AKAMAI 白皮书

面向 Akamai 的设计：初级读本

借助 Akamai 解决方案优化网站性能和安全性的最佳做法

Akamai
FASTER FORWARD

目录

执行摘要

数以千计的企业依赖 Akamai 来加速和保护他们的在线业务。组织不仅借助于 Akamai 灵活且可扩展的全球平台来对其 Web 基础设施进行可靠的扩展，还将该平台用作其 Web 应用程序层的智能组件。

此初级读本介绍了设计和开发在线应用程序时的重要注意事项。它将帮助您以最优的方式利用 Akamai 的广泛服务，包括 Web 和移动应用程序交付、流媒体交付和云安全解决方案。其中还提供了最佳做法建议，以帮助您最大程度增加缓存能力、增强移动体验、提高视频质量以及实施深入防御安全策略 - 旨在为组织提供一流的应用程序性能、可扩展性和安全性，同时通过简化的工作流程和优化的源站来降低操作复杂性。

基础知识

通过将负载和功能转移到互联网边缘，Akamai 可提升网站性能、可扩展性和安全性。但是，为了获得最大优势，我们不仅要将它用作 Web 基础设施的扩展，还要用于扩展 Web 应用程序本身 - 围绕每个请求提供智能上下文，从而实现更快、更安全、更相关的体验。本文旨在帮助网站架构师和开发人员了解如何以最佳方式设计他们的网站和应用程序来实现此目的，从而充分利用 Akamai 的丰富功能，以最低的复杂性提供最佳的用户体验。

此文档的结构

我们首先会概述面向客户的重要 Akamai 平台组件，在这一过程中，我们会首先说明从最终用户请求到 Akamai 响应的信息流程，然后介绍如何控制该平台的内容处理行为。

本文的后续章节将围绕五个主要主题介绍重要的设计注意事项和最佳做法：

- 源站架构（包括云托管的源站）
- 缓存能力和 Web 应用程序性能（包括应用程序编程接口或 API）
- 移动网站和应用程序
- 媒体交付
- 网站安全性

第一个和最后一个主题包含了广泛适用于各种在线网站和服务的设计要点，中间三个主题则聚焦于与某些类型的应用程序（特别是 Web、移动和媒体）密切相关的注意事项。本文涵盖了广泛的交叉主题领域，以便为读者全面概述相关的设计注意事项和可能性；有关特定主题的更多深入信息，请联系您的 Akamai 销售或支持代表，或参阅本文结尾处的其他资源。

最终用户请求剖析

最终用户访问通过 Akamai 提供的网页时，系统将快速连续地执行多个步骤。我们使用虚构网站 www.example.com/page.htm（由 XYZ 公司拥有）来说明：

请求剖析：最终用户访问 www.example.com/page.htm

1. 最终用户的浏览器请求域名系统 (DNS) 查找 www.example.com。客户 XYZ 的 DNS 服务器做出响应，表明它已通过 CNAME 将 www.example.com 主机名映射到了 Akamai。此外，XYZ 应设置第二个主机名，例如 q65e2zb-www.example.com（其中，外部源站名称将附加随机字符串），Akamai 使用该主机名访问 XYZ 的源站服务器。

2. 最终用户的本地 DNS 解析程序会联系 Akamai 的 DNS 服务器以解析 www.example.com。Akamai DNS 根据 Akamai 的实时全球映射算法为该用户请求发回最佳的 Akamai 边缘服务器的 IP 地址。
3. 最终用户的浏览器从该 IP 地址（转至最佳的 Akamai 边缘服务器）发出针对 page.htm 的 HTTP 请求。故障转移和容错能力融入到了这一流程中，以处理服务器、数据中心或网络层发生的故障。
4. Akamai 边缘服务器对请求作出响应，它使用 www.example.com 的配置文件来确定如何处理请求的内容 - 即如何在缓存中查询它、如何确保它是最新的、它的源站服务器是什么以及是否要向它应用任何特殊功能，例如 Cookie 处理、访问控制、URL 重写、协议优化、内容修改等。如果请求的内容已在缓存中，边缘服务器将向它应用所有相关策略，并将它发送给最终用户。这可能包括新鲜度检查，通过向源站 (q65e2zb-www.example.com) 发送 HTTP If-Modified-Since 请求来执行此检查。
5. 如果请求的内容不在缓存中，边缘服务器将从源站服务器 (q65e2zb-www.example.com) 请求它，应用相关规则，并将其发送给最终用户。

请注意，源站内容通过高效的（按需）请求模型（而非推送模型）填充 Akamai 平台。内容提供商不需要向 Akamai 网络推送任何内容更改。通过使用生存时间 (TTL) 设置和 Akamai 快速清除功能来使内容保持最新。快速清除可在几秒内从全球网络删除指定的内容。用户下一次请求内容时，它需要（通过 Akamai）从源站服务器重新提取该内容。在有关理解缓存控制的章节中，将会更深入地讨论这些机制。

Akamai 平台上的内容控制

Akamai Intelligent Platform™ 使用一套高度灵活、基于规则的系统，可帮助内容提供商控制在平台上对于每项内容的处理方式。它涵盖了一切事务，包括是否应缓存内容（以及缓存多长时间）、在交付内容之前将对该内容应用哪些高级边缘服务，等等。这些规则可驱动配置几乎所有 Akamai 解决方案（包括各种内容交付）以及前端优化、图像管理、Web 应用程序防火墙和爬虫程序管理等功能。

客户可以使用 Property Manager 引导界面（在 Luna Control Center 中）配置规则，或以编程方式通过 Property Manager API 进行配置。每条规则都采用如下基本形式：

如果满足特定条件，则向请求的内容应用这些行为。

例如，规则可能显示：“如果请求的内容是来自 /foo 目录的 .png 文件，则将其缓存三个小时”或“如果请求来自法国境内网络，则重定向到网站的法语版本”或“如果请求没有已登录的 Cookie，则显示网站的通用/可缓存版本。”

规则条件可能基于一些不同的特征，包括以下特征（此列表并不全面）：

- **HTTP/S 请求功能，**比如主机名、目录、请求方法、请求标头、Cookie、用户代理、位置、查询字符串、引用网站等。
- **所请求内容的特征，**比如文件类型、文件名、文件大小或来自源站的响应标头（包括缓存控制标头或 Akamai 控制标头）。
- **发出请求的客户端的特征，**比如 IP 地址或支持的 SSL 版本和密文
- **有关客户端的 Akamai 平台智能，**比如设备类型、网络速度、位置、信誉或爬虫程序类型

规则行为包括缓存控制[1] - 比如 TTLS、计划的失效、异步预刷新、部分对象缓存和修改缓存键 - 以及广泛的 Akamai 功能，包括 Cookie 处理、自适应压缩、故障转移、重定向、防火墙保护、访问控制、标头修改、路由优化、移动设备检测、预取、前端优化 (FEO)、爬虫程序处理、地理位置定位和基于客户端信誉的服务。

Akamai 的规则引擎具有极高的灵活性，可以精确控制内容处理。它支持条件通配符匹配以及条件组合（例如，匹配列表中的任意或所有条件），以及规则的排序和嵌套。客户还可以利用嵌入到 Property Manager 的预构建规则模板中的最佳做法。可在几分钟内跨全球 Akamai 网络推送配置和后续更改，使得组织能够对大量应用程序和基础设施保留快速而灵活的控制。

源站架构注意事项

在本节中，我们会介绍与源站服务器基础设施相关的设计注意事项，涵盖的主题包括 DNS 架构、会话管理、云托管、站点部署和协议迁移。这些主题通常适用于许多不同类型的在线服务。Akamai 可与各种源站架构 - 无论是自托管、并置或管理；单站点、多站点、云或混合云 - 无缝协作，下述建议可以帮助组织利用 Akamai 解决方案来简化他们的源站架构，同时使它们变得更为强大。

DNS 架构

规划网站安全性和可扩展性时，源站基础设施经常被忽略的一个因素是域名系统 (DNS)。许多组织只使用一个或两个 DNS 服务器，通常没有分布在不同的地理位置或不具有网站独立性，使得 DNS 服务容易成为分布式拒绝服务 (DDoS) 攻击的目标。即使 Akamai 为其客户处理 DNS 解析的最后步骤（将最终用户映射到最佳的 Akamai 服务器），内容提供商仍负责初始 DNS 解析。因此，这些提供商需要可以抵御攻击的强大 DNS 基础设施。此外，如果使用第三方 DNS 提供商，内容所有者应确保他们能够在需要时快速而安全地进行配置更改，从而方便与 Akamai 服务集成。

或者，内容提供商可以使用 Akamai 的 Fast DNS 服务来提供 DNS 解析。Fast DNS 可设置为主要或辅助权威名称服务器，从而提供高性能的全球分布式 DNS 基础设施，它可以实现全天候 DNS 可用性、更快的 DNS 响应速度以及抵御最大规模 DNS DDoS 攻击的能力。借助 Akamai 域名系统安全扩展 (DNSSEC)，Fast DNS 还可以针对 DNS 伪造和操纵提供增强的安全性。

负载平衡器和会话管理

Akamai 服务能够与前端负载平衡器（比如 Cisco、F5 和 A10 提供的负载平衡器）良好兼容；但是，为了维持会话粘性（以便最终用户在会话期间继续映射到同一服务器），Akamai 建议使用基于 Cookie 的保持，而不是基于 IP 或 SSL 会话 ID 的保持。默认情况下，许多负载平衡器使用客户端 IP 地址以维持会话粘性，但与 Cookie 不同，IP 可能对于每个用户而言并非唯一。出于性能或故障转移的原因，Akamai 可能会使用同一最终用户会话的不同 IP 地址连接到源站，或者，Akamai 可能会通过同一保持连接发送来自不同最终用户的请求。

请注意，如果您使用 F5 BigIP 负载平衡器，必须配置 OneConnect 功能以支持正确重用打开的连接，否则 BigIP 将假设连接上的所有请求都来自同一用户，导致不必要的服务器粘性（以及不平衡的负载分布）。

最后，作为一般设计原则，尽可能保持无状态设计对于性能非常有益。它允许尽可能自然地平衡流量，而无需粘滞到特定数据中心和机器。

提示：利用基于 Cookie 的负载平衡保持会话粘性。

多站点负载平衡

对于具有多个活动区域或数据中心的源站，区域间的负载平衡和会话管理是关键注意事项。如上所述，应使用 Cookie 维持会话粘性，应尽可能将应用程序设计为无状态，以便降低复杂性。

选择的全局负载平衡解决方案必须稳定且可扩展，以确保它不会发生单点故障。Akamai Global Traffic Management (GTM) 服务提供了此类解决方案。此解决方案是一款可扩展性极高、基于 DNS 的智能流量重定向产品，它提供了复杂的流量分配功能，包括加权负载平衡、基于性能的实时平衡、自动故障转移和根据地理位置或 IP 定向流量的能力。GTM 使用基于 Cookie 的会话粘性以确保在会话期间将最终用户重新路由到同一区域。

故障转移

Akamai 的交付服务在应用程序层提供了自动故障转移功能。Akamai 没有从源站服务器收到响应时，或收到某些 HTTP 5xx 错误代码时，它将执行为该内容配置的故障转移操作，比如提供过时的内容，提供替代内容（例如友好的错误页面）或从替代源站（例如，NetStorage）请求内容。Akamai 还可以配置为在故障转移之前重试请求（如果它在可配置的超时时间段内没有从源站收到响应）。[2] 默认情况下，仅重试 GET 请求，因为重试 POST、PUT、PATCH 和 DELETE 请求可能会导致意外执行两次数据库更改操作。但是，内容提供商可将这些类型的请求配置为在适当的时候重试，或者，提供商可以发回一条错误消息，允许最终用户或应用程序处理重试。

如前所述，GTM 也在网络 (DNS) 级别提供故障转移功能。GTM 对客户源站服务器执行连续运行状况检查，并在检测到问题时自动将流量转移到替代源站上。如果源站完全故障，GTM 通常会比上述基于 HTTP 的故障转移方案提供更快的最终用户响应，因为上述方案在触发故障转移操作之前，会涉及每个单独请求的 HTTP 超时和重试。借助 GTM，一旦确定源站停机（通常会在 90 秒内检测），所有流量都将自动定向到替代源站。使用此方法，后续请求不会遇到重试/等待延迟，源站免于面对持续请求，从而有机会进行恢复。但是，Akamai 仍建议在使用 GTM 的同时也配置 HTTP 故障转移操作，以便在 GTM 正式将源站标记为离线之前，处理 90 秒时间期内定向到已停机的服务器的所有请求。

为了实现复杂性低、可用性超高的解决方案，公司可以将替代源站设置为托管在 Akamai NetStorage 上的静态站点。NetStorage 提供了快速、全自动、多区域的复制，并具有 100% 正常运行时间服务级别协议 (SLA)。凭借正确的设计，这可以实现一套强大的故障转移解决方案，该方案可在一套源站基础设施中提供 100% 的可用性以及大约 90% 的站点功能，并且该基础设施的管理复杂性远低于完全复制、多地区的热备用故障转移架构。

提示：NetStorage 上的静态故障转移站点可以提供 100% 的可用性和 90% 的站点功能，并且复杂性远低于完全复制的热备用架构。

托管静态内容

许多站点还可通过使用 NetStorage 上的静态对象域（使它与源站基础设施的计算和数据库功能隔离开）受益。这使公司能够将静态对象流量完全分载到几乎无需维护、具有高可用性的高性能云源站上。随后，内部源站资源可以完全聚焦于处理更高价值的事务。

云托管的源站

总体而言，对于通过云服务（如 Amazon Web Services (AWS)、Microsoft Azure 或 Google App Engine）托管的源站基础设施和非云服务源站基础设施，Akamai 服务提供了相同的工作方式和相同的优势。尽管云源站让内容提供商实现了更低的前期资本开支和一定程度的“按需”可扩展性，但他们可能需要数十分钟或更长时间来处理流量大幅激增的情况。通过使用 Akamai 解决方案，云托管的源站可以提供一致高水平的最终用户性能 - 即使在出现完全无法预测的流量模式时，比如突发的大量访问或 DDoS 攻击。此外，云托管基础设施通常受限于狭小的地理分布，它们远离大多数最终用户，因此，Akamai 的高度分布式平台使他们能极大地受益于增强的性能、可用性、安全性和智能服务。Akamai 还有助于避免内容提供商受限于特定的云端，因为它的服务不需要部署任何硬件或虚拟设备。Akamai 服务还可以跨任何云托管提供商和任何类型的架构无缝运行 - 无论是公共云、私有云，还是混合云。

与非云基础设施上的多站点架构一样，对于多区域云源站而言，负载平衡和会话管理是重要的注意事项。如上所述，应使用 Cookie 维持会话粘性，应尽可能将应用程序设计为无状态，以便降低复杂性。

每个云托管提供商的原生负载平衡解决方案在工作方式方面略有不同，因此，请将您选择的提供商告知 Akamai 服务团队，以确保设置正确的配置选项，从而更均匀地分布负载。或者，内容提供商可以利用 Akamai GTM 以提供改进的性能、可扩展性、可靠性和智能，而不是大多数云托管服务提供的更加基本的负载平衡功能。例如，Amazon Elastic Load Balancer (ELB) 提供了循环流量分布，而 Akamai GTM 提供了加权负载平衡、基于性能的实时平衡、基于地理位置的平衡和自动故障转移等功能。

提示：Akamai GTM 在云区域之间提供了具有极高可扩展性的智能负载平衡，支持加权、基于地理位置和基于性能的策略。

云提供商还为持久连接超时提供了不同的默认设置。为获取最佳性能，源站超时应设置为比 Akamai 超时长一秒时间。默认情况下，通常将它设置为 300 秒。

尽管云托管提供商可能运营着大型数据中心，但他们可能无法提供足够的可扩展性和安全性来为客户的源站服务器实现强大的保护。至少，内容提供商应确保他们的应用程序针对自动扩展进行了正确设计和配置。但是，计算和存储资源的自动扩展无法抵御“吵闹邻居”风险或防范数据中心带宽容量被 DDoS 攻击大量占用。此外，使用云提供商的 Web 应用程序防火墙服务的内容提供商应评估防火墙的性能、可扩展性和效力。本文的“站点安全”章节将详细讨论这些以及其他安全注意事项。

在构建故障转移保护方面，跨不同的云数据中心完全复制工作负载是一个复杂的过程，这部分是因为不同中心内的功能和服务可能有所不同。对于那些需要这种故障转移水平的客户，Akamai 建议使用单一主要云源站，然后通过本地或位于同一位置的故障转移源站进行备份。此外，网站的轻量级静态版本（托管在 NetStorage 或高度可靠的替代托管平台上）应作为第三级故障转移环境（如果需要）。

站点部署、开发和 QA

部署新代码时，内容提供商必须考虑是否可接受站点停机。对于可以接受停机的应用程序，Akamai 的 Visitor Prioritization Cloudlet[3] 提供了一种简单快捷的方法来将部分或全部流量定向到标有品牌的等待空间内，直到新站点正常运行为止。对于希望避免停机的站点，建议使用两个源站：一个热站点和一个冷站点。新站点可部署到冷服务器上，随后只需将 DNS 解析指向新服务器，或使用全局负载平衡解决方案（比如 Akamai Global Traffic Management 或 Load Balancing Cloudlet），便可将流量定向到新服务器上。这两个 Akamai 解决方案均使用 DNS 来将流量定向到新服务器，可以采用渐进的方式定向，也可以一次性全部定向，具体视需求而定。在 Akamai 的帮助下，也可以使用 Phased Release Cloudlet 或 Audience Segmentation Cloudlet（两者均在 HTTP 层运行），在应用程序层进行更改。这些方案使您可以方便地逐步将部分流量迁移到新代码或新基础设施中，并且在出现问题时提供了自动故障转移/回滚。通过非技术配置启用所有 Akamai Cloudlet，不需要任何编码或源站更改。

Akamai 还建议采用以下最佳做法：在开发和 QA 环境中尽可能完整地复制完整堆栈生产环境。这包括使用任何负载平衡器、防火墙、Akamai 服务和其他第三方产品和服务。随着 Web 架构日益复杂，这是确保在影响到生产环境之前捕获潜在问题的最佳方法。

SSL 和安全合规性

Akamai 通过符合 PCI 标准的安全网络交付 HTTPS 内容。它的网络、管理基础设施和相关流程及程序符合 PCI、ISO、BITS、FISMA 和 HIPAA 的最佳实践安全要求 - 因此可以帮助客户减少风险，并更快地履行法规和审计义务。作为管理 SSL 证书的安全流程的一部分，Akamai 要求客户为他们希望通过 Akamai 交付的每个 HTTPS 域获取新证书。认证过程通常需要三到四周的时间。此外，由于 HTTPS 内容是通过独立于 HTTP 内容的安全网络交付的，内容提供商应通过与 HTTP 内容不同的主机名提供 HTTPS 内容。

不断发展的协议：IPv6 和 HTTP/2

尽管互联网很有可能会经过很长的时间才能从 IPv4 过渡到 IPv6，以及从 HTTP 1.1 过渡到 HTTP/2，但这些较新的协议是未来的明确发展方向，它们可以提供性能优势 - 尤其是在移动领域。本文的针对移动受众进行优化章节将进一步讨论这两个协议带来的影响。在漫长的过渡期内，内容提供商需要同时通过旧协议和新协议来接触客户。Akamai 使他们能够无缝执行此操作 - 无需对源站基础设施做出任何更改。通常，只需拨动配置开关便可以启用新协议。

Akamai 广泛的服务提供了强大的 IPv6 支持，其中大多数服务可配置为对最终用户启用双重堆栈支持，使客户能够通过 IPv6 提供内容，而无需在他们的源站基础设施中支持 IPv6。但是，为确保可靠的运行，组织仍应检查负责处理 IP 地址的源站或第三方系统对于 IPv6 的支持情况。其中包括：

- 存储客户端 IP 的数据库 - 确保数据库字段对于 IPv6 而言拥有足够的长度。
- 基于 IP 地址的服务（例如，基于 IP 的访问控制、地理位置工具、客户端信誉/防欺诈和审查系统）。
- 网络防火墙。
- 日志解析和分析软件。
- 使用 IP 地址的 Cookie。

尽管 HTTP/2 不需要源站做出上述更改，但要充分利用 HTTP/2 的新功能（比如加密、TCP 多路复用和服务器推送），仍需要进行谨慎考虑。Akamai 可以帮助指导客户完成此过程，一方面是通过产品（比如 FEO 和自适应加速，将在后续章节中详细讨论），一方面是通过它的专业服务和支持。

优化缓存能力和 Web 应用程序性能

最大限度提高缓存能力是提高网站性能和可扩展性并降低管理复杂性的最有效方法之一。借助 Akamai 高度灵活的缓存平台，内容提供商通常可以缓存多到难以想象的内容，包括 API 响应、时间敏感数据、产品搜索、位置特定信息以及某些个性化页面。

在本节中，我们将了解一些重要概念和最佳做法，以便帮助内容提供商借助 Akamai 解决方案最大程度提高 Web 应用程序性能。小节的结构如下：

- **了解缓存控制 -** 如何控制缓存，以及适用于不同类型的内容的缓存配置和管理建议
- **缓存 API 和动态内容 -** 用于最大程度提高动态内容的缓存能力的策略
- **加速无法缓存的内容 -** 使用路由和传输优化以及自适应加速来加快交付无法缓存的内容
- **其他性能提示 -** 有关各种主题（从源站服务器配置，到主机名的使用，再到优化第三方内容调用）的最佳做法

本节中的建议适用于所有类型的网站和应用程序，包括以移动为中心的网站和应用程序。有关针对移动受众进行优化的后续章节提供了与移动访问的站点和应用程序尤为相关的额外设计提示和注意事项。

理解缓存控制

控制缓存对象并确保它们维持新鲜度的能力是任何成功的缓存策略的核心所在。在本小节中，我们先来了解缓存中的几个关键概念，然后提供借助 Akamai 解决方案实施有效缓存控制的策略，包括适用于不同类型的内容的 TTL 设置建议。

边缘缓存与客户端缓存

在 Web 应用程序的交付中，有多个位置可能发生缓存，如图 1 中所示。我们使用术语“边缘缓存”来指代 Akamai 服务器完成的缓存，而“客户端缓存”是指最终用户的浏览器完成的缓存。我们将重点介绍这两种缓存，在制定缓存策略时必须同时考虑这两种类型。一般而言，大多数类型的内容可以通过边缘缓存受益，但以下内容除外：每个最终用户的唯一个人信息，或出于特定业务原因而必须由源站提供的内容。边缘缓存可以被视为源站架构的扩展，因为内容提供商能够充分控制他们在边缘缓存中的内容。网络提供商可以指定如何处理和缓存内容，同时还能在必要时快速清除网络上的边缘缓存中的内容。

客户端缓存提供了巨大的性能优势，因为内容缓存在最终用户设备上，但必须谨慎使用这种方式，因为无法清除客户端缓存内容或使其失效。尽管如此，只要慎重使用，它将会成为边缘缓存的有力补充。请注意，如果确定部分内容可能已经过时，则必须将它的边缘和客户端缓存的 TTL 相加。可以通过与客户端缓存类似的方式利用其他类型的下游缓存（比如 ISP 和公司代理）。然而，务必记住，这些缓存超出了内容提供商的控制范围。可以设置生存时间 (TTL)，也可以对其提供支持（尽管无法提供保证），但无法使内容失效。

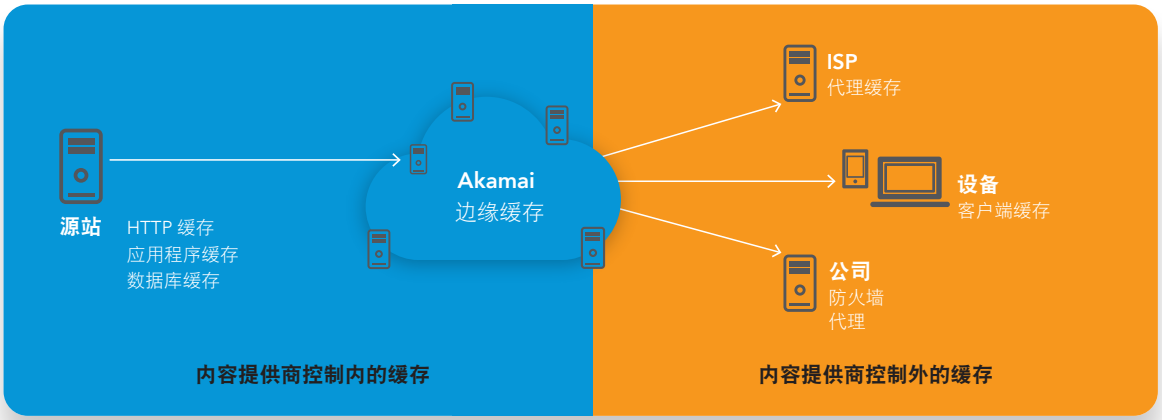

图 1：内容提供商对于边缘缓存的控制力较强，但对客户端缓存的控制力较弱

管理内容新鲜度：TTL 和失效

如上所述，可以通过两种主要方法来维持 Akamai 网络上的缓存内容的新鲜度，大多数内容提供商将同时使用这两种方法。第一个方法是设置生存时间 (TTL)，如果自上次检查（或首次检索内容）以来，生存时间已过，则此设置会指示缓存与源站服务器进行核对以查找较新的内容（使用 HTTP If-Modified-Since 请求）。请注意，TTL 设置不一定与内容本身的更改频率有关。相反，与内容的“时间敏感度”有关的业务规则 - 也就是说，在不对用户体验造成重大影响的情况下，可以在多长时间内提供过时的内容 - 是设置 TTL 的关键因素。较长的 TTL 可提供更大的缓存分载，但对于热门内容而言，几秒的 TTL 可以让提供商受益。

在 Akamai 的帮助下，可以通过配置规则设置内容 TTL，前文中有关 Akamai 平台上的内容控制的章节对此进行了讨论。配置规则允许根据多种不同的条件定义 TTL，比如请求的 URL（或其中的一部分）、内容类型或请求标头；或者，可以使用源站响应标头设置它们，包括标准 HTTP 过期和缓存控制标头[4] 或特定于 Akamai 的边缘控制标头。

控制新鲜度的第二种方法是使内容失效或将其从缓存中清除。Akamai 的快速清除功能使内容提供商能够在几秒内从整个 Akamai 全球网络删除资产。此功能可以通过快速清除 OPEN API 直接集成到网站内容管理系统中。Akamai 的快速清除不仅让内容提供商更好地控制他们的内容，它还实现了“随时待命”的缓存策略，其中，内容提供商可以使用超长 TTL（比如一个月），并在内容更改时清除内容。如果为新内容设置了定期发布计划，要进行促销或在既定时间启动活动，也可以提前计划内容失效。

提示：快速清除允许使用较长的 TTL 和“随时待命”的缓存策略。

最后，请注意，每个对象的“缓存键”（即缓存中的唯一索引）通常是该对象的 URL。Akamai 提供了修改缓存键的方法，将在有关缓存 API 和动态内容的章节中对此进行深入讨论。这意味着，通过在自动发布新版本时更改对象的名称，可确保提供新版本的对象。这是最高效的缓存策略，因为可以使用超长 TTL，同时保证内容始终为最新，因此，只要可行，就应当尽可能采用此策略。

缓存示例和建议

通过最大程度增加内容可在缓存中保留的时间，可以提高缓存命中率，从而提高最终用户性能。但是，使用较长的 TTL 也可能导致内容陈旧过时，因此，需要实现适当的平衡。在下文中，我们建议了一些策略和 TTL 值 - 适用于边缘和客户端缓存 - 其目标是最大程度提高不同类型的内容的缓存性能，而又不牺牲内容新鲜度。

内容特征	示例	缓存策略	附加说明
静态或受版本控制的内容	图像文件或其他文件（当内容更改时，URL 或文件名也会随之更改）	1 个月（或更长时间）边缘 TTL + 1 个月客户端 TTL	最高效的缓存方案。
具有低到中等时间敏感度的内容（例如，可接受超过 15 分钟的陈旧性）	搜索结果、用户评论、样式表、天气预报、社交更新	15 分钟到 1 天边缘 TTL（基于时间敏感度）+ 5 分钟客户端 TTL	如果使用快速清除来使内容失效，则边缘 TTL 可以设置得更长。对于低时间敏感度的内容，客户端缓存可以使用 2 倍于中等用户会话持续时间的 TTL。请记住，不能使它们失效，因此需要相对较低的 TTL。
具有较高时间敏感度和低更改频率的内容	突发新闻、促销活动	1 个月边缘 TTL + 0 秒客户端 TTL + FastPurge（使过时内容失效）	使用 FastPurge API 来实现编程失效。
具有较高时间敏感度和高更改频率的内容	体育赛事比分、股票价格、产品供货情况	1 秒到 10 分钟边缘 TTL（基于时间敏感度）+ 0 秒客户端 TTL	对于较高的更改频率，使用 TTL（而不是 FastPurge）来维持新鲜度的方式通常更加高效
具有计划时间更改的内容	定时促销、产品发布	倒计时 TTL -或- 1 个月边缘 TTL + 0 秒客户端 TTL + FastPurge（更改时）	倒计时 TTL 可根据距离下一次计划更改的时长动态设置值
包含个人信息的内容	购物车、个性化建议或帐户信息	不在边缘服务器或客户端上缓存	在某些情况下，如果个人信息是严格由源站生成的内容，比如个性化建议 - 而不是由用户生成，比如购物车内容 - 则可以考虑客户端缓存（具有相当低的 TTL）。但是，在所有情况下，都必须注意个人信息的数据隐私。

图 2：不同类型的内容的缓存策略和 TTL 准则

通常，Akamai 建议尽可能地对内容和对象 URL 进行版本控制，从而消除内容的时间敏感性。这可确保在使用超长 TTL 时提供最新的内容，从而提供最佳的缓存性能。此外，在微调性能时，检查日志文件能够为您提供帮助：过多地出现“未修改”响应可能表明可以使用更长的 TTL。

提示：要最大程度提高缓存性能，请尽可能地对内容 URL 进行版本控制，从而消除内容的时间敏感性。

最后，要改进 HTML 页面的缓存能力，最好不要直接在 HTML 中嵌入个人信息。而是应让客户端通过 AJAX 调用或读取专用 Cookie 来获取个人数据。这样就能在边缘服务器和客户端上缓存 HTML 页面，从而提升性能。阅读下文中有关缓存 API 和动态内容的章节，以了解有关如何提高动态内容的缓存能力的更多提示。

使用 Akamai 方案时的 TTL 配置和管理策略

Akamai 的规则引擎内置的灵活性使其能够支持多种站点架构（具有许多不同的内容管理系统和内容组织结构）。但是，如果可以使用简单而有效的配置，则可以为成功提供极大的帮助。

许多内容提供商首先使用内容类型（例如 JPG 与 HTML）来为内容的缓存能力分类。在 HTML 页面的分类中，一种实用的策略是将内容分类为多个缓存能力组，并使用 URL 中的标记以反映这些组。例如，对于零售站点，单独的产品页面可能具有极高的缓存能力，可以长期存在，而类别页面的缓存生命周期可能较短。主页可能仍然具有较短的生命周期，而购物车可能完全无法缓存（产品图像除外）。通过使用内容管理系统或对站点结构提前进行少量规划，可以为 URL 创建特定的结构，以确定每个内容的缓存能力级别。在此特定示例中，/product/* 页面可能具有一个月的 TTL，而 /category/* 页面可能具有一周的 TTL，主页则可能具有一小时的 TTL。使用 URL 标记是借助 Akamai 解决方案优化缓存能力和站点性能并且最大程度减少维护开销的最简单方法之一。

由于通常不应缓存包含个人信息的内容，也可以从结构上分隔包含此类信息的内容，以便识别此类内容。例如，通常可以缓存 PDF 文件，但个人帐户报表的 PDF 则无法缓存。在这种情况下，开发人员可以定义规则来缓存除 /statements/* 中的文件以外的所有 PDF 文件类型。

最后，也可使用 HTTP 标头 - 可以使用标头本身，也可以与 URL 标记结合使用，从而配置或微调缓存设置。例如，如果客户拥有对于时间敏感且在白天（通常不在晚上）经常更改的内容，则可以使用 Akamai 边缘控制标头来为一天中不同时间的同一内容设置不同的 TTL。

缓存 API 和动态内容

虽然可能不那么明显，但许多类型的动态内容也可以通过缓存受益。这包括 API（经常用于移动应用程序、单页应用程序、B2B 应用程序和机器间通信）。开发人员可能会因其动态性质和相对较小的有效载荷大小而忽略此类内容的缓存能力，但在许多情况下，通过缓存这些响应，内容提供商可大幅降低源站服务器和后端数据库承受的负载，同时改进面向最终用户的响应时间。

以下一些方法可以借助 Akamai 解决方案最大程度提高 API 和其他动态内容的整体性能 - 包括可缓存和不可缓存的内容。

缓存非个人动态内容

任何动态内容场景（向一组用户显示相同的内容）都有机会使用缓存。例如，可以缓存返回区域化内容（比如天气、即将放映的电影时间或商店位置）的 Web 查询或 API 调用，并通过 Akamai 边缘服务器提供。通过将位置信息用作“缓存密钥”- 缓存中的索引（或唯一标识符）- 的一部分来实现此目的。可以通过无数种方法确定请求者的位置信息，例如，在查询字符串或 Cookie 中确定，或者使用 Akamai 的位置智能服务确定。通过将此信息添加到缓存键，来自同一位置的未来请求可以直接从缓存接收响应。

类似地，可以使用查询字符串的相关部分 - 包含产品 ID 或搜索词 - 作为缓存键的一部分，从而缓存针对产品详细信息、用户评论或搜索结果的 Web 查询。在这些情况下，可以考虑如何限制潜在缓存键的数量，以最大程度增加缓存命中率。例如，基于位置的应用程序可能会将缓存键限制为请求者的邮政编码或位置 ID，而不是使用更具体的 GPS 坐标或更详细的位置信息。类似地，查询字符串中通常有多个字段，其中很多都不需要作为缓存键的一部分。Akamai 允许高度灵活地定义可将哪些内容用作缓存键的一部分，使得内容提供商能够最大程度地提高动态内容的缓存能力。针对每个给定查询，开发人员应竭力减少不同的缓存键数量，以便最大程度提高缓存性能。请注意，默认情况下，Akamai 使用生成缓存键时收到的查询字符串，因此，在 Web 应用程序代码中，URL 参数应执行标准化和均匀排序，以防创建无关的同等缓存键。

提示：API 和 Web 查询通常可以缓存。针对每个给定查询，应竭力减少不同的缓存键数量，以便最大程度提高缓存性能。

缓存个人内容

如前所述，即便是包含个人信息的内容，有时也可以通过一些小调整使之可以缓存。例如，站点的某些页面或许根据已登录的用户名或购物车中的商品数量进行了个性化，但其他部分可能与未登录的访客看到的内容完全相同。在这种情况下，通过将个性化内容分解为 AJAX 调用，仍可从缓存中同时为登录和未登录访客提供整个页面 - 包括基本 HTML、CSS、JavaScript 和图像。在某些情况下，通过在 Cookie 中存储个性化信息（比如用户的名称），可通过 JavaScript 个性化设置页面，而无需使用 Ajax 调用。

提示：将页面的个性化部分分隔为 AJAX 调用，从而允许缓存个性化 HTML 页面。

缓存 API 身份验证

API 经常要求身份验证，这会将每个内容请求转化成两个 - 身份验证请求和原始请求。为了在这些情景下缓解源站负载，Akamai 可以在每个用户的唯一缓存键下缓存身份验证响应，一次持续几秒钟，从而不必对每个请求重新进行身份验证。通过验证时间敏感型令牌，Akamai 也可以在边缘服务器上直接对请求进行身份验证。这可以提高最终用户性能和分载源站服务器，同时维持所需的访问控制级别。

加速无法缓存的内容

尽管最大程度提高内容缓存能力对于优化性能至关重要，但某些类型的内容就是无法通过缓存受益。例如，这包括高度个性化的信息或长尾搜索词。对于这些情况，Akamai 的动态加速功能（包括路由和传输层协议优化）和自适应预测技术能够以独一无二的方式，在不一致的互联网中提供一致而迅捷的最终用户体验。

路由和传输优化

由于具备高度分布式架构，Akamai 可以通过 TCP 或传输层协议优化提供显著的性能优势，比如基于实时网络条件调整 TCP 参数，从而通过高效连接在长距离互联网上传输无法缓存的内容，减少呈现网页所需的往返次数。

Akamai 还提供了独一无二的路由优化功能 (SureRoute)，此功能可以在“直接”BGP 路由拥塞时，经由中间服务器通过更快的路由发送流量，从而有效地覆盖 BGP。路由优化对 TCP 优化进行了补充，它可以减少数据往返时间延迟，对于提高 API、嘈杂的 AJAX 应用程序和其他简短突发流量的性能尤为重要。

可以通过 Akamai Property Manager 配置轻松实施路由和传输优化，不需要更改源站服务器。

自适应加速

借助 Akamai 独特的自适应加速 (A2) 功能，组织可以利用复杂的机器学习算法来自动应用有效的性能优化。根据对于网站真实用户数据的观察，A2 可以预测用户接下来可能需要的内容和连接，并智能地决定最好在何时向客户端预推送资产（利用 HTTP/2 服务器推送）或预连接到第三方服务器，从而实现更快的页面加载和呈现。预连接和资源推送充分利用了其他情况下当客户端只能等待服务器响应时处于闲置的网络。

随时间推移，A2 在站点发生更改或用户行为演变时不断调整优化。不需要开发团队做出努力便可以完成上述所有操作 - 配置 A2 的过程只涉及在配置中进行或停止所需的操作。请注意，A2 优化与 FEO（前端优化）的功能在某种程度上存在重叠，但这两个服务可以互补。在有关前端优化的章节中将详细讨论此内容。

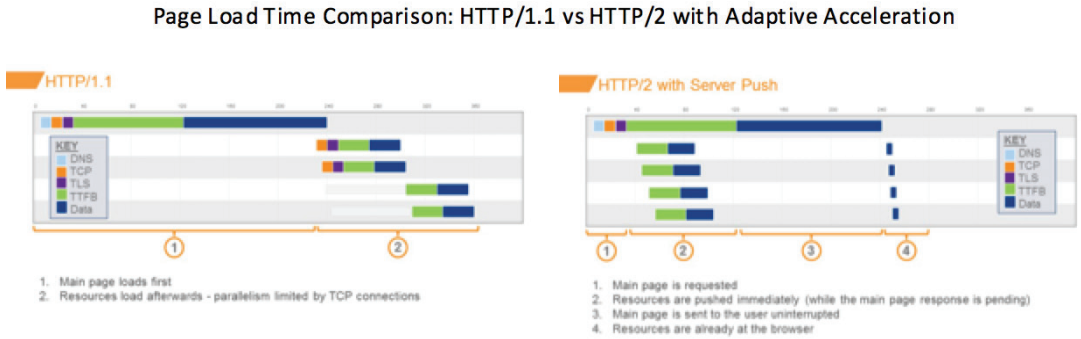

图 3：通过在空闲时间推送嵌入式资源，可将加载和呈现上述示例中的页面所需的时间缩短接近三分之一。

API Prioritization

当无法缓存的 API 请求开始让源站服务器超载时，提供商可以利用 Akamai 的 API Prioritization 功能来限制流量，从而确保重要用户和事务能够优先得到处理。在意外的流量高峰期间，可以为低优先级用户群体提供预定义的替代 API 响应，使得源站可以处理来自更高优先级流量的响应。借助 API Prioritization Cloudlet，可以在数分钟内配置和部署此功能，而无需更改源站基础设施或代码。

其他性能提示

在本节中，我们会提供更多指导，旨在帮助开发人员通过 Akamai 解决方案实现尽可能最佳的 Web 应用程序性能。虽然并不全面，但我们提供了有关各种主题的建议，包括源站服务器配置、主机名的使用、迁移 URL、优化第三方内容调用以及使用真实用户监控 (RUM)。

源站服务器配置

在源站服务器上使用正确的设置是一种简单而重要的性能优化操作。请确保：

- 使用具有正确超时的 HTTP 持久连接。理想情况下，Akamai 超时应设置为比源站服务器超时大约短一秒时间。
- 支持 If-Modified-Since 请求，设置 Last-Modified-Time 标头，并确保服务器时钟时间正确无误。
- 最大程度减少主机名的使用

尽管有正当理由在一个网站内使用多个主机名，但为页面上的所有资源（包括 HTML、嵌入式对象和 API 调用）使用单一主机名时，通常可以减少了 DNS 查询和 TCP 连接设置开销，从而实现更好的性能。对于通过 SSL/TLS 提供的内容，这一点尤为重要，因为设置每个连接所涉及的开销成本更高。

此外，尽管在 HTTP/1.1 环境中，某些情况下可能会建议使用域分片（即跨多个域分割页面资源，以提高浏览器同时下载的资源数），但随着 Web 朝着支持多路复用的 HTTP/2 发展，域分片可能会降低性能。Akamai 前端优化 (FEO) 动态提供了视情况而定的适当域分片，再次强调，建议尽可能使用单一主机名。

此外，某些 Akamai 优化（比如预取）要求将嵌入式内容请求映射到与页面其余部分相同的服务器上。如果嵌入式内容驻留在与页面相同的主机上，可以大幅降低实现此操作的难度。最大程度减少主机名数量也能让 Akamai 配置管理变得更加容易，因为每个主机名都有自己的配置文件。

处理 CORS OPTIONS 调用

尽可能为所有资源使用单一主机名的另一个原因是，从脚本内的另一个主机名请求资源时（比如 AJAX 调用），将触发跨源站资源共享 (CORS) OPTIONS 调用。这需要通过单独的请求来确认允许跨域资源请求，从而会在检索资源时造成额外的时间延迟并对服务器造成额外的开销负载。

如果无法避免 CORS OPTIONS 调用，通过为此类资源使用相同的主机名，可以利用 Akamai 来生成 CORS OPTIONS 响应，从而最大程度减少性能下降。这消除了对于源站基础设施的影响，并提高了响应速度，因为 OPTIONS 请求直接由靠近最终用户的 Akamai 边缘服务器负责处理。

迁移和重定向 URL

重新构建网站的过程通常涉及更改 URL，这会对用户体验、SEO 或其他爬虫程序流量产生影响。要最大程度减少负面影响，可将 Akamai 配置为同时启用旧的和新的 URL 以指向相同的源站内容，从而在无需重定向的情况下支持新的和旧的 URL - 并降低源站服务器的复杂性。然后，随着时间的推移，可以在必要时弃用旧 URL。

提示：重新构建网站时，利用 Akamai 方案来轻松支持新的和旧的 URL，无需进行重定向。

在其他需要 URL 重定向的情况下，Akamai 边缘服务器可以处理重定向，从而减轻源站服务器的负担。这减少了复杂性和错误几率，同时可以为最终用户提高性能。借助 Edge Redirector Cloudlet，即使非技术型用户也可以方便地在 Akamai 网络上配置，调配和管理灵活的重定向规则。

缓解第三方性能迟滞

Web 和移动应用程序中的第三方内容调用（比如广告、分析、A/B 测试平台和社交小组件）越来越常见，通常构成了页面上的大多数请求。遗憾的是，这些第三方调用通常会大大降低页面性能、可靠性和安全性 - 有时会导致页面完全无法正常呈现。

要最大程度减少问题，必须首先审核和理解当前使用的第三方内容[5]，然后建立一个清晰的流程来将此类代码添加到网站上。如果可能，请使用异步 JavaScript 来做出这些调用，使得它们不会干扰页面呈现。Akamai FEO 可以动态实施这一最佳做法，不需要任何编码更改。通过使用 DNS 预取和 TCP/TLS 预连接功能，也有助于最大程度降低第三方调用造成的延迟。这些方法允许浏览器提前建立检索第三方内容所需的连接。Akamai FEO 可以自动实施这些指令，使得无需修改 HTML 代码便可以采用这些最佳做法。

真实用户监控 (RUM)

Akamai 真实用户测量 (RUM) 功能可捕获性能指标以及与网站中的实际网页请求和交付结果有关的其他数据。[6] 除了详细分析实际用户体验到的站点性能以外，RUM 还可帮助内容提供商根据用户设备、协议（例如 HTTP/1.1 与 HTTP/2，IPv4 与 IPv6）或网站更改（例如，应用 FEO 之前与之后）等因素轻松比较性能差异。

RUM 实施简单到只需通过 Akamai Luna Control Center 门户指定要监视的页面。Akamai 的边缘服务器随后会向指定的页面插入一小段异步、非阻塞式 RUM 特定 JavaScript，然后再将页面提供给最终用户。此 JavaScript 可在呈现页面时收集性能数据，并通过一个 1x1 的像素向 Akamai 做出反馈。随后可在门户中对数据进行可视化处理。

其他功能

为满足客户独特的业务和技术要求，Akamai Intelligent Platform™ 支持其他许多边缘功能，包括更先进的缓存以及边缘计算。要针对此处未提及的使用情形获得进一步帮助，请与 Akamai 客户代表或支持/服务团队联系。

针对移动受众进行优化

借助以移动为中心的强大功能，以及可扩展到移动网络中的边缘服务器部署，Akamai 可帮助客户接触快速增长的移动群体 - 从而让提供广泛覆盖范围的移动网站以及与忠诚消费者进行更深入的互动的移动应用程序得到加速。在本节中，我们将了解其中每个渠道的主要设计注意事项，以及有关如何借助 Akamai 方案来更有效地利用大量移动商机的建议。

移动应用程序的设计注意事项

大多数移动应用程序的运行基于一个假设，即始终可以使用快速、 可靠的网络连接，而实际上，移动网络经常可能变慢或不稳定。为了提供更强大的用户体验，不仅需要优化网络相关调用（即图像和 API 调用）的性能，还要将应用程序设计为能够适应网络，并能根据不断变化的网络条件做出智能的用户体验选择。

图像性能和管理

图像和富媒体构成了大量移动应用程序网络流量，它们可通过边缘缓存大大受益 - 就像在非移动 Web 环境中一样。但是，应用程序和 Web 的移动群体可以通过网络自适应图像交付功能进一步受益。Akamai 边缘服务器可在最终用户的真实网络条件缓慢时自适应地压缩图像，从而在不降低感知图像质量的前提下提供响应迅速的应用程序体验。

此外，考虑到移动环境中多种不同的显示屏外形规格，图像管理可能会变成一个严重的难题。内容提供商需要考虑他们要支持多少种不同的宽高比、屏幕分辨率级别、背景色和浏览器文件格式 - 因为每个因素都让每个图像资产所需的衍生版本数量倍增。在 Akamai 的帮助下，很多管理难题可以迎刃而解。内容提供商只需为 Akamai 提供单一原始图像并配置所需的策略，Akamai 将处理所有资源密集型任务（生成，存储和交付图像变体）- 针对每个最终用户的设备适当优化。此外，在清除图像时，内容提供商只需清除原件，所有变体都会自动删除。

提示：为移动环境中的多种设备提供支持时，需要提供每个图像文件的多个变体，而 Akamai Image Manager 有助于缓解这一难题：生成，管理，存储和交付这些变体。

要实现最佳的最终用户体验，需要在创建大量图像变体以针对不同的显示屏进行优化以及使用更少的变体以提高缓存命中率之间建立平衡。通常，最好为每个图像提供三到五个尺寸。通过查看 Akamai 分析报告，可以很好地了解访问网站的设备和显示屏的类型。此外，审核日志文件以查看缓存落空率对于微调要提供的图像变体数量十分有用，因为内容和受众概况不同，最佳设置也有所不同。

API 性能

除了图像和富媒体以外，API 调用也构成了移动应用程序流量的另一主要组成部分。如前所述，许多 API 调用（即便是动态调用）都可以通过 Akamai 方案进行缓存。设计应用程序以最大程度提高缓存能力（如缓存 API 和动态内容中所述）对于优化性能至关重要。此外，通过充分利用 Akamai 的动态加速功能（如 加速无法缓存的内容中所述），有助于确保为无法缓存的 API 调用尽可能降低延迟。

网络感知应用程序设计

如今，大多数移动应用程序依赖于一个有缺陷的假设：始终可以使用快速、可靠的网络连接。然而，开发人员很难访问与其应用程序中的实时网络条件有关的实用信息。Akamai 的移动应用程序性能软件开发套件 (MAP SDK) 允许用户方便地访问此网络智能，使得开发人员能够更简单地构建可在动态网络环境中快速流畅运行的应用程序。

提示：Akamai 的移动 SDK 可实现新型网络自适应移动应用程序，这种应用程序可以在动态的网络条件下提供响应迅速的体验。

例如，如果网络拥塞严重，网络自适应应用程序可以延迟第三方 API 调用，或默认使用本地存储的内容。当用户使用 Wi-Fi 连接时，它可以主动下载目标内容，比如突发新闻或推荐的视频剪辑，方便用户随后获得“即时开启”的体验（即使设备处于脱机状态）。它可以应用最后一英里加速技术（适当时针对蜂窝网络进行优化）。网络自适应应用程序也可以定制服务器端响应 - 例如，在用户的网络速度较慢时请求较少的图像、搜索结果或产品建议。在设计应用程序时，必须考虑这种新的网络自适应模式创造的可能性，因为这有助于为移动群体开发具有吸引力的体验。

测量性能

与移动 Web 性能不同，移动应用程序性能并非由一组标准化性能指标所确定。因此，初始字节响应时间或总下载时间等测量指标可能与客户体验不太相关。这意味着，要对应用程序性能进行测量，需要能够在应用程序中轻松定义与测量用户体验有关的自定义事件和操作，以及它如何对组织的业务目标产生影响。

Akamai 的移动 SDK 通过提供真实用户监控和轻松标记自定义事件实现了此功能。这允许将 API 调用集与业务定义的操作进行关联，比如加载初始应用程序屏幕、登录或完成购买。此类标记使组织能够测量和改进应用程序性能及其业务影响。

移动网站的设计注意事项

Akamai 网络上大概有一半的 Web 访问发生在移动设备上（截至 2017 年初），因此，移动网站已成为各个行业的关键通信渠道。同时，移动渠道的分层复杂性要高于 Web 环境。因此，除了有关优化缓存能力和 Web 应用程序性能的章节中介绍的常规设计要点外，移动开发人员还面临其他一些注意事项 - 包括响应性 Web 设计、前端优化和单页应用程序的使用。

响应性 Web 设计（和 RESS）与单独的移动网站的对比

有两种主要的基本方法来接触 Web 上的移动用户：提供单独的移动网站（使用单独的 URL，比如 m.website.com）或使用响应性 Web 设计 (RWD)。响应性 Web 设计在所有设备中使用了相同的代码库和相同的 URL，但通过适合屏幕尺寸的灵活网格布局来适应不同的设备。

通过提供单独的移动网站，开发人员能够为移动用户创建不同的体验。但是，这种方式可能导致用户更难跨设备分享内容或查看内容，因为站点不同，内容 URL 也不同。此外，随着网站演变，维护网站的多个版本会造成极大的复杂性。

第二个方案 - 响应性 Web 设计 - 需要更多的提前规划，但长期维护（包括网站更改和新设备的支持）通常更加容易。通过使用单个 URL，还可为最终用户提供更加简洁的体验，避免增加重定向延迟，并让受众能够以设备不可知的方式更轻松地分享内容。但是，视实施方式而定，RWD 的性能可能受到影响。通常，跨所有设备和所有网络交付相同的 HTML 代码和媒体。这意味着，具有小屏幕和慢速网络的移动用户最终会“过度下载”富媒体资产，比如适用于高分辨率桌面显示器的全尺寸图片。此外，RWD 通常需要在客户端/浏览器中处理 Javascript，以在呈现时使用正确的布局。

考虑到许多移动设备的处理能力有限，一些开发人员现在更倾向于具有服务器端组件 (RESS) 的响应性 Web 设计，这种策略将采用 RWD 实践，但会增加服务器端逻辑来预先确定要发送到每个客户端的布局和富媒体资产。只要服务器能准确检测和确定发出请求的设备的功能和网络条件，RESS 就能最大程度减少过度下载并缩短客户端呈现时间，从而提供更快、响应性更强的最终用户体验。

行业正朝响应性设计发展，因此 Akamai 建议在大多数情况下使用此方法。建议采用响应性设计，这种设计不仅易于维护，还能跨所有设备提供更一致的最终用户体验。尽管如此，Akamai 为这两种方法都提供了支持，不管内容提供商选择哪种方法，都可帮助他们简化管理和提高性能。

准确的设备特征分析

无论是维护单独的移动网站或使用 RWD/RESS，准确的设备特征描述对于移动内容提供商而言都是一项挑战。用户代理字符串（用于区分设备）难以分析，获得的支持也不均匀，并且没有提供关键信息，比如屏幕尺寸和分辨率。Akamai 的边缘设备特性分析 (EDC) 功能可解决这一短板，它利用全面且不断更新的设备数据库来促进交付针对上下文优化的网站。通过为开发人员针对每个请求提供准确的设备特征来实现上述目的 - 包括屏幕大小和分辨率、JavaScript 支持、Flash 和动画 GIF 支持、浏览器和操作系统版本、GPS 坐标，等等。

内容提供商也可以使用 Akamai Edge Side Includes (ESI) 标记语言以及 EDC 来将 RESS 服务器端逻辑分载到 Akamai 边缘服务器上，从而显著提高性能、可扩展性和可靠性。

前端优化 (FEO)

前端优化 (FEO) 包括多种最佳做法，用于改进最终用户体验，特别是在移动 Web 环境中。这些技术包括 JavaScript 和 CSS 文件缩小、减少每页 HTTP 请求数、按需图像加载和推迟第三方内容调用。在为任何移动网站编码时，Akamai 建议尽可能遵循基本的 FEO 原则。但是，尽管许多 FEO 技术可以直接融入到编码过程中，实施过程可以仍然非常复杂，常常需要分析多个策略之间的权衡。此外，随着浏览器和协议发展，最佳做法也在不断变化 - 例如，HTTP/1.1 的优化与 HTTP/2 不同 - 对指定协议应用错误的优化可能会降低网站速度。

Akamai 的 FEO 服务为内容提供商提供了一个更简单的方法来利用 FEO 的优势，而不必重新编码现有网站以满足不断发展的最佳做法。以异步方式分析站点代码，然后在响应时内嵌应用预先计算的转换。通过针对每个最终用户的背景和环境进行优化的方式来完成此操作。即便在站点更改时，优化也会继续生效。它们还可以自适应协议，从而根据客户端使用的是 HTTP/1.1 或 HTTP/2 来自动应用适当的优化。

Akamai 的 FEO 解决方案还利用了基于边缘的智能，而任何类型的本地 FEO 解决方案都无法实现这一点。例如，独特的 EdgeStart 功能显著缩短了初始字节响应时间。此外，通过利用一个事实（对于所有用户而言，页面中的初始 HTML 内容 - 包括样式表和其他资源 - 可能完全相同），EdgeStart 可呈现无法缓存的个性化网页。Akamai 的边缘服务器可以立即开始向用户提供这些内容，同时从源站获取页面的其余部分。这样使得浏览器可以更快开始呈现页面，从而缩短对最终用户的响应时间。Akamai 还可以预取 DNS 解析，并在出现请求之前为页面中的嵌入式对象设置 TCP 连接，以及在需求出现之前预取到边缘服务器或（在客户端上）预加载资源，从而提供响应性更强的最终用户体验。

提示：通过立即提供通用的初始 HTML 和资源内容，Akamai 独特的 EdgeStart FEO 功能可以为无法缓存的页面显著缩短收到第一个响应的字节所花费的时间。

客户可以控制要应用哪些 FEO 规则，然后 Akamai 会以优化的方式，针对每个最终用户的特定上下文应用这些规则。有些客户选择阶段性方法，他们首先使用更简单的规则（比如图像压缩和滞后图像加载），然后逐步添加更高级的优化。可以根据需要启用和禁用规则，而无需关闭源站或对现有站点代码进行任何更改；可以在几分钟内在整个 Akamai 网络中推送规则更改。为了确保获得最佳效果，应在站点更改时，定期重新检验 FEO 规则应用程序。此外，必须确保对于 FEO 的应用包含在网站测试环境中，以及优化和未优化的页面的行为保持一致。只需向任何 URL 追加查询字符串“?akamai-feo=off”，便始终可以请求未优化的页面版本。

请注意，如果使用 Akamai 的 自适应加速 (A2)，应关闭某些 FEO 功能，因为它们存在功能重叠或因为 FEO 会动态更改文件名，从而对 A2 产生负面影响。这些功能包括 DNS 预取、及早期字体加载、智能嵌入、Edgestart、CSS 和 JS 优化以及页面和资源预取。但是，其他 FEO 功能（特别是那些延迟加载的功能 - 例如异步 JP 和按需图像加载）可与 A2 高度互补。

图像性能和管理

就像移动应用程序一样，图像和富媒体构成了很大一部分移动 Web 流量。因此，内容提供商可以大大受益于如前所述的 Akamai 的图像性能和管理功能。与移动应用程序一样，Akamai 建议使用它的分析报告来了解访问站点的设备类型，以帮助决定要为每个图像提供多少种尺寸和宽高比，还建议查看日志中的缓存命中/落空比例，以便随时间推移微调这一决策。必须考虑到一点，即很多浏览器已开始支持自己优化的图像文件格式（Chrome 的 WebP、Microsoft Edge 与新版 Internet Explorer 的 JPEG XR 以及 Safari 的 JPEG 2000），与 JPG 和 PNG 等标准相比，这些格式在保证相同质量水平的情况下提供了优异的压缩质量。Akamai 可以代表内容提供商创建，管理和交付所有这些图像文件版本，从而降低管理复杂性。

URL 重定向处理（针对单独的移动网站）

选择托管单独的移动网站的组织需要能够根据发出请求的设备，将传入请求重定向到相应的网站 URL。在 Akamai 的帮助下，内容提供商可定义规则，从而使用 Akamai 的边缘设备特征分析功能来确定要将哪些设备重定向到何处。通过在网络边缘处理此任务，可最大程度降低最终用户的重定向延迟以及源站上的负载。

单页应用程序 (SPA) 的注意事项

采用单一 HTML 页面结构，并通过 Javascript 和 API 来处理应用程序导航，单页应用程序代表了一种日益流行的混合浏览器原生应用程序架构 - 尤其是在移动环境中。如果没有进行谨慎设计，SPA 的初始加载时间可能会非常缓慢，因为默认实施会在应用程序启动过程中尝试加载和执行所有静态资源和 JavaScript 进程。这意味着，主页可能需要许多秒才能呈现，特别是在使用慢速蜂窝网络的受限移动设备上。

由于初始用户交互至关重要，Akamai 建议优化第一个页面。为了做到这一点，我们会优先提供框架的缩减版本，仅加载/处理显示第一页所需的资源，从而为其他资源使用滞后和/或异步加载及执行。此外，应最小化 JavaScript 程序包以仅包括必要的库。与 RESS 类似，开发人员可能还希望考虑服务器端呈现，以便减少设备上必须执行的处理量。除了利用智能服务（比如 Akamai 的自适应加速）之外，对于客户端缓存的灵活使用可为这些类型的应用程序大大提高性能。

最后，在评估 SPA 中的最终用户体验时，必须记住一点：传统指标（比如加载事件和页面加载时间）基本毫无意义，因为浏览器中仅加载一个页面。内容提供商应使用 W3C 的用户计时规范来标记代码以提取指标 - 比如框架加载时间、虚拟页面加载完成时间和 API 响应时间 - 这些指标可帮助他们从最终用户的角度更好地了解应用程序性能。

不断发展的协议：移动环境下的 HTTP/2 和 IPv6

HTTP/2 和 IPv6 等协议更改将导致出现对 Web 产生巨大影响的过渡期，而它们无疑在移动领域会造成更大的影响。例如，HTTP/2 对于多路复用、标头压缩和服务器推送的支持提供了性能优势，这些优势在质量不一或速度缓慢的移动蜂窝网络中尤为有用。在客户考虑过渡到 HTTP/2 时，Akamai 可帮助他们向最终用户提供 HTTP/2 支持，而无需对源站服务器进行更改，并且还可以通过 RUM（真实用户测量）报告评估 HTTP/2 的性能对最终用户造成的影响。Akamai 的 FEO 等服务可以自适应 HTTP/2，从而部分根据他们使用的是 HTTP/1.1 或 HTTP/2 来自动为每个最终用户应用适当的优化。此外，通过智能地使用设备和网络空闲时间，Akamai 的自适应加速功能使内容提供商能够自动利用 HTTP/2 的服务器推送功能 - 仍然无需对源站基础设施或代码做出任何更改 - 来改善用户体验。

提示：Akamai FEO 可以自适应 HTTP/2，从而根据客户端使用的是 HTTP/1.1 或 HTTP/2 来应用适当的优化。

Akamai 建议移动站点和应用程序采用端到端 IPv6 通信以提供最佳的移动性能，因为许多移动运营商都已开始使用仅限 IPv6 的网络。Akamai、Facebook 和 LinkedIn 开展的独立 RUM 性能研究表明，与 IPv4 相比，IPv6 在美国主要移动网络中实现了显著的性能改进。此外，Apple 现在要求 App Store 提交支持仅限 IPv6 的环境。同样地，内容提供商可以利用 Akamai 轻松获得这些性能提升。无需对源站基础设施做出更改，便可以向支持 IPv6 的最终客户端启用原生 IPv6 交付，在与源站和 IPv4 客户端通信时，则使用 IPv4。

优化媒体交付

无论交付的是 OTT 视频、快速变化的新闻、社交媒体、软件和游戏下载或其他富媒体内容，发行商都需要可实现最高质量的大规模媒体交付的媒体交付工作流程 - 跨各种类型的连接设备 - 并且没有过高的复杂性。Akamai 的服务旨在帮助发行商实现这两个目标，从而不仅提供无与伦比的媒体交付，还要提供一个基于云的全面工作流程，以便极大简化管理的同时，提高交付质量和见解。发行商可以选择使用此工作流程的任意或所有组件，因为每个部分都具有供应商不可知性，使得公司能够选择满足自身需求的最佳解决方案。

图 4：直播和点播视频的工作流程中的关键组件

Akamai 估计，自身网站出现的流媒体质量问题中，有 50–70% 是由视频获取、转码、封装或存储过程中出现的“交付前”问题造成的。这些交付前工作流步骤变得极其复杂，因为发行商需要对数据流进行封装，以便支持各种外形大小、屏幕分辨率和网络功能 — 要支持各种格式、编解码器和协议更是如此。如何安全、可靠地存储收集到的大量生成的文件也是一大难题。

通过对这些需要占用大量资源且容易出错的任务实行自动化和紧密集成，Akamai 可帮助确保从视频交付链的源头就提供最佳质量的视频。发行商需要做的只是生成单源视频，Akamai 负责准备，存储和交付，这样可大大简化发行商的任务并缩短上市时间。Akamai 还为播放和分析提供了解决方案。但是，此工作流程的每个组件都具有供应商不可知性，因此，发行商可以选择在内部或通过第三方供应商处理任何组件。

在下文中，我们将介绍为点播视频 (VOD) 和实时流媒体显示的每个工作流程步骤的重要注意事项。我们还会介绍视频交付的其他注意事项，包括视频格式、广告交付和托管服务方案。

点播视频工作流程

VOD 工作流程：获取

对于点播视频 (VOD) 内容，关键的第一步是创建原始夹层文件，并将内容摄入到视频平台中。首先，必须始终尽可能实现最高质量的内容，以便提供最高质量的播放体验。但是，存在一个收益递减点，在此点之后，更高的来源质量（在存储、传输、处理能力和时间方面具有真实成本）无法为用户提供明显更好的播放质量。根据适用于来源内容的经验法则，Akamai 建议使用的比特率等于生成的最高质量衍生文件的比特率的两倍。如果来源材料仅使用第一个视频轨道，则来源材料应只使用单一视频轨道。此外，为来源内容使用轻度压缩和行业标准格式可最大限度减少兼容性和质量问题，因此强烈建议使用具有 H.264 编解码器的 MPEG 容器（尽管并非必需）。

提示：对于原始夹层文件，使用的比特率应为最高质量衍生文件的比特率的两倍。

随后，发行商可以选择多种利用 Akamai 服务的方式。他们可以选择向 Akamai 直接上传夹层文件，从而利用它的端到端工作流程来处理视频转码、封装、存储、来源、交付和播放。或者，他们可以选择在内部处理部分工作流程。

VOD 工作流程：准备

视频准备指的是将内容转码为支持多种最终用户设备所需的编解码器、大小、帧率和比特率的过程，这些设备包括手机、平板电脑、智能电视和游戏主机，此过程可将内容封装到必要的自适应比特率格式中（例如 HLS、HDS、Smooth Streaming 和 MPEG-DASH）并在必要时使用数字版权管理 (DRM) 封装对内容进行保护。准备步骤可在本地由内容提供商执行，也可在云中由 Akamai 处理。要实现最佳播放效果，强烈建议发行商按照 Akamai 的编码最佳实践手册中提供的设置和原则执行内部转码和封装。

由于转码和封装流会造成高度可变的资源密集需求，而这种需求不太适合不灵活的基础设施，因此，Akamai 的云转码服务提供了经济高效的高性能按需方案，此方案可极大减少容量规划难题和管理开销。借助此方案，客户不再需要向 Akamai 上传大量来自每个原始夹层文件的衍生文件，即可支持多个比特率、大小、编解码器、格式和 DRM 软件包。相反，发行商只需上传夹层文件，Akamai 将使用正在申请专利的并行处理来快速高效地生成必要的衍生版本。只需在云中调整转码设置，便可以支持新的格式和设备；无需更改源站基础设施。Akamai 提供了集成 DRM 封装方案，该方案使用 Microsoft PlayReady 和 Adobe Access 等技术来保护内容。此外，对于不需要数字版权管理的内容，Akamai 的令牌授权、地理位置阻止和媒体加密功能有助于防止内容盗版和深度链接。

VOD 工作流程：存储

使用 Akamai 方案来进行媒体交付的发行商可以选择 (1) 利用 Akamai 方案来执行所有内容准备和存储，(2) 内部管理内容准备，使用 Akamai 方案来进行存储，或 (3) 内部执行所有内容准备和存储。在所有情况下，“存储”一词指的都是存储和源站托管服务。

许多发行商更喜欢第一个选项，以便最大程度减少容量规划难题和基础设施复杂性。要实现媒体文件的高可用性托管和存储，可能会面临挑战，因为在处理大量库和大型文件大小时，典型的互联网可靠性、可扩展性和性能障碍会被显著放大 - 其中，单个错误可能会导致需要重新启动整个操作。在 Akamai 的帮助下，内容提供商只需将原始夹层文件上传到 Akamai NetStorage，Akamai 将处理所有衍生文件的生成、存储和托管。

NetStorage 是一个安全、可扩展、按需且可 100% 正常运行的解决方案，可自动跨地域分散的数据中心复制内容，并且具有动态映射，可以实现高性能托管。它支持大量上传选项，包括 FTP/S、SFTP、SCP、RSYNC、基于 SSH 的 RSYNC 和安全的 NetStorage API。但是，要实现最高效的上传，Akamai 建议使用 Aspera Upload Acceleration 选项。Aspera 利用了优化的传输协议，该协议可以大大提高大文件传输的吞吐量，从而大幅加快上传速度 - 即使使用高延迟通道。可通过上传客户端以及支持直接集成到发布工作流程中的 API 访问它。

对于选择第二个选项（内部准备外加 Akamai 存储）的发行商，我们更是强烈建议采用 Aspera 上传方案。在传输包含大量呈现版本和衍生文件的库时，此方案可大幅缩短上传时间和潜在错误。

提示：Aspera Upload Acceleration 方案可明显加快面向 NetStorage 的上传速度，同时还减少了错误。

如果选择第三个选项（比如内部准备和存储），发行商将负责规划和管理他们自己的可扩展转码和容错存储功能。从 Akamai 的角度来看，发行商只需要确保其源站兼容 HTTP/1.1 并具有足够的容量来从容处理 Akamai 平台发出的所有源站请求。Akamai 通过媒体交付服务提供了巨大的分载，但源站带宽要求仍将取决于多种因素，包括视频库的大小和流行程度，以及受众人口统计数据和需求特征。Akamai 的客户团队可以帮助发行商估计所需的源站容量。但是，发行商还应意识到，源站负载可能很不均匀，例如，在促销或新发布后的前几分钟，需求会出现峰值。

最后，请注意，对于付费内容，Akamai 还为视频的云转码、存储和交付提供了一个完全安全的云工作流程（由美国电影协会审核）- 从而在工作流程的每个步骤（从原始源文件到最终客户）保护内容。

VOD 工作流程：交付

Akamai 的交付平台使用自适应的高效映射、缓存、传输和交付技术来为每个用户大规模提供最高质量的视频交付。许多此类智能都是自动进行的。但是，为了实现最佳效果，可以向 Akamai 提供内容和受众概况并明确解答以下问题：

- 媒体文件有多大?
- 内容流行度曲线的外观是怎样的；哪些内容是热门内容，哪些是长尾内容?
- 预期观众规模是怎样的?
- 观众位于什么位置?
- 观众在使用哪些设备和网络?
- 内容源自哪里？存储在哪里?

内容和受众概况信息可帮助指导配置缓存映射和功能，以便提供尽可能最佳的视频体验。

VOD 工作流程：播放

Akamai 提供了自适应比特率流，以便在动态实时网络条件下减少缓冲并最大程度提高流媒体质量。此外，Akamai 还提供了传输层优化以提高最后一英里 - 位于边缘服务器和最终用户之间 - 的流媒体质量。与 Akamai 用于加快实时流媒体接收的专有协议类似，这些优化可以实现 TCP 级别的可靠性和 UDP 级别的吞吐量，从而改进视频播放质量 - 即使底层网络条件糟糕。

此外，Akamai 可以通过 Adaptive Media Player (AMP) 帮助简化媒体交付工作流程中的播放步骤，Adaptive Media Player (AMP) 是一套统一播放解决方案，它通过上述加速传输协议在 HTML5、Flash、原生 iOS 和原生 Android 平台设备上提供自适应比特率流媒体。对于喜欢快速和简化的媒体播放器部署路径的内容提供商而言，AMP 的全包式功能还包括完全集成的流媒体保护、分析（Akamai、Nielsen、Comscore、Omniture）、广告（DoubleClick/VAST、Autitude、Freewheel）、DVR 功能和隐藏字幕支持。Adaptive Media Player (AMP) 独立于工作流程，因此，发行商可以将它与首选的内容管理、转码、交付、广告和分析解决方案配合使用。通过简单统一的配置文件启用功能 - 无需进行编码、工作流程修改或多平台更改。

VOD 工作流程：分析

发行商可以选择使用 Akamai 以及其他第三方分析解决方案来测量性能，并深入了解受众人口统计数据和观众体验。Akamai 媒体分析提供了一个可高度扩展的跨平台智能解决方案，它可帮助发行商深入了解哪些作品受到追捧、观众在使用哪些设备、广告加载如何影响观看时间、观众体验到的质量水平以及问题是否正在影响放弃率。此外，Akamai 媒体分析提供了实时 QoS 监视功能，使得内容提供商可以实时深入检测质量问题，它还提供了观众诊断功能，可以捕捉细分到单个用户级别的性能和参与度指标。

与任何媒体分析解决方案一样，要充分利用 Akamai 媒体分析，需要做出一些前期思考和规划。发行商必须确定他们在查看指标时想要采用的维度。例如，他们可能想要按周中日、特定地区、特定内容风格或联号来源查看指标（例如，播放数、观众群体大小、首帧时间、缓冲时间、观看时间、观众操作等）。其中一些指标要求将内容划分为多个类别和层次结构：例如，可以首先按联赛来组织体育活动，然后按球队，接着按比赛。类似地，电视节目可以首先按流派进行整理，然后按子流派，接着按节目，然后按剧集。必须提前确定这些类别和层次结构，并通过某种方式指示（比如播放 URL 的一部分或通过播放器做出的特定调用），以便 Akamai 媒体分析可以配置为在播放时捕获相关指标数据。无法逆向进行分类。

为实现最灵活和细致的数据收集，Akamai 建议使用客户端数据收集（通过将 Akamai 媒体分析插件集成到播放器中，或使用 Akamai 预先集成的 Adaptive Media Player）。但是，服务器端数据收集是一种可行的替代方案。它基于 Akamai 服务器日志，但它支持的功能范围不像客户端收集那么广泛。

实时流媒体工作流程

实时工作流程：获取

对于直播活动和线性节目编排，媒体交付工作流程具有与 VOD 工作流程类似的组件，但在架构方面稍有差异。但是，与 VoD 内容一样，原始接收流媒体的质量对于最终观看体验极为重要。要最大程度减少源站流可能出现的问题，Akamai 强烈建议内容提供商使用符合 Akamai 合格条件的实时流媒体编码器（比如 Akamai 预先测试的列表中列出的编码器）。这些编码器具有提供可靠、高质量的实时流媒体所需的稳定性，而使用不合格编码器的提供商可能会遇到各种限制，包括不受支持的安全机制、功能不兼容性和更难的问题解决过程。此外，与 VOD 内容一样，Akamai 建议使用具有 H.264 编解码器的 MPEG 容器，以最大程度减少兼容性和质量问题。

如果必须通过互联网发送原始流媒体视频以到达接收点，也可能很难实现高质量的第一英里。但是，借助 Akamai Media Services Live Origin，内容提供商可以利用先进的流媒体加速技术，通过专有传输协议来同时受益于 TCP 的可靠性与 UDP 的吞吐量。这可确保在从发起点到 Akamai 网络的过程中，实现最高质量的实时流媒体。发行商只需使用 Akamai 的编码器插件来加快发送到最近的 Akamai 分布式网络入口点的实时流媒体。

提示：Akamai 的增强传输协议可在关键的第一英里 - 流媒体获取 - 最大程度降低质量损失。

建议通过第二个编码器（与主编码器时间同步和 GOP 对齐）来向网络独立于第一个编码器的第二个 Akamai 入口点提供备用实时流媒体。对于特大规模或任务关键型事件，内容提供商可能会考虑使用两个独立的网络提供商来将他们的主要和辅助来源流媒体传输给 Akamai。使用两个提供商是最佳做法，以防一个数据中心连接故障。通过设置 GOP 合规的流媒体，可以在主要和备用流媒体之间实现无缝故障转移。未对齐的流媒体仍可提供冗余，但最终用户通常需要重新启动流媒体才能继续观看。

实时工作流程：准备

与 VOD 内容一样，必须将实时流媒体实时转码和封装到大量编解码器、大小、帧率、比特率和格式中，以便支持许多不同的最终用户设备和网络。内容提供商可以选择让 Akamai 在其高容量的云网络中运行此处理密集型步骤。或者，内容提供商可以选择亲自充当“实时源站”，在内部处理此步骤，然后将封装的流媒体传输给 Akamai 接收点进行交付。后一种选择要求发行商内部具有可扩展的高可用性转码、封装和数字版权管理服务，从而提供足够的带宽，以便通过强大的容错方式同时将每个实时流媒体的多个转码和封装版本传输到 Akamai。对于需要 DRM 保护的实时流媒体内容，发行商必须在内部执行内容准备（包括 DRM 加密），然后再将它发送到 Akamai 进行交付。

对于非 DRM 内容，Akamai Media Services Live Origin 允许出版商为源站服务（比如实时流媒体转码和封装）使用 Akamai 的高可用性网络。通过这种方法，内容提供商只需要分配带宽以将单一高分辨率内容（以及可选的备份）输送到 Akamai，如上文的实时工作流程：获取步骤中所述。Akamai 的云平台为实时流媒体提供了具有容错、高性能、高可扩展性的实时转码和封装，这大大减少了发行商的基础设施复杂性。与 VoD 内容一样，只需调整 Akamai 的转码设置，便可添加对于新设备或格式的支持 - 无需更改接收流本身。

在编码配置文件方面，截至 2017 年初，美国的流媒体事件的平均比特率大于 3 Mbps，并且在继续增长。根据目标受众和设备人口统计数据，典型的编码配置文件可能包含大约 8 至 10 个比特率变体 - 从 364 Kbps 到超过 10 Mbps。另一个重要事项是，为自适应比特率流媒体选择相应的分段长度。对于实时和点播流媒体，通过使用较长的分段大小（和更长的关键帧时间间隔），通常可以实现更高质量的视频。遗憾的是，它还会导致对于变化的网络条件的适应性降低。对于实时视频，还存在一个注意事项：更短的分段可在实时流媒体中实现更短的实时延迟。弊端在于，使用较短的分段时，也会对编码、封装和网络资源造成更大的负荷，因此也可能降低观看质量。图 5 提供了针对不同情况的建议分段长度设置。

分段持续时间（秒）	**用于设置分段持续时间的查询字符串值**	**已针对**	**实时编码器上可能的关键帧值优化**
10	最流畅	最流畅的流媒体体验，具有最少的缓冲事件，但它会导致实时流媒体延迟	1、2、10
6	高质量	更接近实时流媒体，但仍偏向于交付质量，而非延迟	1、2、6
4	响应迅速	低延迟的实时流媒体；可能发生一定程度的质量下降	1、2、4

图 5：建议的实时流媒体分段长度。

实时工作流程：存储

存储通常被视为按需内容的源站托管组件的一部分，而对于实时流媒体，除了启用 DVR 功能以外，存储更多起到存档作用。在 Akamai 帮助下，实时和线性广播可传输到 NetStorage 中进行存档，同时还可以交付给直播观众。这使得发行商可以提供 DVR 功能（比如暂停或回放实时流媒体）以及稍后观看流媒体内容。

实时工作流程：交付/播放/分析 - 和监控

对于实时内容和按需内容而言，最后三个工作流程组件非常相似。请参阅以上类似的 VOD 工作流程章节以了解详细信息。

对于大型直播活动，实时监控通常发挥着更关键的作用，可通过 Luna Event Center 对实时监控提供支持，该产品的 Control Room 仪表板可以在活动期间实现实时监控、警报和诊断。要监视的一些关键指标包括并发观众数量、总带宽、重新缓冲率和 HTTP 错误数量。如果前三个指标中的任何一个发生突然变化，则可能表明存在流媒体问题。另一个有效的方法是，在调查问题点时，在观众分段（基于地理位置、设备类型、操作系统、网络提供商、网络连接类型等）内对这些指标进行深入分析。

媒体交付的其他注意事项

在以下内容中，我们为希望优化视频交付和提高流媒体质量的发行商提供了有关视频格式、广告交付和托管流媒体服务的额外指导。

视频技术和格式

相互竞争和不断演变的视频编解码器、格式和协议一直都是 OTT 提供商面临的难题。在协议方面，行业在过去几年从专有流媒体协议（比如 RTMP、MMS 和 RTP）转变为了通过 HTTP/S 使用自适应比特率流。但是，即使对于统一传输协议，仍存在一些相互竞争的自适应比特率格式，即 HDS、Smooth、HLS 和 MPEG DASH。尽管行业似乎一致朝着 HLS 和 MPEG DASH 发展，它仍然可能需要支持当前市面上的全部四种格式，以便在现有设备中实现最大的覆盖范围。每增加一个格式，就意味着要对每个内容额外进行一次编码、封装和存储 - 因此需要更多缓存空间，并且会降低交付效率。对于 DRM 的需求使此问题进一步加剧，因为流媒体格式和流行的 DRM 解决方案（例如 PlayReady、Widevine、FairPlay Streaming 和 Adobe Access）之间存在一个复杂的兼容性矩阵，因此每个作品需要更多的衍生版本。

行业现在已开始采取明确的措施来支持名为 CMAF（通用媒体应用程序格式）的单一媒体文件格式，尽管要让市面上的大多数设备支持 CMAF 还需要经历数年时间。通用媒体应用程序格式并不能解决 OTT 行业面临的所有碎片化问题，因为编解码器和加密模式仍存在多种相互竞争的方案，仍然需要支持旧格式以覆盖较旧的设备。但是，CMAF 是通往正确方向的一步，因为使用单一通用媒体文件格式可以改进缓存、存储和媒体文件传输效率。在这一过渡期中，借助云转码平台，Akamai 可以缓解相互竞争的格式、封装和协议造成的难题，使发行商能够专注于制作内容，而不必担心如何覆盖市场中多种不同的设备和平台。

广告交付

广告交付会对观众体验造成重大影响 - 由于广告拦截程序或广告缓冲，这些影响通常是负面的。Akamai 建议将服务器端广告插入作为最佳做法，而不是客户端插入。服务器端的插入可减少对于客户端媒体播放器的要求和负载，从而实现更广泛的设备覆盖，包括机顶盒、智能电视和移动设备。它还消除了客户端广告插入所需的媒体播放器处理造成的负面性能影响。此外，服务器端广告插入更能灵活对抗广告屏蔽技术，因此有助于保护盈利。

通过 Akamai 提供内容和广告可以带来额外的架构和安全优势。它还允许通过一致的比特率随内容一起无缝交付广告，无需缓冲延迟，从而实现更好的最终用户体验。Akamai 提供了与主要广告插播提供商预先集成的解决方案，使发行商能够在最广泛的范围内提供最高质量的广告和内容体验。

提示：使用服务器端广告插入以实现最佳的观众体验并降低广告屏蔽技术造成的影响。

托管广播服务

对于想要利用 Akamai 的媒体团队的专业知识和经验的发行商，Akamai 的托管广播服务可对整个播放工作流程提供全天候实时监控。其中包括主动系统组件评估、内容完整性和交付检查以及观众实时 QoS 反馈，以便轻松检测和缓解任何可能发生的问题。

对于要求最苛刻的广播客户，Akamai 先进的 Broadcast Operations Control Center (BOCC) 提供了最高的服务水平，可以为最大规模的观众群体实现完美的观看体验。除了提供专家工作流程评估和最佳做法建议，BOCC 还提供了其他专业资源。它提供了出色的主动监控，以便及早识别和快速解决流媒体工作流程中每个步骤（从编码到播放）的问题。

网站安全性

稳定的多层防御策略变得比以往任何时候都更加重要。组织必须保护在线业务对抗不断变化和不断增长的威胁形势。Akamai 云安全解决方案独一无二的功能和无与伦比的规模可以在任何此类战略中发挥关键作用，通过久经验证的能力来保护网站和应用程序抵御最大规模和最复杂的网络攻击。

在本节中，我们将了解安全在线架构的部分关键组件 - 从 DNS 基础设施，到 Web 应用程序保护，再到爬虫程序管理。最佳做法要求在编码时始终将安全牢记在心。下述防火墙和其他外围防御可提供可靠的保护。此外，新发现漏洞时，Web 应用程序防火墙虚拟修补等技术可以快速实施有利的短期解决方案。但是，从根源创建安全的代码和修复确定的安全漏洞应始终是努力的目标。

DNS 保护

如前所述，DNS 是一个在源站基础设施中至关重要、但常常被忽略的组件，因此它特别容易遭到 DDoS 攻击。希望保护 DNS 架构的客户可以采用 Akamai 的 Fast DNS 服务。此服务利用了由数千个全球分布式名称服务器组成的高性能网络，使它能够有效抵御互联网规模的 DDoS 攻击。Fast DNS 还可防止 DNS 伪造和操纵，并且无需更改现有 DNS 管理流程。

Web 应用程序保护

Web 应用程序和 API 需要通过互联网规模的防御能力来抵御各种网络攻击。事件包括网络层 DDoS 攻击、应用程序层漏洞（比如 SQL 注入和跨站点脚本攻击），等等。这些攻击的规模、频率和复杂性在不断增长 - 通常采用多种攻击方式，一波又一波地发起。分布式拒绝服务 (DDoS) 攻击如今的峰值高达数百 Gbps - 几乎足以让最大公司的基础设施停机。攻击者可以在流量高峰时间发起攻击以最大程度增加破坏，从而充分利用已经过载的基础设施。

Akamai 的 Kona Site Defender (KSD) 利用了 Akamai Intelligent Platform 的数十万个服务器来提供永不停机的 DDoS 和 Web 应用程序防火墙 (WAF) 防御。这些防御可以无缝处理最大规模的互联网攻击，同时确保为合法的 Web 和 API 流量提供高性能。在攻击流量到达源站前，在互联网边缘及早将其阻止。此外，KSD 的 WAF 利用了可配置的丰富规则集，我们通过 Akamai 网络中收集的真实数据对这些规则集进行了连续测试和更新。此连续测试提供了远比行业标准规则集准确的规则集。

可单独使用 Kona Site Defender，也可与 Akamai 的其他交付和安全服务配合使用。要进行实施，只需要通过 CNAME 映射到 Akamai（已在使用任何 Akamai 交付服务时完成此映射），并配置要使用的 WAF 和 DDoS 规则即可。了解流量概况 - 比如从每日、每周和每月的角度分析站点一般拥有多少流量，这些流量来自什么位置，这些信息有助于调整规则和速率控制。

源站服务器保护

使用 Akamai 交付服务时，所有针对源站的主机名寻址请求都将自动定向到 Akamai 网络，因为主机名已通过 CNAME 映射到 Akamai。但是，仍然可以使用源站 IP 地址对源站服务器发起攻击（绕过 DNS）。Akamai Site Shield 是 Kona Site Defender 的一个组件，它可限制客户端直接向源站发送流量，从而抵御这些类型的攻击 - 实际上，Site Shield 会从公共互联网隔离源站。

要实施 Site Shield，源站需要只允许特定 Akamai 边缘服务器 IP 地址通过的防火墙设置。此 IP 地址列表可能每 30 到 90 天更改一次，具体取决于客户的产品配置。因此，内容提供商应针对更改 IP 白名单设置详尽和高效的流程。可以手动完成此流程，或通过与 Akamai 的 Site Shield API 集成来自动完成。内容提供商应知晓，如果防火墙是由内容提供商的 ISP 处理（而不是直接由内容提供商处理），则白名单 IP 流程会更加麻烦。此外，一些云源站提供商可能会出现问题，因为他们可能会限制可在防火墙中配置的 IP 数量。

请注意，Site Shield 无法为源站服务器提供全面的 DDoS 保护，因为攻击者仍可以通过大量请求让源站防火墙过载。如下所述，Prolexic 服务为这些场景提供了保护。

源站数据中心保护

Akamai 的 Prolexic Routed 服务为源站基础设施提供了强大的保护功能以抵御 DDoS 攻击 - 包括路由器、负载平衡器和 Web 应用程序服务器以及非基于 Web 的服务，比如游戏服务器、VOIP 或其他基于 IP 的企业应用程序。作为完全托管服务，Prolexic Routed 可以保护整个 IP 子网抵御高达数百 Gbps 的网络和应用程序层 DDoS 攻击。此外，还通过全天候专家服务和业界领先的缓解时间 SLA 来为其提供支持。

Prolexic Routed 面向的是希望至少保护 /24 的 IP 子网的客户。启用服务时，不再可以直接通过互联网路由客户源站；相反，针对源站 IP 的所有 Web 和非 Web 流量将首先通过 BGP 路由至 Akamai 的其中一个全球分布式 Prolexic 清理中心。这些高性能中心（具有 Tbps 的专用容量）通过 Akamai 的专用主干网回程传输流量。然后，此高性能中心会通过一般路由封装 (GRE) 隧道或虚拟租用线路将清理后的流量转发到源站网关路由器。因此，源站数据中心仅接收和响应清理后的流量。

提示：Akamai Prolexic 可保护源站基础设施 - 包括 DNS、负载平衡器、基于 IP 的服务、VPN 和 Web 应用程序 - 抵御互联网规模的 DDoS 攻击。

Prolexic Routed 可设置为按需或永不停机的服务。使用按需配置时，内容提供商需要能够更改 BGP 通告以打开和关闭服务，对于让第三方提供商来管理边缘路由器的组织而言，这可能更加麻烦。

可单独使用 Prolexic，也可与其他 Akamai 交付和安全服务配合使用。将 Prolexic 与其他 Akamai 服务配合使用时，请求将从最终用户转至 Akamai 边缘网络 - 在那里，可在边缘得到处理的所有请求将立刻寻址 - 包括应用的任何保护服务，比如 WAF。需要源站响应的请求将被转发到 Prolexic 清理中心进行清理，然后再发送到源站。然后，源站的响应被发回 Akamai 边缘网络，边缘网络将对客户端做出回复。在某些情况下，将 Prolexic 与 Akamai 交付服务配合使用时，最终用户延迟可能会受到影响。因此，Akamai 建议使用 Akamai 交付服务的客户配置 Prolexic 作为按需服务，并根据需要开启保护功能（例如，受到攻击时）。

将 Prolexic 与 Fast DNS 或 KSD 配合使用时，功能会出现重叠。在这种情况下，因为它们构成了外围防御，Fast DNS 和 KSD 将提供 DDoS 保护以抵御那些以 DNS 基础设施和 Web 应用程序为目标的攻击。Prolexic 为直接针对源站基础设施（或针对基于 IP 的非 Web 服务）的攻击提供 DDoS 保护。单独使用 Prolexic 时，它可以提供全部三种 DDoS 保护 - DNS 基础设施、Web 应用程序和源站基础设施。但是，Prolexic 不提供 FAST DNS 中包含的其他功能（例如，高性能、高可用性、安全增强 DNS 基础设施）以及 KSD 中包含的其他功能（例如，互联网规模的 WAF 保护）。

多层防御：Akamai 云安全解决方案概览	DNS DDoS	DNS 伪造	Web 应用程序 DDoS	Web 应用防火墙	指向源站的 DDoS	源站掩蔽
Fast DNS	✔	✔				
Kona Site Defender			✔	✔		✔
Prolexic			✔		✔	

图 6：Akamai 的安全产品提供了重叠防御层，这些防御层可以独立使用、共同使用，和/或与 Akamai 交付服务组合使用。

爬虫程序管理

许多组织没有认识到，现在爬虫程序在网站流量中占据了极大比例 - 在许多情况下，占了超过一半的流量 - 这可能消耗组织的大量带宽和服务器资源，以及影响合法最终用户的性能。但是，并非所有爬虫程序流量都是有害的。其中既包括有用的爬虫程序（比如搜索引擎爬虫程序和合作伙伴公司的爬虫程序），也包括有害的爬虫程序（比如 DDoS 攻击者、采集者），还有许多爬虫程序介于这两者之间（例如聚合器或其他站点采集服务使用的爬虫程序）。但是，即使有益的爬虫程序也可能具有侵略性，可能会在不适当的时候让站点负担过重。

这意味着，处理爬虫程序的最佳方法是智能加以管理，而不是盲目予以抵御。借助 Bot Manager，Akamai 使组织能够根据已知、未知和自定义的爬虫程序签名检测并分类爬虫程序。随后可以根据遇到的爬虫程序类型应用策略（比如警报、阻止、延迟、静默拒绝、从缓存提供或提供替代内容/替代源站），以便直接在 Akamai 边缘服务器上处理爬虫程序流量 - 从而保护源站。

客户端信誉智能

借助 Akamai 的客户端信誉服务，网站可以收到每个发起请求的 IP 地址的信誉得分，此得分可指明 IP 地址有多大可能属于恶意类别 - Web 攻击者、拒绝服务攻击者、扫描工具或 Web 采集者。得分基于在 Akamai 网络上观察到的此 IP 的最近行为，并与合法和攻击流量概况进行比较。组织可以利用此信息改进安全决策，既可借助 HTTP 标头提供的得分直接在源站服务器上进行改进，也可通过 Kona Site Defender 操作进行改进。

托管安全服务

随着网络攻击的规模和复杂程度不断增加，人工专业知识在检测和对抗威胁方面变得至关重要。Akamai 的托管服务产品通过 Akamai 的全球分布式安全运营中心 (SOC) 提供了全天候监控和响应性攻击缓解，该中心配备了超过 100 位经验丰富的安全专家，他们每周会积极缓解数百次 DDoS 攻击。

或者，具有人员完备的安全中心的组织可以选择为 Akamai 的安全解决方案提供自助服务。此外，他们可以利用 Akamai 的 OPEN API 来将报告数据源和自动配置更改直接集成到应用程序工作流程中。最后，Akamai 在项目基础上提供了安全优化服务，以帮助现场安全团队执行安全审查并优化安全配置以获得最优效果。

其他资源

Akamai 的活跃社区论坛 (https://community.akamai.com) 包含大量与 Akamai 的产品和服务相关、以开发人员为中心的信息，并为 Akamai 客户提供了一个相互沟通的渠道，还有涉猎多种主题的 Akamai 主题专家常驻于此。以下子领域可能特别值得关注：

- https://community.akamai.com/community/developer - Akamai 的 {OPEN} API 开发人员社区
- https://community.akamai.com/community/services-and-support - 一个论坛，其中，Akamai 的服务和支持专家会发布博客以介绍最佳做法和回答客户问题
- https://community.akamai.com/community/akamai-university - Akamai 大学全球课堂和在线培训课程，包括有关 Akamai 产品的高级培训
- https://community.akamai.com/community/security-research-and-intelligence - Akamai 的安全研究和智能论坛

还设置了聚焦于 Akamai 的每个主要产品线的子论坛，包括：

- https://community.akamai.com/community/web-performance - Web 性能
- https://community.akamai.com/community/media-delivery - 媒体交付
- https://community.akamai.com/community/cloud-security - 云安全

此外，Akamai 开发人员网站 https://developer.akamai.com/ 提供了 Akamai 的 API 和 SDK 的文档和示例代码，以及面向开发人员和架构师的、与 Akamai 平台及其功能有关的学习资源库（位于 https://developer.akamai.com/learn/），它对我们此处已经探讨过的许多主题进行了扩充。

最后，Luna Control Center（https://control.akamai.com/；需要客户登录）是所有 Akamai 管理和控制功能（包括用于配置 Akamai 服务的 Property Manager）以及所有 Akamai 监控、报告和分析工具的 Web 界面。客户能够通过 Luna Control Center 为他们的 Akamai 产品和服务提供完全自助服务。

资料来源

1. 在有关理解缓存控制的章节中将详细讨论缓存
2. 默认情况下，使用 HTTP/1.1 时，Akamai 为 GET 请求使用 30 秒连接超时和 120 秒读取超时。对于 HTTP/2，Akamai 使用 30 秒连接超时和 30 秒读取超时。可以根据需要调整这些值，但要记住预期的服务器处理时间，特别是针对数据库调用或第三方事务。
3. 默认情况下，使用 HTTP/1.1 时，Akamai 为 GET 请求使用 30 秒连接超时和 120 秒读取超时。对于 HTTP/2，Akamai 使用 30 秒连接超时和 30 秒读取超时。可以根据需要调整这些值，但要记住预期的服务器处理时间，特别是针对数据库调用或第三方事务。
4. 默认情况下，Akamai 将忽略这些面向下游缓存的标头。但是，可以方便地通过标准配置规则指示 Akamai 服务器支持这些标头。
5. http://requestmap.webperf.tools/ 为页面上的第三方调用提供了一种强大的可视化工具。
6. 相反，综合能测试提供了通过自动测试代理捕获的指标。