欢迎学习模块 14：灾难规划。

本模块包含以下章节：

1. 架构需求
2. 灾难规划策略
3. 灾难恢复模式

该模块还包括一个指导实验，您将在实验中启用 Amazon S3 跨区域复制。您将配置文件网关并将文件共享挂载到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上。

最后，您需要完成一份知识测验，以测试您对本模块中涵盖的关键概念的理解程度。

模块目标

学完本模块后，您应该能够：

- 确定灾难规划策略
- 定义恢复点目标 (RPO) 和恢复时间目标 (RTO)
- 描述备份和灾难恢复的四种常见模式以及实施方法
- 使用 AWS Storage Gateway 实现本地到云备份解决方案

学完本模块后，您应该能够：

- 确定灾难规划策略
- 定义恢复点目标 (RPO) 和恢复时间目标 (RTO)
- 描述备份和灾难恢复的四种常见模式以及实施方法
- 使用 AWS Storage Gateway 实现本地到云备份解决方案

模块 14：灾难规划

第 1 节：架构需求

介绍第 1 节：架构需求。

咖啡馆业务要求

如果咖啡馆的基础设施不可用，员工必须能够在企业可以接受的时间内让应用程序重新运行。他们需要一种支持灾难恢复计划的架构，同时也能优化成本。

到目前为止，咖啡馆已经实施了几个可在 AWS 上运行的应用程序。他们还在 AWS 云中存储大量业务关键型数据。Sofía 意识到如果咖啡馆的基础设施不可用，则他们必须能够在企业可以接受的时间内让应用程序重新运行和可访问。目前，该咖啡馆的员工尚未制定任何全面的灾难恢复计划。

Sofía 向 Frank 和 Martha 提出了这种担忧。他们都同意，将备份和灾难恢复计划落实到位非常重要。他们的目标是实施一种支持灾难恢复时间目标的架构，同时还能优化成本。他们还同意，随着收入的增长，他们将能够负担得起支持较短恢复时间目标的解决方案。

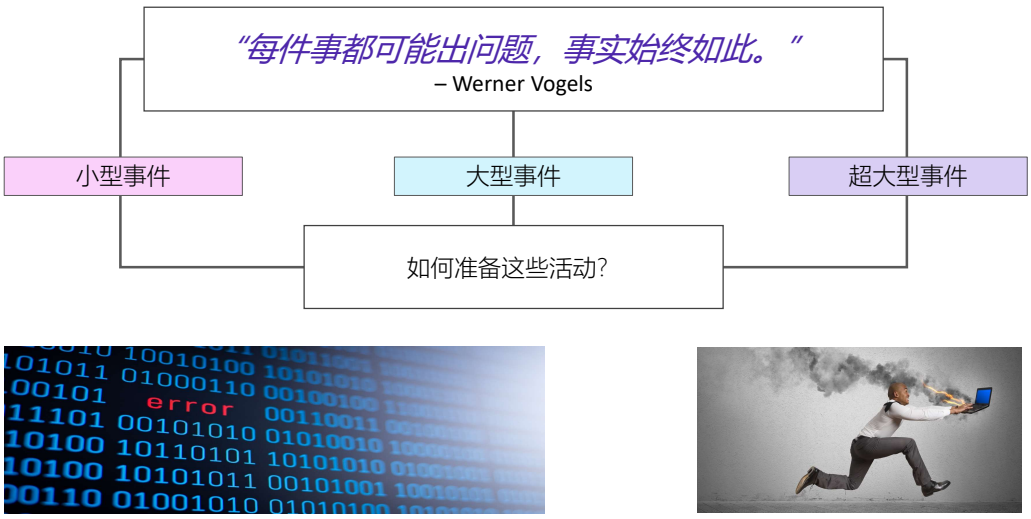
在本模块中，您将了解支持数据备份和灾难恢复的主要 AWS 服务功能。了解这些功能后，您应该能够帮助咖啡厅满足这一基本业务要求。

模块 14：灾难规划

第 2 节：灾难规划策略

介绍第 2 节：灾难规划策略。

针对故障的规划



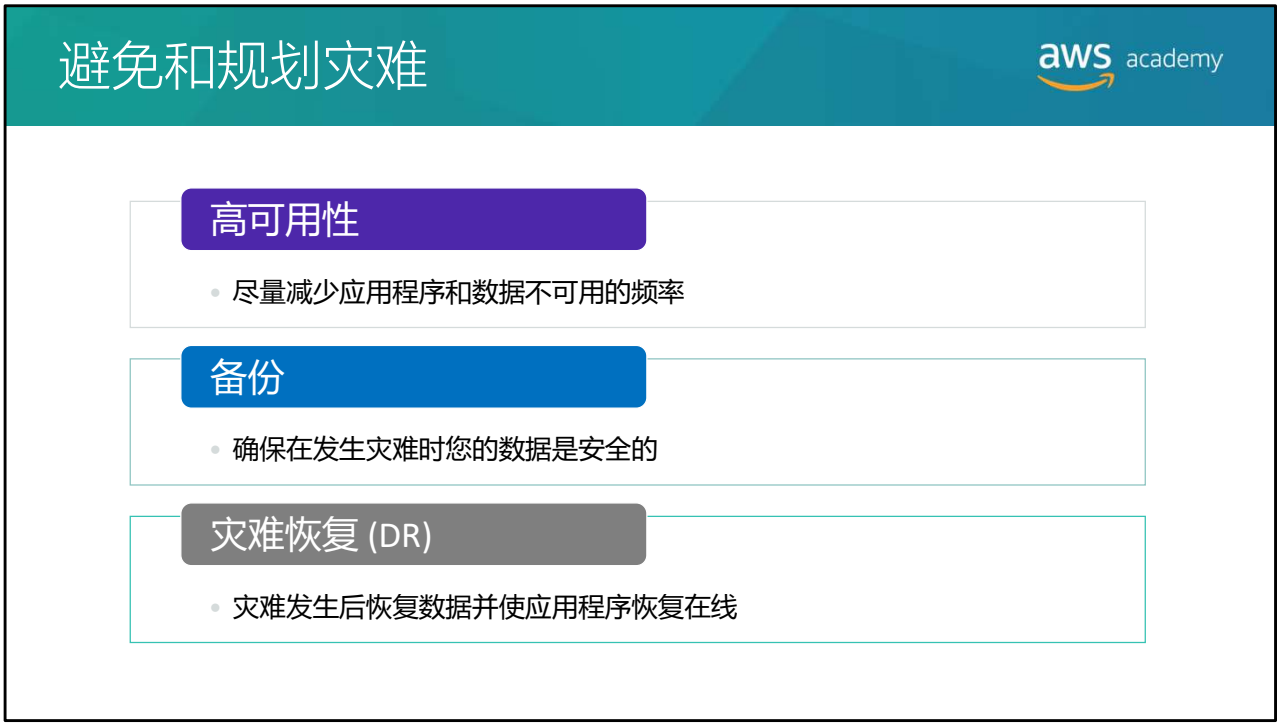
AWS 的首席技术官 (CTO) Werner Vogels 在不止一次场合中曾着重指出：“一直以来，所有事情都在失败。”他的这句发声多年来一直影响着云计算架构设计，因为这是一个真实的说法。

不应将失败视为不太可能出现的异常情况。相反，应该假设失败，无论大小，都可能会发生，也将会发生。如何准备这些活动?

故障可以归类为以下三种类型之一：

- 小*规模事件* – 例如，单台服务器停止响应或脱机
- 大*规模事件* – 在这种情况下，多种资源将受到影响，甚至可能是一个区域内的多个可用区
- 超大*规模事件* – 在这种情况下，故障很普遍，会影响到大量用户和系统

为了最大限度地减少灾难造成的影响，企业必须投入大量的时间和资源为灾难做前期的规划和准备，并培训员工、记录和更新流程。特定系统的灾难计划的投资额可能会因潜在服务中断的成本而有很大差异。



您可以通过三种方式努力避免灾难并进行规划：

- *高可用性*提供了冗余和容错能力。当系统能够承受单个或多个组件（例如，硬盘、服务器或网络链接等）的故障时，这个系统即为高度可用的。生产系统通常已定义了正常运行时间要求

- *备份*对保护数据和确保业务连续性来说至关重要。但是，要实施也是一个挑战。数据的生成速度呈指数级增长，同时，本地磁盘的密度和持久性没有同样的增长率。即便如此，在发生灾难时，保持关键数据已备份至关重要。

- *灾难恢复 (DR)* 是指为灾难做好预防准备以及从灾难中恢复。灾难*是所有会对公司的业务连续性或财务带来负面影响的事件*。此类事件包括硬件或软件故障、网络中断、停电、建筑物的物理性损坏（如火灾或洪水）。原因可能是人为错误或其他重大事件。灾难恢复是一套策略和程序，可在发生任何灾难后恢复或延续至关重要的技术基础设施和系统。

相关的 AWS 架构完善框架的设计原则

aws academy

卓越运营支柱

- 预见故障
- 经常优化运行程序

可靠性支柱

- 测试恢复流程
- 自动从故障中恢复

考虑一些与灾难恢复主题相关的设计原则。

AWS 架构完善的框架的*卓越运营*支柱指出了*预测失败*的重要性。它建议您执行预先练习，以识别潜在的故障源，从而消除或缓解故障。您必须测试您的故障情况，并验证您对故障影响的理解。AWS 架构完善的框架还描述了经常改进操作程序的好处，以便您可以寻找改进它们的机会。然后，随着工作负载的增加，您可以相应地改进您的程序。

可靠性*支柱描述了*设计系统的重要性。您必须能够从基础设施或服务中断中恢复，以及减少中断（例如配置错误或短暂的网络问题）。

它提到的设计原则之一是*测试恢复程序*。测试系统的故障情况，验证您的恢复过程。您可以使用自动化功能来模拟不同的故障或重新创建先前导致故障的场景。此测试可以在实际故障场景出现之前暴露故障路径，以便您进行测试和修复。它降低了在组件出现故障之前未经过测试的风险。

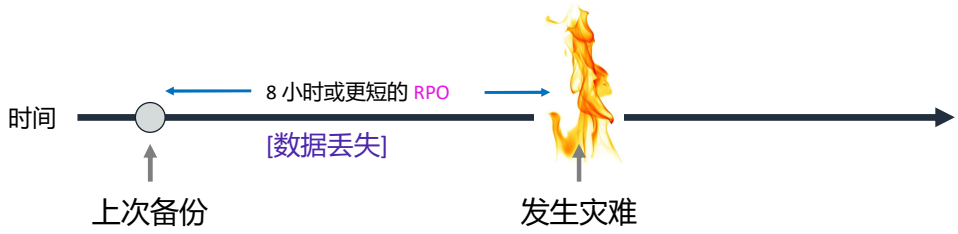
另一个设计原则是*自动从故障中恢复*。通过监控系统的关键性能指标 (KPI)，您可以在超出阈值时触发自动化。这些 KPI 应衡量商业价值，而不是服务运营方式的技术方面。您的自动化可以提供通知和跟踪故障，并自动执行可解决故障或修复故障的恢复过程。

恢复点目标 (RPO)

恢复点目标 (RPO) 是按时间衡量的可接受的最大数据丢失量。

您的数据必须多久备份一次?

示例 RPO: *企业（最多）可以从丢失过去 8 个小时的数据中恢复。*



各种规模的组织，无论大小，通常都有业务连续性计划 (BCP)。BCP 的一个典型部分是提供 IT 服务连续性，包括 IT 灾难恢复计划。

灾难恢复计划最重要的措施之一是定义*恢复点目标 (RPO)*。要计算 RPO，首先根据您的 BCP 确定可接受的数据丢失量。然后，作为时间衡量标准，找出数据丢失可能发生的速度。

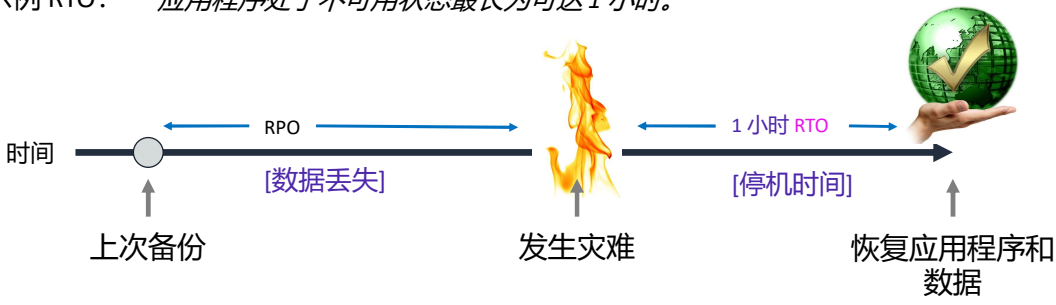
例如，假设您确定应用程序生成的数据很重要但不关键，因此丢失 800 条记录是可以接受的。您进一步计算出，即使在高峰时段，一小时内创建的记录也不超过 100 条。在这种情况下，您决定 8 小时的 RPO 足以满足您的需求。如果随后实施了符合此 RPO 的灾难恢复计划，则必须至少每 8 小时进行一次数据备份。然后，如果在 22:00 发生灾难，系统应该能够在下午 14:00 之前恢复系统中的所有数据。

恢复时间目标 (RTO)

恢复时间目标 (RTO) 是在发生灾难后，业务流程可以保持失效的最大可接受时间。

应用程序和数据必须以多快的速度恢复？

示例 RTO： *应用程序处于不可用状态最长为可达 1 小时。*



灾难恢复计划的另一个重要措施是定义*恢复时间目标* (RTO)。RTO 是中断*后*恢复应用程序和恢复数据所需的时间。要继续上一个示例，假设灾难发生在 22:00，RTO 为 1 小时。在这种情况下，灾难恢复过程应在 23:00 之前将业务流程恢复到可接受的服务级别。

当系统不可用时，公司通常会根据对业务造成的财务影响的决策来决定可接受的 RPO 和 RTO。该公司通过考虑许多因素来确定财务影响。这些因素包括因停机和缺乏系统可用性导致的业务损失和声誉损害。

然后，IT 组织计划解决方案，以提供经济高效的系统恢复。这些解决方案基于时间表内的 RPO 和 RTO 确定的服务级别。

用于灾难恢复的计划

有意识地了解数据的存储位置以及应用程序的运行位置。

最强大的灾难恢复计划跨越多个区域。

要正确确定灾难恢复计划的范围，您必须全面审视 AWS 的使用情况。大多数组织使用的服务组合可以广泛归类为包含以下五大服务分类领域：

- 存储
- 计算
- 联网
- 数据库
- 部署编排服务

如果发生灾难，您的 RPO 和 RTO 将在这些服务领域指导您的备份和恢复计划和程序。它们还可能会影响您的生产部署架构。

同样重要的是要记住，尽管整个区域都不可用是不太可能的，但它是在可能性范围内。如果某些大规模事件影响某个区域（例如，陨石撞击），您的数据是否仍可用？您的应用程序仍然可以访问吗？AWS 在世界各地提供了多个区域。因此，除了完全部署系统的站点外，您还可以为灾难恢复站点选择最合适的位置。

图中引用了以下服务：

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Storage Service Glacier (Amazon S3 Glacier)

要开始制定详细的灾难计划，请查看数据存储层（暂时推迟对数据库层的讨论）。

您的 AWS 云存储可以由数据块存储、文件系统存储和对象存储的组合组成。同时，您的组织也可能使用将本地数据中心连接到 AWS 云的 AWS 服务。

在接下来的几张幻灯片中，您将了解这三个领域中每个领域的高级别最佳实践。

您可能不熟悉的一项服务是 *AWS DataSync*。使用 AWS DataSync，可以在本地存储与 Amazon S3、Amazon EFS 或 Amazon FSx for Windows File Server 之间移动大量在线数据。它支持从本地网络文件系统 (NFS) 和服务器消息块 (SMB) 存储传输脚本复制作业和计划数据传输。它还可以选择性地使用 AWS Direct Connect 链接。

对于许多组织来说，他们存储在 AWS 上的大部分数据都在提供对象存储的 Amazon S3 中。

回想一下，S3 存储桶存在于特定的 AWS 区域中。您在创建存储桶时选择区域。Amazon S3 为 S3 标准、S3 标准 – IA、S3 单区 – IA 和 Amazon S3 Glacier 存储类提供了 11 个 9 (99.999999999%) 的持久性。Amazon S3 标准、S3 标准 – IA 和 Amazon S3 Glacier 的设计还可在整个 Amazon S3 可用区丢失的情况下保留数据。它们通过在*单个* AWS 区域中自动将对象存储在至少三个相隔数英里的可用区中，从而提供这种稳定性。

对于希望获得更高级别数据安全性的关键应用程序和数据场景，最佳做法是配置 S3 跨区域复制。要启用复制，请将复制配置添加到*源存储桶*。最低配置必须指明您希望 Amazon S3 复制所有对象或所有对象的子集的目标存储桶。它还必须包含 AWS Identity and Access Management (IAM) 角色，该角色授予 Amazon S3 将对象复制到目标存储桶的权限。

复制的对象保留其元数据。目标存储桶*可以属于另一个存储类*。例如，S3 标准存储桶的内容可能会复制到 Amazon S3 Glacier 存储桶。您可以为目标存储桶中的对象分配不同的所有权。您还可以使用 S3 复制时间控制 (S3 RTC) 在可预测的时间范围内跨不同区域复制您的数据。S3 RTC 可以在 15 分钟内复制存储在 Amazon S3 中的 4 个 9 (99.99%) 的新对象。

最佳实践：EBS 卷快照

- 创建 EBS 卷的时间点快照
  - 快照提供增量备份（它们备份自上一个快照以来更改的数据块）
- 快照使您能够将数据还原到新的 EBS 卷
- 使用 Amazon Data Lifecycle Manager 自动创建、保留和删除快照
- 您无法快照实例存储

关于数据块存储，您可以通过创建时间点*快照*将 EBS 卷上的数据备份到 Amazon S3。快照是*增量*备份，这意味着仅保存设备上在最新快照之后更改的数据块。由于无需复制数据，此架构将最大限度缩短创建快照所需的时间和增加存储成本节省。

每个快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。当您基于快照创建 EBS 卷时，新卷将开始作为原始卷的精确副本。该原始卷用于创建快照。复制的卷将在后台加载数据，让您可以立即开始使用数据。如果您访问尚未加载的数据，卷会立即从 Amazon S3 下载请求的数据。然后，它将继续在后台加载该卷的其余数据。

Amazon EBS 卷可提供脱离实例的存储，该存储独立于实例的生命周期，并在可用区中的多个服务器之间进行复制。卷可以防止任何单个组件发生故障造成数据丢失。创建快照后，快照将完成复制到 Amazon S3（快照状态完成后）。然后，您可以将其从一个 AWS 区域复制到另一个，或在同一区域内复制。

您可以*使用 Amazon Data Lifecycle Manager* 来自动创建、保留和删除为备份 EBS 卷而拍摄的快照。通过自动执行快照管理，您可以：

- 通过实施定期备份计划来保护重要数据
- 按照审计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

您无法创建 EC2 实例存储卷的快照但是，如果必须备份实例存储中的数据，则可以创建一个新的 EBS 卷并对其进行格式化。然后，将新卷挂载到 EC2 实例客户端操作系统，然后将实例存储卷上的数据复制到 EBS 卷。回想一下，*实例存储*卷提供了临时数据块级存储，该存储非常适合频繁更改的信息，例如缓冲区、缓存和临时数据。您可能会发现必须备份实例存储中的数据。如果是，您可能需要重新考虑为什么首先将这些数据存储在实例存储卷上。

复制文件存储也是最佳实践。

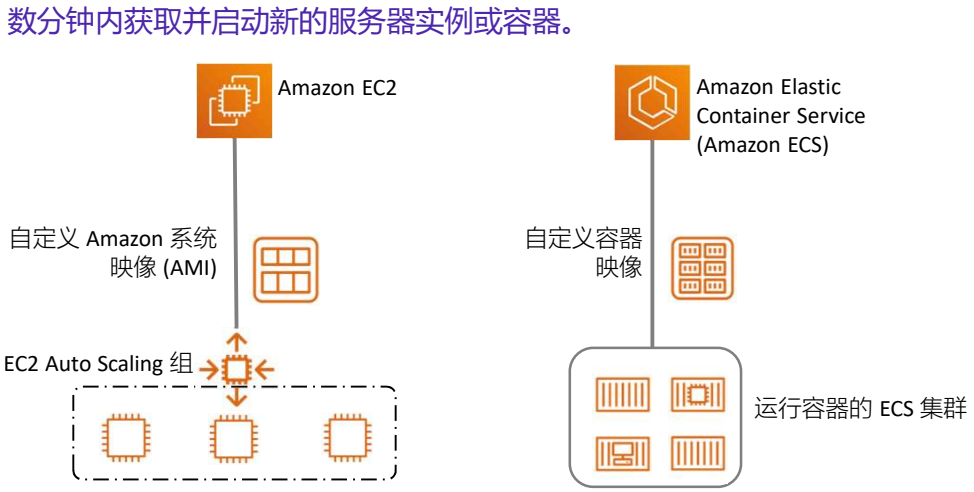
AWS DataSync 使数据在两个 EFS 或 Amazon FSx Windows File Server 文件系统之间，或者在本地存储和 AWS 文件存储之间更快地移动数据。您可以使用 DataSync 通过 DX 或互联网传输数据集。使用该服务用于一次性数据迁移或持续工作流以进行数据保护和恢复。

您可以了解有关如何使用 *AWS Backup* 管理 EBS 卷备份和自动化 EFS 文件系统备份的更多信息。有关详细信息，请参阅使用 Amazon EFS 和 AWS Backup 计划自动备份博客。

FSx for Windows File Server 会每天自动备份文件系统，使您能够随时进行更多备份。Amazon FSx 将备份存储在 Amazon S3 中。每日备份时段是您在创建文件系统时指定的 30 分钟时段。为文件系统指定的每日备份保留期，决定了每日自动备份的保留天数。（默认情况下为 7 天。）

与大多数 Amazon S3 存储类一样，跨可用区复制数据同样适用于 Amazon EFS 和 FSx for Windows File Server 文件系统。您的灾难恢复要求可能会指定您需要多区域恢复解决方案。在这种情况下，最佳实践是将 Amazon EFS 和 FSx for Windows File Server 文件系统复制到第二个区域。您可以使用 AWS DataSync 获取此复制。要使用 DataSync 简化在两个 EFS 文件系统之间传输文件的过程，您可以使用 AWS DataSync 云端快速入门和计划程序。

计算容量应该能够快速恢复



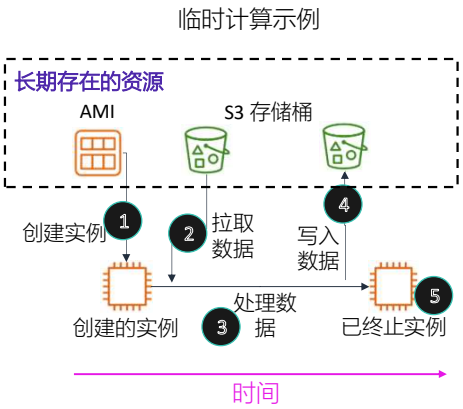
在灾难恢复环境下，能够快速创建您可控制的虚拟机至关重要。通过在单独的可用区中启动实例，可以保护应用程序免受单个站点故障的影响。

当底层硬件的系统状态检查出现故障时，您可以安排自动恢复 EC2 实例。该实例已重新启动（必要时在新硬件上启动），但将保留其实例 ID、IP 地址、EBS 卷附件和其他配置详细信息。为了完成恢复，请确保实例配置为在其初始化过程中自动启动任何服务或应用程序。

Amazon 系统映像 (AMI) 已预先配置了操作系统，而且一些预配置的 AMI 可能还包括应用程序堆栈。您还可以配置自己的自定义 AMI。在进行灾难恢复时，AWS 强烈建议您配置和标识自己的 AMI，以便它们可以作为恢复过程的一部分启动。此类 AMI 应预配置您选择的操作系统以及应用程序堆栈的相应部分。

计算资源的灾难恢复策略

- 使用 Amazon EC2 快照功能进行备份
  - 快照可以手动执行，也可以计划执行（例如，使用 AWS Lambda）
- 不经常使用系统或实例级系统备份，并且作为不得已的手段
  - 提高了快速使用的存储成本
  - 改为更喜欢从配置或代码存储库进行自动重建
- 跨区域 AMI 复制
- 跨区域快照复制
- 考虑临时计算架构
  - 将基本数据存储在实例之外



对于计算资源的灾难恢复，您可能需要使用 Amazon EC2 快照功能。快照可以手动拍摄，也可以定时拍摄。

尽管您可以创建系统或实例级系统备份，但广泛使用此方法会增加存储成本。更好的方法是配置自动重建过程，将源代码存储在存储库中。

您可能希望跨区域复制 Amazon S3，并且可能还希望跨区域复制最关键的 AMI 和快照。

最后，考虑架构设计计算资源的使用，将基本数据存储在实例之外。正如您在示例中看到的那样，您的数据可以存储在 S3 存储桶中。当您必须处理数据时，您可以从使用应用程序软件预配置的自定义 AMI 启动一个或多个 EC2 实例。实例启动后，它就可以从 S3 存储桶中提取所需的数据并处理数据。然后，它可以将输出数据写回 Amazon S3（也许写入另一个 S3 存储桶）。实例在完成计算任务后，实例可以终止。这种架构（当它仍然可以满足您的业务需求时）可以更轻松地设计灾难恢复策略。它还可以节省成本，因为不常用的服务器可以被终止，然后在需要时重新创建。

网络：为弹性和恢复能力而设计

Amazon Route 53

- 流量分配
- 故障转移

Elastic Load Balancing

- 负载均衡
- 运行状况检查和故障转移

Amazon Virtual Private Cloud (Amazon VPC)

将现有的本地网络拓扑扩展到云

AWS Direct Connect

将大型本地环境快速一致地复制和备份到云

当您努力从灾难中恢复时，很可能必须修改网络设置才能将系统故障切换到另一个站点。AWS 可提供多种让您能够管理和修改网络设置的服务和功能，在下方将突出显示其中的几种服务和功能。

Amazon Route 53 提供负载均衡和网络路由功能，以便您分配网络流量。它还提供了在多个终端节点之间进行故障切换的功能，甚至可以故障转移到 Amazon S3 中托管的静态网站。

Elastic Load Balancing *服务可以在多个 EC2 实例间自动分配传入的应用程序流量。*它可以提供响应应用程序传入流量所需要的负载均衡容量，让您实现应用程序容错性能。您可以预先分配负载均衡器，以便其域名系统 (DNS) 名称已知，这可以简化灾难恢复计划的实施。

您可以使用 *Amazon Virtual Private Cloud (Amazon VPC)* 将现有本地网络拓扑扩展到云。当您恢复可能托管在内部网络上的企业应用程序时，此扩展尤为适合。

最后，*AWS Direct Connect* 可以简化从本地数据中心到 AWS 的专用网络连接设置。使用 DX 可以减少网络花费、增加带宽吞吐量，同时提供优于 Internet 连接的稳定网络体验。

数据库：支持恢复的功能

Amazon Relational Database Service (Amazon RDS)

- 创建数据快照并将其保存在一个单独的区域
- 将只读副本与多可用区部署相结合，构建弹性灾难恢复策略
- 保留自动备份

Amazon DynamoDB

- 数秒内备份整个表
- 使用时间点恢复，持续备份表的时间可长达 35 天
- 只需在控制台中单击一下鼠标或调用一次应用程序编程接口 (API) 即可启动备份
- 使用全局表构建多区域、多主数据库，为大规模扩展的全球分布式应用程序提供快速的本地性能

AWS 提供了许多数据库服务。下面将介绍 Amazon RDS 和 Amazon DynamoDB 的一些与灾难恢复方案相关的关键功能。

考虑在灾难恢复*准备阶段*使用 *Amazon RDS*，将关键数据的副本存储在已运行的数据库中。然后，在灾难恢复的*恢复阶段*使用 Amazon RDS 来运行生产数据库。

如果您实施多区域灾难恢复计划，通过 Amazon RDS，您可以将从一个区域捕获的快照数据存储到另一个区域。您最多可以与其他 20 个 AWS 账户共享手动快照。

将只读副本与多可用区部署相结合，您可以构建弹性灾难恢复策略并简化数据库引擎升级过程。通过使用 Amazon RDS 只读副本，您可以创建数据库实例的一个或多个只读副本。您可以在同一 AWS 区域或另一个 AWS 区域中创建这些副本。然后，对源数据库所做的更新将异步复制到只读副本。只读副本在需要时也能升级成独立的数据库实例。

在准备阶段使用*Amazon DynamoDB* 将数据复制到另一个区域的 DynamoDB 或复制到 Amazon S3。在灾难恢复的恢复阶段，您可以在几分钟内扩展。DynamoDB 全局表会在您选择的 AWS 区域中自动复制您的 DynamoDB 表。它们可以解决更新冲突并使应用程序保持高度可用，即使在整个区域被隔离或受到降级影响这些不太可能发生的情况下也是如此。

自动化服务：快速复制或重新部署环境

AWS CloudFormation

- 按需使用模板快速部署资源集合
- 在几分钟内在新区域或 VPC 中重复生产环境

AWS Elastic Beanstalk

- 只需单击几下即可快速重新部署整个堆栈

AWS OpsWorks

- 自动主机更换
- 在恢复阶段将其与 AWS CloudFormation 结合使用
- 预置支持已定义 RTO 的新堆栈

使用自动化服务时，可以快速复制或重新部署环境。

AWS CloudFormation 使您可以在文本文件中为整个基础设施建模和部署。此模板可成为您的基础设施的唯一可信来源。当您使用 AWS CloudFormation 管理整个基础设施时，它也成为灾难恢复规划工具包中的强大工具。例如，它使您能够在几分钟内将复杂的生产环境复制到新区域或新 VPC。

AWS CloudFormation 以可重复的方式预置资源，这使您能够构建和重建基础设施和应用程序。您无需执行手动操作或编写自定义脚本。

如果您使用 *AWS Elastic Beanstalk* 托管您的应用程序，您可以上传更新后的应用程序源数据包并将其部署到您的 AWS Elastic Beanstalk 环境。或者，您可以重新部署以前上传的应用程序版本。您还可以将之前上传的应用程序版本部署到其任意环境。

最后一点，*AWS OpsWorks* 是一种应用程序管理服务，可以轻松部署和运行各种类型和规模的应用程序。您可以将环境定义为一系列层，并将每一层配置为应用程序的一个层。AWS OpsWorks 具有自动主机替换功能，因此如果实例发生故障，会自动进行替换。您可以在灾难恢复*准备阶段*使用 AWS OpsWorks 来模拟您的环境，并且在恢复恢复的灾难阶段将其与 AWS CloudFormation 结合使用。

第 2 节要点

aws academy

- 要选择正确的灾难恢复策略，首先确定恢复点目标 (RPO) 和恢复时间目标 (RTO)
- 使用 S3 跨区域复制、 EBS 卷快照和 Amazon RDS 快照等功能来保护数据
- 使用联网功能（如 Route 53 故障转移和 Elastic Load Balancing ）来提高应用程序可用性
- 使用自动化服务作为灾难恢复策略的一部分（例如 AWS CloudFormation），在需要时快速部署重复环境

本模块中这节内容的要点包括：

- 要选择正确的*灾难恢复*策略，首先确定恢复点目标 (RPO) 和恢复时间目标 (RTO)
- 使用 S3 跨区域复制、EBS 卷快照*和* RDS 快照等功能来保护数据
- 使用联网功能（如 *Route 53 故障转移*和 *Elastic Load Balancing*）来提高应用程序可用性
- 使用自动化服务作为灾难恢复策略的一部分（例如 *AWS CloudFormation*），*在需要时*快速部署重复环境

模块 14：灾难规划

第 3 节：灾难恢复模式

介绍第 3 节：灾难恢复模式。

AWS 上的常用灾难恢复模式

四种灾难恢复模式

- 备份与还原
- “Pilot light”式
- 热备份
- 多站点

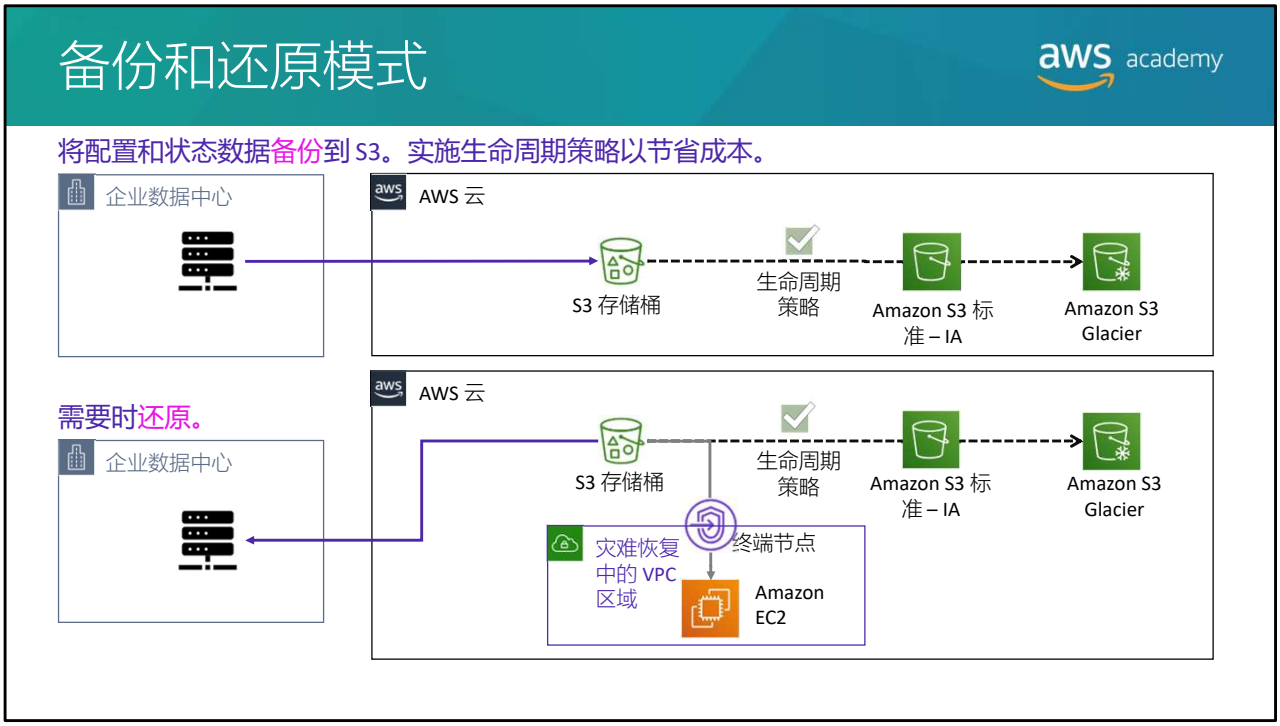
每种模式都适合以下不同的组合：

- 恢复点目标
- 恢复时间目标
- 成本效益

组织经常使用以下四种常见的灾难恢复模式：

- 备份与还原
- “Pilot light”式
- 热备份
- 多站点

正如您将在下面的细节中发现的那样，每种模式都非常适合不同的要求。其中一些模式提供了更好的成本效益。其他一些模式则提供更快的 RPO 和更快的 RTO，但维护成本更高。



第一种灾难恢复方法是*备份和还原模式*。

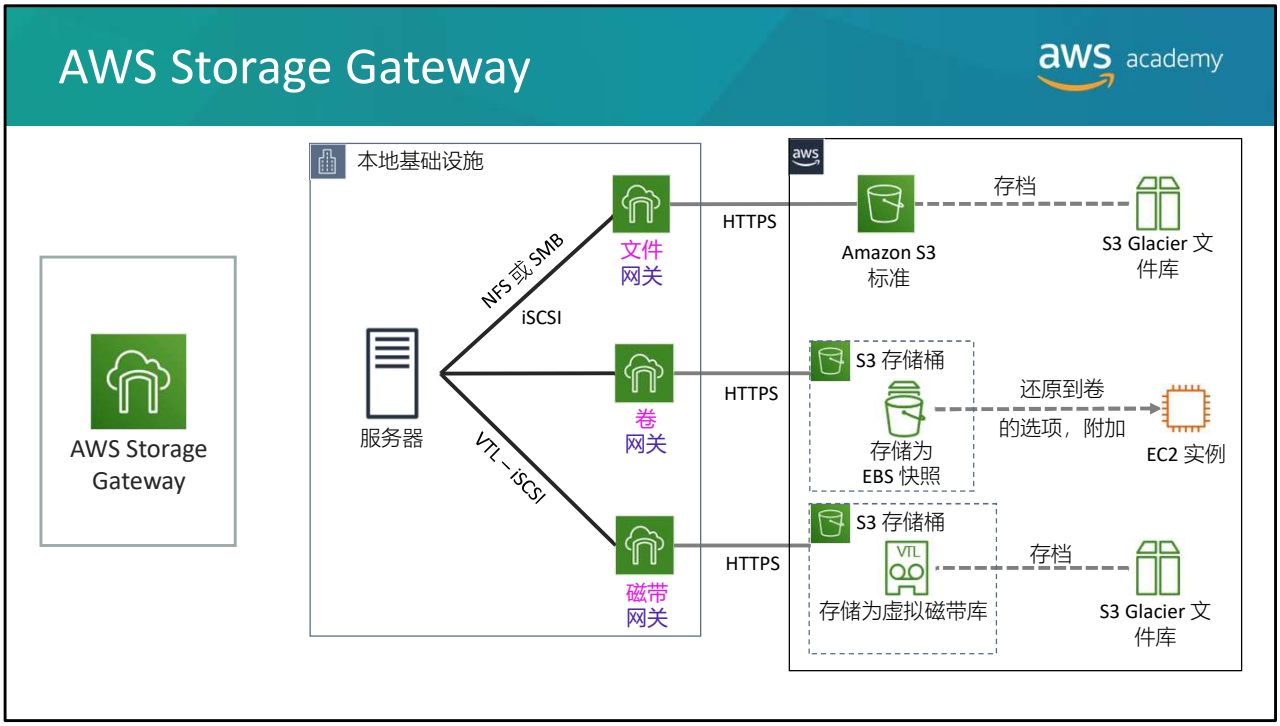
大多数传统环境中都会将数据备份到磁带并定期发送到异地。如果使用此方法，则在发生灾难时恢复系统可能需要很长时间。

Amazon S3 为执行恢复亟需的备份数据提供了一个更容易访问的目标。数据传入和传出 Amazon S3 通常都通过网络完成，因此可以从任意位置访问。

在示例备份场景中，数据从本地数据中心复制到 Amazon S3。AWS DataSync 或 Amazon S3 Transfer Acceleration 可以选择用作此配置的一部分，以自动化或提高数据传输速度。然后，应用于存储桶的 S3 生命周期配置稍后会将备份数据移动到成本较低的 Amazon S3 存储类中。备份数据移动到 Amazon S3 Glacier 或 Amazon S3 标准 – IA，随着数据老化而且不经常访问，可节省成本。

在示例还原方案中，本地数据可能会暂时或永久丢失。然后，备份数据可以从 Amazon S3 下载回本地服务器。

如果您的公司数据中心仍处于离线状态，您可以进一步确保将数据还原到服务器的功能。您可以在指定灾难恢复区域的 VPC 中使用 Amazon EC2 服务器。此区域可以连接到包含备份应用程序数据的 S3 存储桶。它可以读取这些数据，也许可以在恢复数据中心的同时临时托管应用程序。



作为备份和还原模式的一部分，您可能会发现使用 AWS Storage Gateway 意义重大。

AWS Storage Gateway 是一种混合存储服务，您的本地应用程序可以借助它来使用 AWS 云存储。您可以使用该服务进行备份、存档、灾难恢复、云数据处理、存储分层和迁移。

您的应用程序可以使用标准存储协议通过虚拟机或硬件网关设备连接到该服务。这些协议包括 NFS、SMB、虚拟磁带库 (VTL) 和互联网小型计算机系统接口 (iSCSI)。网关会连接到 Amazon S3、Amazon S3 Glacier、Amazon EBS 等 AWS 存储服务，这些服务为文件、卷和虚拟磁带提供存储。该服务包括优化的数据传输机制。它提供带宽管理、自动实现网络弹性、高效传输数据以及本地缓存，让您能够对最活跃的数据进行低延迟本地访问。

使用*文件网关*，您可以在 Amazon S3 中存储和检索对象（通过使用 NFS 或 SMB 协议）。您可以使用本地缓存实现低延迟对您最近使用的数据访问。当您将文件传输到 Amazon S3 之后，它们将作为对象存储，并允许通过 NFS 挂载点进行访问。

Storage Gateway *卷*接口为您的应用程序提供了数据块存储磁盘卷，可以使用 iSCSI 协议访问这些卷。这些卷上的数据将作为时间点 EBS 快照进行备份，因此您可以在必要时通过 Amazon EC2 对其进行访问。

Storage Gateway *磁带*接口 以虚拟磁带库的形式将 Storage Gateway 呈现给您的现有备份应用程序。此库由虚拟介质转换器和虚拟磁带驱动器组成。您可以继续使用现有的备份应用程序，同时写入虚拟磁带集。每个虚拟磁带均存储在 Amazon S3 中。当您不再需要访问虚拟磁带上的数据时，您的备份应用程序可以将其从虚拟磁带库存档到 Amazon S3 Glacier。

备份与还原：检查清单

aws academy

准备阶段

- 创建当前系统备份
- 将备份存储在 Amazon S3 中
- 记录从备份还原的过程
- 了解：
  - 根据需要使用和构建哪些 AMI
  - 如何从备份中还原系统
  - 如何将流量路由到新系统
  - 如何配置部署

发生灾难时

- 从 Amazon S3 中检索备份
- 恢复所需的基础设施
  - 来自准备好的 AMI 的 EC2 实例
  - Elastic Load Balancing 负载均衡器
  - 由 AWS CloudFormation 堆栈创建的 AWS 资源 – 自动部署以恢复或复制环境
- 从备份中恢复系统
- 将流量路由到新系统
  - 相应地调整域名系统 (DNS) 记录

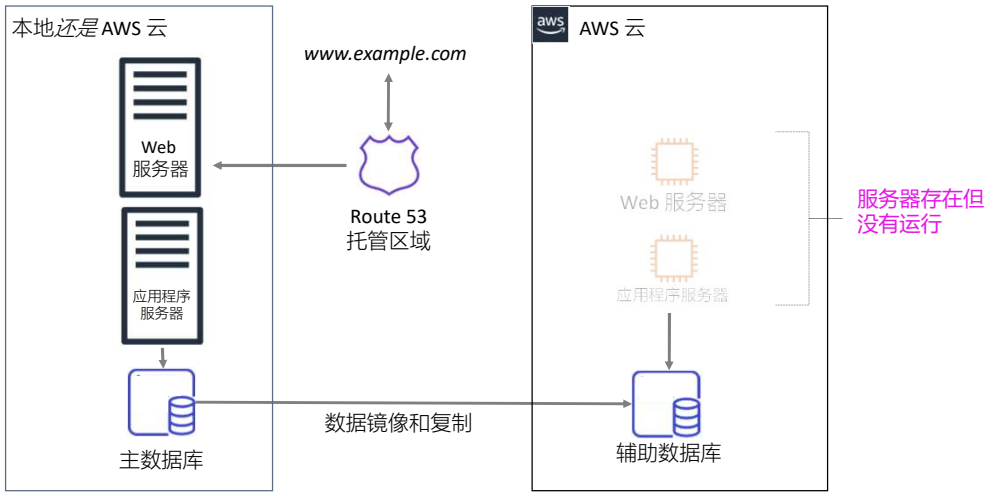
如果实施备份和还原灾难恢复模式，则在*准备阶段*应完成的关键步骤是：

- 创建当前系统备份
- 将备份存储在 Amazon S3 中
- 记录从备份还原的过程

如果实施此模式，在发生*灾难时要完成的*关键步骤是：

- 从 Amazon S3 中检索备份
- 开始所需的基础设施
- 从备份中还原系统
- 最后，将流量路由到新系统

“Pilot light”式灾难恢复模式：准备阶段



第二种灾难恢复方法是 *“Pilot light”式灾难恢复模式*。

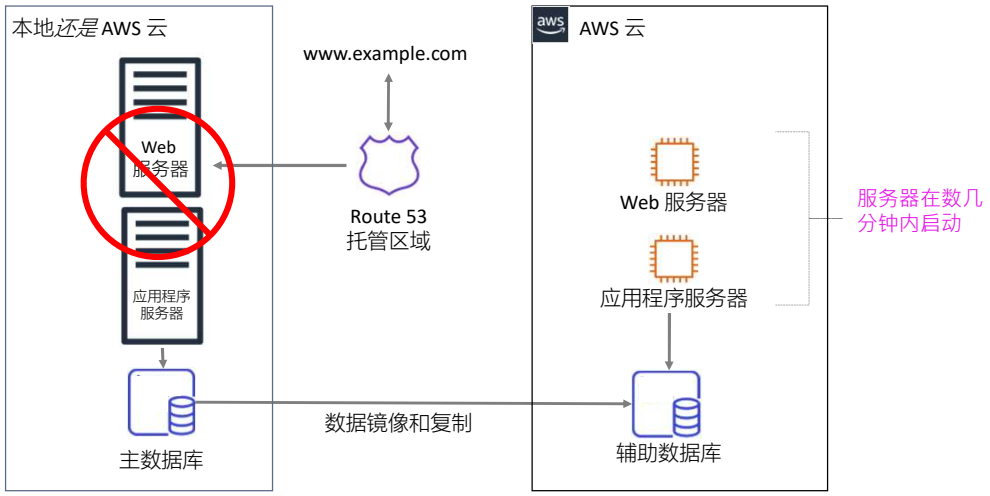
*“Pilot light”式灾难恢复模式*描述了一种灾难恢复模式，*其中环境的*最低*备份版本*始终在运行。标灯类比源于燃气取暖器：即使在加热器关闭的情况下，小火焰（或标灯）始终燃起。标灯可以迅速点燃整个炉灶，让房间变暖。在示例模式中，标灯是始终在运行的辅助数据库。

标灯方案类似于备份和恢复方案。但是，恢复时间通常会更快，因为系统的核心部分已经在运行并持续保持最新状态。恢复时，您可以快速预置关键核心周围的完整生产环境。

标灯本身的基础设施要素通常包括您的数据库服务器。这种分组是该系统的关键核心（标灯）。可以快速预置所有其他基础设施部件，以恢复整个系统。要预置基础设施的其余部分，您通常将预置的服务器捆绑为可立即启动的 AMI。（或者它们可能是处于停止状态的实例。）恢复开始时，这些实例将以其预定义的角色快速启动，从而使它们能够连接到数据库。

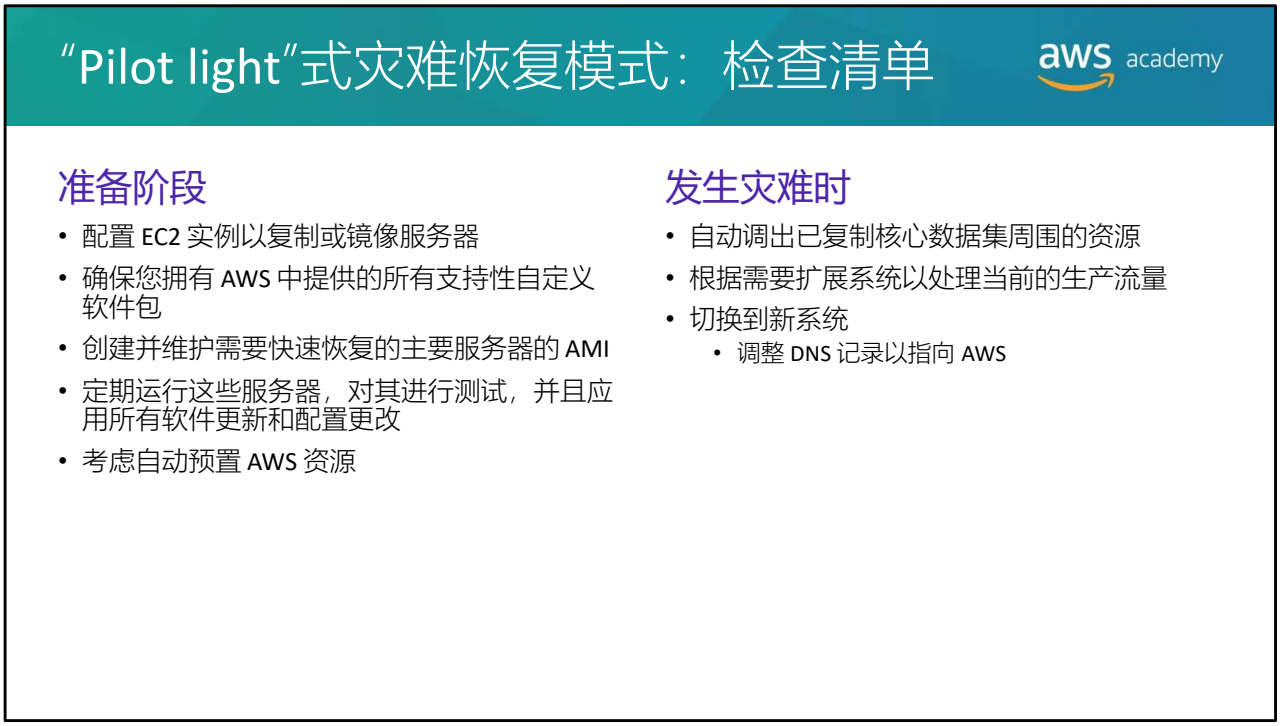
此模式实施起来相对经济实惠。必须将定期更改的数据复制到标灯中，即整个环境在恢复阶段启动的小核心。操作系统和应用程序等不经常更新的数据可以定期更新并存储为 AMI。

“Pilot light”式灾难恢复模式：在发生灾难的情况下



假设发生灾难，主应用程序将离线。在这种情况下，您可以快速委托计算资源运行应用程序或编排故障转移以在 AWS 中标记资源。在此示例中，辅助数据库用于存储关键数据。如果发生灾难，新的 Web 服务器和应用程序服务器将启动并连接到辅助数据库。Amazon Route 53 配置为然后将流量路由到新的 Web 服务器。

主环境可以存在于本地数据中心，也可以存在于 AWS 上的另一个区域或可用区中。无论哪种方式，您都可以使用标灯模式来满足恢复时间目标 (RTO)。

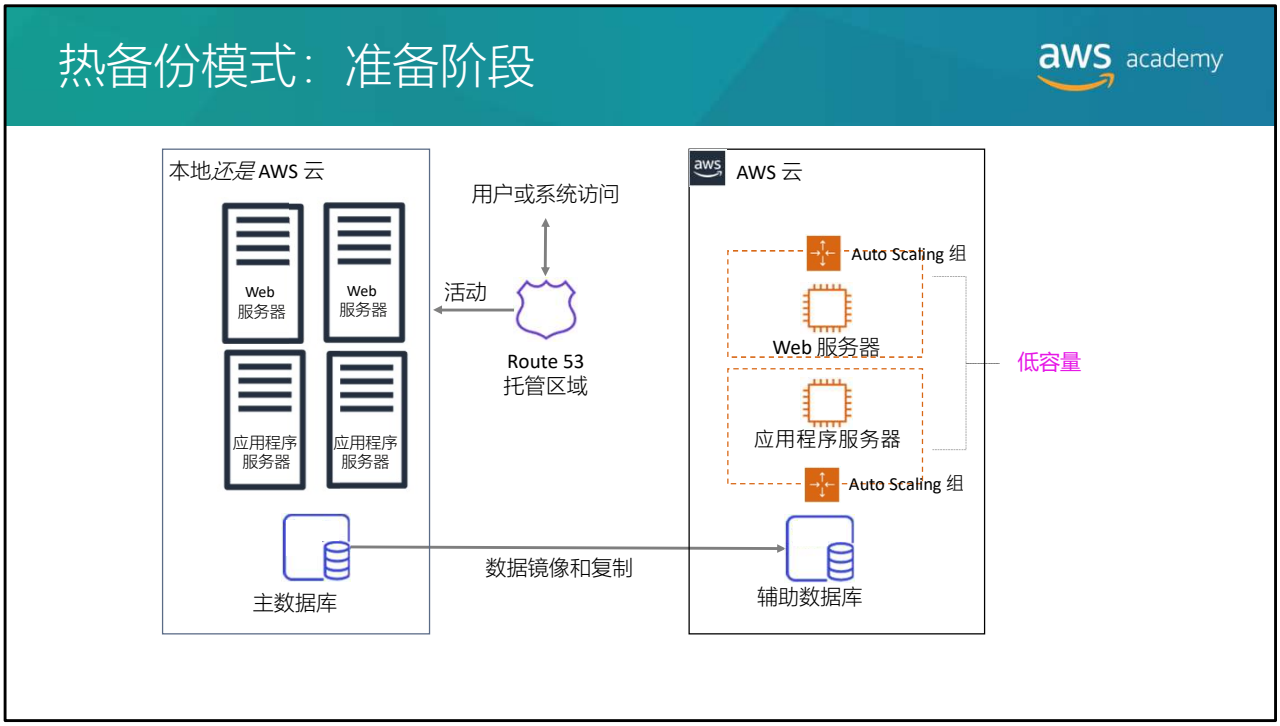


如果实施标灯灾难恢复模式，则在*准备阶段*应完成的关键步骤是：

- 配置 EC2 实例
- 确保您拥有提供的所有支持性自定义软件包
- 创建并维护需要快速恢复的必要 AMI。
- 定期运行并测试这些服务器，并且应用软件更新和配置更新
- 考虑自动预置 AWS 资源

如果实施此标灯模式，在发生*灾难时要完成的*关键步骤是：

- 自动调出已复制核心数据集周围的资源
- 根据需要扩展系统以处理当前的生产流量
- 通过调整 DNS 记录以指向备份部署，切换到新系统



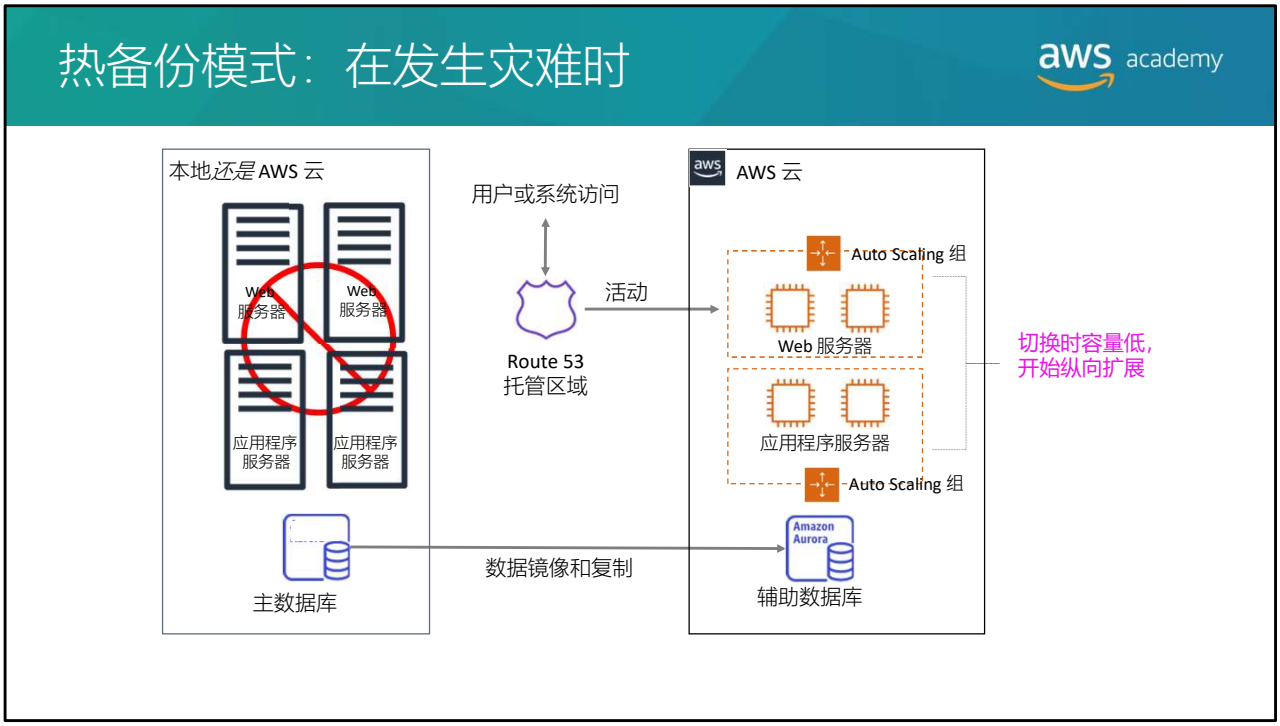
第三种灾难恢复方法是*热备份灾难恢复模式*。

热备份灾难恢复模式与“Pilot light”式灾难恢复模式一样，但更多的资源已经在运行。“*热备份*”一词用于描述灾难恢复场景，在此场景下，功能完备的缩小版环境始终在云中运行。热备份解决方案扩充了“Pilot light”式灾难恢复的元素和准备工作，进一步缩短了恢复时间，因为某些服务一直在运行。通过识别您的业务关键型系统，您可以完全复制这些系统并让它们始终保持运行。

这些服务器可以在队列规模最小，实例大小最小的 EC2 实例队列上运行。此解决方案并未经过扩展，无法承担全部生产负载，但它的功能完备。尽管它用于灾难恢复目的，但您也可以将其用于非生产性工作，例如测试、质量保证和内部使用。

在示例中，两个系统正在运行。主系统可能在本地数据中心或 AWS 区域中运行，并且 AWS 上运行的是低容量系统。使用 Amazon Route 53 在主系统和备份系统之间分发请求。

热备份模式：在发生灾难时



在灾难中，如果主环境不可用，Amazon Route 53 会切换到辅助系统。

然后，辅助系统可以迅速开始向上扩展以便处理生产负载。您可以通过向负载均衡器添加更多 EC2 实例来实现这此增长。或者，您可以调整小容量服务器的大小，以便在较大的 EC2 实例类型上运行。 横向扩展（创建更多 EC2 实例）优先于纵向扩展（增加现有实例的大小）。

热备份模式：检查清单

准备工作

- 与“Pilot Light”式类似
- 所有必要组件全天候运行，但不因生产流量而扩展
- 最佳实践：持续测试
  - 促使生产流量的统计子集慢慢移动到灾难恢复站点

发生灾难时

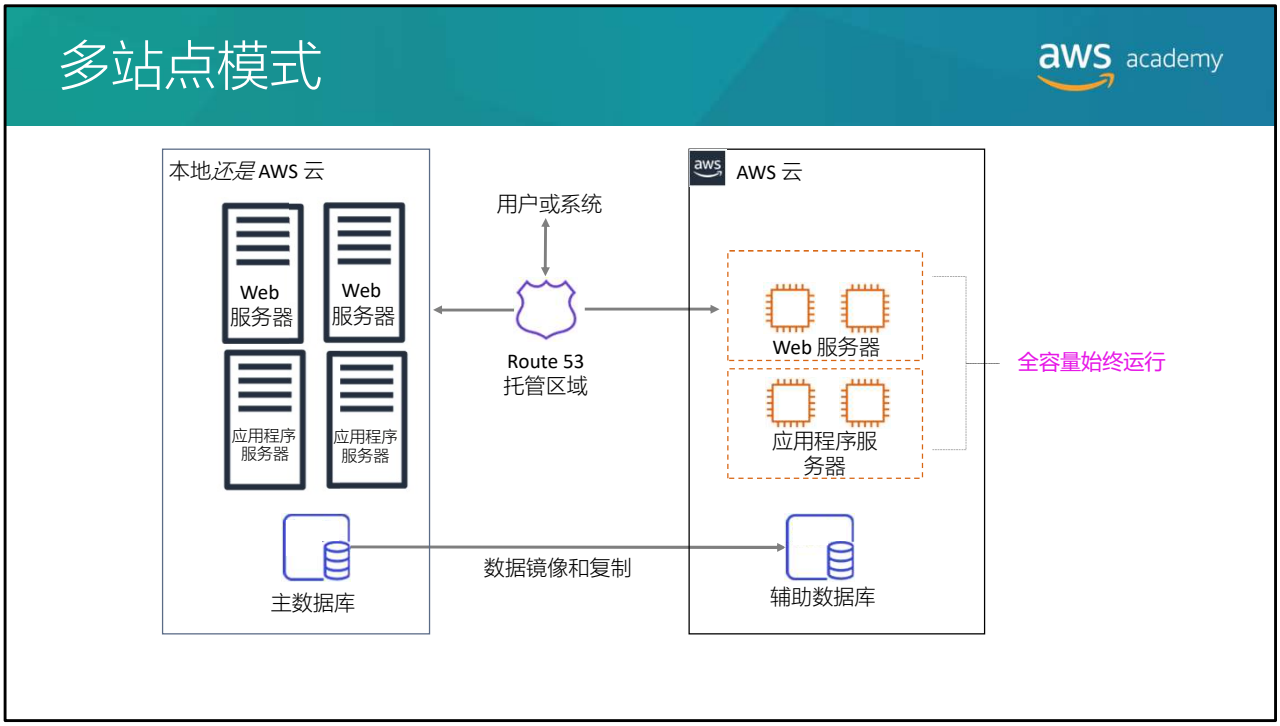
- 立即对关键生产负载进行故障转移
  - 调整 DNS 记录以指向 AWS
- 进一步（自动）扩展系统以处理所有生产负载

如果实施热备份灾难恢复模式，那么*准备阶段*至关重要。在准备阶段，您应该完成的关键步骤与为“Pilot light”式灾难恢复模式完成的步骤类似。最显著的区别是，所有必要的组件都应保持全天候运行，但不能根据生产流量进行扩展。

作为最佳实践，进行持续测试。您还可能会促使生产流量的统计子集慢慢移动到灾难恢复站点因此，您可以验证它是否与主系统一样可无缝用于用户和系统。

使用热备份模式，*在发生灾难时*，要完成的关键步骤是：

- 立即对最关键的生产负载进行故障转移
- 调整 DNS 记录以指向 AWS
- 进一步（自动）扩展系统以处理所有生产负载



第四种也是最后一种灾难恢复方法是*多站点模式*。使用这种模式，您将拥有一个功能齐全的系统，其在第二个 AWS 区域运行。它与本地系统或在其他 AWS 区域中运行的系统同时运行。

多站点解决方案在*双活配置*中运行。您使用的数据复制方法由您选择的恢复点决定。

由于两个站点都可以支持全部生产容量，因此您可以选择使用支持加权路由的 DNS 服务。Amazon Route 53 就是一个例子，它将生产流量路由到交付相同应用程序或服务的两个站点。在这种情况下，一部分流量会流入 AWS 中的基础设施，其余流量会流入您的现场基础设施。（或者，如果这两个环境存在于不同的 AWS 区域中，则流量在这两个区域之间按比例分布。）

如果现场或主要 AWS 区域出现灾难，您可以调整 DNS 权重并将*所有*流量发送到第二个部署。然后，第二个部署的容量可以快速提高以按需处理整个生产负载。您可以使用 Amazon EC2 Auto Scaling 自动执行这一流程。您可能需要使用某种应用程序逻辑来检测主数据库服务的故障，然后切换到已运行的并行数据库服务。

此场景的成本取决于正常操作期间的生产流量总量。在恢复阶段，您只需支付整个灾难恢复环境持续时间内您所使用的内容。您可以为始终运行的 AWS 服务器购买 Amazon EC2 预留实例，以进一步降低成本。

多站点：检查清单

准备工作

- 类似于热备份
- 配置为完全向内扩展或向外扩展以实现生产负载

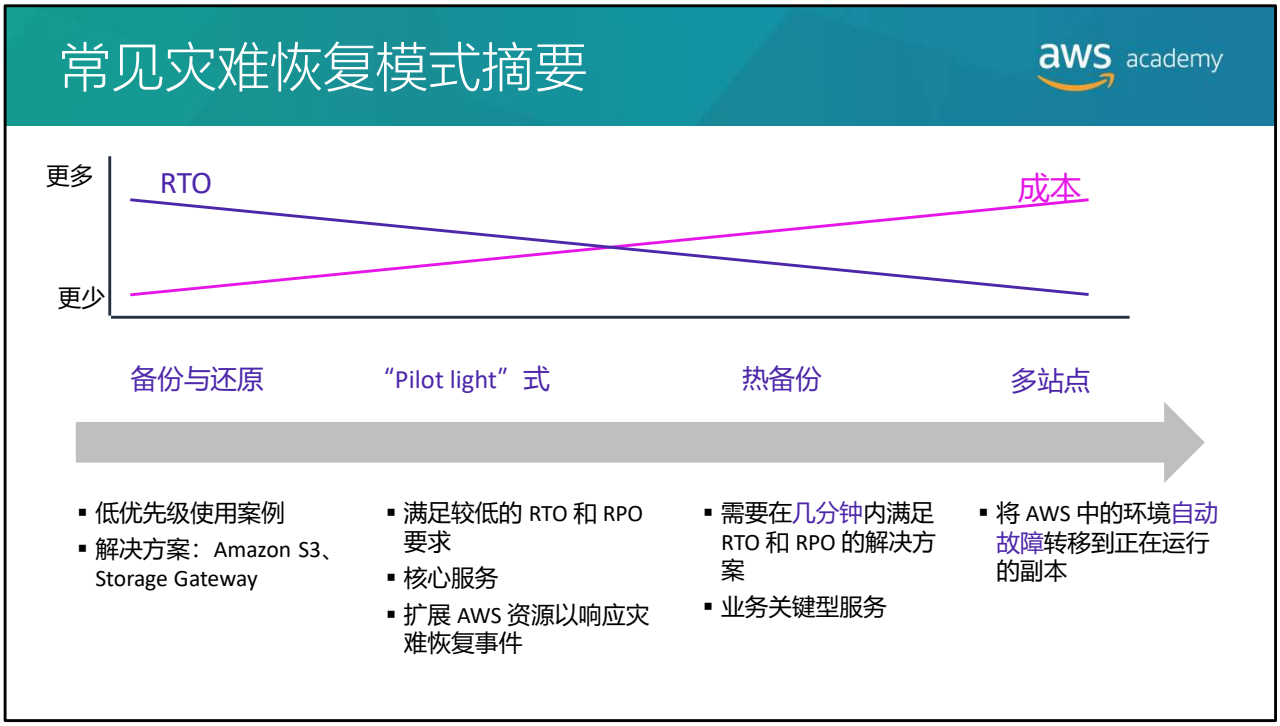
发生灾难时

- 立即对所有生产负载进行故障转移

如果您正在实施多站点灾难恢复模式，则*准备阶段*要完成的关键步骤与热备份模式类似。您必须将备份部署配置为完全扩展和缩减生产负载。您应该让服务器运行并准备好接收流量。

使用多站点模式，*在发生灾难*时，您只需完成一个关键步骤。这一步是立即将所有生产负载故障转移到备份站点。

多站点模式的停机时间可能最少。但是，由于需要运行的系统更多，它的成本确实更高。



总而言之，四种灾难恢复模式中的每种模式都提供了不同的优势组合。

此图显示了四种场景的图谱，按照灾难恢复事件发生后系统可重新供用户使用的速度排列。

备份和还原模式通常可以最低的成本完成任务，但它的 RTO 较长。因此，您的系统的恢复速度可能比选择其他模式更慢。

热备份模式和多站点模式支持快得多的 RTO，但是由于需要一直运行的额外系统，因此成本会更高。

您能够使用 AWS 经济高效地执行每种灾难恢复策略。重要的是要注意，这里列举的只是一些可行的模式示例，您也可以有多种模式变体或将其组合使用。如果您的应用程序在 AWS 上运行，则可以使用多个区域，同样的灾难恢复策略仍然适用。

灾难恢复准备：最佳实践

简单开始

检查软件许可问题

方案演练
练习

制定全面的灾难恢复计划可能是一项复杂的任务。但是，大多数组织都认识到（可能是从过去的事件中吸取经验教训），这值得付出努力。

尽管制定和实施完整计划需要时间，但这不应阻止您迈出简单的第一步。简单开始，然后再自行扩展。例如，作为第一步，创建数据存储、数据库和关键服务器的备份。然后，作为持续努力的一部分，努力逐步改善 RTO 和 RPO。

软件许可证是创建备份站点时可能会出现的问题。查看您必须获得的软件许可证，以确定当前的许可证合同是否支持您的灾难恢复计划。根据需要升级许可证或以其他方式进行调整。

最后，始终如一地运用灾难恢复解决方案是一种最佳做法，以确保其按预期工作。一些建议的步骤包括：

- 方案演练。这些练习可测试关键系统脱机的场景，甚至整个区域。如果整个队列崩溃，该怎么办？
- 确保正在创建备份、快照和 AMI，并且可以使用它们成功恢复数据。
- 监控您的监控系统。

测试您的响应程序，确保它们有效且团队熟知如何将其付诸实践。设置定期的实际试用，以测试工作负载和团队对模拟事件的反应。

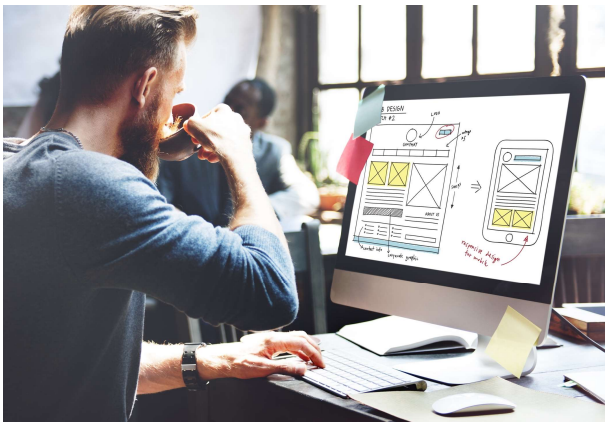
第 3 节要点

- AWS 上常见的灾难恢复模式包括备份和恢复、“Pilot light”式、热备份模式和多站点。
- 备份和恢复是最具成本效益的方法。但是，它拥有最高的 RTO。
- 多站点提供了最快的 RTO。但是，它的成本最高是因为它提供了一个完全运行的生产就绪副本。
- AWS Storage Gateway 提供三个接口（文件网关、卷网关和磁带网关），用于本地和 AWS 云之间的数据备份和恢复。

本模块中这节内容的要点包括：

- AWS 上常见的*灾难恢复模式*包括备份和恢复、“Pilot light”式、热备份模式和多站点。
- *备份和恢复*是最经济高效的方法，但它具有最高的 RTO。
- *多站点*提供了最快的 RTO，但其成本最高，因为它提供了一个完全运行的生产就绪副本。
- *AWS Storage Gateway* 提供三个接口（文件网关、卷网关和磁带网关），用于本地和 AWS 云之间的数据备份和恢复。

模块 14 – 指导实验：使用 AWS Storage Gateway 文件网关进行混合存储和数据迁移



现在，您将完成开始模块 14 – 指导实验：使用 AWS Storage Gateway 文件网关进行混合存储和数据迁移

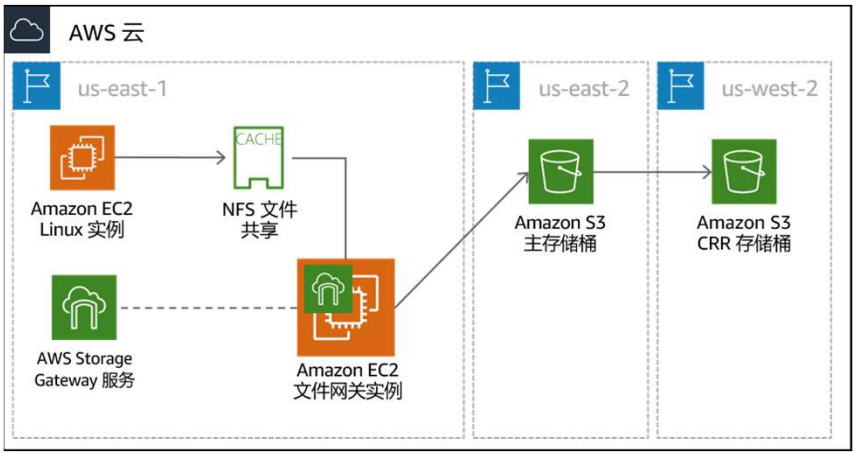
指导实验：任务

1. 查看实验架构
2. 创建主 S3 存储桶和辅助 S3 存储桶
3. 启用跨区域复制
4. 配置文件网关并创建 NFS 文件共享
5. 将文件共享挂载到 Linux 实例并迁移数据
6. 验证数据是否已迁移

在本指导实验中，您将完成以下任务：

1. 查看实验架构
2. 创建主 S3 存储桶和辅助 S3 存储桶
3. 启用跨区域复制
4. 配置文件网关并创建 NFS 文件共享
5. 将文件共享挂载到 Linux 实例并迁移数据
6. 验证数据是否已迁移

指导实验：最终产品



该图总结了您完成指导实验后将会构建的内容。您将使用 AWS Storage Gateway 中的文件网关选项成功将数据迁移到 Amazon S3。

现在可以开始指导实验了。

指导实验总结：要点

完成这个指导实验之后，您的讲师可能会带您讨论此指导实验的要点。

模块 14：灾难规划

模块总结

现在来回顾下本模块，并对知识测验和对实践认证考试问题的讨论进行总结。

模块总结

aws academy

总体来说，您在本模块中学习了如何：

- 确定灾难规划策略
- 定义 RPO 和 RTO
- 描述备份和灾难恢复的四种常见模式以及实施方法
- 使用 AWS Storage Gateway 实现本地到云备份解决方案

总体来说，您在本模块中学习了如何：

- 确定灾难规划策略
- 定义 RPO 和 RTO
- 描述备份和灾难恢复的四种常见模式以及实施方法
- 使用 AWS Storage Gateway 实现本地到云备份解决方案

完成知识测验

现在可以完成本模块的知识测验。

样题

aws academy

公司销售人员每天上传销售数据。解决方案架构师需要为这些文档提供持久存储解决方案，以防止用户意外删除重要文档。

哪项操作可以防止用户意外操作？

A. 将数据存储在 EBS 卷中，并每周创建一次快照。
B. 将数据存储在 S3 存储桶中并启用版本控制。
C. 将数据存储在不同 AWS 区域的两个 S3 存储桶中。
D. 将数据存储在 EC2 实例存储中。

请查看答案选项，并根据之前突出显示的关键字排除错误选项。

正确答案是 B：“将数据存储在 S3 存储桶中并启用版本控制。” 使用这种方法，如果删除了某个受版本控制的对象，仍然可以通过检索最终版本来恢复该对象。

选项 A 将丢失自上一个快照以来提交的任何更改。选项 C 将数据存储在两个 S3 存储桶中，它提供的保护比选项 A 稍大一些。但是，用户仍然可以从两个存储桶中删除对象。选项 D 不是一种好方法，因为 EC2 实例存储是短暂的，并且永远不要应用于需要持久性的数据。

其他资源

- Amazon S3 复制
- Amazon S3 对象生命周期管理
- Amazon EBS 快照
- 将 AWS Lambda 用于计划的事件
- 备份和还原资源中心
- 借助 AWS 实现灾难恢复（视频）

如果您想了解本模块所涵盖主题的更多信息，下面这些资源可能会有所帮助：

- Amazon S3 复制
- Amazon S3 对象生命周期管理
- Amazon EBS 快照
- 将 AWS Lambda 用于计划的事件
- 备份和还原资源中心
- 借助 AWS 实现灾难恢复（视频）

感谢您完成本模块的学习。