

文章

[Li Yan](#) · 一月 18, 2021 阅读大约需 22 分钟

在 Amazon EC2 上部署 InterSystems 技术 - 参考架构

企业需要快速有效地扩展和管理其全球计算基础设施，同时优化和管理资本成本及支出。Amazon Web Services (AWS) 和 Elastic Compute Cloud (EC2)

计算和存储服务提供高

度稳健的全球化的计算基础设施，可满足最苛刻的基于 Caché 的应用程序的需求。Amazon EC2 基础设施使各公司能够迅速预置计算能力和/或快速灵活地将其现有内部基础架构扩展到云端。AWS 针对安全、网络、计算和存储提供了一套丰富的服务和强大的企业级机制。

AWS 的核心是 Amazon EC2。

它是支持各种操作系统和机器配置（例如 CPU、RAM、网络）的云计算基础设施。AWS 提供预先配置的虚拟机 (VM) 映像（称为 Amazon 系统映像或 AMI），客户操作系统包括各种 Linux® 和 Windows 发行版及版本。可以将其它软件用作 AWS 中运行的虚拟化实例的基础。您可以将这些 AMI 用作实例化以及安装或配置其他软件、数据等的起点，以创建特定于应用程序或工作负载的 AMI。

与任何平台或部署模式一样，必须留心以确保考虑到应用程序环境的各个方面，例如性能、可用性、操作和管理程序。

本文将详细介绍以下每个方面。

- **网络设置和配置。** 此部分介绍基于 Caché 的应用程序在 AWS 中的网络设置，包括为参考架构内不同层级和角色的逻辑服务器组提供支持的子网。
- **服务器设置和配置。** 此部分介绍为每一层设计各种服务器时涉及的服务和资源。还包括用于跨可用区实现高可用性的架构。
- **安全。** 此部分讨论 AWS 中的安全机制，包括如何配置实例和网络安全以实现整体解决方案以及层和实例之间的授权访问。
- **部署和管理。** 此部分提供有关打包、部署、监控和管理的详细信息。

架构和部署方案

本文提供了几个在 AWS 内实现的参考架构，作为提供基于 InterSystems 技术（包括 Caché、Ensemble、HealthShare、TrakCare）以及相关嵌入式技术（如 DeepSee、iKnow、CSP、Zen 和 Zen Mojo）的高性能和高可用性应用程序的示例。

为了了解如何在 AWS 上托管 Caché 及相关组件，我们先来回顾一下典型 Caché 部署的架构和组件，并探讨一些常见的方案和拓扑。

[Caché 架构回顾](#)

InterSystems

数据平台不断发展，提供先进的数据库管理系统和快速的应用程序开发环境，以在处理和分析复杂数据模型以及开发 Web 和移动应用程序方面实现突破。

这是新一代的数据库技术，提供多种数据访问模式。

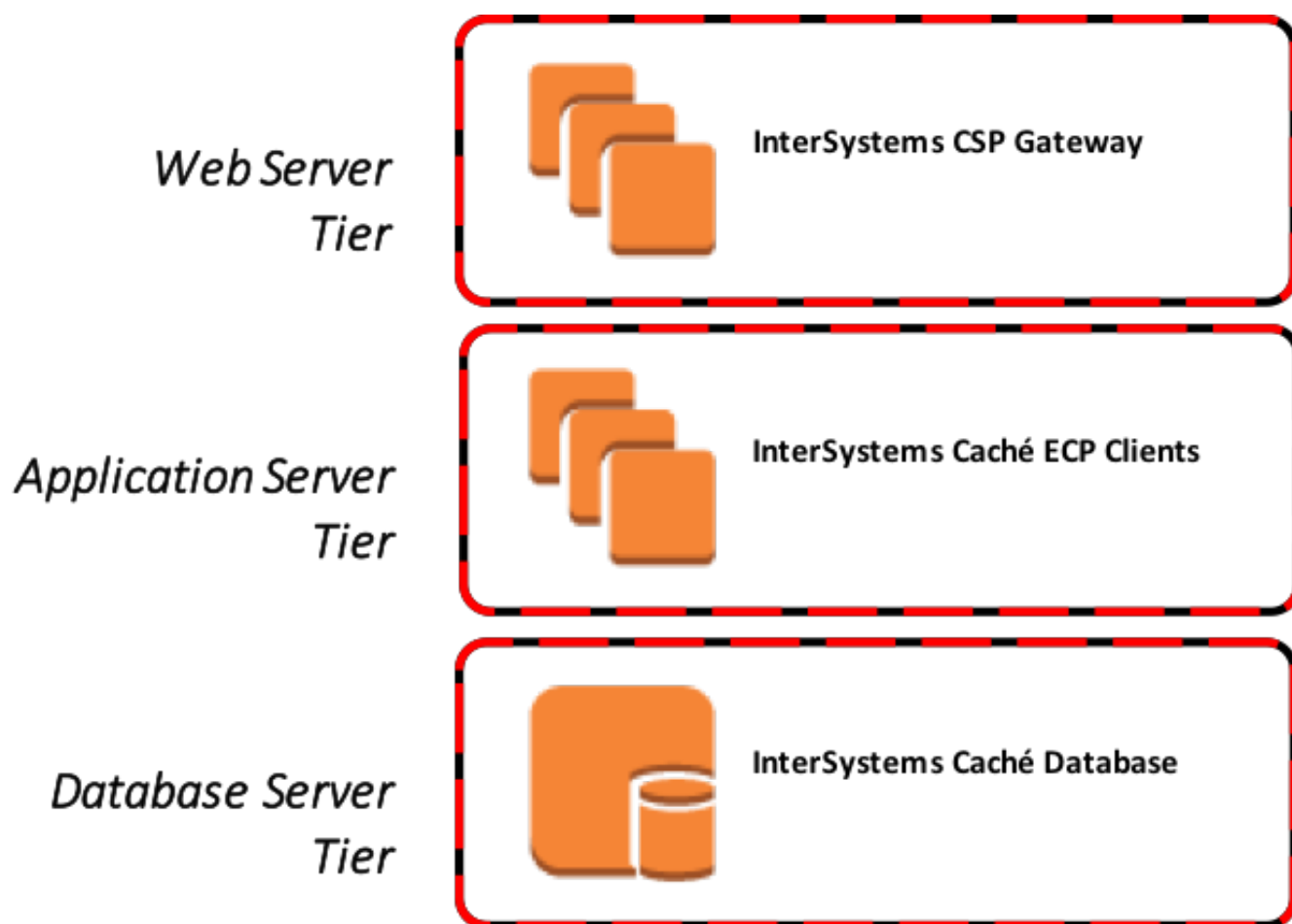
数据只在单个集成数据字典

中描述一次，并且可以通过对象访问、高性能 SQL

和强大的多维存取即时进行访问 – 所有这些方式可以同时访问相同数据。

图 1 说明了可用的 Caché 高级架构组件层和服务。这些通用层也适用于 InterSystems TrakCare 和 HealthShare 产品。

图 1：高级组件层



常见部署方案

部署有许多可能的组合，但本文将介绍两种方案：混合模型和完整的云托管模型。

混合模型

在此方案中，公司希望在需要时将企业内部资源和 AWS

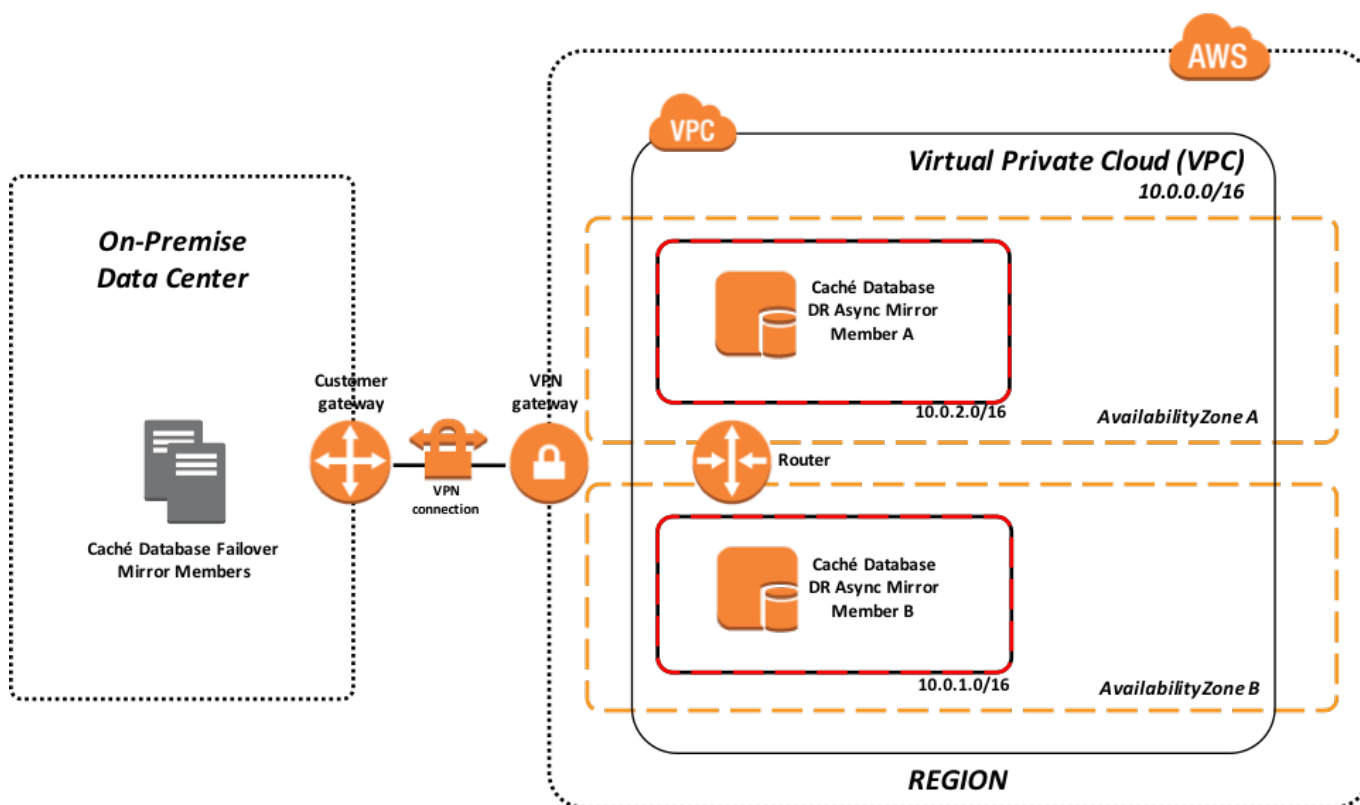
EC2 资源都用于灾难恢复、内部维护应急、重新平台化计划或短期/长期扩容。

此模型可以为内部故障转移镜像成员集群提供业务连续性和灾难恢复的高可用性。

在该方案中，此模型的连接依赖于内部部署和 AWS 可用区之间的 VPN 隧道，将 AWS 资源作为企业数据中心的扩展。还有其他连接方法，例如 AWS Direct Connect_。但是，这不是本文涵盖的内容。有关 AWS Direct Connect 的更多详细信息，可以在[here](#)找到。

有关设置此 Amazon Virtual Private Cloud (VPC) 示例以支持内部数据中心灾难恢复的详细信息可以在[here](#)找到。

图 2：使用 AWS VPC 提供内部灾难恢复的混合模型



上面的示例展示了一个故障转移镜像对通过与 AWS VPC 的 VPN 连接在内部数据中心的运行。所示的 VPC 在给定 AWS 区域的双可用区中提供了多个子网。有两个灾难恢复 (DR) 异步镜像成员 (每个可用区有一个) 提供弹性。

云托管模型

在此方案中，基于 Caché 的应用程序（包括数据层和表示层）完全放在 AWS 云中，使用了单个 AWS 区域内的多个可用区。可以使用相同的 VPN 隧道 AWS Direct Connect，甚至纯互联网连接模型。

图 3：支持完整生产工作负载的云托管模型

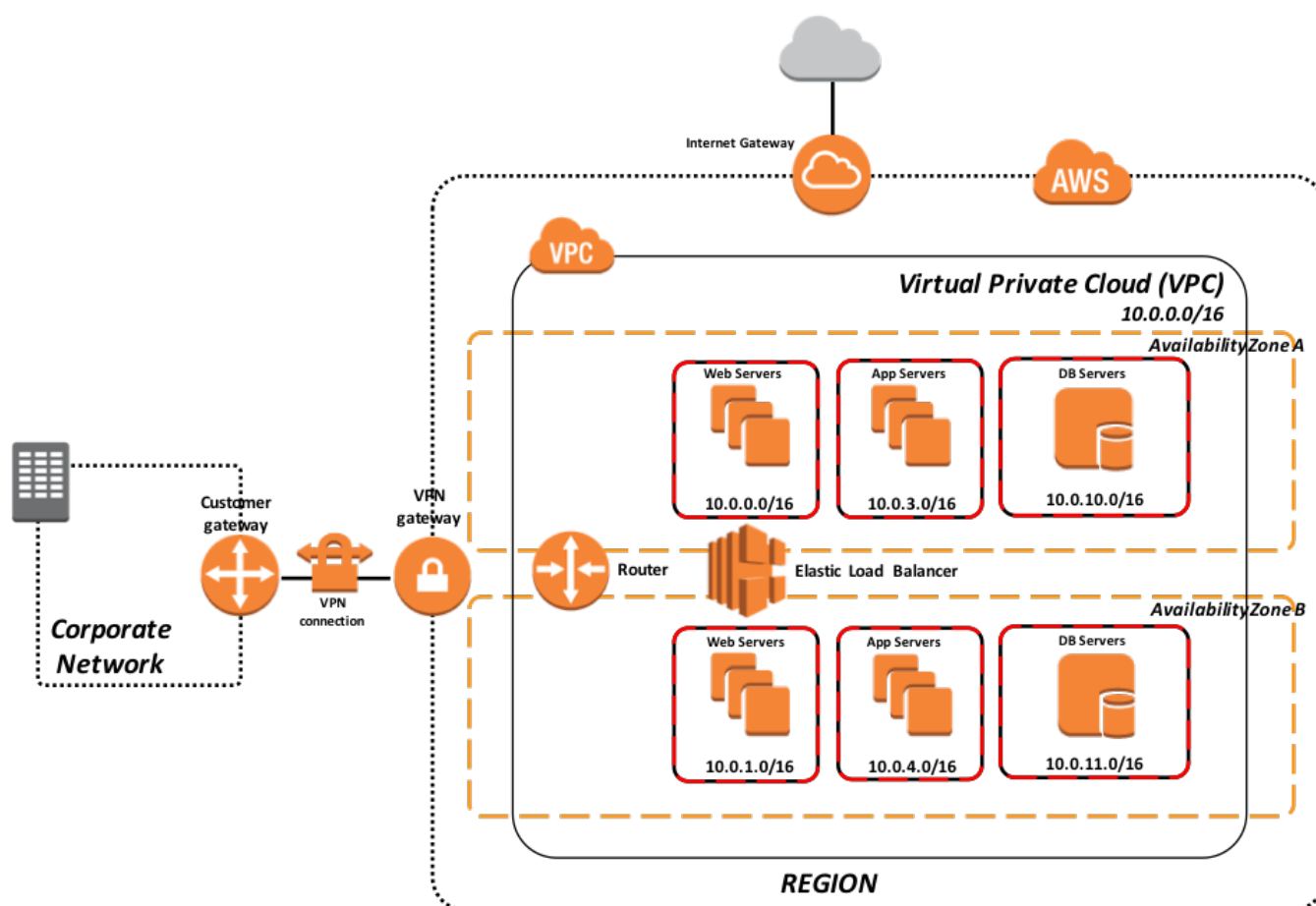


图 3 中的示例说明了在 VPC 中支持整个应用程序生产部署的部署模型。

此模型利用双可用区，在可

用区之间同步故障转移镜像，同时将负载均衡 Web 服务器和相关应用程序服务器作为 ECP 客户端。

每个层都隔离在一个单独的安全组中，

以进行网络安全控制。IP 地址和端口范围仅根据应用程序的需要开放。

存储和计算资源

存储

有多种类型的存储选项可供选择。就本参考架构而言，将针对几种可能的用例讨论 *Amazon Elastic Block Store* (Amazon EBS) 和（也称为临时驱动器）卷。

各种存储选项的更多详细信息可以在 [here](#) 和 [here](#) 找到。

[Elastic Block Storage \(EBS\)](#)

EBS 提供了可与 Amazon

EC2 实例（虚拟机）配合使用的持久块级存储，在 Linux 或 Windows

中可以将其格式化并挂载为传统文件系统，最重要的是，这些卷是非实例存储，独立于单个 Amazon EC2 实例的运行寿命而持续存在，这对于数据库系统非常重要。

此外，Amazon EBS 还提供了创建卷的时间点快照的功能，这些快照会持久保存在 Amazon S3 中。

这些快照可以用作新的 Amazon EBS 卷的起点，并保护数据以实现长期耐久性。同一快照可用于实例化任意数量的卷。这些快照可以跨 AWS 区域复制，因此可以更容易地利用多个 AWS 区域进行地理扩张、数据中心迁移和灾难恢复。Amazon EBS 卷的大小范围为 1 GB 到 16 TB，以 1 GB 为增量进行分配。

Amazon EBS 内有三种不同的类型：磁介质卷、通用型 (SSD) 和预置 IOPS (SSD)。以下各小节提供了每种类型的简要介绍。

磁介质卷

磁介质卷为具有中等或突发 I/O 要求的应用程序提供经济高效的存储。磁介质卷设计为平均每秒提供约 100 次输入/输出操作 (IOPS)，最大突发能力为数百 IOPS。磁介质卷也非常适合用作启动卷，其突发能力提供了快速的实例启动时间。

通用型 (SSD)

通用型 (SSD) 卷提供具有成本效益的存储，是各种工作负载的理想选择。这些卷的延迟只有个位数毫秒，能够长时间突发至 3,000 IOPS，基准性能为 3 IOPS/GB，最高可达 10,000 IOPS (3,334 GB)。通用型 (SSD) 卷的大小范围为 1 GB 到 16 TB。

预置 IOPS (SSD)

预置 IOPS (SSD) 卷设计用于为 I/O 密集型工作负载（例如对存储性能和随机访问 I/O 吞吐量的一致性敏感的数据库工作负载）提供可预测的高性能。在创建卷时指定 IOPS 速率，然后 Amazon EBS 在给定一年的 99.9% 的时间内提供 10% 内的预置 IOPS 性能。预置 IOPS (SSD) 卷的大小可以为 4 GB 到 16 TB，每个卷最多可预置 20,000 IOPS。预置的 IOPS 与请求的卷大小之比最大为 30；例如，IOPS 为 3,000 的卷必须至少为 100 GB 大小。预置 IOPS (SSD) 卷对每个预置的 IOPS 的吞吐量限制为 256 KB，最高 320 MB/秒 (1,280 IOPS)。

本文讨论的架构使用 EBS 卷，因为这些卷更适合需要可预测的低延迟每秒输入/输出操作 (IOPS) 和吞吐量的生产工作负载。选择特定的虚拟机类型时必须小心，因为并非所有 EC2 实例类型都可以访问 EBS 存储。

注意: 由于 Amazon EBS 卷是网络附加设备，Amazon EC2 实例执行的其他网络 I/O 以及共享网络上的总负载可能会影响单个 Amazon EBS 卷的性能。为了让 Amazon EC2 实例充分利用 Amazon EBS 卷上的预置 IOPS，可以将选定的 Amazon EC2 实例类型作为 Amazon EBS 优化的实例启动。

有关 EBS 卷的详细信息，可以在[here](#) 找到。

EC2 实例存储（临时驱动器）

EC2 实例存储由托管您的正在运行的 Amazon EC2 实例的同一台物理服务器上的磁盘存储的预配置和预附加块组成。提供的磁盘存储量因 Amazon EC2 实例类型而异。在提供实例存储的 Amazon

EC2 实例系列中，较大的实例往往提供更多更大的实例存储量。

存储优化 (I2) 和密集存储 (D2) 的 Amazon EC2 实例系列提供针对特定用例的专用实例存储。例如，I2 实例提供了非常快的 SSD 实例存储，能够支持超过 365,000 的随机读取 IOPS 和 315,000 的写入 IOPS，并提供具有成本吸引力的定价模型。

与 EBS 卷不同，该存储不是永久性的，只能用于实例的生命周期，不能分离或附加到其他实例。实例存储用于临时存储不断变化的信息。在 InterSystems 技术和产品领域中，诸如将 Ensemble 或 Health Connect 用作企业服务总线 (ESB) 的项目、使用企业缓存协议 (ECP) 的应用程序服务器或将 Web 服务器与 CSP 网关一起使用，对于这种类型的存储和存储优化的实例类型，以及使用预置和自动化工具来提高有效性和支持弹性的操作来说，都是很好的用例。

有关实例存储卷的详细信息，可以在[here](#) 找到。

计算

EC2 实例

有多种实例类型可供使用，它们针对各种用例进行了优化。实例类型包括 CPU、内存、存储和网络容量的不同组合，从而实现无数种组合来合理调整您的应用程序的资源要求。

就本文档而言，将参考 `_通用 M4_Amazon` EC2 实例类型作为优化环境大小的方法，这些实例提供 EBS 卷的功能和优化。根据您的应用程序的容量要求和定价模型，还可能有替代方案。

M4 实例是最新一代的 `_通用_` 实例。此系列提供了计算、内存和网络资源的平衡配置，对于许多应用程序来说是很好的选择。容量范围为 2 到 64 个虚拟 CPU 和 8 到 256GB 的内存，以及相应的专用 EBS 带宽。

除了各个实例类型，还有分层的分类，例如专用主机、Spot 实例、预留实例和专用实例，每个类别的定价、性能和隔离都不同。

在 [here](#) 确认当前可用实例的可用性和详细信息。

可用性和操作

[Web/App 服务器负载均衡](#)

您的基于 Caché 的应用程序可能需要外部和内部负载均衡的 Web 服务器。外部负载均衡器用于通过互联网或 WAN (VPN 或 Direct Connect) 进行的访问，内部负载均衡器可用于内部流量。AWS Elastic Load Balancing 提供两种类型的负载均衡器 – 应用程序负载均衡器和传统负载均衡器。

传统负载均衡器

传统负载均衡器根据应用程序或网络信息对流量进行路由，是在多个需要高可用性、自动扩展和强大安全性的 EC2 实例之间实现简单的流量负载均衡的理想选择。

具体的详细信息和功能可在[here](#) 找到。

应用负载均衡器

应用程序负载均衡器是 Elastic Load

Balancing 服务的负载均衡选项，该服务在应用程序层运行，允许您根据一个或多个 Amazon EC2 实例上运行的多个服务或容器中的内容定义路由规则。此外，还支持

WebSockets 和 HTTP/2。具体的详细信息和功能可在[here](#)找到。

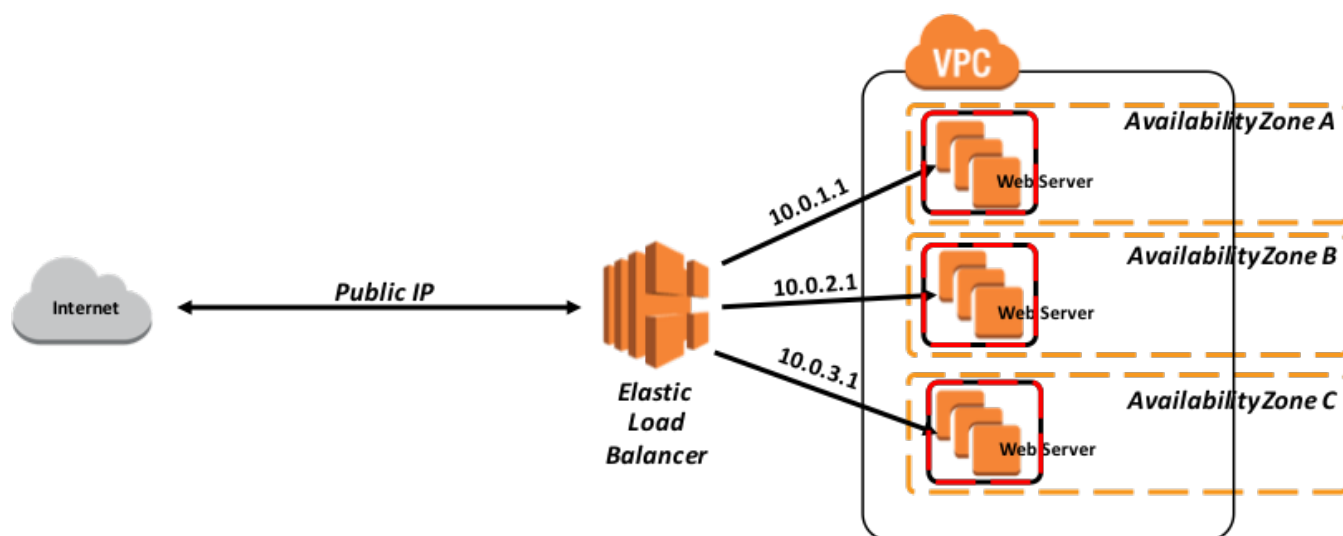
示例

在以下示例中，定义了一组三个 Web

服务器，每个服务器都在一个单独的可用区，以提供最高级别的可用性。必须为 Web 服务器负载均衡器配置粘性会话，才能支持使用 cookie 将用户会话固定到特定 EC2 实例的功能。当用户继续访问您的应用程序时，流量将路由到相同实例。

图 4 给出了 AWS 中的传统负载均衡器的一个简单示例。

图 4：传统负载均衡器示例



数据库镜像

在 AWS 上部署基于 Caché 的应用程序时，如果要为 Caché 数据库服务器提供高可用性，则需要在给定的主 AWS 区域使

用同步数据库

镜像来提供高可用性，还可

能需要使用异步数据库镜像将数据复制到辅助 AWS

区域中的热备份以实现灾难恢复，具体取决于正常运行时间服务水平协议要求。

数据库镜像是两个数据库系统的逻辑分组，也就是所说的故障转移成员，它们在物理上是仅通过网络连接的独立系统。在这两个系统之间进行仲裁后，镜像会自动将其中一个系统指定为主系统；另一个成员自动成为备份系统。外部客户端工作站或其他计算机通过镜像虚拟 IP (VIP) 连接到镜像，该虚拟 IP 在镜像配置期间指定。镜像 VIP 会自动绑定到主镜像系统上的接口。

注意: 在 AWS 中，无法以传统方式配置镜像 VIP，因此设计了替代解决方案。不过，镜像可跨子网获得支持。

目前在 AWS

中部署数据库镜像的建议是，在跨越三个不同可用区的同一个 VPC 中配置三个实例（主要、备份、仲裁器）。这可以确保在任何给定时间，AWS 都将保证可以从外部连接其中的至少两个虚拟机，SLA 达到 99.95%。这样可以为数据库数据本身提供充分的隔离和冗余。有关 AWS EC2 服务水平协议的详细信息，可在[here](#) 找到。

故障切换成员之间的网络延迟没有硬性上限。

延迟增加所产生的影响因应用程序而异。

如果故障转移成员之间的往返时间与磁盘写入服务时间相似，则预计不会产生影响。但是，当应用程序必须等待数据变为持久保存（有时称为日志同步）时，响应时间可能是一个问题。有关数据库镜像和网络延迟的详细信息，可在[here](#) 找到。

虚拟 IP 地址和自动故障转移

大多数 IaaS 云提供商缺乏提供虚拟 IP (VIP) 地址的能力，这种地址通常用在数据库故障转移设计中。为解决这一问题，Caché、Ensemble 和 HealthShare 中增强了几种最常用的连接方法，尤其是 ECP 客户端和 CSP 网关，从而不再依赖 VIP 功能使它们实现镜像感知。

xDBC、直接 TCP/IP 套接字等连接方法或其他直接连接协议仍需要使用 VIP。为解决这些问题，InterSystems 数据库镜像技术通过使用 API 与 AWS Elastic Load Balancer (ELB) 进行交互以实现类似 VIP 的功能，使得在 AWS 中为这些连接方法提供自动故障转移成为可能，从而在 AWS 中提供完整而强大的高可用性设计。

此外，AWS 最近推出了一种新类型的 ELB，称为应用程序负载均衡器。这种类型的负载均衡器在第 7 层运行，支持基于内容的路由，并支持在容器中运行的应用程序。基于内容的路由对于使用分区数据或数据分片部署的大数据类型项目尤其有用。

与虚拟 IP

一样，这是网络配置的突然变化，不涉及任何应用逻辑，不会向已连接到发生故障的主镜像成员的现有客户端发出正在进行故障转移的通知。根据故障的性质，这些连接终止的原因可能是故障本身、应用程序超时或错误、新的主镜像实例强制旧的主镜像实例停机，或者客户端使用的 TCP 保持连接定时器过期。

结果，用户可能必须重新连接并登录。您的应用程序的行为将决定此行为。有关各种类型的可用 ELB 的详细信息，可在[here](#)找到。

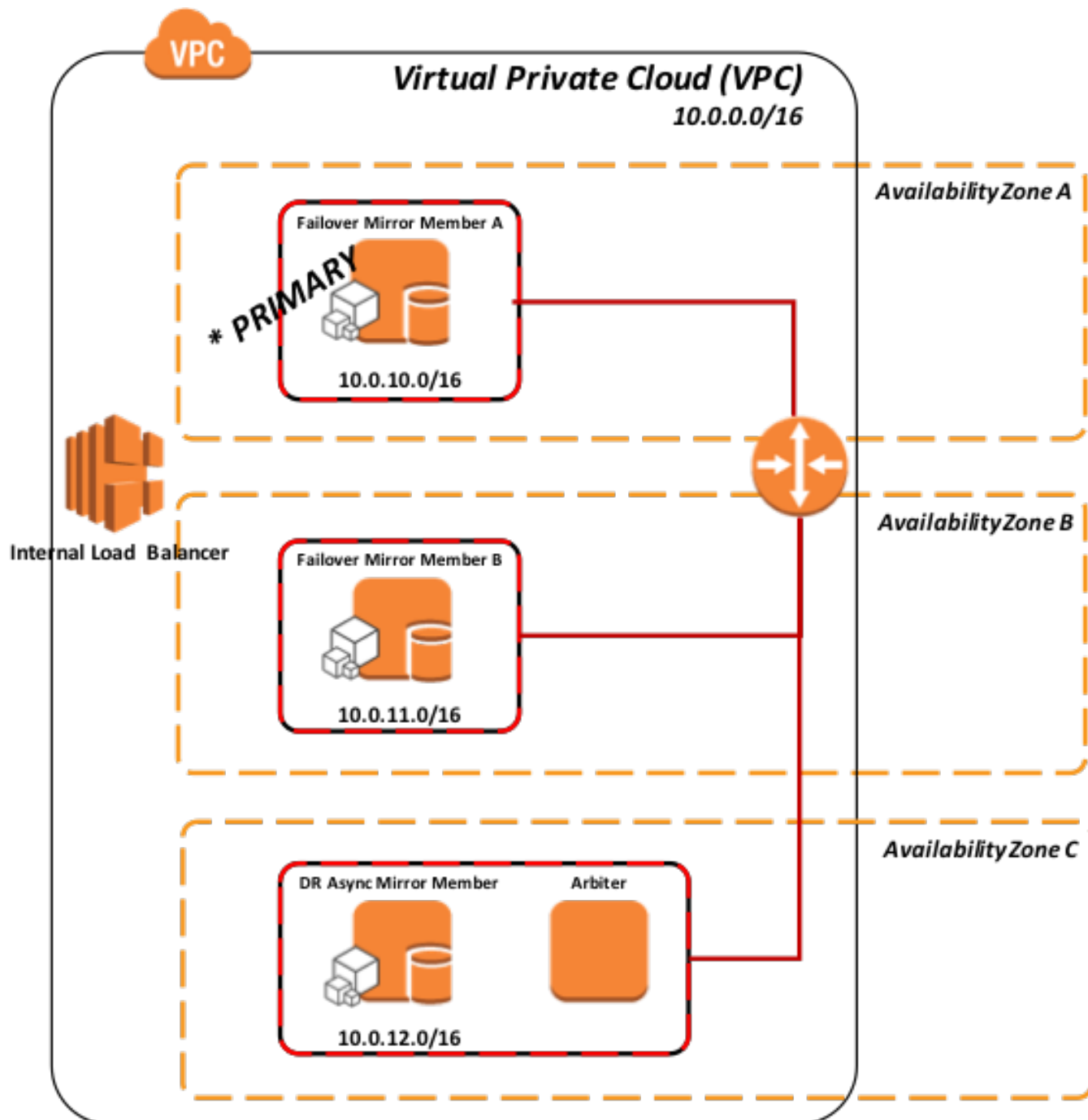
AWS EC2 实例对 AWS Elastic Load Balancer 方法的调用

在此模型中，ELB

可以定义一个包含故障转移镜像成员和潜在 DR

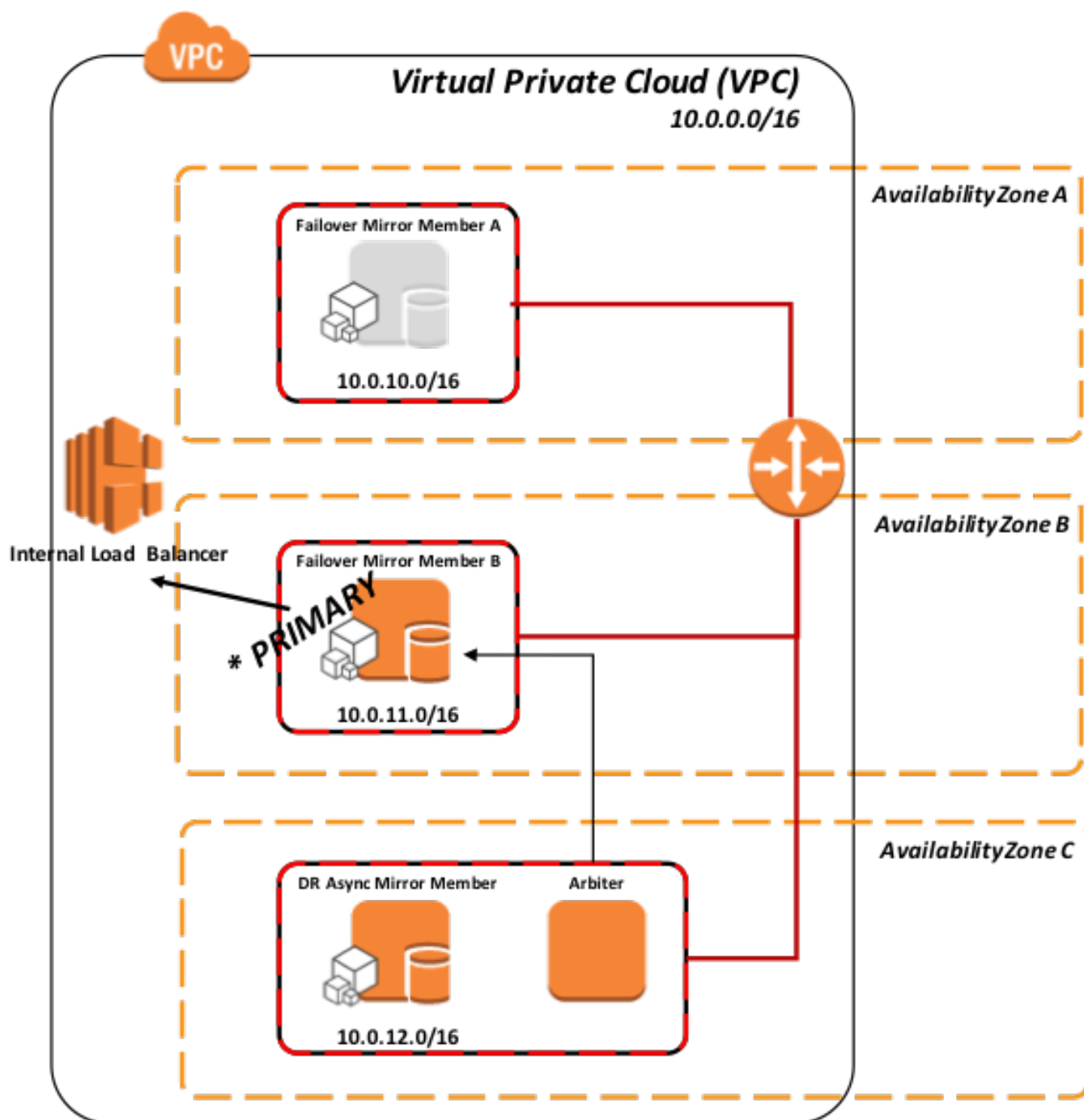
异步镜像成员的服务器池，其中只有一个活动条目是当前主镜像成员，或者只定义一个具有单个活动镜像成员条目的服务器池。

图 5：与 Elastic Load Balancer 交互的 API 方法 (内部)



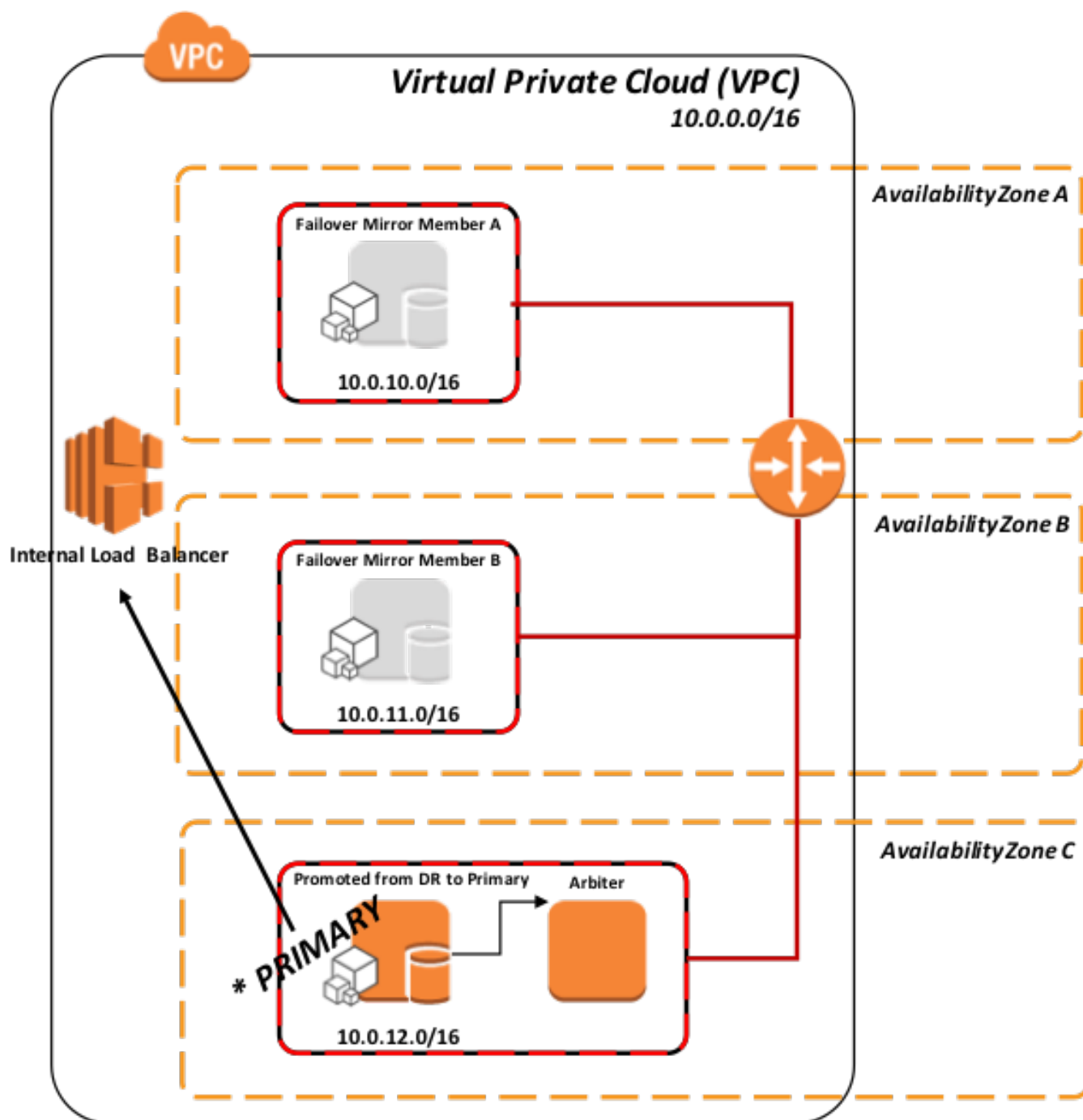
当某个镜像成员成为主镜像成员时，会从您的 EC2 实例向 AWS ELB 发出一个 API 调用，以调整/指示新主镜像成员的 ELB。

图 6：使用负载均衡器的 API 故障转移到镜像成员B



如果主镜像成员和备份镜像成员都变得不可用，同一模型也适用于升级 DR 异步镜像成员。

图 7：使用负载均衡器的 API 将 DR 异步镜像成员升级为主镜像成员



按照标准推荐的 DR 过程，上面的图 6 中的 DR 成员升级需要人为决策，因为异步复制可能会造成数据丢失。不过，一旦执行该操作，就不再需要对 ELB 执行管理操作。在升级期间调用 API 后，将自动路由流量。

API 详细信息

这个用于调用 AWS 负载均衡器资源的 API 在 ^ZMIRROR 例程中专门定义为以下过程调用的一部分：

`$$CheckBecomePrimaryOK^ZMIRROR()`

在此过程内，插入您选择的要从 AWS ELB REST API、命令行界面等使用的任何 API 逻辑或方法。

与 ELB 进行交互的一种有效且安全的方法是使用 AWS Identity and Access Management (IAM) 角色，这样不必为 EC2 实例分配长期凭据。IAM 角色提供了 Caché 可以用来与 AWS ELB 进行交互的临时权限。有关使用分配给 EC2 实例的 IAM 角色的详细信息，可在 [here](#) 找到。

AWS Elastic Load Balancer 轮询方法

2017.1 提供了一种使用 CSP 网关的 *mirrorstatus.cmx* 页的轮询方法，可以将其用作 ELB 监控每个已添加到 ELB 服务器池的镜像成员运行状况的轮询方法。只有主镜像会响应 “SUCCESS” 因而网络流量只定向到活动的主镜像成员。

此方法不需要向 ^ZMIRROR 添加任何逻辑。
请注意，大多数负载均衡网络设备对运行状态检查的频率有限制。
通常，最高频率不少于5秒，这通常是可接受的，可支持大多数正常运行时间服务水平协议。

一个对以下资源的 HTTP 请求将测试本地缓存配置的镜像成员状态。

/csp/bin/mirrorstatus.cmx

对于所有其他情况，这些镜像状态请求的路径应解析到适当的缓存服务器和命名空间，它们与用于请求实际 CSP 页的缓存服务器和命名空间使用相同的分层机制。

示例：在 */csp/user/* 路径中测试服务于应用程序的配置的镜像状态：

/csp/user/mirrorstatus.cmx

注意：调用镜像状态检查不消耗 CSP 许可证。

根据目标实例是否为活动的主要成员，网关将返回以下 CSP 响应之一：

**** Success (Is the Primary Member)**

=====

HTTP/1.1 200 OK

Content-Type: text/plain

Connection: close

Content-Length: 7

SUCCESS

**** Failure (Is not the Primary Member)**

=====

HTTP/1.1 503 Service Unavailable

Content-Type: text/plain

Connection: close

Content-Length: 6

FAILED

**** Failure (The Cache Server does not support the *MirrorStatus.cwx* request)**

=====

HTTP/1.1 500 Internal Server Error

Content-Type: text/plain

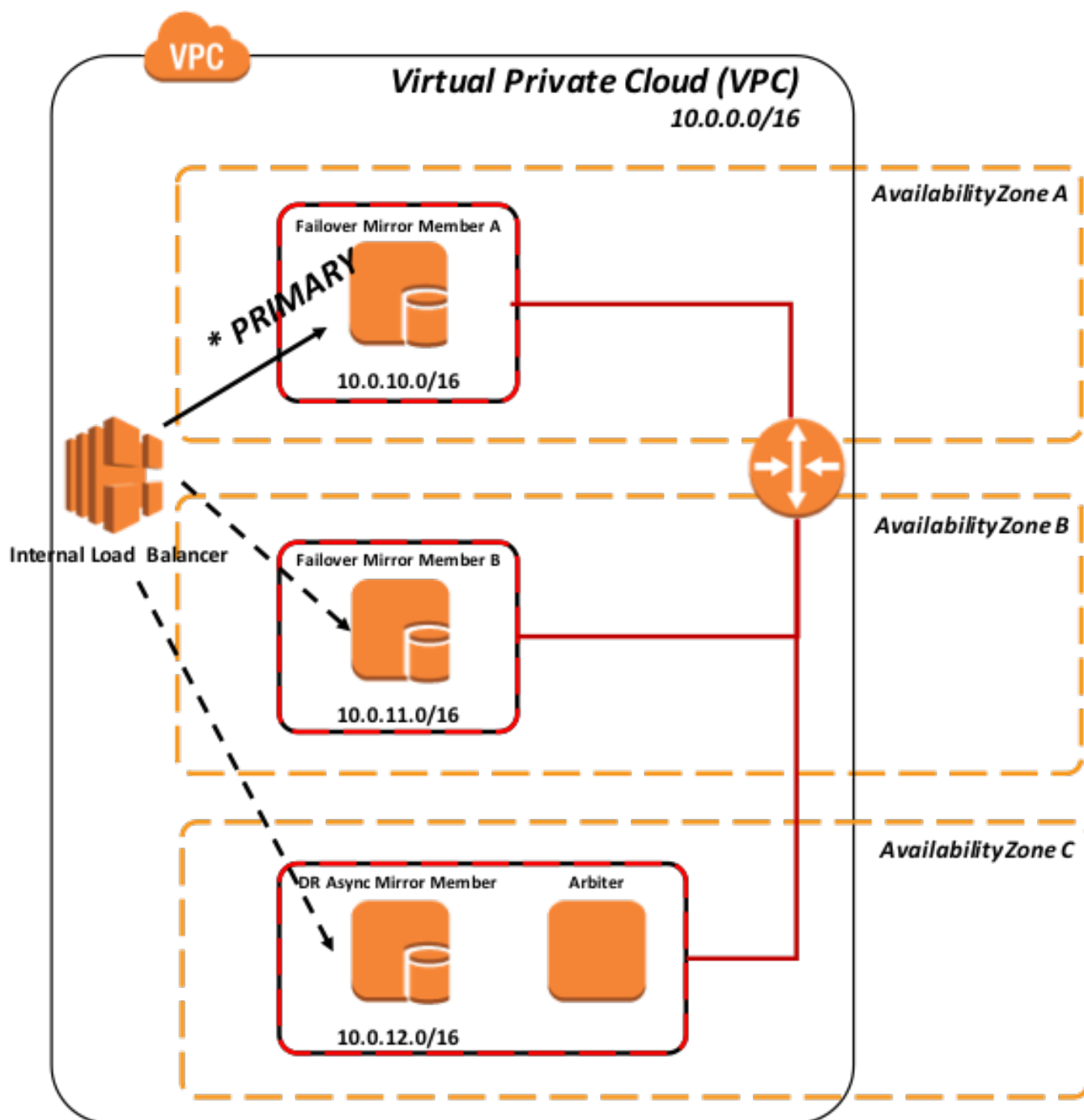
Connection: close

Content-Length: 6

FAILED

下图说明了各种使用轮询方法的方案。

图 8：轮询所有镜像成员

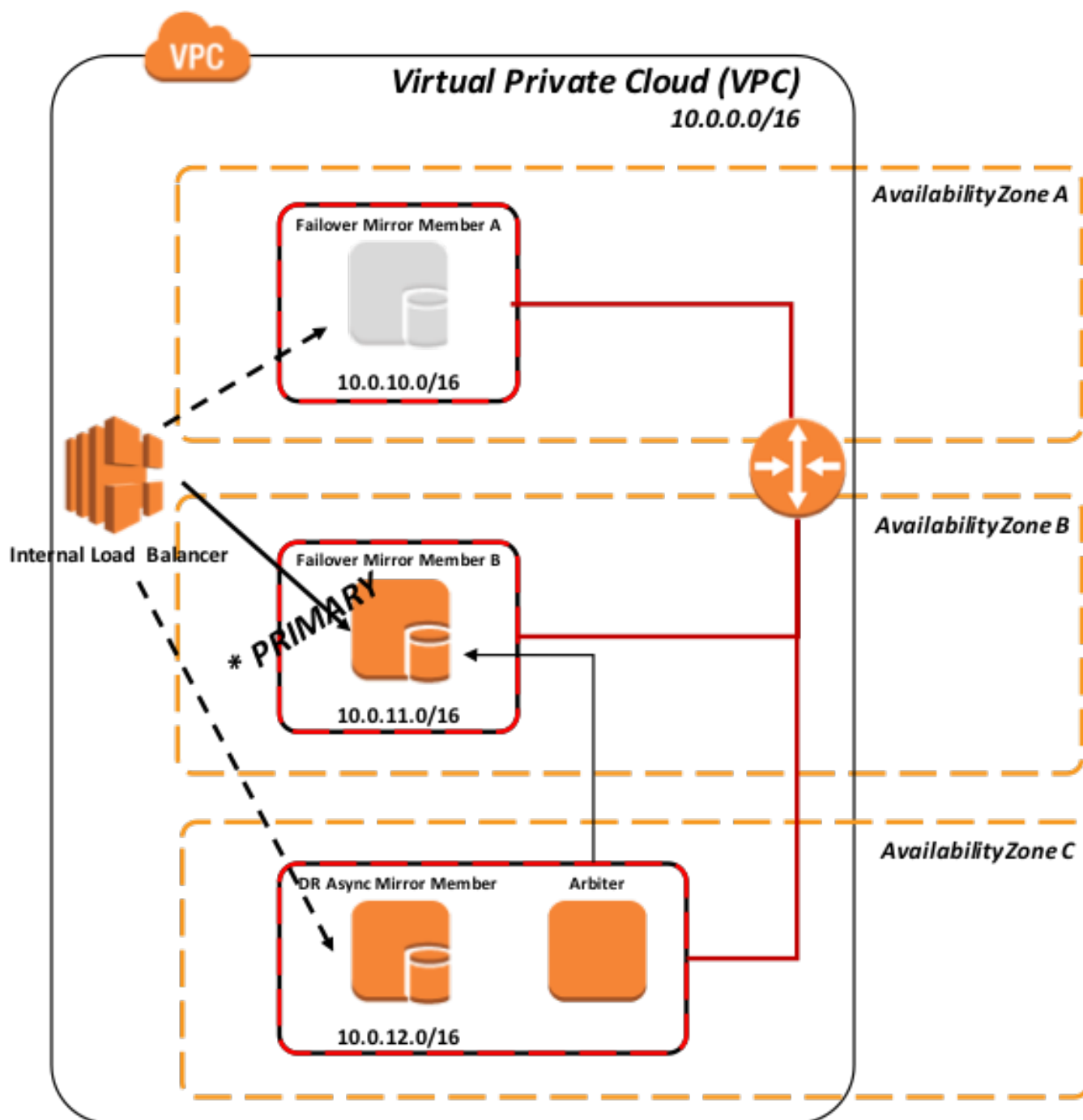


如上面的图 8

所示，所有镜像成员都在运行，只

有主镜像成员向负载均衡器返回 " SUCCESS " 因此网络流量将只定向到该镜像成员。

图 9：使用轮询故障转移到镜像成员 B

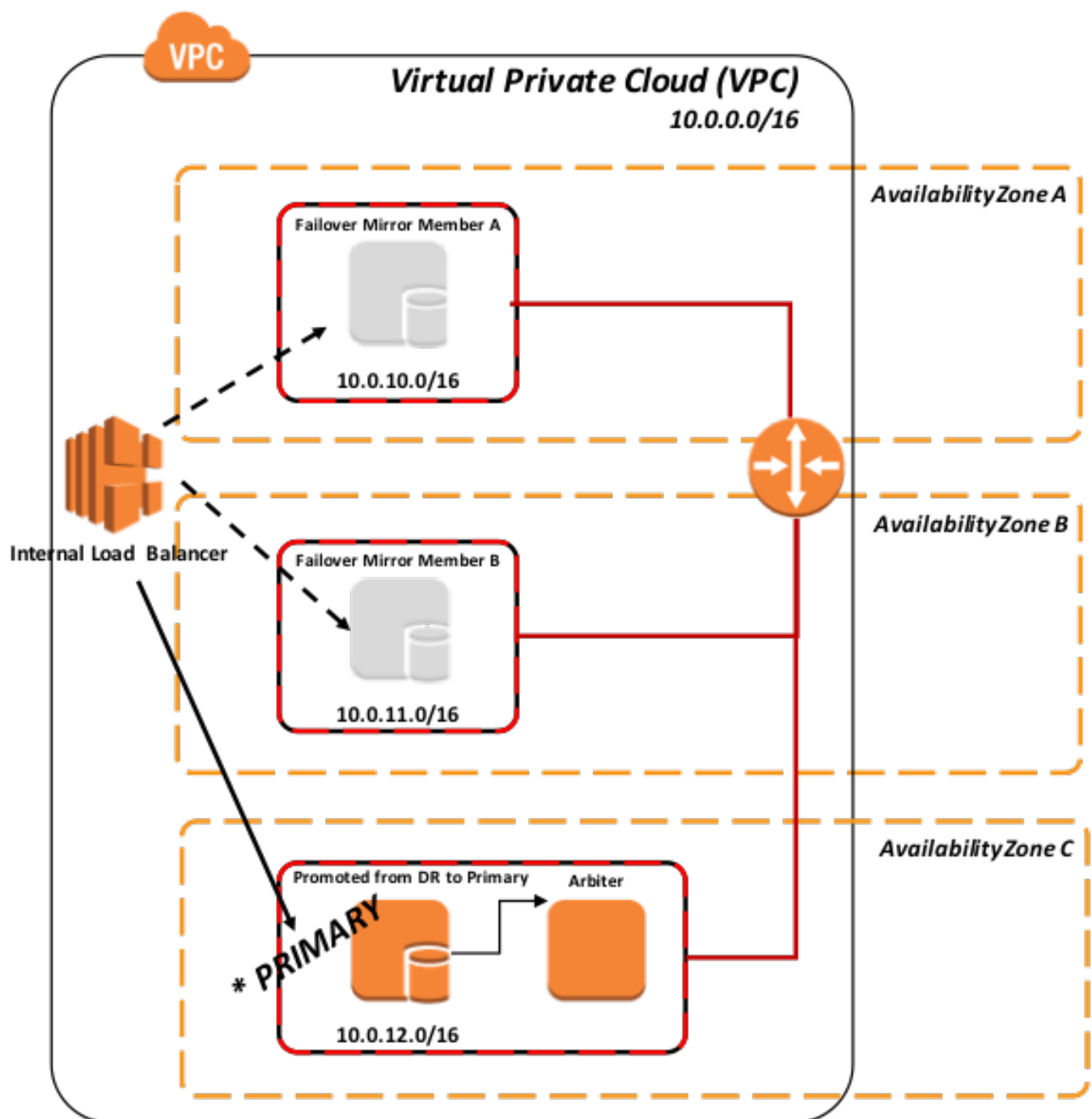


上图演示了将 DR

异步镜像成员升级到负载均衡池中的过程，这通常假定同一台负载均衡网络设备为所有镜像成员提供服务（本文稍后将介绍按地理位置划分的方案）。

按照标准推荐的 DR 过程，DR 成员升级需要人为决策，因为异步复制可能会造成数据丢失。不过，一旦执行该操作，就不再需要对 ELB 执行管理操作。它会自动发现新的主镜像成员。

图 10：使用轮询对 DR 异步镜像成员进行故障转移和升级



备份和还原

备份操作有多个选项。对于 InterSystems 产品的 AWS 部署，可以使用以下三个选项。前两个选项包括一个快照类型过程，该过程在创建快照前会暂停将数据库写入磁盘，然后在快照成功建立后恢复更新。执行以下高级步骤使用任一快照方法创建干净备份：

- 通过数据库冻结 API 调用暂停对数据库的写入。
- 创建操作系统和数据磁盘的快照。
- 通过数据库解锁API 调用恢复 Caché 写入。
- 将设施存档备份到备份位置。

可以定期添加完整性检查等其他步骤，以确保备份干净一致。
决定使用哪个选项取决于组织的运营要求和策略。InterSystems 可与您详细讨论各种选项。

EBS 快照

EBS 快照是在高度可用和成本较低的 Amazon S3

存储上创建时间点快照的非常快速且有效的方法。EBS 快照连同 InterSystems 外部冻结和解锁 API 功能，可以实现真正的 24x7 弹性运行，并确保干净的定期备份。使用 AWS 提供的服务（如 Amazon CloudWatch Events）或市场上的第三方解决方案（如 Cloud Ranger 或 N2W Software Cloud Protection Manager 等等），有许多选项可以使该过程自动化。

此外，还可以使用 AWS 直接 API 调用，以编程方式创建您自己的自定义备份解决方案。有关如何利用 API 的详细信息，请参见[here](#) 和[here](#)。

注意：InterSystems 不为上述任何第三方产品背书或明确进行验证。测试和验证取决于客户。

逻辑卷管理器快照

或者，通过在虚拟机自身内部署单独的备份代理，并利用文件级备份与 Linux 逻辑卷管理器 (LVM) 快照或 Windows 卷影复制服务 (VSS) 相结合，可以使用市场上的许多第三方备份工具。

此模型的主要优点之一是能够对基于 Windows 或 Linux 的实例进行文件级还原。该解决方案有几点需要注意，由于 AWS 和大多数其他 IaaS 云提供商不提供磁带介质，因此所有备份存储库都基于磁盘进行短期归档，而且能够利用 Amazon S3 低成本存储并最终使用 Amazon Glacier 实现长期保留 (LTR)。如果使用此方法，强烈建议使用支持去重技术的备份产品，以最有效地利用基于磁盘的备份存储库。

这些具有云支持的备份产品的示例包括但不限于：Commvault、EMC Networker、HPE Data Protector 和 Veritas Netbackup。

注意：InterSystems 不为上述任何第三方产品背书或明确进行验证。测试和验证取决于客户。

Caché 在线备份

对于小型部署，内置 Caché 在线备份工具也是一个可行选项。该 InterSystems 数据库在线备份实用工具通过捕获数据库中的所有块来备份数据库文件中的数据，然后将输出写入顺序文件。这种专有的备份机制旨在使生产系统的用户不停机。

在 AWS 中，在线备份完成后，必须将备份输出文件和系统使用的所有其他文件复制到用作文件共享的 EC2 (CIFS/NFS)。该过程需要在虚拟机中编写脚本并执行。

在线备份是入门级方法，适合于希望实施低成本备份解决方案的小型站点。但是，随着数据库的增大，建议将使用快照技术的外部备份作为最佳做法，其优势包括：备份外部文件、更快的恢复时间，以及企业范围的数据视图和管理工具。

灾难恢复

在 AWS 上部署基于 Caché 的应用程序时，建议将 DR 资源（包括网络、服务器和存储）放在不同的 AWS 区域中，或者至少放在单独的可用区中。指定的 DR AWS 区域所需的容量取决于您组织的需求。在大多数情况下，以 DR 模式运行时需要 100% 的生产能力，但作为一个弹性模型，可以先预置较少的能力，直到需要更多能力。较少的能力可以体现为较少的 Web 和应用程序服务器，甚至可能使用较小的 EC2 实例类型作为数据库服务器，升级后，EBS 卷将附加到较大的 EC2 实例类型。

异步数据库镜像用于连续复制到 DR AWS 区域的 EC2 实例。镜像使用数据库事务日志以对主系统性能影响最小的方式通过 TCP/IP 网络复制更新。强烈建议对这些 DR 异步镜像成员配置日志文件压缩和加密。

公共互联网上所有希望访问应用程序的外部客户端都将通过作为附加 DNS 服务的 Amazon Route53 进行路由。Amazon Route53 用作将流量定向至当前活动数据中心的交换机。Amazon Route53 执行三种主要功能：

- **域注册** – 允许您注册 example.com 之类的域名。
- **域名系统 (DNS) 服务** – Amazon Route53 将类似 www.example.com 的友好域名转换为 192.0.2.1 之类的 IP 地址。Amazon Route53 使用全球权威 DNS 服务器网络来响应 DNS 查询，从而降低延迟。
- **运行状况检查** – Amazon Route53 通过互联网向您的应用程序发送自动请求，以验证其是否可达、可用和正常运行。

这些功能的详细信息可在 [here](#) 找到。

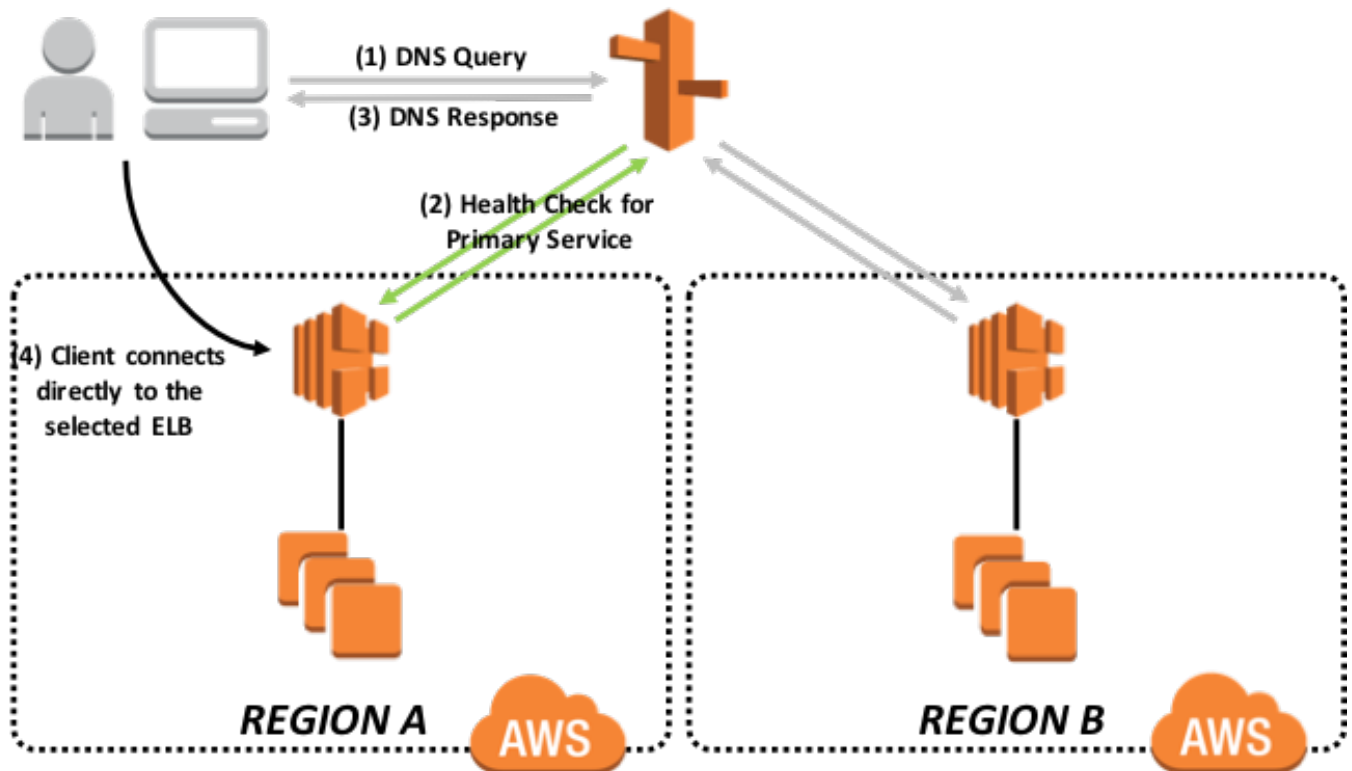
就本文档而言，将讨论 DNS 故障转移和 Route53 运行状况检查。运行状况检查监控和 DNS 故障转移的详细信息可在 [here](#) 和 [here](#) 找到。

Route53 的工作方式是向每个端点发出常规请求，然后验证响应。如果某个端点未能提供有效响应，它将不再包含在 DNS 响应中，而是返回一个替代的可用端点。这样，用户流量就会从发生故障的端点转向可用的端点。

使用上述方法，将只允许流量转向特定区域和特定镜像成员。这是由端点定义控制的，它是本文先前讨论过的 [mirrorstatus.cwx](#) 页，由 InterSystems CSP 网关提供。只有主镜像成员会在运行状况检查中报告 HTTP 200 来表示 “SUCCESS”

下图演示了高级别的故障转移路由策略。此方法和其他策略的详细信息可在 [here](#) 找到。

图 11 : Amazon Route53 故障转移例程策略



在任何给定时间，只有一个区域会根据端点监控进行在线报告。

这样可以确保流量在给定时间只流向一个区域。

区域之间的故障转移无需增加步

骤，因为端点监控将检测到指定的主 AWS

区域中的应用程序已关闭，并且该应用程序此时在次要 AWS 区域中处于活动状态。

这是因为 DR 异步镜像成员已被手动升级为主镜像成员，随后允许 CSP 网关将 HTTP 200 报告给 Elastic Load Balancer 端点监控。

上述解决方案有很多替代方案，可以根据您组织的运营要求和服务水平协议进行自定义。

监控

Amazon CloudWatch 可用于为您的所有 AWS 云资源和应用程序提供监控服务。Amazon CloudWatch

可用于收集和跟踪指标，收集和

监控日志文件，设置警报，并自动对 AWS 资源的变化做出反应。Amazon

CloudWatch 可以监控 AWS 资源，如 Amazon

EC2 实例，以及您的应用程序和服务生成的自定义指标，还有您的应用程序生成的任何日志文件。

您可以使用 Amazon

CloudWatch 获得系统范围内的资源利用率、应用程序性能和运行状况的可见性。

详细信息可在[here](#)找到。

自动预置

目前，市场上有许多工具，包括 Terraform、Cloud Forms、Open Stack 和 Amazon 自己的 CloudFormation。

使用这些工具并与其他工具（如 Chef、Puppet、Ansible

等) 相结合, 可以提供完整的基础设施即代码, 来支持 DevOps 或简单地以完全自动化的方式引导您的应用程序。Amazon CloudFormation 的详细信息可在[here](#)找到。

网络连接

根据您的应用程序的连接要求, 有多种连接模型可用: 使用互联网、VPN 或使用 Amazon Direct Connect 的专用链接。选择方法取决于应用程序和用户需求。三种方法的带宽使用情况各不相同, 最好通过 AWS 代表或 Amazon 管理控制台确认给定区域的可用连接选项。

安全

当决定通过任何公共 IaaS 云提供商部署应用程序时, 都需要谨慎。应遵循您组织的标准安全策略或专门针对云制定的新策略, 以保持您组织的安全合规性。当组织的数据存储在其国家/地区之外, 并受数据所在国家/地区的法律约束时, 相关的数据主权也是您必须了解的。现在, 云部署增加了数据在客户数据中心和物理安全控制之外的风险。强烈建议对静态数据 (数据库和日志) 和动态数据 (网络通信) 使用 InterSystems 数据库和日志加密, 分别使用 AES 和 SSL/TLS 加密。

与所有加密密钥管理一样, 您需要按照您组织的策略记录并遵循正确的程序, 以确保数据安全, 防止不必要的数据访问或安全漏洞。

Amazon 提供了大量文档和示例, 为基于 Caché 的应用程序提供高度安全的运行环境。请务必查看[here](#) 关于 Identity Access Management (IAM) 的各种讨论主题。

架构图示例

下图说明了典型的 Caché 安装, 其以数据库镜像 (同步故障转移和 DR 异步)、使用 ECP 的应用程序服务器, 以及多个负载均衡 Web 服务器的方式提供高可用性。

[TrakCare](#) 示例

下图说明了典型的 TrakCare 部署, 其中包含多个负载均衡 Web 服务器, 两个作为 ECP 客户端的 EPS 打印服务器, 以及数据库镜像配置。虚拟 IP 地址仅用于与 ECP 或 CSP 网关不关联的连接。ECP 客户端和 CSP 网关可感知镜像, 不需要 VIP。

如果您正在使用 Direct Connect, 则可为灾难恢复方案启用包括多线路和多区域访问在内的多个选项。与电信提供商合作以了解他们支持的高可用性和灾难恢复方案至关重要。

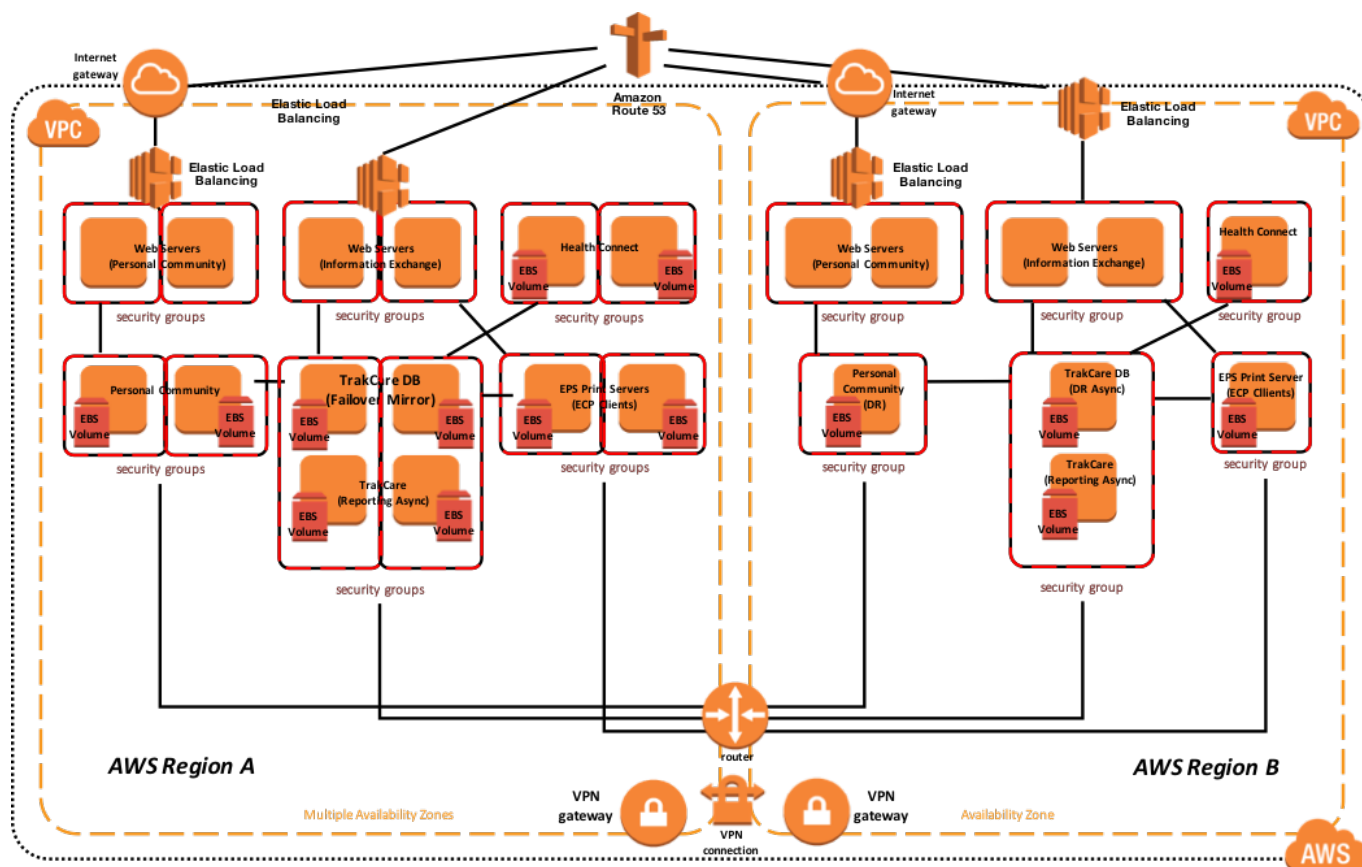
下面的示例参考架构图包括活

动或主要区域中的高可用性，以及在主要 AWS 区域不可用时到其他 AWS 区域的灾难恢复。

而且在此示例中，数据库镜像包含 TrakCare DB、TrakCare

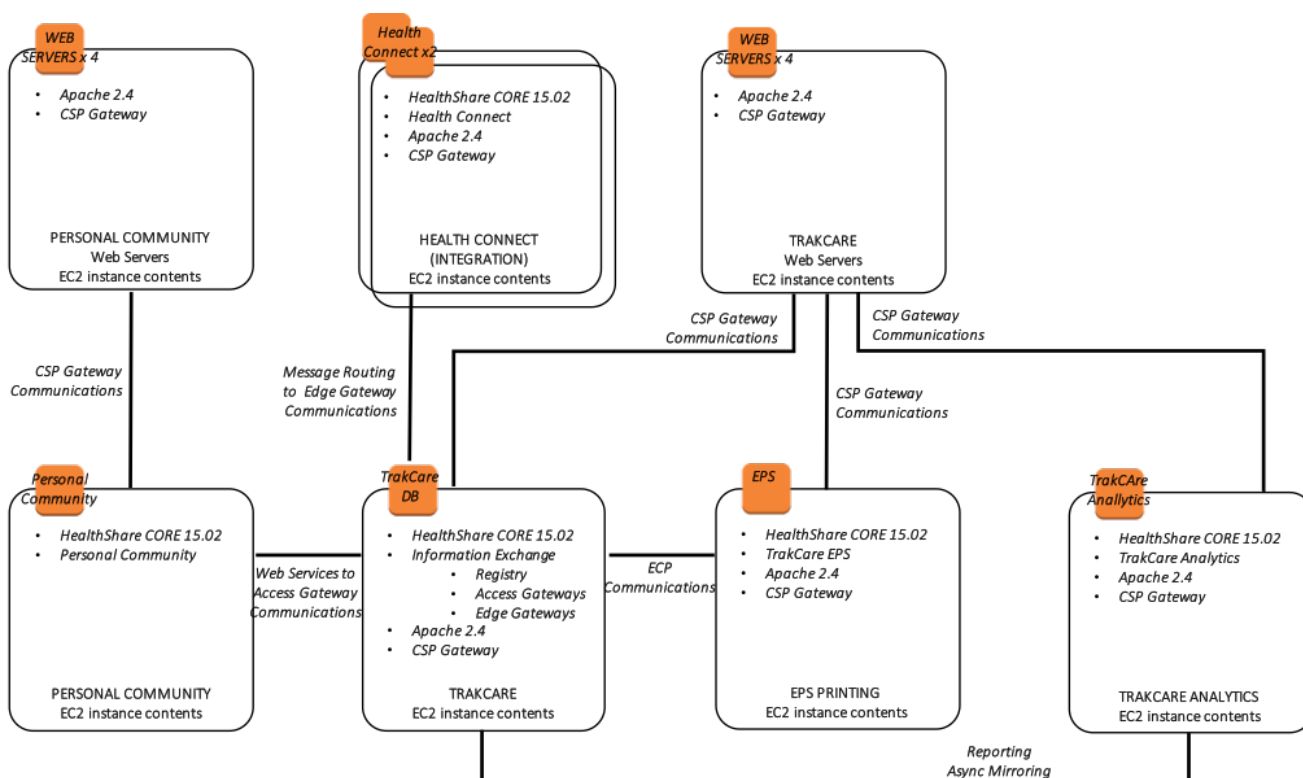
Analytics 和 Integration 命名空间，全部在单个镜像集内。

图 12 : TrakCare AWS 参考架构图 - 物理架构



此外，下图显示了更有逻辑的架构图，其中包含所安装的相关高级软件产品及功能用途。

图 13 : TrakCare AWS 参考架构图 - 逻辑架构



HealthShare 示例

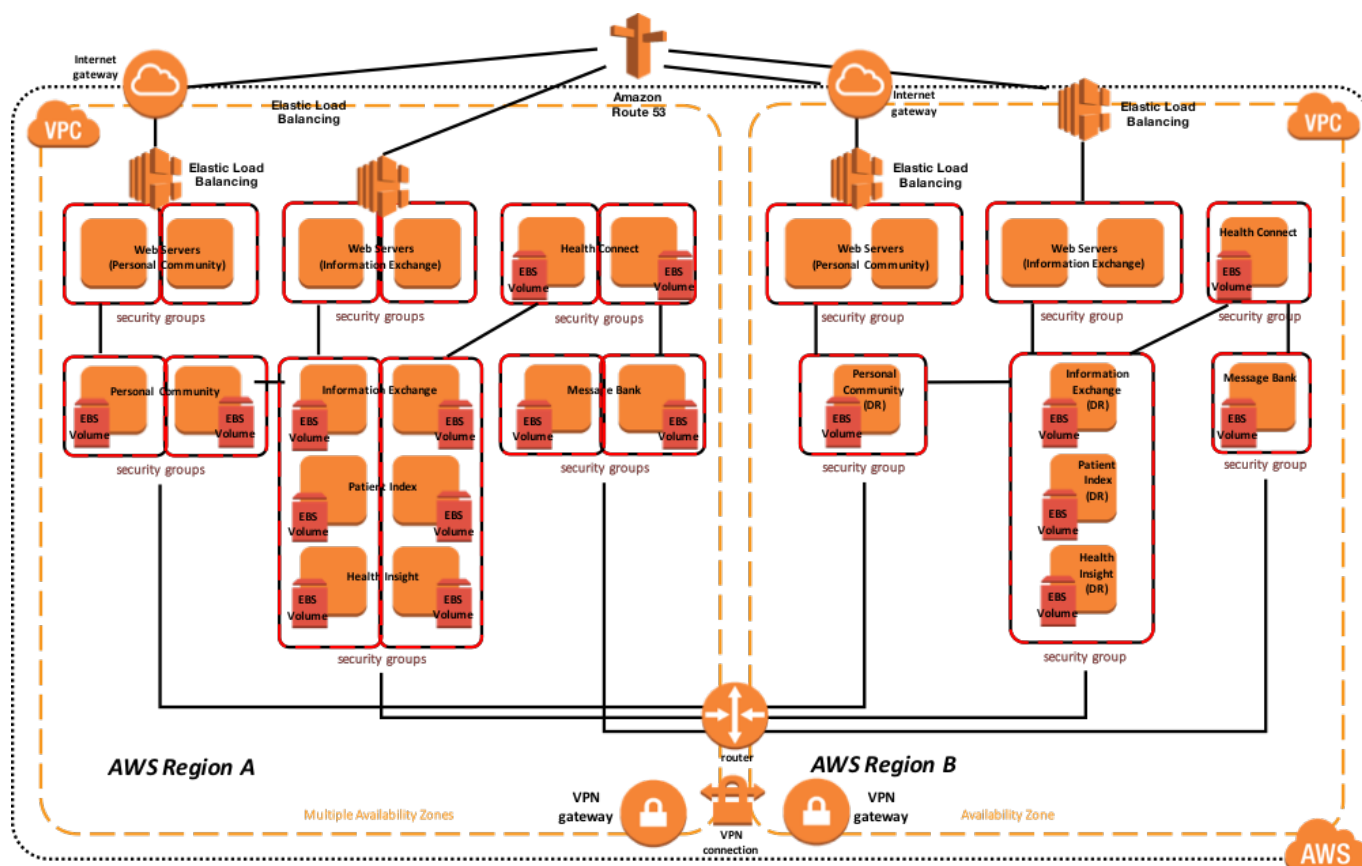
下图显示了一个典型的 HealthShare 部署，其中含有多个负载均衡 Web 服务器，以及多个 HealthShare 产品，包括 Information Exchange、Patient Index、Personal Community、Health Insight 和 Health Connect。这些产品中的每一个都包含一个数据库镜像对，以在多个可用区内提供高可用性。虚拟 IP 地址仅用于与 ECP 或 CSP 网关不关联的连接。用于 HealthShare 产品之间的 Web 服务通信的 CSP 网关可感知镜像，不需要 VIP。

下面的示

例参考架构图包括

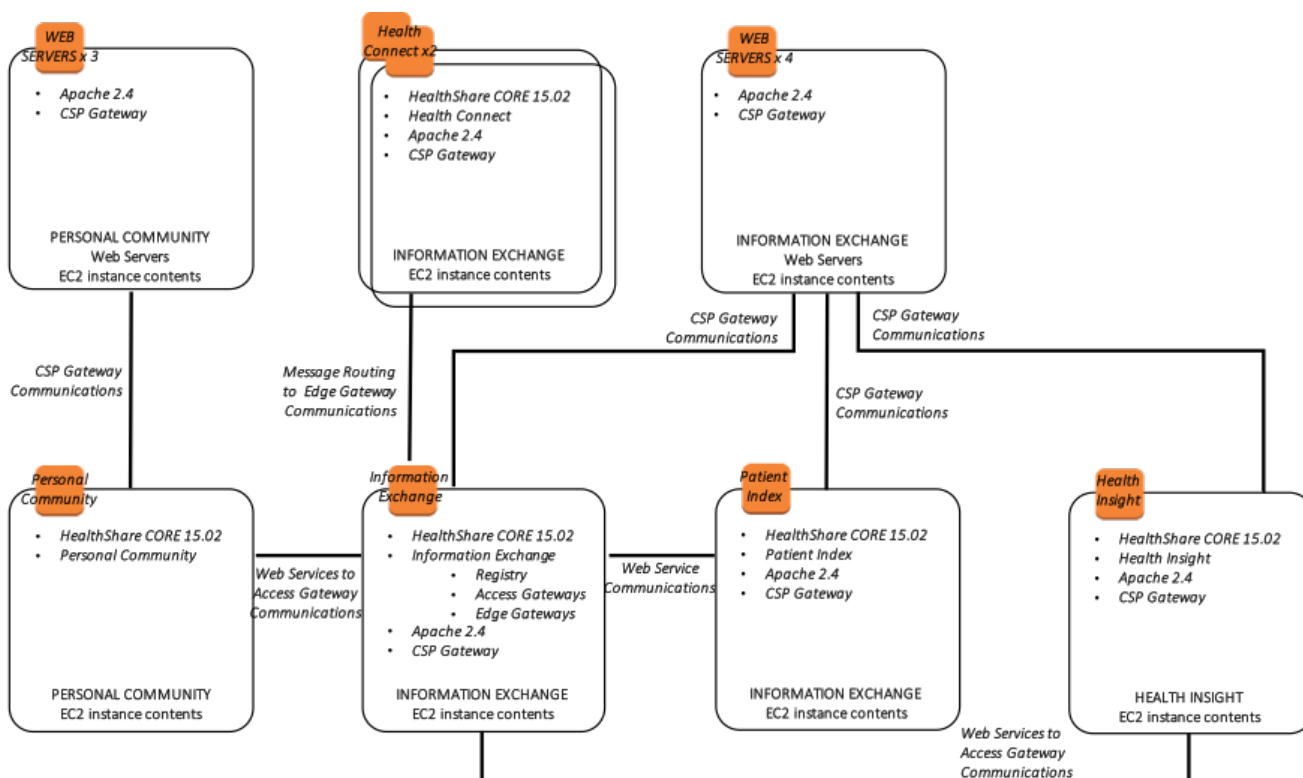
活动或主要区域中的高可用性，以及在主要区域不可用时到其他 AWS 区域的灾难恢复。

图 14 : HealthShare AWS 参考架构图 - 物理架构



此外，下图显示了更有逻辑的架构图，其中包含所安装的相关高级软件产品、连接要求和方法，以及相应的功能用途。

Figure-15: HealthShare AWS 参考架构图 - 逻辑架构



在 Amazon EC2 上部署 InterSystems 技术 - 参考架构

Published on InterSystems Developer Community (<https://community.intersystems.com>)

[#AWS](#) [#iFind](#) [#InterSystems](#) [业务解决方案和架构](#) [#云](#) [#系统管理](#) [#Caché](#)

源

URL:<https://cn.community.intersystems.com/post/%E5%9C%A8-amazon-ec2-%E4%B8%8A%E9%83%A8%E7%B D%B2-intersystems-%E6%8A%80%E6%9C%AF-%E5%8F%82%E8%80%83%E6%9E%B6%E6%9E%84>