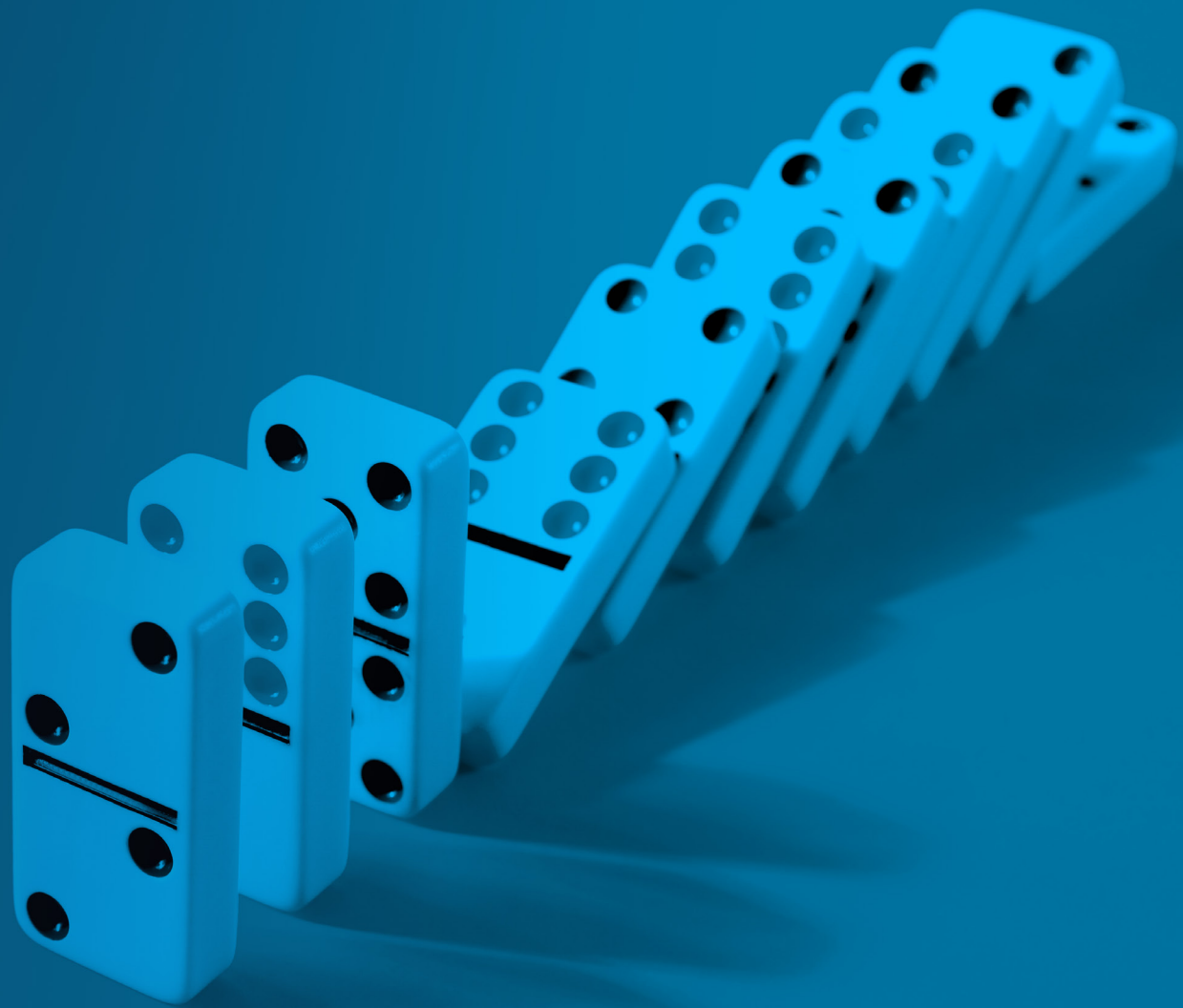




任何一天都可以是节假日

助您应对商业高峰活动的秘诀

电子书



目录

前言	03
第 1 章：提前做好准备，应对高峰时期的性能需求	04
秘诀 1：提前检查缓存设置	04
秘诀 2：提升活动期间的分载率	04
秘诀 3：优化图像和视频	05
秘诀 4：识别和管理爬虫程序	05
秘诀 5：坦然面对“正常降级”	05
第 2 章：做好应对最坏情况的准备	06
秘诀 6：执行压力和负载测试	06
秘诀 7：部署等候室	06
秘诀 8：制定灾难恢复计划	07
秘诀 9：尽可能提升监控能力	07
第 3 章：增强安全框架	08
秘诀 10：查看行动手册	08
秘诀 11：做好应对 DDoS 攻击的准备	08
秘诀 12：时刻铭记客户	08
秘诀 13：了解您的 API 攻击面	09
秘诀 14：调整告警以减少噪声	09
秘诀 15：加强对恶意爬虫程序的防御	09
第 4 章：总结经验教训	10
特别秘诀 16：开展正式评估	10
彻底改变应对高峰活动的策略	11

前言

美国有传统的“三大”购物节：感恩节、黑色星期五和网络星期一，而对于零售业、旅游业以及酒店行业的企业而言，迎来高峰活动的时机并不仅限于这些节日。根据您的业务或行业情况，任何一天都可能迎来高峰活动。例如，对于花店而言，情人节无疑是一年中的黄金时刻，而对于旅游和服务类公司而言，暑假则显得尤为重要。医疗保险公司会在新生注册期间迎来访客激增，而零售公司的高峰期则出现在新产品备受欢迎或开学购物季拉开帷幕之时。如果我们把目光投向美国之外，不难发现，奥运会、世界杯等大型赛事的举办会引发高峰活动，同样，排灯节、中国春节以及慕尼黑啤酒节等节日也会带来同样的热潮。

在传统的高峰节假日期间管理性能需求和安全风险时所积累的经验教训，同样适用于任何高峰活动或高流量活动。不论是哪种情况，您都必须成功应对一天之内的流量激增，并妥善管理远高于日常水平的风险。每种情况都伴随着高风险：在管理这些活动的过程中，任何纰漏都可能导致收入损失和声誉受损；成功管理这些活动则能够带来收入增长，令客户满意。

在针对高峰活动进行准备时，您需要优化平台性能，做好充分准备以应对最糟糕的情况，及时更新安全态势，并进行事后反思，确保顺利应对下一次的高峰活动。

在接下来的四章中，我们将介绍 15 个最佳做法，旨在帮助您做好准备以应对任何高峰活动，无论这些高峰活动发生在何时，也无论其发生的频率如何。

见解：高峰活动在不断改变，您的高峰策略也应随之改变。

如今，客户期望[节假日能够更早开始并且持续时间更长](#)，不再是仅仅几天，而是希望以周甚至月为单位延续下去。消费支出的转变、选举和政治事件，以及其他宏观因素的影响，都为未来增添了更大的不确定性。这意味着商业企业在准备应对高峰活动时，不能再仅仅将这种活动视为一个孤立的大规模事件来制定应对策略。持续性的高峰活动要求公司建立可持续的运营流程，以确保能够几乎即时地应对一系列高峰活动，同时避免给客户或运营带来任何干扰。

第 1 章： 提前做好准备，应对高峰时期的性能需求

在优化网站性能以应对高于正常水平的流量负载时，预先规划显得尤为重要。毫无疑问，出色的内容交付网络 (CDN) 是您策略中不可或缺的组成部分。但与此同时，您还需要规划如何在大量访客与网站交互时确保网站的顺畅运行，以及制定在系统面临压力时的应对策略。在这种情况下，为了充分提升性能和分载能力，您需要对下面三种内容类型采取不同的处理方式：



HTML 页面结构，这构成了网站的基本内容（目标分载率应为 50%）



其他静态内容，例如 JavaScript、CSS、图像和视频（目标分载率至少应为 80%，但我们建议尽可能达到 90% 及更高）



API 流量，例如移动应用程序、定价、登录和结算（目标分载率不定，具体取决于 API 调用的性质以及所检索数据的性质）

下面将介绍五种最佳做法，以确保针对高峰活动优化和调整您系统的性能，以达到最佳状态。

秘诀 1：提前检查缓存设置

在考虑高峰活动之前，先评估您要缓存的内容以及缓存的位置，以确保您的缓存策略能够充分满足日常需求。这样做的目标是在充分提升个性化程度的同时，优化网站的外观，并尽可能快地交付您所期望的 Web 体验。缓存设置主要应用于静态内容和静态资产，您应根据业务需求尽可能多地缓存它们。特别是图像，最好缓存在源站的负载均衡器或 CDN 上，甚至可以直接推送到用户设备上，无需从 Web 服务器上拉取。

使用 HTML 时，可缓存的内容远比乍看起来要多。您可以通过优化网站结构，并将内容分割成多个片段，以此实现更高的 HTML 分载率。例如，如果网站的许多用户未登录（即不需要为他们动态提供个性化内容），那么可以为这部分用户群缓存内容并重复使用。结论：如果有很大比例的用户未登录，那么可以为其缓存相应的内容。对于其他类型的静态内容，您应该努力实现 90% 及以上的分载率。我们知道，您可能已经花费了大量精力来优化这些类型的网站内容，不过您不妨再仔细检查一下，以确保达成目标。最后，对于 API 的处理，尽管有些数据更新过于频繁而不适合缓存，但我们仍然可以考虑哪些 API 调用是可以进行缓存的，例如运费信息、店铺位置或定价。如果库存信息每 60 秒更新一次，那么我们完全可以考虑将其缓存 30 秒。如果定价信息在每天午夜更新，那么我们可以安排每 12 个小时对所有 API 调用进行一次缓存。在高峰活动期间，每一点资源都显得尤为重要，而缓存的每一秒都能提升您的分载率，从而在关键时刻发挥出重要作用。

秘诀 2：提升活动期间的分载率

接下来，我们将寻找那些在活动期间仅通过缓存某些内容就能实现性能显著提升的场景。以定价或运费响应为例，如果我们将这些信息缓存几分钟，就能释放服务器资源，进而在降低成本的同时，获得更高的扩展能力。另外，还有一些方法涉及到缓存重定向（例如动态页面组装、预渲染以及图像优化），这些内容您应该在边缘进行缓存。在活动期间乃至活动结束后，仍有许多内容可以进行分载处理，这涵盖了业务逻辑、用户体验、重定向、SEO 优化以及爬虫程序管理。



秘诀 3：优化图像和视频

图像和视频可能是静态内容，不过有多种方法可以帮助您更简单且更智能地将这些内容提供给客户。为了确保在高峰活动期间提供出色的用户体验，提前进行图像和视频优化显得尤为关键。为此，您很可能需要与图像优化提供商合作，以确保能够在合适的时机，为每位客户提供大小适中、格式兼容且视角恰当的图像或视频资产。在此过程中，您还需要全面考虑客户可能使用或拥有的各种设备、浏览器、操作系统，甚至还要考虑网络连接。通过优化图像和视频，您可以：

-  减轻页面负载，提升响应速度（减少传输的字节而不降低质量）
-  改善加载时间和网站响应能力
-  简化资产管理，从而减少创意和设计团队的工作量

秘诀 4：识别和管理爬虫程序

研究表明，爬虫程序占到了所有互联网流量的近 50%，这意味着近乎一半的流量对您的系统构成了不必要的负担。因此务必要制定策略，防止爬虫程序在高峰活动期间引发意外问题。为了确保能够满足付费客户的需求，您应当尽量保留足够的系统容量，然而，若爬虫程序在高峰活动期间过度消耗资源，将会削弱您为这些客户提供服务的能力。通过运用先进的工具集，您可以识别出哪些类型的客户发出了请求，以及该事务背后的意图。这一能力让您能够有针对性地聚焦于特定的爬虫程序交互，同时减少对另一些交互的关注度。要想减少爬虫程序负载，有一种策略是从另一个源站向爬虫程序提供预先渲染的缓存内容。另一种策略是在高峰期间关闭所有网站爬虫程序，尽管这可能暂时地影响搜索引擎优化 (SEO)，但可以实现收益最大化。面对大量的爬虫程序，您应该掌握相应的工具和技能，以便在高峰活动期间能够针对不同类型的爬虫程序做出更细致的决策，尤其是当您不希望耗费过多资源向这些爬虫程序提供服务时。

秘诀 5：坦然面对“正常降级”

您应该能够通过让网站暂时失去部分功能，来确保网站整体仍然保持运行。实际上，在运行过程中，您可能从未完全避免过某些功能的短缺，即进入一种“正常降级”状态，这是一个源自复杂系统的概念。您可以通过精心设计系统架构，使系统在高峰负载期间策略性地在“降级”状态下运行，从而实现更优的性能表现。例如，一家大型在线零售商在购物高峰期间暂停其推荐功能，因为在此期间，该功能带来的商业价值与其对系统产生的负载不相匹配。

第 2 章： 做好应对最坏情况的准备

现在，您已经设计了系统，能够顺利处理高峰活动期间预计会出现的负载。接下来，您需要考虑的是，在实际情况偏离预期时应该如何应对。

在峰值流量时刻，由于系统已经承受了巨大压力，这可能会使您的运营瓶颈和脆弱领域面临更大的挑战。面对高峰时期的巨大压力，您可能无暇及时发现问题，更不用说应对了。正因如此，提前准备，对可能出现的问题做好应对预案，就显得至关重要，这样才能避免影响到您的客户或收入。在峰值到来之前，请务必花一些时间，深入了解预计会出现的负载情况，以及它可能对系统的安全性、性能和可靠性造成的影响。验证您的系统在何种情况下能够正常运行，并针对无法正常运行的情况制定应急预案。

下面介绍了四种最佳做法，可助您为可能出现的各种情况做好准备。

秘诀 6：执行压力和负载测试

此过程的第一步是明确哪些后果是不可接受的。其目标在于识别出哪些情况会超出可接受范围，并针对这些越界情况制定应对计划。您可以通过执行压力测试和负载测试来明确这些界限，并了解可能发生的各种情况。在高峰活动到来前的几个月里，多次运行压力测试，并预设系统可能一开始就面临崩溃来进行模拟。这样，您就能拥有足够的时间来纠正问题，并且随着时间的推移，您对自己能够妥善处理必要负载的信心也会日益增强。

秘诀 7：部署等候室

您的网站必须能够根据需求灵活限制流量。通过实施等候室机制，您可以在高峰时段维护结账流程的运行，并在遇到意外问题导致流程速度减慢时，妥善管理用户体验。您还可以借助此方法来实现正常降级，比如通过时间偏移管理或提供早期的独占访问权限。等候室的一大关键益处在于，当系统发生错误时，它能够用作故障恢复手段。详细了解[应对促销活动或流量高峰](#)并仍能培养客户忠诚度的策略。

见解：负载上升会出现什么情况？

系统的负载上升可能仅仅是由小假期带来的小幅增加，也可能是由社会性事件所引发的大幅攀升。例如，2020 年 4 月，新冠疫情迫使许多人居家隔离并上网，[Akamai 观察到](#)全球互联网流量因此增加了 30%，短短几周内的增长幅度就相当于全年的增幅。



秘诀 8：制定灾难恢复计划

灾难恢复计划旨在应对自然、网络或业务方面发生的大型灾难，其恢复过程通常需要几天到几周的时间。如果灾难发生在高峰活动时，您应该怎么办？例如，如果故障转移需要四天的时间，而您的业务活动只持续四个小时，这就表明您缺乏一个有效的灾难恢复计划。您的灾难恢复计划及其实战演练应当与实际可能遭遇灾难的风险相匹配，同时确保所设定的时间框架和执行能力能够满足应对此类风险的需求。最后，采用双活方法，而不仅仅是从灾难恢复的角度进行准备，这样可以帮助您确保业务运营不会因任何单一灾难事件而受到损害。

秘诀 9：尽可能提升监控能力

通过实施监控措施，您可以了解系统在高峰活动期间的表现情况。同时，监控技术指标与业务指标同样至关重要。在您的仪表板中，可能会有一半的功能专门用于监控技术指标，如 CPU 利用率、吞吐量和页面加载时间，而将另一半的功能用于跟踪业务指标，如点击率、购物车遗弃率和转化率。您需要同时关注这两种指标，因为技术指标只能揭示系统性能问题的原因，但无法反映这些问题对实际用户体验的影响。为此，您需要相关的业务指标。尽可能提升对这些指标的监控能力，将有助于您发现异常情况，并触发相应的自动操作来修复问题。

第 3 章： 增强安全框架

在讨论安全性时，我们离不开对风险的考量：风险识别、风险抵御、风险影响、风险可能性等多个方面，而且决定如何应对这些风险至关重要。本质上，这是一项寻求平衡的行动。例如，在高峰活动期间，您可以选择采取更积极的措施来应对潜在风险，但需注意这可能会对用户体验造成一定影响。为了确保安全性，最佳做法包括确保平台配备精心调整的控制措施，设定流量阈值，明确如何运用告警系统，以及制定计划来确定在出现问题时的应对方法。

[查看这六个最佳做法。](#)

秘诀 10：查看行动手册

您的行动手册应当详细地阐述安全策略中所涉及的人员、流程及先决条件的所有相关信息。关于人员方面，需列出轮班时间表、知识库及存在的差距，以及必需的培训。关于流程方面，应当制定协议或绘制流程图，以确保在各种可能出现的情况下，每个人都能清楚地了解自己的职责所在以及应当联系谁。关于先决条件，说明安全事件上报时的从属关系和通信要求。行动手册还应列出尽可能保护源服务器的应急协议。

秘诀 11：做好应对 DDoS 攻击的准备

为了防范 DDoS 攻击，请确保您的平台配备了经过精心调整的速率控制措施。当检测到流量超过特定阈值时，应拒绝该流量，并发送正常的 HTML 反馈以迷惑爬虫程序流量。在对抗 DDoS 攻击时，缓存是一种有效的防御手段。因此，请尽可能充分地利用缓存来提高防御能力。开展桌面演练，以便发现事件响应流程中存在的盲点或低效之处。为了实现高度有效的防御控制措施，与您合作的供应商应具备务实态度，并了解您的环境以及您面向 Web 的应用程序的性质。

秘诀 12：时刻铭记客户

随着 [Web 数据窃取](#)、[供应链](#)和 [Magecart 攻击](#)的增加，您务必（而且需要使用 PCI DSS 4.0）管理和监控 Web 应用程序上的所有 JavaScript 执行行为，从而防范高峰活动期间以及[其他时间](#)发生的[客户端攻击](#)。假日季同样也是欺诈者挟持您品牌的黄金时段，他们会[创建假冒网站和社交媒体帐户](#)，意图窃取凭据和信用卡信息，或者出售假冒商品或进行虚假预订。在您的策略中，请确保切实部署监控工具，并制定在检测到虚假网站或滥用情况时的应对计划，以此维护客户忠诚度，巩固与客户的信赖关系。

见解：DDoS 攻击次数创下记录

[DDoS 攻击一直在大幅增长](#)，不论是规模还是复杂程度都是如此。实际上，在 Akamai 防范的最大规模的 10 次 DDoS 攻击中，有 8 次发生在 2022 年中期到 2023 年底之间。2023 年 2 月，Akamai 保护一家客户成功顶住一场大规模 DDoS 攻击，此次攻击的峰值速度为每秒 900.1 Gb (Gbps)，每秒数据包数达到了 1.582 亿 (Mpps)。



秘诀 13：了解您的 API 攻击面

对于任何企业，尤其是商业领域中的企业，API 蔓延都是一个挑战。因此，您需要建立针对 API 的清单发现流程，并进行严格的审核。应用程序团队会在平台上运行较新的 API，而安全团队可能对这些新 API 并不熟悉。因此，将这些新 API 注册到平台，并确保清单的准确无误，就显得尤为重要。如果安全团队不认识某个 API，他们可能会选择阻止该 API 的运行。然而，一旦该 API 完成了注册，安全团队就会对其提供保护。另一个最佳做法是确保 Web 应用程序防火墙保持更新并处于自动模式。

秘诀 14：调整告警以减少噪声

监控所有指标固然重要，但同时也存在造成过多噪声的风险。告警过多实际上就等于没有告警，因为团队可能无法从大量的告警中筛选出真正重要的信息。您需要调整告警设置以减少噪声，从而帮助您提升响应能力。这一步骤应在高峰活动之前完成，而非等到最后一刻才进行。另外，非常重要的一点是，要为告警制定路由计划，确保关键信息能够及时传递给相应的人员，以便他们能够做出响应。

秘诀 15：加强对恶意爬虫程序的防御

某些爬虫程序可能无关紧要，但另一些则可能被用于发起 DDoS 攻击、抓取网站内容或清单、开立虚假帐户、执行撞库攻击，甚至从事更为恶劣的活动。在关键的高峰活动期间，即便是良性的爬虫程序，也可能导致网站速度大幅变慢，达到无法接受的程度。您应制定积极的爬虫程序管理策略，因为您需要关闭恶意爬虫程序，并将重心放在应急协议上，明确可以采取的行动、如何完成任务，以及与谁协作，以消除这些恶意爬虫程序的影响。为此，您可以利用一些工具来分别跟踪这些爬虫程序，并准确地评估它们可能导致的帐户受损、服务中断甚至数据泄露等攻击的影响。

第 4 章： 总结经验教训

在准备和实施高峰活动的过程中，需要从技术和业务的角度出发提供许多信息，这使得总结经验教训以帮助团队进行改进显得至关重要。然而，抽出时间和精力来开展正式的评估可能会非常困难，特别是在年底假期之后。对于定期或经常遇到高峰活动的公司而言，在不同活动之间腾出时间进行评估确实非常困难。然而，我们认为有一个至关重要的最佳做法，那就是将活动后评估纳入日程安排，这样做能提高进行评估的可能性。

为了支持您开展此项工作，我们为您提供了一条特别秘诀。

特别秘诀 16：开展正式评估

在企业中的所有人对活动仍记忆犹新之时，及时开展活动后评估。当大家都能清晰地回忆起活动时，他们便能够总结出切实可行的见解，解读从活动中收集到的宝贵数据，并明确下一次活动的优先事项。



您是否衡量了合适的指标？



在您的指标或流程中，是否存在需要在下次活动之前弥补的不足之处？

提前为活动后的正式技术和业务绩效评估做好充分准备，这样您就能从所学到的经验教训和所收集的数据中获益良多。





彻底改变应对高峰活动的策略

如果任何一天都可能会出现高峰，那么您的目标应当是尽量让高峰活动不再是例外事件，而是将其转变为您已做好充分准备、能够从容应对的新常态。这正是我们能提供帮助的地方。借助 Akamai 专家团队的支持，您可以极大地简化整个应对流程。就像上文讲过，您可以将准备工作逐步融入到技术架构、流程以及企业文化之中，使其成为一种根深蒂固的技能。这样，无论哪一天成为节假日，您的团队都能够随时待命，应对自如。

您准备好提升企业在高峰活动时的表现了吗？

[详细了解](#) Akamai 面向零售、旅游和服务行业提供的见解和解决方案，或者[联系 Akamai 专家](#)。



扫码关注，获取最新 CDN 前沿资讯



无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 [akamai.com](#) 和 [akamai.com/blog](#)，或者扫描下方二维码，关注我们的微信公众号。