，可以使用延迟为个位数毫秒的同步复制。它们的设计不会同时受到共同命运情景的影响，例如公用事业电力、水中断、光纤隔离、地震、火灾、龙卷风或洪水。常见的故障点（例如发电机和冷却设备）不是在可用区之间共享的，而是由独立的变电站提供的。在为其服务AWS部署更新时，会及时将部署到同一区域的可用区域分开，以防止出现相关故障。

一个区域中的所有可用区域都通过完全冗余的专用城域光纤与高带宽、低延迟的网络互连。一个区域中的每个可用区都通过两个中转中心连接到互联网，那里AWS有多个一级互联网提供商（有关更多信息，请参阅 Amazon Web Ser vices 概述）。

这些功能使可用区彼此之间具有很强的隔离，我们称之为可用区独立性 (AZI)。下图描述了可用区的逻辑结构及其与互联网的连接。



可用区由一个或多个物理数据中心组成，这些数据中心相互冗余连接并与互联网相连

区域

每个可用区都AWS 区域由一个地理区域内的多个独立且物理上独立的可用区组成。所有区域目前都有三个或更多可用区。区域本身是孤立的，独立于其他区域，但本文档后面会提到一些例外（请参阅全球单一区域操作）。区域间的这种分隔将服务故障发生时限制在单个区域内。在这种情况下，其他地区的正常运营不受影响。此外，除非您明确使用AWS服务提供的复制或复制功能或自己复制资源，否则您在一个区域创建的资源和数据不存在于任何其他区域。

截至 2022 年 12 月的当前和计划中的 AWS 区域

AWSLocal Zones

AWSL@@ ocal Z ones 是一种基础架构部署，它将计算、存储、数据库和其他精选AWS服务放在靠近人口众多和行业中心的地方。您可以在本地区域中使用AWS诸如计算和存储服务之类的服务在边缘运行低延迟应用程序或简化混合云迁移。Local Zones 具有本地互联网入口和出口，以减少延迟，但也通过 Amazon 的冗余和高带宽专用网络连接到其父区域，从而使在 L AWS ocal Zones 中运行的应用程序可以快速、安全、无缝地访问所有服务。

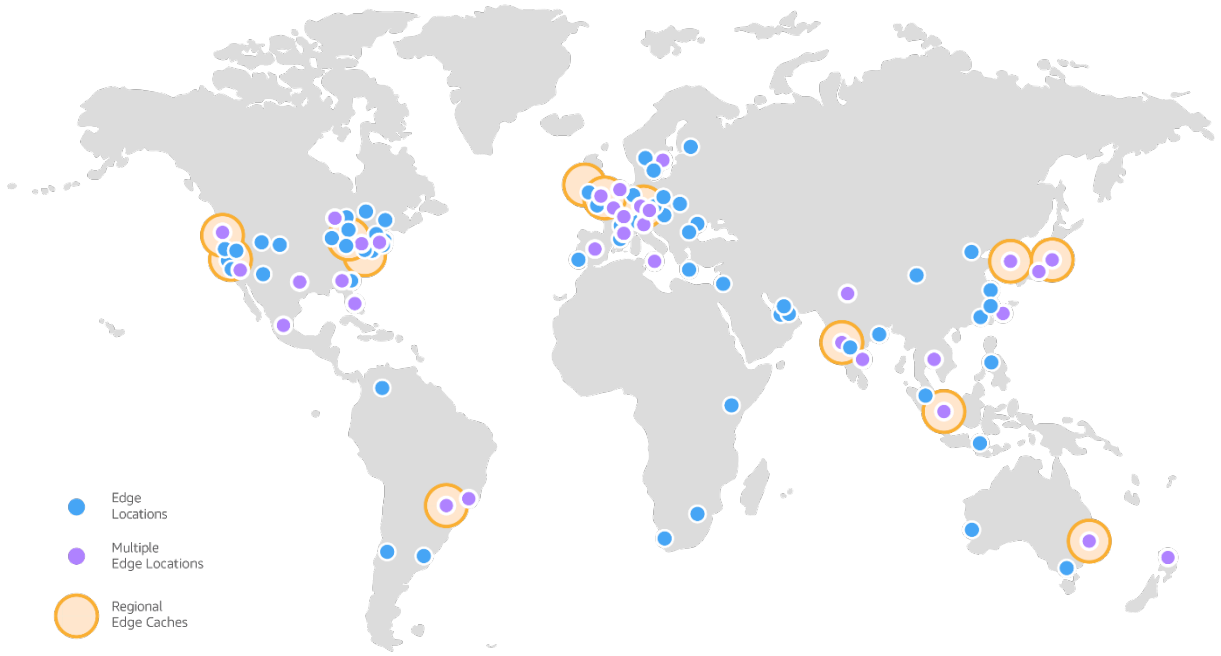
AWS Outposts

AWS Outposts是一系列完全托管的解决方案，可向几乎任何本地或边缘位置提供AWS基础设施和服务，以实现真正一致的混合体验。 Outposts 解决方案允许您在本地扩展和运行原生AWS服务，并且有多种外形可供选择，从 1U 和 2U Outposts 服务器到 42U Outposts 机架以及多机架部署。

使用AWS Outposts，您可以在本地运行选定的AWS服务，并连接到父级中提供的各种服务AWS 区域。 AWS Outposts是完全托管且可配置的计算和存储机架，AWS采用精心设计的硬件构建，允许客户在本地运行计算和存储，同时无缝连接到AWS云中的各种服务。

存在点

除AWS 区域和可用区外，AWS还运营着全球分布的接入点 (PoP) 网络。它们 PoPs 托管内容分发网络 (CDN) 亚马逊、公共域名系统 (DNS) 解析服务 Amazon Route 53 和边缘网络优化服务AWS全球加速器 (AGA)。 CloudFront全球边缘网络目前由 410 多个边缘站点组成 PoPs，包括 400 多个边缘站点，以及 48 个国家/地区的 90 多个城市的 13 个区域中端缓存（当前状态可在此处找到：A mazon CloudFront 主要功能）。



亚马逊 CloudFront 全球边缘网络

每个 PoP 都与其他 PoP 隔离，这意味着影响单个 PoP 或大都市区的故障不会影响全球网络的其余部分。该AWS网络与全球数千家1/2/3级电信运营商同行，与所有主要接入网络连接良好，可实现最佳性能，并拥有数百太比特的部署容量。边缘站点AWS 区域通过网络主干与AWS网络主干相连，这是一种完全冗余的多个 100GbE 并行光纤，环绕全球并与成千上万个网络连接，以改善来源获取和动态内容加速。

分区

AWS将区域分组为分区。每个区域恰好位于一个分区中，每个分区都有一个或多个区域。分区具有独立的 AWS Identity and Access Management (IAM) 实例，在不同分区中的区域之间提供了硬边界。 AWS商业区域位于aws分区中，中国区域位于aws-cn分区中，AWS GovCloud 区域位于aws-us-gov分区中。有些AWS服务旨在提供跨区域功能，例如 Amazon S3 跨区域复制或 T AWS ransit Gateway 区域间对等互连。只有同一分区中的区域之间才支持这些类型的功能。您不能使用来自一个分区的 IAM 凭证与其他分区中的资源进行交互。

控制面板和数据面板

AWS将大多数服务分为控制平面和数据平面的概念。这些术语来自网络世界，特别是路由器。路由器的数据平面是其主要功能，它根据规则四处移动数据包。但是路由策略必须从某个地方创建和分发，而这正是控制平面的用武之地。

控制平面提供用于创建、读取/描述、更新、删除和列出 (CRUDL) 资源的管理 API。例如，以下都是控制平面操作：启动新的亚马逊弹性计算云 (Amazon EC2) 实例、创建亚马逊简单存储服务 (Amazon S3) 存储桶以及描述亚马逊简单队列服务 (Amazon SQS) 队列。当您启动 EC2 实例时，控制平面必须执行多项任务，例如查找具有容量的物理主机、分配网络接口、准备 A mazon Elastic Block Store (Amazon EBS) 卷、生成 IAM 证书、添加安全组规则等。控制平面往往是复杂的编排和聚合系统。

数据平面是提供服务主要功能的平面。例如，以下是所涉及的每项服务的数据平面的所有部分：正在运行的 EC2 实例本身、读取和写入 EBS 卷、获取和放入 S3 存储桶中的对象，以及 Route 53 应答 DNS 查询和执行运行状况检查。

与控制平面相比，数据平面故意不那么复杂，活动部件更少，控制平面通常实现由工作流程、业务逻辑和数据库组成的复杂系统。这使得从统计学上讲，与控制平面相比，数据平面中发生故障事件的可能性较小。虽然数据平面和控制平面都为服务的整体运营和成功做出了贡献，但AWS认为它们是截然不同的组成部分。这种分离具有性能和可用性两方面的好处。

静态稳定性

AWS服务最重要的弹性特征之一就是所AWS谓的静态稳定性。该术语的含义是，系统在静态状态下运行，并且在依赖关系出现故障或不可用期间无需进行更改即可继续正常运行。我们做到这一点的一种方法是防止服务中的循环依赖，因为循环依赖可能会阻止其中一个服务成功恢复。我们这样做的另一种方法是维护现有状态。我们考虑了这样一个事实，即从统计学上讲，控制平面比数据平面更有可能出现故障。尽管数据平面通常依赖于来自控制平面的数据，但即使面对控制平面损坏，数据平面仍会保持其现有状态并继续工作。数据平面对资源的访问一旦配置，就不依赖于控制平面，因此不受任何控制平面损坏的影响。换句话说，即使创建、修改或删除资源的能力受到损害，现有资源仍然可用。这使得AWS数据平面可以静态稳定地抵御控制平面中的损伤。你可以实现不同的模式，以保持静态稳定，抵御不同类型的依赖失败。

可以在 Amazon EC2 中找到静态稳定性的示例。EC2 实例启动后，它与数据中心的物理服务器一样可用。它不依赖任何控制平面 API 来保持运行或在重启后重新开始运行。VPC、Amazon S3 存储桶和对象以及 Amazon EBS 卷等其他AWS资源也具有相同的属性。

静态稳定性是一个在AWS设计其服务时根深蒂固的概念，但它也是一种可供客户使用的模式。实际上，以弹性方式使用不同类型AWS服务的大部分最佳实践指南是为生产环境实现静态稳定性。最可靠

的恢复和缓解机制是那些需要最少更改即可实现恢复的机制。预先配置额外容量有助于实现静态稳定性，而不是依赖 EC2 控制平面启动新的 EC2 实例来从出现故障的可用区中恢复。因此，消除恢复路径中对控制平面（实现资源变更的 API）的依赖有助于生成更具弹性的工作负载。有关静态稳定性、控制平面和数据平面的更多详细信息，请参阅 Amazon Builders 库文章使用可用区的静态稳定性。

Summary

AWS在我们的基础架构中利用不同的故障容器来实现故障隔离。核心基础设施故障容器包括分区、区域、可用区、控制平面和数据平面。接下来，我们将研究不同类型的AWS服务，如何在设计中使用这些故障容器，以及如何使用它们构建工作负载以保持弹性。

AWS 服务类型

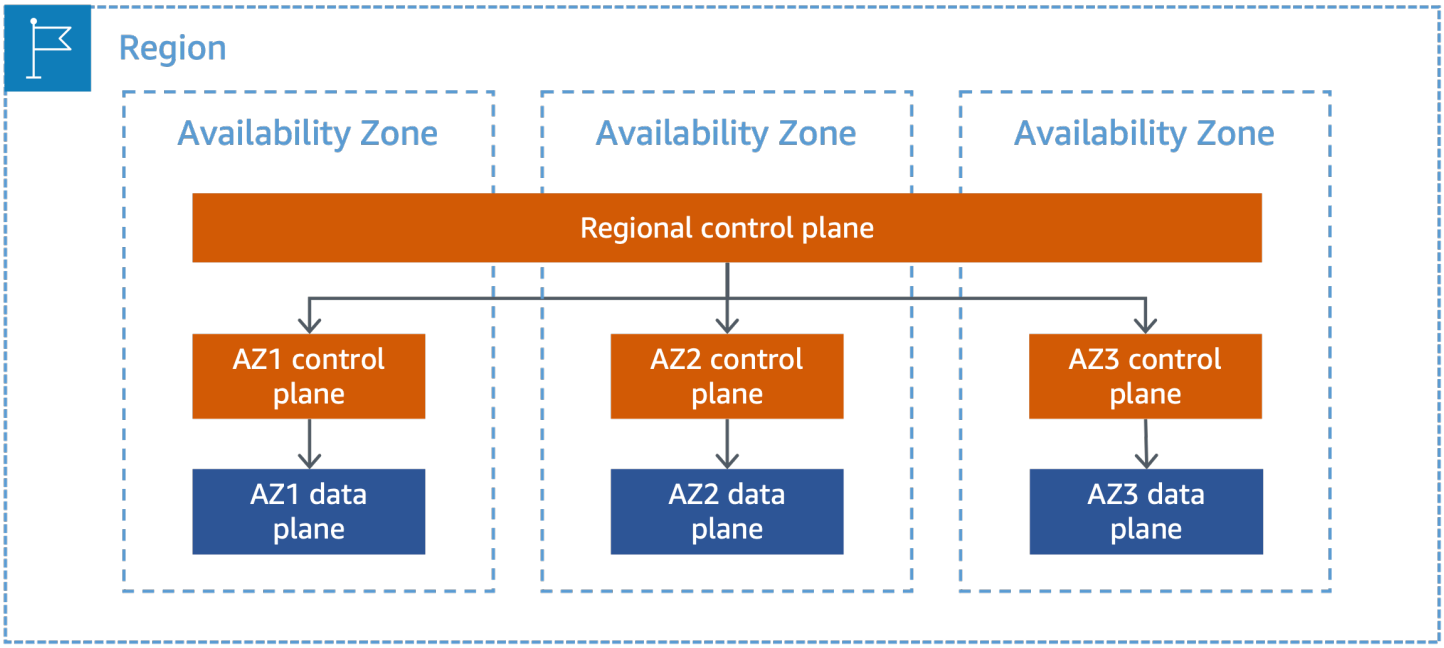
AWS 根据故障隔离边界运营三种不同类别的服务：区域性、区域性和全球性。本节将更详细地描述这些不同类型的服务是如何设计的，以便您可以确定特定服务类型的服务中的故障将如何影响您的工作负载 AWS。它还提供了有关如何设计工作负载以弹性方式使用这些服务的高级指导。对于全球服务，本文档还提供了规范性指导附录 B-边缘网络全球服务指南，可以帮助您防止服务中的附录 A-分区服务指南控制平面损伤对工作负载产生影响，从而帮助您安全地依赖全球 AWS 服务，同时最大限度地减少引入单点故障。

主题

- 区域服务
- 区域服务
- 全球服务

区域服务

可用区独立 (AZI) AWS 允许提供区域服务，例如亚马逊EC2和亚马逊EBS。区域服务是指能够指定将资源部署到哪个可用区的服务。这些服务在一个区域内的每个可用区中独立运行，更重要的是，这些服务在每个可用区中也独立失效。这意味着一个可用区中的服务组件不依赖于其他可用区中的组件。我们可以这样做，因为区域服务具有区域数据平面。在某些情况下（例如使用）EC2，该服务还包括用于区域对齐操作（例如启动实例EC2）的区域控制平面。对于这些服务， AWS 还提供了区域控制平面终端节点，便于与服务进行交互。区域控制平面还提供区域范围的功能，并充当区域控制平面之上的聚合和路由层。如下图所示。



具有区域隔离控制平面和数据平面的分区服务

与单个数据中心相比，可用性区域使客户能够操作更高的可用性、容错性和可扩展性。当一个工作负载使用多个可用区时，可以更好地隔离和保护客户，使其免受影响单个可用区物理基础设施的问题。这可以帮助客户构建跨可用区域的冗余服务，如果架构正确，即使一个可用区出现故障，也能保持正常运行。客户可以利用它AZI来创建高度可用且具有弹性的工作负载。AZI在您的架构中实施可以帮助您快速从孤立的可用区故障中恢复，因为您在一个可用区域中的资源可以最大限度地减少或消除与其他可用区域中资源的交互。这有助于消除跨可用区的依赖关系，从而简化可用区的撤离。有关创建可用区疏散机制的更多详细信息，请参阅高级多可用区弹性模式。此外，您可以通过遵循一些与其自身服务相同的最佳实践 AWS 来进一步利用可用区，例如一次只能将更改部署到单个可用区，或者在可用区的更改失败时将该可用区从服务中删除。

静态稳定性也是多可用区架构的重要概念。对于多可用区架构，您应规划的故障模式之一是可用区的丢失，这可能会导致可用区的容量丢失。如果您没有预先配置足够的容量来应对可用区的丢失，则可能会导致您的剩余容量被当前负载所淹没。此外，你还需要依靠区域服务的控制平面来替换丢失的容量，这可能不如静态稳定的设计那么可靠。在这种情况下，预先配置足够的额外容量可以帮助您保持静态稳定，以防故障域（例如可用区）丢失，因为无需进行动态更改即可继续正常运行。

您可以根据工作负载的需求，选择使用部署在多个可用区域的 auto Scaling EC2 实例组来动态扩展和缩小。对于在几分钟到几十分钟内逐渐发生的使用量变化，自动缩放效果很好。但是，启动新EC2实例需要时间，尤其是在您的实例需要引导（例如安装代理、应用程序二进制文件或配置文件）的情况下。在此期间，您的剩余容量可能会被当前负载所淹没。此外，通过 auto Scaling 部署新实例依赖于EC2控制平面。这就需要权衡取舍：为了保持静态稳定性，以防单个可用区的丢失，您需要在其他可用区中预

置足够的EC2实例来处理已从受损可用区转移的负载，而不是依赖 auto scaling 来配置新实例。但是，预先配置额外容量可能会产生额外费用。

例如，在正常操作期间，假设您的工作负载需要六个实例来为三个可用区的客户流量提供服务。为了在单个可用区出现故障时保持静态稳定，您将在每个可用区部署三个实例，总共部署九个实例。如果单个可用区域的实例出现故障，则还剩下六个实例，并且无需在故障期间预置和配置新实例即可继续为客户流量提供服务。实现EC2容量的静态稳定性需要额外的成本，因为在本例中，您运行的实例数量增加了50%。并非所有可以预配置资源的服务都会产生额外费用，例如预配置 S3 存储桶或用户。您需要权衡实现静态稳定性与超出工作负载所需恢复时间的风险。

AWS Local Zones 和 Outposts 使特定 AWS 服务的数据平面更接近最终用户。这些服务的控制平面位于父区域。您的本地区域或 Outposts 实例将依赖于区域服务，例如EC2您在其中创建本地区域或 Outposts 子网的可用区。EBS它们还将依赖区域控制平面来提供区域服务，例如Elastic Load Balancing (ELB)、安全组和由亚马逊弹性 Kubernetes Service（EKS亚马逊）管理的 Kubernetes 控制平面（如果你使用）。EKS有关 Outposts 的更多信息，请参阅文档以及支持和维护。FAQ使用 Local Zones 或 Outposts 时实现静态稳定性，以帮助提高弹性，以控制飞机损伤或与父区域的网络连接中断。

区域服务

区域服务是在 AWS 多个可用区之上构建的服务，因此客户不必弄清楚如何充分利用区域服务。我们在逻辑上将部署在多个可用区的服务组合在一起，为客户提供单个区域终端节点。亚马逊SQS和亚马逊Dynam oDB 就是区域服务的示例。它们利用可用区域的独立性和冗余性来最大限度地减少基础设施故障，这是可用性和耐久性风险中的一类。例如，Amazon S3 将请求和数据分散到多个可用区，旨在自动从可用区的故障中恢复。但是，您只能与服务的区域终端节点进行交互。

AWS 相信大多数客户可以通过使用依赖区域服务的区域服务或多可用区架构在单个区域实现其弹性目标。但是，某些工作负载可能需要额外的冗余，您可以使用的隔离 AWS 区域 来创建用于高可用性或业务连续性的多区域架构。两者之间的物理和逻辑分离 AWS 区域 避免了它们之间的相关故障。换句话说，与您是EC2客户并可以通过跨可用区部署来从隔离可用区中受益类似，通过跨多个区域进行部署，您也可以获得同样的优势来获得区域服务。这要求您为应用程序实施多区域架构，这可以帮助您抵御区域服务的损害。

但是，实现多区域架构的好处可能很困难；要利用区域隔离，同时又不能在应用程序层面撤消任何东西，需要谨慎行事。例如，如果您要在区域之间对应用程序进行故障切换，则需要在每个区域的应用程序堆栈之间保持严格分离，注意所有应用程序依赖关系，并将应用程序的所有部分一起进行故障转移。使用复杂的、基于微服务的架构实现这一目标，该架构在应用程序之间存在许多依赖关系，需要许多工程和业务团队进行规划和协调。允许单个工作负载自己做出故障转移决策可以降低协调的复杂性，但是由于不同区域之间发生的延迟与单个区域内部的延迟存在显著差异，从而引入了模态行为。

AWS 目前不提供同步跨区域复制功能。使用跨区域异步复制的数据存储库（由提供 AWS）时，当您在区域之间对应用程序进行故障转移时，可能会出现数据丢失或不一致的情况。为了减少可能的不一致性，您需要一个值得信赖的可靠数据协调流程，并且可能需要对工作负载组合中的多个数据存储进行操作，或者您需要愿意接受数据丢失。最后，你需要练习故障转移，才能知道它会在你需要的时候起作用。定期在区域之间轮换应用程序以练习故障转移需要大量的时间和资源投入。如果您决定使用跨区域同步复制的数据存储来支持在多个区域同时运行的应用程序，那么跨越 100 或 1000 英里的此类数据库的性能特征和延迟与在单个区域中运行的数据库有很大不同。这要求您从头开始规划应用程序堆栈，以应对这种行为。它还使两个区域的可用性成为硬性依赖，这可能会导致工作负载的弹性降低。

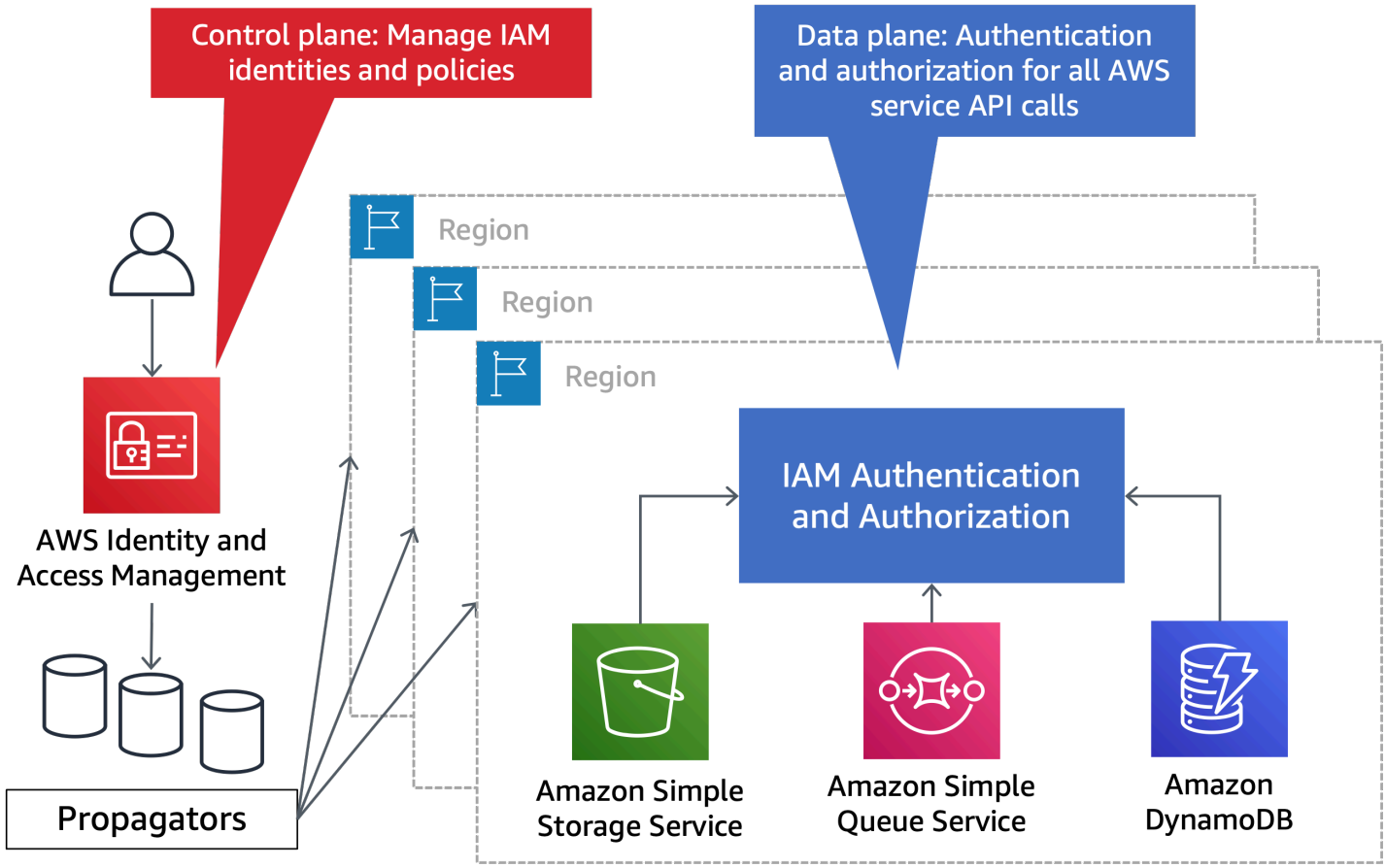
全球服务

除了区域和区域 AWS 服务外，还有一小部分 AWS 服务的控制平面和数据平面不是在每个地区独立存在的。由于它们的资源不是特定于区域的，因此它们通常被称为全球资源。全球 AWS 服务仍然遵循传统的 AWS 设计模式，将控制平面和数据平面分开，以实现静态稳定性。大多数全球服务的显著区别在于，它们的控制平面托管在单个服务器中 AWS 区域，而其数据平面则是全球分布的。根据您选择的配置，有三种不同的全球服务类型和一组看起来像是全球性的服务。

以下各节将确定每种类型的全球服务以及它们的控制平面和数据平面是如何分开的。您可以使用这些信息来指导如何构建可靠的高可用性 (HA) 和灾难恢复 (DR) 机制，而无需依赖全球服务控制平面。这种方法有助于消除架构中的单点故障，避免潜在的跨区域影响，即使您在与托管全球服务控制平面不同的区域中运营也是如此。它还可以帮助您安全地实现不依赖于全局服务控制平面的故障转移机制。

按分区划分的唯一全球服务

每个分区中都存在一些全局 AWS 服务（本 paper 中称为分区服务）。分区服务将其控制平面合而为一 AWS 区域。某些分区服务（例如 AWS Network Manager）仅限控制平面并协调其他服务的数据平面。其他分区服务（例如）有自己的数据平面IAM，该数据平面是隔离的，分布在分区 AWS 区域中的所有分区中。分区服务中的故障不会影响其他分区。在`aws`分区中，IAM服务的控制平面位于`us-east-1`区域中，分区的每个区域都有隔离的数据平面。分区服务在和`aws-cn`分区中也有独立的控制平面`aws-us-gov`和数据平面。的控制平面和数据平面的分离如下图所示。IAM



IAM具有单个控制平面和区域化数据平面

以下是分区服务及其控制平面在aws分区中的位置：

- AWS IAM (us-east-1)
- AWS Organizations (us-east-1)
- AWS 账户管理 (us-east-1)
- Route 53 应用程序恢复控制器 (ARCus-west-2) ()-此服务仅存在于aws分区中
- AWS 网络管理器 (us-west-2)
- 53 号公路私人 DNS (us-east-1)

如果这些服务控制平面中的任何一个发生影响可用性的事件，则可能无法使用这些服务提供的 CRUDL-type 操作。因此，如果您的恢复策略依赖于这些操作，那么对控制平面或托管控制平面的区域的可用性影响将降低成功恢复的机会。 附录 A-分区服务指南提供了在恢复期间消除对全局服务控制平面依赖的策略。

> **建议**
>
> 在恢复路径中，不要依赖分区服务的控制平面。相反，请依赖这些服务的数据平面操作。附录A-分区服务指南有关应如何设计分区服务的更多详细信息，请参阅。

边缘网络中的全球服务

下一组全球 AWS 服务在aws分区中有一个控制平面，并将其数据平面托管在全局接入点 (PoP) 基础架构中（ AWS 区域 也可能如此）。 PoPs 可以从任何分区的资源以及互联网访问托管的数据平面。例如，Route 53 `us-east-1` 在该地区运营其控制平面，但其数据平面分布 PoPs 在全球数百个以及每个区域 AWS 区域 （以支持该区域DNS内的公共 53 号公路和私有路线）。Route 53 运行状况检查也是数据平面的一部分，从aws分区 AWS 区域 中的 8 个开始执行。客户端可以从互联网上的任何地方DNS使用 Route 53 公共托管区域进行解析 GovCloud，包括其他分区，例如 AWS 虚拟私有云 (VPC)。以下是全球边缘网络服务及其在aws分区中的控制平面位置：

- 53 号公路 DNS (`us-east-1`)
- 亚马逊 CloudFront (`us-east-1`)
- AWS WAF 经典 fo CloudFront r (`us-east-1`)
- AWS WAF 对于 CloudFront (`us-east-1`)
- 适用于 (ACM) 的 Amazon Certifice Manager CloudFront (`us-east-1`)
- AWS全球加速器 (AGA) (`us-west-2`)
- AWS Shield Advanced (`us-east-1`)

如果您对EC2实例或弹性 IP 地址使用运行AGA状况检查，则使用 Route 53 运行状况检查。创建或更新AGA健康检查将取决于中的 Route 53 控制平面`us-east-1`。运行AGA状况检查的执行利用 Route 53 运行状况检查数据平面。

在影响托管这些服务的控制平面的区域或影响控制平面本身的故障时，您可能无法使用这些服务提供的CRUDL-type操作。如果您在恢复策略中依赖这些操作，那么与仅依赖这些服务的数据平面相比，该策略成功的可能性可能要小。

> **建议**
>
> 在恢复路径中，不要依赖边缘网络服务的控制平面。相反，请依赖这些服务的数据平面操作。有关如何在边缘网络中设计全球服务的更多详细信息，请参阅附录 B-边缘网络全球服务指南。

全球单一区域运营

最后一个类别由具有全球影响范围的服务中的特定控制平面操作组成，而不是像前面的类别那样由整个服务组成。当您与指定区域中的地区和区域服务进行交互时，某些操作对与资源所在位置不同的单个区域有潜在的依赖关系。这些服务与仅在单个地区提供的服务不同；有关这些服务的列表，请参阅。附录C-单区域服务

在影响底层全局依赖关系的故障期间，您可能无法使用依赖操作的 CRUDL-type 操作。如果您在恢复策略中依赖这些操作，那么与仅依赖这些服务的数据平面相比，该策略成功的可能性可能要小。恢复策略应避免依赖这些操作。

以下是其他服务可能依赖的服务列表，这些服务具有全局范围：

- 53 号公路

  一些 AWS 服务创建的资源可提供特定于资源的DNS名称。例如，当您配置 Elastic Load Balancer (ELB) 时，该服务会在 Route 53 中为创建公共DNS记录和运行状况检查ELB。这依赖于 53 号公路的控制飞机`us-east-1`。您使用的其他服务可能还需要预置ELB、创建公共 Route 53 DNS 记录或创建 Route 53 运行状况检查作为其控制平面工作流程的一部分。例如，配置亚马逊API网关RESTAPI资源、亚马逊关系数据库服务 (AmazonRDS) 数据库或亚马逊 OpenSearch 服务域都会导致在 Route 53 中创建DNS记录。以下是服务列表，这些服务的控制平面依赖于 Route 53 控制平面`us-east-1`来创建、更新或删除DNS记录、托管区域和/或创建 Route 53 运行状况检查。此列表并不详尽；它旨在重点介绍一些最常用的服务，这些服务的创建、更新或删除资源的控制平面操作取决于 Route 53 控制平面：

  - 亚马逊 API Gateway REST 和 HTTP APIs
  - 亚马逊RDS实例
  - 亚马逊 Aurora 数据库
  - Amazon ELB 负载均衡器
  - AWS PrivateLink VPC端点
  - AWS Lambda URLs
  - Amazon ElastiCache
  - 亚马逊 OpenSearch 服务
  - Amazon CloudFront
  - Amazon MemoryDB
  - Amazon Neptune
  - 亚马逊 DynamoDB 加速器 () DAX

- AGA
- 带有DNS基于服务发现功能的亚马逊弹性容器服务 (AmazonECS)（使用管理 Route 53DNS）AWS Cloud Map API
- 亚马逊 EKS Kubernetes 控制飞机

  值得注意的是，主机名等VPCDNS服务独立存在于每个EC2 AWS 区域 主机名中，不依赖于 Route 53 控制平面。为VPCDNS服务中的EC2实例 AWS 创建的记录（例如、`ip-10-0-10.ec2.internal``ip-10-0-1-5.compute.us-west-2.compute.internal`、`i-0123456789abcdef.ec2.internal`、`i-0123456789abcdef.us-west-2.compute.internal`、和）不依赖于中的 Route 53 控制平面`us-east-1`。

  > **建议**
  >
  > 不要依赖创建、更新或删除恢复路径中需要创建、更新或删除 Route 53 资源记录、托管区域或运行状况检查的资源。预先配置这些资源，例如ELBs，以防止在恢复路径中依赖于 Route 53 控制平面。

- Amazon S3

  以下 Amazon S3 控制平面操作与`aws`分区`us-east-1`中的底层依赖关系。影响 Amazon S3 或其他服务的故障`us-east-1`可能会导致其他地区的这些控制平面操作受损：

```
PutBucketCors
DeleteBucketCors
PutAccelerateConfiguration
PutBucketRequestPayment
PutBucketObjectLockConfiguration
PutBucketTagging
DeleteBucketTagging
PutBucketReplication
DeleteBucketReplication
PutBucketEncryption
DeleteBucketEncryption
PutBucketLifecycle
DeleteBucketLifecycle
PutBucketNotification
PutBucketLogging
DeleteBucketLogging
```

```
PutBucketVersioning
PutBucketPolicy
DeleteBucketPolicy
PutBucketOwnershipControls
DeleteBucketOwnershipControls
PutBucketAcl
PutBucketPublicAccessBlock
DeleteBucketPublicAccessBlock
```

Amazon S3 多区域接入点 (MRAP) 的控制平面仅托管在中 us-west-2，创建、更新或删除请求直接MRAPs针对该区域。的控制平面MRAP还依赖于 AGA in us-west-2、Route 53 in us-east-1 以及配置MRAP为从ACM中提供内容的每个区域。您不应依赖恢复路径或您自己系统的数据平面中MRAP控制平面的可用性。这与MRAP故障转移控制不同，后者用于为中的每个存储段指定主动或被动路由状态。MRAPAPIs它们分为五 AWS 区域个托管，可用于使用服务的数据平面有效地转移流量。

此外，Amazon S3 存储桶名称是全球唯一的us-east-1，所有对CreateBucket和的调用都DeleteBucketAPIs依赖于aws分区中的名称以确保名称的唯一性，即使API调用指向要在其中创建存储桶的特定区域。最后，如果您有关键的存储桶创建工作流程，则不应依赖存储桶名称的任何特定拼写是否可用，尤其是那些遵循明显模式的拼写。

> **建议**
>
> 不要依赖删除或创建新的 S3 存储桶或更新 S3 存储桶配置作为恢复路径的一部分。使用必要的配置预置所有必需的 S3 存储桶，这样您就无需进行更改即可从故障中恢复。这种方法MRAPs也适用于。

- CloudFront

  Amazon API Gateway 提供边缘优化的API端点。创建这些端点取决于中的 CloudFront控制平面us-east-1，以便在网关终端节点前面创建分发。

> **建议**
>
> 不要依赖创建新的边缘优化的API网关端点作为恢复路径的一部分。预配置所有必需的API网关终端节点。

本节中讨论的所有依赖关系都是控制平面操作，而不是数据平面操作。如果您的工作负载配置为静态稳定，则这些依赖关系不应影响您的恢复路径，请记住，静态稳定性需要额外的工作或服务才能实现。

使用默认全局端点的服务

在少数情况下， AWS 服务会提供默认的全局端点，例如 AWS 安全令牌服务 (AWS STS)。其他服务可能会在其默认配置中使用此默认的全局端点。这意味着您正在使用的区域服务可能对单个服务具有全球依赖性 AWS 区域。以下详细信息说明了如何删除对默认全局终端节点的意外依赖关系，这将有助于您以区域方式使用该服务。

AWS STS: STS 是一项 Web 服务，允许您为IAM用户或经过身份验证的用户（联合用户）申请临时的、有限权限的证书。STS AWS 软件开发套件 (SDK) 和命令行界面 (CLI) 中的用法默认为`us-east-1`。该STS服务还提供区域终端节点。这些终端节点在默认情况下也处于启用状态的区域中处于启用状态。您可以随时通过配置SDK或CLI遵循以下说明来利用这些优势：AWS STS区域化终端节点。使用 Sigv4a 还需要从区域终端节点请求临时证书。STS您不能使用全局STS终端节点执行此操作。

> **建议**
>
> 更新您的SDK和CLI配置以使用区域终STS端节点。

安全断言标记语言 (SAML) 登录：所有SAML服务都存在。 AWS 区域要使用此服务，请选择相应的区域SAML终端节点，例如 https://us-west-2.signin.aws.amazon.com/saml。您必须更新信任策略和身份提供商 (IdP) 中的配置才能使用区域终端节点。有关具体细节，请参阅AWS SAML文档。

如果您使用的 IdP 也托管在其上 AWS，则它们也有可能在 AWS 故障事件期间受到影响。这可能导致您无法更新 IdP 配置，或者可能无法完全联合。您应该预先配置 “破碎玻璃” 用户，以防您的 IdP 受损或不可用。有关如何以附录 A-分区服务指南静态稳定的方式创建 breakglass 用户的详细信息，请参阅。

> **建议**
>
> 更新您的IAM角色信任政策以接受来自多个区域的SAML登录。在故障期间，如果您的首选SAML终端节点受损，请更新您的 IdP 配置以使用其他区域终端节点。创建漏洞用户，以防您的 IdP 受损或不可用。

AWS IAMIdentity Center：Identity Center 是一项基于云的服务，可轻松集中管理对客户 AWS 账户和云应用程序的单点登录访问。身份中心必须部署在您选择的单个区域。但是，该服务的默认行为是使用托管在中的全局SAML终端节点 (https://signin.aws.amazon.com/saml) `us-east-1`。如果您已将 Identity Center 部署到不同的服务器中 AWS 区域，则应更新每个权限集URL的中继状态，使其定位到与身份中心部署相同的区域控制台终端节点。例如，如果您将 Identity Center 部署到中`us-west-2`，则应将权限集的中继状态更新为使用 https://us-west-2.console.aws.amazon.com。这将`us-east-1`从您的身份中心部署中移除对的任何依赖。

此外，由于 IAM Identity Center 只能部署到单个区域，因此您应预先配置 “破碎玻璃” 用户，以防部署受损。有关如何以附录 A-分区服务指南静态稳定的方式创建 breakglass 用户的详细信息，请参阅。

> **建议**
>
> 在 Ident IAM ity Center 中设置权限集的中继状态URL，使其与部署服务的区域相匹配。如果您的 Ident IAM ity Center 部署不可用，请创建漏洞用户。

Amazon S3 存储镜头：存储镜头提供了一个名为的默认控制面板 default-account-dashboard。仪表板配置及其相关指标存储在中`us-east-1`。您可以通过为仪表板配置和指标数据指定主区域，在其他区域创建其他控制面板。

> **建议**
>
> 如果在中出现影响服务的故障期间，您需要来自默认 S3 Storage Lens 仪表板的数据`us-east-1`，请在备用主区域创建其他仪表板。您也可以复制您在其他区域中创建的任何其他自定义仪表板。

全球服务摘要

全球服务的数据平面采用与区域 AWS 服务相似的隔离和独立原则。影响某个区域的数据平面的故障不会影响另一个 AWS 区域区域IAM中该IAM数据平面的运行。同样，影响 PoP 中 53 号公路数据平面的故障不会影响其余部分 53 号公路数据平面的运行。 PoPs因此，我们必须考虑的是影响控制平面运行区域或影响控制平面本身的服务可用性事件。由于每个全局服务只有一个控制平面，因此影响该控制平面的故障可能会对 CRUDL-type 操作（这些配置操作通常用于设置或配置服务，而不是直接使用服务）产生跨区域影响。

设计工作负载以弹性方式使用全球服务的最有效方法是使用静态稳定性。在故障场景中，设计工作负载时无需使用控制平面进行更改以减轻影响或故障转移到其他位置。有关如何附录 A-分区服务指南利用这些类型的全球服务来消除控制平面依赖关系并消除单点故障的规范性指导，请参阅和。附录 B-边缘网络全球服务指南如果您需要控制平面操作中的数据进行恢复，请将这些数据缓存在可通过其数据平面访问的数据存储中，例如 Sy AWS stems Manager 参数存储（SSM参数存储）参数、DynamoDB 表或 S3 存储桶。为了实现冗余，您也可以选择将该数据存储在其他区域。例如，按照 Route 53 应用程序恢复控制器 (ARC) 的最佳实践，您应该对五个区域群集终端节点进行硬编码或添加书签。在发生故障事件期间，您可能无法访问某些API操作，包括未托管在极其可靠的数据平面集群上的 Route 53 ARC API 操作。您可以使用`DescribeClusterAPI`操作列出 Route 53 ARC 集群的终端节点。

以下是一些最常见的错误配置或反模式的摘要，这些错误配置或反模式引入了对全局服务控制平面的依赖性：

- 对 Route 53 记录进行更改，例如更新 A 记录的值或更改加权记录集的权重，以执行故障转移。
- 在故障转移期间创建或更新IAM资源，包括IAM角色和策略。这通常不是故意的，但可能是由于故障转移计划未经测试所致。
- 依靠 IAM Identity Center 让操作员在故障事件期间访问生产环境。
- 将IAM身份中心部署到其他区域`us-east-1`后，依靠默认的 Identity Center 配置来使用控制台。
- 更改AGA流量拨号权重以手动执行区域故障转移。
- 更新 CloudFront 分配的源配置，使其无法从受损的来源中移开。
- 配置灾难恢复 (DR) 资源，例如ELBs故障事件期间的RDS实例，这些资源依赖于在 Route 53 中创建DNS记录。

以下是本节中提供的以弹性方式使用全球服务的建议摘要，这将有助于防止以前的常见反模式。

建议摘要

在恢复路径中，不要依赖分区服务的控制平面。相反，请依赖这些服务的数据平面操作。附录A-分区服务指南有关应如何设计分区服务的更多详细信息，请参阅。

在恢复路径中，不要依赖边缘网络服务的控制平面。相反，请依赖这些服务的数据平面操作。有关如何在边缘网络中设计全球服务的更多详细信息，请参阅附录 B-边缘网络全球服务指南。

不要依赖创建、更新或删除恢复路径中需要创建、更新或删除 Route 53 资源记录、托管区域或运行状况检查的资源。预先配置这些资源，例如ELBs，以防止在恢复路径中依赖于 Route 53 控制平面。

不要依赖删除或创建新的 S3 存储桶或更新 S3 存储桶配置作为恢复路径的一部分。使用必要的配置预置所有必需的 S3 存储桶，这样您就无需进行更改即可从故障中恢复。这种方法MRAPs也适用于。

不要依赖创建新的边缘优化的API网关端点作为恢复路径的一部分。预配置所有必需的API网关终端节点。

更新您的SDK和CLI配置以使用区域终STS端节点。

更新您的IAM角色信任政策以接受来自多个区域的SAML登录。在故障期间，如果您的首选SAML终端节点受损，请更新您的 IdP 配置以使用其他区域终端节点。创建漏洞用户，以防您的 IdP 受损或不可用。

在 Ident IAM ity Center 中设置权限集的中继状态URL，使其与部署服务的区域相匹配。如果您的 Identity Center 部署不可用，请创建漏洞用户。

如果在中出现影响服务的故障期间，您需要来自默认 S3 Storage Lens 仪表板的数据`us-east-1`，请在备用主区域创建其他仪表板。您也可以复制您在其他区域中创建的任何其他自定义仪表板。

结论

AWS为故障隔离边界提供了几种不同的结构。您应该考虑如何架构区域、区域和全球服务，以及在控制平面受损期间对工作负载和工作负载恢复能力的潜在影响。静态稳定性是您在使用AWS服务时避免控制平面依赖关系并创建可靠且有弹性的 HA 和 DR 机制的主要方法之一。

附录 A-分区服务指南

对于分区服务，应实现静态稳定性，以便在AWS服务控制平面受损期间保持工作负载的弹性。以下内容提供了规范性指导，说明如何考虑对分区服务的依赖以及在控制平面损伤期间哪些会起作用和可能不起作用。

AWS Identity and Access Management (IAM)

AWS Identity and Access Management(IAM) 控制平面由所有公共 IAM API 组成（包括 Access Advisor，但不包括 Access Anywhere 的 Access Any 这包括`CreateRole`、、`AttachRolePolicyChangePasswordUpdateSAMLProvider`、和等操作`UpdateLoginProfile`。IAM 数据平面为每个AWS 区域平台中的 IAM 主体提供身份验证和授权。在控制平面受损期间，IAM 的 CRUDL 类型操作可能不起作用，但现有主体的身份验证和授权将继续有效。STS 是一项独立于 IAM 且不依赖于 IAM 控制平面的纯数据平面服务。

这意味着，当你计划依赖于 IAM 时，你不应该在恢复路径中依赖 IAM 控制平面。例如，对于 “break-glass” 管理员用户，静态稳定的设计是创建一个附加适当权限的用户，设置密码并配置访问密钥和私有访问密钥，然后将这些凭证锁定在物理或虚拟保管库中。在紧急情况下需要时，从保管库检索用户凭证并根据需要使用它们。一种non-statically-stable设计是在出现故障时为用户进行配置，或者预先配置用户，但仅在需要时附加管理员策略。这些方法将取决于 IAM 控制平面。

AWS Organizations

AWS Organizations控制平面由所有公共Organizations API 组成，如`AcceptHandshakeAttachPolicyCreateAccountCreatePolicy`、、和`ListAccounts`。没有专用的数据平面AWS Organizations。它为 IAM 等其他服务协调数据平面。在控制平面受损期间，Organizations 的 CRUDL 类型的操作可能不起作用，但是服务控制策略 (SCP) 和标签策略等策略将继续有效，并作为 IAM 授权过程的一部分进行评估。Organizations 支持的其他AWS服务中的委托管理员权能和多账户功能也将继续发挥作用。

这意味着，在规划依赖关系时，在恢复路径中不应依赖 AWS Organizations Organizations 控制平面。取而代之的是，在恢复计划中实现静态稳定性。例如，一种non-statically-stable方法可能是更新 SCP 以AWS 区域通过`aws:RequestedRegion`条件取消对允许的限制，或者为特定 IAM 角色启用管理员权限。这依赖于Organizations 控制平面来进行这些更新。更好的方法是使用会话标签来授予管理员权限的使用。您的身份提供商 (IdP) 可以包含可以根据`aws:PrincipalTag`条件进行评估的会话标签，这可以帮助您动态配置某些主体的权限，同时帮助您的 SCP 保持静态。这消除了对控制平面的依赖关系，仅使用数据平面操作。

AWS 账户管理

AWS账户管理控制平面托管在 us-east-1 中，由所有用于管理的公共 API 组成AWS 账户，例如和。`GetContactInformation` `PutContactInformation`它还包括AWS 账户通过管理控制台创建或关闭新的。`CloseAccount`、`CreateAccount``CreateGovCloudAccount`、和的 API `DescribeAccount` 是控制平面的一部分，AWS Organizations控制平面也托管在 us-east-1 中。此外，在外部创建GovCloud账户AWS Organizations依赖于 us-east-AWS 账户 1 中的管理控制平面。此外，GovCloud账户必须以 1:1 的比例链接到`aws`分区AWS 账户中的。在`aws-cn`分区中创建账户的 us-eaaast-1 不依赖于 us-eaaast-1 的 的数据平面AWS 账户是账户本身。在控制平面受损期间，CRUDL 类型的操作（例如创建新账户或获取和更新联系信息）AWS 账户可能不起作用。IAM 政策中对账户的引用将继续有效。

这意味着，当你计划依赖AWS账户管理时，在恢复路径中不应依赖账户管理控制平面。尽管账户管理控制平面不提供您在恢复情况下通常使用的直接功能，但有时候您可能会这样做。例如，静态稳定的设计是预先配置故障转移所需的所有资源AWS 账户。一种non-statically-stable设计是在故障事件发生AWS 账户期间创建新的资源来托管您的灾难恢复资源。

Route 53 应用程序恢复控制器

Route 53 ARC 的控制平面由用于恢复控制和恢复就绪的 API 组成，具体参见：Amazon Route 53 应用程序恢复控制器终端节点和配额。您可以使用控制平面管理就绪检查、路由控制和集群操作。ARC 的数据平面是您的恢复集群，它管理 Route 53 运行状况检查查询的路由控制值，还实施安全规则。Route 53 ARC 的数据层面功能可通过您的恢复集群 API 进行访问，例如`https://aaaaaaaa.route53-recovery-cluster.eu-west-1.amazonaws.com`。

这意味着你不应该在恢复路径中依赖 Route 53 ARC 控制平面。有两种最佳做法可帮助实施本指南：

- 首先，将五个区域集群终端节点加入书签或硬编码。这样就无需在故障转移场景中使用DescribeCluster控制平面操作来发现端点值。
- 其次，使用 Route 53 ARC 集群 API，使用 CLI 或 SDK 对路由控制进行更新，而不是AWS 管理控制台。这消除了管理控制台对故障转移计划的依赖关系，并确保它仅依赖于数据平面操作。

AWS 网络管理器

AWS网络管理器服务主要是托管在 us-west-2 中的仅限控制飞机的系统。其目的是跨AWS 账户区域和本地位置集中管理 WAN 核心网络和 Transit Gateway 网络的 Tr AWS ansit Gateway 网络。AWS Cloud它还会汇总您在 us-west-2 中的云广域网指标，也可以通过数据平面访问这些指标。CloudWatch

如果 Network Manager 受到损害，则其协调的服务的数据平面不会受到影响。us-we CloudWatch ast-2 的 Cloud WAN 的 us-weast-2 的 WAN 如果您想要历史指标数据，例如每个区域的进出字节，以了解在影响 us-west-2 的故障期间或出于其他运营目的可能会有多少流量转移到其他区域，则可以直接从CloudWatch控制台将这些指标导出为 CSV 数据或使用以下方法：将亚马逊CloudWatch指标发布到 CSV 文件。数据可以在`AWS/Network Manager`命名空间下找到，您可以按自己选择的时间表执行此操作，然后将其存储在 S3 或您选择的其他数据存储中。要实施静态稳定的恢复计划，请勿使用 AWS Network Manager 对网络进行更新，也不要依赖其控制平面操作中的数据进行故障切换输入。

53 号路由私有 DNS

每个分区都支持 Route 53 私有托管区域；但是，Route 53 中私有托管区域和公共托管区域的注意事项是相同的。请参阅附录 B-边缘网络全球服务指南中的 Amazon Route 53。

附录 B-边缘网络全球服务指南

对于边缘网络全球服务，应实现静态稳定性，以便在AWS服务控制平面受损期间保持工作负载的弹性。

Route 53

Route 53 控制平面由所有公共 Route 53 API 组成，涵盖托管区域、记录、运行状况检查、DNS 查询日志、可重复使用的委托集、流量策略和成本分配标签等功能。它托管在 us-east-1。数据层面是权威 DNS 服务，它运行在 200 多个接入点 POP 位置，根据您的托管区域和运行状况检查数据应答 DNS 查询。AWS 区域此外，Route 53 有一个用于运行状况检查的数据平面，它也是一项分布在多个服务器上的全球分布式服务。AWS 区域该数据层面可执行运行状况检查、汇总结果并将它们传送到 Route 53 公有和私有 DNS 和 AGA 的数据层面。在控制平面受损期间，Route 53 的 CRUDL 类操作可能无法正常运行，但是 DNS 解析和运行状况检查以及因运行状况检查变化而导致的路由更新将继续有效。

这意味着，在规划对 Route 53 的依赖关系时，在恢复路径中不应依赖 Route 53 控制平面。例如，静态稳定的设计是使用运行状况检查状态在区域之间执行故障转移或撤出可用区。您可以使用 R oute 53 应用程序恢复控制器 (ARC) 路由控制来手动更改运行状况检查的状态并更改对 DNS 查询的响应。您可以根据自己的要求实现与 ARC 提供的模式相似的模式。使用 Route 53 创建灾难恢复机制和高级多可用区弹性模式运行状况检查断路器部分概述了其中一些模式。如果您选择使用多区域 DR 计划，请预先配置需要创建 DNS 记录的资源，例如 ELB 和 RDS 实例。一种non-statically-stable设计是通过 `ChangeResourceRecordSets` API 更新 Route 53 资源记录的值、更改加权记录的权重或创建新记录以执行故障转移。这些方法取决于 53 号公路控制平面。

Amazon CloudFront

亚马逊CloudFront控制平面由所有用于管理分发的公共 CloudFront API 组成，托管在 us-east-1 中。数据平面是边缘网络PoPs中的分布本身。它对您的原始内容执行请求处理、路由和缓存。在控制平面受损期间，CRUDL 类型的操作CloudFront（包括失效请求）可能不起作用，但您的内容将继续被缓存和提供服务，原始故障转移将继续有效。

这意味着，当你计划依赖关系时CloudFront，你不应该在恢复路径中依赖CloudFront控制平面。例如，静态稳定的设计是使用自动原点故障转移来减轻损坏对您的某个来源的影响。您也可以选择使用 Lamda @Edge 构建原始负载平衡或故障转移，有关该模式的更多详细信息，请参阅使用 Amazon 的高可用性应用程序的三种高级设计模式CloudFront以及使用 Amazon CloudFront 和 Amazon S3 构建多区域活跃地理邻近应用程序。一种non-statically-stable设计是手动更新发行版的配置以应对源故障。这种方法将取决于CloudFront控制平面。

亚马逊Certificate Manager

如果您在CloudFront发行版中使用自定义证书，则还依赖于 ACM。在您的CloudFront发行版中使用的是来自us-east-1 区域内的 ACM 控制层面。在控制层面损坏期间，您在分发中配置的现有证书将继续有效，证书会自动续订。不要依赖更改发行版的配置或创建新证书作为恢复路径的一部分。

AWSWeb 应用程序防火墙 (WAF) 和 WAF 经典版

如果您在CloudFront发行版中AWS WAF使用，则依赖于 WAF 控制平面，该平面也托管在 us-east-1 区域。在控制平面受损期间，配置的 Web 访问控制列表 (ACL) 及其相关规则将继续发挥作用。不要依赖更新 WAF Web ACL 作为恢复路径的一部分。

AWS Global Accelerator

AGA 控制平面由所有公共 AGA API 组成，托管在 us-west-2 中。数据平面是 AGA 向您的注册端点提供的 anycast IP 地址的网络路由。AGA 还利用 Route 53 运行状况检查来确定您的 AGA 终端节点（作为 Route 53 数据平面的一部分）的运行状况。在控制飞机损伤期间，AGA 的 CRUDL 类操作可能不起作用。路由到您的现有终端节点，以及用于将流量路由或转移到其他终端节点和终端节点组的现有运行状况检查、流量拨号和终端节点权重配置将继续有效。

这意味着，当你计划依赖于 AGA 时，你不应该在恢复路径中依赖 AGA 控制平面。例如，静态稳定的设计是利用已配置的运行状况检查的状态来排除不健康的端点。有关此配置的示例，请参阅AWS使用AWS全球加速器中的部署多区域应用程序。一种non-statically-stable设计是在受损期间修改 AGA 流量拨号百分比、编辑端点组或从端点组中删除端点。这些方法将取决于 AGA 控制平面。

亚马逊Shield

亚马逊 Shield Advanced 控制平面由所有公共 Shield Advanced API 组成，托管在 us-east-1。这包括`CreateProtection`、、`CreateProtectionGroupAssociateHealthCheckDesribeDRTAccess`、和等功能`ListProtections`。数据层面是 Shield Advanced 提供的 DDoS 防护，也是Shield Advanced指标的创建。如果你配置了 Route 53 生命值检查（这是 Route 53 数据平面的一部分），Shield Advanced 还会使用这些检查。在控制平面受损期间，Shield Advanced 的 CRUDL 类操作可能无法运行，但是为您的资源配置的 DDoS 保护以及对运行状况检查变更的响应将继续运行。

这意味着你不应该在恢复路径中依赖 Shield Advanced 控制平面。尽管 Shield Advanced 控制平面不提供你通常在恢复情况下使用的直接功能，但有时候你可能会这样做。例如，静态稳定的设计是将您的灾难恢复资源配置为保护组的一部分并对其进行相关的运行状况检查，而不是在故障发生后配置该保护。这样可以防止依赖 Shield Advanced 控制平面进行恢复。

附录 C-单区域服务

以下是仅在单个区域中可用的服务或该服务中的特定功能（在服务名称后的括号中列出）的列表。当您需要规划对这些服务的控制平面和数据平面的依赖时，为其他全局服务提供的实现静态稳定性的指导同样适用于这些服务。

- Alexa for Business
- AWS Marketplace（AWS Marketplace 目录API、 AWS Marketplace 商务分析、 AWS Marketplace 授权服务）
- B@@ illing and Cost Managem ent（AWS Cost Explorer、 AWS 成本和使用情况报告、 AWS 预算、Savings Plans）
- AWS BugBust
- Amazon Mechanical Turk
- Amazon Chime
- Amazon Chime SDK（PSTN音频、消息、身份）
- AWS Chatbot
- AWS DeepRacer
- AWS Device Farm
- Amazon GameSparks

贡献者

本文档的贡献者包括：

- 迈克尔·哈肯，Amazon Web Services 首席解决方案架构师

文档修订

要获得有关文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
小修订	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 9 日
初次出版	白皮书已发布。	2022 年 11 月 16 日

AWS 术语表

有关最新的 AWS 术语，请参阅 AWS 词汇表参考 中的 AWS 词汇表。

版权声明

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AWS的产品供应和做法，如有更改，恕不另行通知；(c) 不构成其关联公司、供应商或许可方的任何承诺或保证。AWS AWS产品或服务 “按原样” 提供，不提供任何形式的明示或暗示的担保、陈述或条件。对客户的责任和责任受AWS协议控制，本文档既不属于也不修改与其客户AWS之间的任何协议。AWS

© 2022 Amazon Web Services 公司或其关联公司。保留所有权利。

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。