负载均衡101：向应用交付控制器演进

序言

对于负载均衡器向当前的应用交付控制器 (ADC) 持续演进，一个令人遗憾的方面是，经常容易忘记一个最基本的问题，即负载均衡器设计的初衷—产生高可用性、高扩展性和可预测的应用服务。我们在智能应用路由、虚拟化应用服务以及共享基础设施部署方面感到迷惑，忘了这样一个事实：如果基础的负载均衡技术中没有一个坚实的基础，则上述这些方面都不可能实现。那么，负载均衡究竟有多重要，其影响又如何能够理顺应用交付流程呢？

负载均衡的推动因素

负载均衡的整个意图是创建一个系统：将来自实际运行服务的物理服务器中的“ 服务” 进行虚拟化处理。更基本的定义是在大量物理服务器之间实现负载均衡，并使这些服务器对外界看起来犹如一个大服务器。实现这一点的原因有许多，但主要的推动因素可以归纳为“ 扩展性” 、“ 高可用性” 和“ 可预测性” 。

扩展性是动态（或容易的）适应负载的增加而不影响现有性能的能力。服务虚拟化为扩展性提供了良好的机会；如果服务（或者用户访问点）与实际的服务器分离，扩展应用只是意味着增加更多的服务器，而最终用户对此一无所知。

高可用性 (HA) 是一个站点即使在一个或多个系统瘫痪的情况下仍保持可用和可接入的能力。服务虚拟化也为高可用性提供了机会；如果用户访问点与实际的服务器分离，单个服务器的瘫痪不会造成整个应用的不可用。

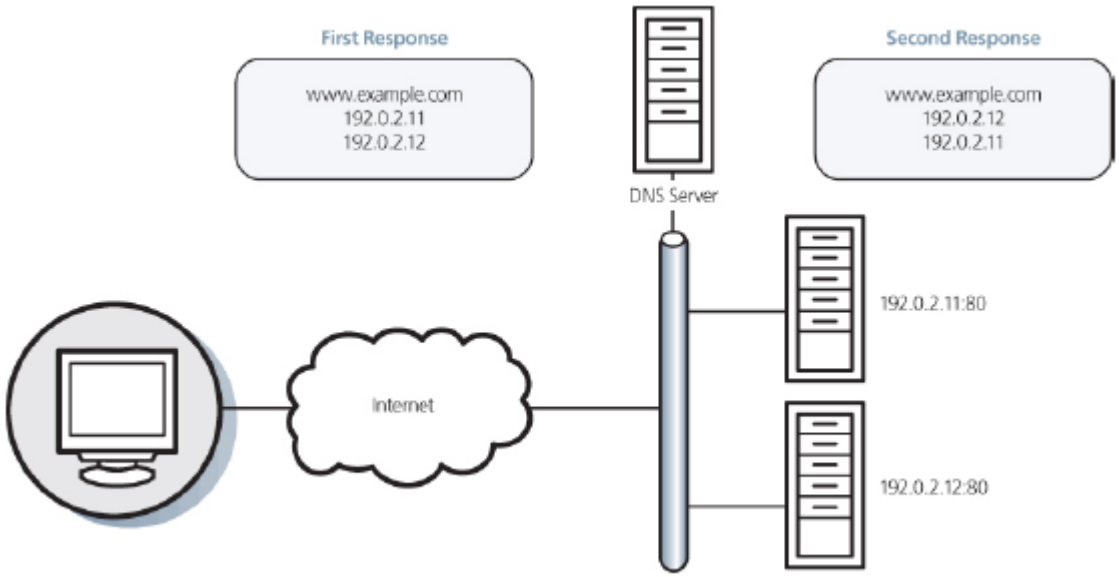
可预测性不是很明确，因为它表示高可用性的某些方面，也展现了在整个过程中吸取到的经验。然而，可预测性的最佳描述是：有信心并且控制如何交付服务以及何时交付以实现高可用性和性能等方面的能力。

负载均衡：历史的观点

在互联网商用的初期，许多准 .com富豪发现其商业计划中的一个严重问题。主机没有Web服务器软件（直到AS/400e出现），即使有，他们的启动预算也难以承受。他们能够承受的是来自其中一家知名PC制造商的标准的、现成的服务器硬件。对他们中的大多数来说，问题是什么？无法使基于单个PC的服务器始终能够处理他们的想法产生的流量，而且如果流量下降、脱机开展业务或者破产，也无法处理。幸运的是，有些人确实通过解决特定的问题制订了让自己成为百万富翁的计划；负载均衡市场应运而生。

最初是DNS

在专用的负载均衡设备实现商用之前，许多人尝试利用现有技术实现扩展性和高可用性的目标。最常用（而且目前仍被使用）的技术是DNS轮询。域名系统 (DNS) 是将人可读的名称 (www.example.com) 转换为机器可识别的IP地址的服务。DNS还使每个名称解析请求能够使用多个IP地址以不同顺序应答。



用户第一次请求解析www.example.com时，DNS服务器会按1、2、3顺序交回多个地址（分别针对托管该应用的每个服务器）。下一次，DNS服务器将交回同样的地址，但这次的顺序是2、3、1。这个解决方案相当简单，而且通过将名称用作虚拟化点并按顺序将用户分配到多个物理机器中而提供了客户希望的基本特征。

从扩展性的角度讲，这一解决方案非常有效；也许是这种方法的衍生方案仍被使用的原因，尤其是在全局负载均衡或者将负载分配到全球不同的服务点时。随着服务需要扩展，所有业务负责人需要增加一台新服务器，将其IP地址包含在DNS记录中，即提高容量。然而，需要注意的一点是：DNS的响应一般都有最大程度，服务的增长或扩展有可能超过该解决方案的能力。

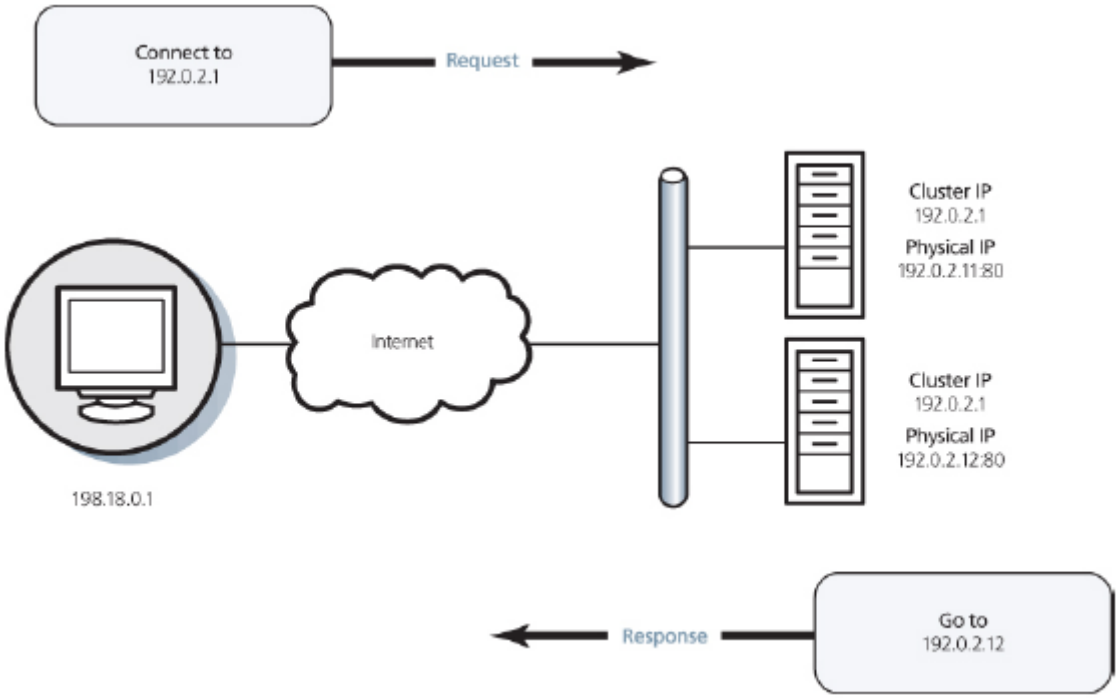
该解决方案对提高可用性几乎没有效果。首先，DNS无法知道所列的服务器是否工作，因此，如果服务器不可用，而且用户在DNS管理员知道服务器瘫痪并从DNS列表中移除之前尝试接入该服务器，用户可能获得不工作的服务器的IP地址。此外，客户端会缓存或者记住名称解析结果。这意味着它们不会始终请求新的IP地址，并且重新回到以前使用的服务器—无论是否工作，也无论是希望虚拟化还是分配负载。

在负载均衡方面，该解决方案还需要几个额外的需求。如上所述，负载均衡设备必须能够自动检测运行故障的物理服务器，并且动态地从可能提供给客户端的服务器列表中移除。同样，任何良好的机制必须能够保证客户端无法通过缓存或其它方式旁路负载均衡，除非有合理的原因。更重要的是，中间DNS服务器的问题（不仅缓存原始的DSN条目，而且自身也会在向客户端提交之前对IP列表重新排序）指出了“负载分配”和“负载均衡”之间的一个显著区别；DNS循环提供了不可控制的分配，但负载均衡效果很差。最后是一个新的推动因素—可预测性。

正如您所知的那样，可预测性是高度相信您能够知道（或者预测）用户被定向到哪个服务器的能力。与不可控制的负载分配相比，它更注重持续性。持续性是保证会话一旦开始后，或者用户恢复以前终端的会话时，用户*不会*通过负载均衡被定向到新的服务器。一个非常重要的问题是，DNS循环没有解析能力。

专用负载均衡软件

最早出现的负载均衡问题专用解决方案是在应用服务器的应用软件或操作系统 (OS) 中直接部署负载均衡能力。尽管正如有许多公司部署这一能力一样，实施的软件也有许多，但大多数解决方案都涉及到基本的网络欺骗。例如，一个解决方案是让集群中的所有服务器监听除自身物理IP地址之外的“ 集群IP” 。



当用户试图连接服务时，用户会连接到集群IP，而非服务器的物理IP。集群中最先对连接请求做出响应的服务器将把用户重定向到物理IP地址（可以是自己的IP地址，或者集群中的另一个系统），服务会话将开始启动。这个解决方案的一个主要优点是应用开发人员可以使用大量信息确定客户端连接哪个物理IP地址。举例来说，集群中的每台服务器可以维护每个集群成员正在服务的会话数量，并将新请求定向到利用率最低的服务器。

最初，该解决方案的扩展性很明显。您需要做的就是构建一台新服务器，将其添加到集群中，这样就可以增加应用的容量。然而，基于应用的负载均衡的扩展性逐渐出现了问题。因为集群成员需要始终互相保持联系，以确定下一个连接会定向给哪个成员，因此，随着新服务器被添加到集群中，集群成员之间的网络流量也会呈指数级增长。

在集群扩展到一定规模（一般是5-10台主机）后，流量就开始影响最终用户的业务流量以及服务器本身的处理器利用率。因此，在可控制的少量的服务器数量范围内（通常少于DNS循环能够处理的数量），这一解决方案的扩展能力就会很强。

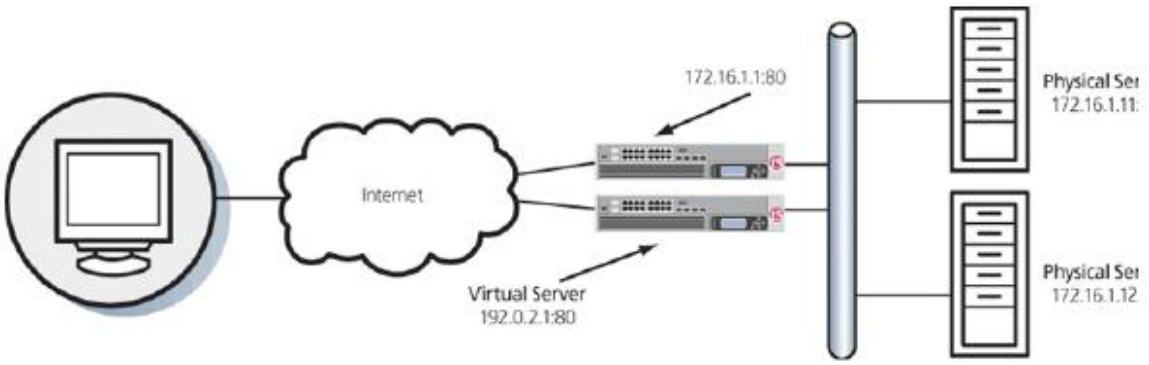
随着这些解决方案的出现，可用性得以显著提高。由于集群成员始终互相通信，而且应用开发人员可以使用综合的应用知识而了解服务器在何时正确地运行，因此，几乎不会出现用户到达一个无法处理请求的服务器的情况。然而，必须指出的是，实现智能的高可用性特征的每个过程都有相应的服务器和网络利用率影响，从而进一步限制扩展能力。对高可用性的另一个负面影响是可靠性。在这些系统中分配流量的许多网络欺骗方法非常复杂，要求大量的网络级监控工作；相应地，这些方法经常会遇到影响整个应用以及应用网络上所有流量的问题。

这些解决方案也提高了可预测性。由于应用设计人员知道用户何时以及为什么需要返回同一台服务器，而不是进行负载均衡，因此，用户能够嵌入逻辑，有助于确保用户在需要时保持持续的连接。这些解决方案还采用同样的“集群”技术在服务器之间复制用户状态信息，从而消除了许多要求在最初位置保持持续连接的情况。最后，由于对应用的深入了解，开发人员能够根据应用的真正健康状态更好地开发负载均衡算法，而不是根据连接等，因为这些方面不能始终指明服务器的负载。

除了对真正的扩展性的潜在限制以及可靠性问题外，基于应用的专用负载均衡软件还有另外一个缺点—它依赖应用供应商提供开发和维护。这样做的主要问题是并非所有应用都提供负载均衡或集群技术，而且提供这些技术的应用无法与其它应用提供商的应用良好配合。虽然有许多企业制作了不依赖供应商的操作系统级负载均衡软件，但它们都遭遇到了同样的扩展性问题。而且由于缺乏与应用的密切集成，这些软件的“解决方案”也遇到了高可用性的挑战。

基于网络的负载均衡软件

专用负载均衡的第二种方式是基于网络的设备。这些设备是当前应用交付控制器的真正祖先。由于这些设备与应用无关，而且位于应用服务器外部，因此，它们能够采用更直接的网络技术实现负载均衡。从本质上讲，这些设备会向外部世界展现一个虚拟服务器地址，而且当用户试图连接时，它会将连接通过双向网络地址转换 (NAT)前转到最适合的真正服务器上。



负载均衡器可以确切地控制哪个服务器接受哪个连接，并且采用“健康状态监视器”监控日益提高其复杂性，保证应用服务器（真正的物理服务器）根据需要进行响应；如果不能做到，它会自动停止向该服务器发送流量，直到产生期望的响应（指出该服务器正确地运行）。尽管健康状态监视器不像应用开发人员设计的解决方案那样全面，但基于网络的硬件理念至少能够以统一的方式为几乎每个应用提供基础的负载均衡服务—最终为每个应用服务器创建真正的虚拟化服务器接入点。

这一解决方案的扩展性仅受负载均衡设备的吞吐量及其连接网络的限制。尽管健康状态监控仍可能影响网络，但网络不会呈指数级扩展，因为只有负载均衡器需要维护整个集群的健康状态信息，而不是每台服务器的信息。这样降低了网络和服务器的管理成本，提供了更大的扩展空间。对于用基于硬件的解决方案取代基于软件的负载均衡方案的企业，很少能看到服务器利用率的显著下降，它们在短期内不必购买额外的服务器，而且从长期来讲，可以获得更高的投资回报。

基于硬件的解决方案也显著增强了高可用性。当然，该解决方案要求这些系统部署HA对，以提供自身容错能力，这样不但可以降低解决方案的复杂性，而且提供应用中立的负载均衡可提高其可靠性，增加其作为解决方案的深度。基于网络的负载均衡硬件使企业负责人能够为*所有的*应用提供总体的可用性，而不是利用专用负载均衡技术为少数应用提供该能力。

可预测性是基于网络的负载均衡硬件增加的一个核心要素。与大部分基于应用的解决方案的合成方法不同，负载均衡决策都具有决定性的影响（包括对连接负载、响应时间等的实际测量），因此，这种方法更容易预测新连接被定向到何处，而且更容易处理。这些设备还能够提供实际的使用量和利用率统计信息，为应用规划团队提供洞察力，并帮助对负载均衡操作的结果进行归档。有意思的是，该解决方案重新引入了对负载分配的积极影响，而未实现负载均衡。如果所有服务器都采用完全相同的配置，负载均衡是一个理想的目标；然而，随着站点的扩展和成熟，情况经常不是这样。在创建可控负载分配时的更高智能化（与动态DNS的不可控分配相对）使企业负责人能够最终以积极的方式使用负载均衡方案，向更大的服务器发送更多连接，而向较小的服务器发送少量连接。

基于网络的负载均衡的出现开辟了应用架构的全新时代。曾经围绕“运行时间”的高可用性的讨论变为关于“可用”含义的讨论（如果用户必须等待30秒才能得到响应，是否可用？一分钟内？）这些讨论也带来了在安全性和管理方面的新优势，例如，将应用服务器的真正身份对互联网屏蔽，并提供将连接从服务器中“剥离”的能力，使其能够在不影响用户的情况下进行脱机维护。这是应用交付控制器 (ADC) 创建的基础。

应用交付控制器

简单地说，ADC是负载均衡器发展的结果。虽然大部分关于ADC的讨论很少提到，但如果没有基于网络的硬件负载均衡器的能力，ADC根本不可能对应用的交付产生影响。如今，我们谈论安全、可用性和性能，但基础的负载均衡技术是所有这些得以执行的关键。

在讨论ADC安全时，基本负载均衡器技术所创建的虚拟化绝对至关重要。无论是讨论SSL/TLS加密负载卸除、集中认证，甚至是“ 应用流畅” 的防火墙，这些解决方案的能力都依赖于这样的一个事实：即硬件负载均衡器是*所有*应用虚拟化的汇集点。集中认证是一个典型的例子。传统的应用和授权机制始终嵌入到应用本身之中。与基于应用的负载均衡相似，每个实施项目都依赖于（而且具有独特性）每个应用的实施，从而产生了许多不同的方法。相反，通过在所有应用的虚拟接入点进行认证。可以实现单一的统一认证方法。这样不仅显著地简化了认证系统的设计和管理，而且无需执行这一功能，最终提高应用服务器本身的性能。此外，这种方法也不需要（尤其是在本地应用中）花费时间和金钱在每个单独的应用中开发认证流程。

可用性是与最初的负载均衡器关联的最简单的ADC属性，因为它与负载均衡器所有的基本属性相关：扩展性、高可用性和可预测性。然而，与负载均衡器相比，ADC进一步提高了这些方面。对ADC来讲，可用性代表先进的概念，例如应用依赖关系和动态配置。ADC能够了解在现实世界中，应用很少在孤立环境中运行；通常要依赖另一个应用才能完成设计。这种理解通过将其它流程考虑在内而提高了ADC提供应用可用性的能力。市场上最具智能化的ADC还提供了编程接口，使其能够根据外部的输入而动态地改变提供服务的方式。这些接口可以实现根据利用率和需求进行动态配置以及添加和/或减少可用服务器。

性能增强是负载均衡器概念的另一个明显的扩展。负载均衡器通过保证连接不仅被分配给可用的服务（在可接受的时间内响应），而且被分配给连接数量和/或处理器利用率最少的服务，从而提高应用的性能。这样可保证每个新连接由最能处理它的系统来服务。然后，随着SSL/TLS负载卸除（采用专用的硬件）成为负载均衡产品能够充分处理的能力，它可以减少加密流量的计算开支，并降低对后端服务器的负载—同样也提高应用的性能。

然而，当前的ADC远不止具有这些功能。这些设备通常包括缓存、压缩、甚至速率整型技术，进一步提高总体性能，并实现应用的交付。此外，ADC不是通过静态实施传统的单机设备提供这些服务，而是采用其固有的应用智能仅在具有性能优势的时候应用这些服务—从而优化其使用率。例如，压缩技术—普遍认为—不一定对应用的所有用户有好处。当然，带宽较少的用户（例如拨号或者移动分组数据）可以通过更小的数据分组而显著受益，因为实际的瓶颈在于吞吐量。即使长距离的连接也能从中受益，原因是更少的往返传输次数可以降低网络延时的影响。然而，高带宽（宽带和光缆/DSL）的短距离连接（例如在同一个局域网内）在应用压缩技术时能够实现最高的性能；由于吞吐量不一定是瓶颈，因此，传统的压缩和解压缩开支增加了延时，而从性能方面来讲，提高的吞吐量并不能充分地弥补。换句话说，如果管理不当，作为一种解决方案的压缩技术可能比最初的问题更糟糕。但通过仅在对整体性能有利的时候智能地应用压缩技术，ADC可以优化压缩技术的使用和成本，将更多的处理器能力留给最充分利用这些能力的功能。

ADC未来展望

ADC是向过去由负载均衡器处理的关键网络领域的自然演进，尽管ADC的许多方面都归功于过去的设备，但它们是完全不同的新种类，不仅提供了可用性，而且提供了性能和安全性。顾名思义，它们关注的是尽可能以最佳方式交付应用的所有方面。

正如负载均衡器演变为ADC，技术领域中不断变化的需求也将继续使ADC更有能力满足应用的可用性、性能和安全要求。随着集成网络接入控制（一般的NAC）的想法、应用缓存/压缩的新想法不断出现，以及将业务规则运用到应用交付管理和控制过程中的重要性日益提高，这些方面将继续扩展这些设备能为企业带来的好处的范围。对用户和应用之间的网络进行整合并减少数量的压力不断提高，将继续使传统的单机技术（例如防火墙、防病毒和IPS）融合到ADC领域中。随着新技术和新协议不断出现，用于满足在任何地点接入应用和数据的需求，未来的ADC可能将提供智能化，以确定这些（以及其它）技术如何集成到现有网络中，以及它们在何处、何时最有效。

尽管尚不清楚有多少新技术将被ADC提供的组件直接取代，但有一点可以明确，即ADC将发展成为主要的渠道和集成点，这些集成的技术通过该渠道和集成点与将要交付以供用户使用的应用连接。