APPLICATION SLA: KNOWING IS HALF THE BATTLE TO CONTINUOUS APPLICATION DELIVERY

Applications have come to define the digital experience. They empower organizations to create new customer-friendly services, unlock data and content and deliver it to users at the time and device they desire, and provide a competitive differentiator over the competition.

Fueling these applications is the "digital core," a vast plumbing infrastructure that includes networks, data repositories, Internet of Things (IoT) devices and more. If applications are a cornerstone of the digital experience, then managing and optimizing the digital core is the key to delivering these apps to the digitized user. When applications aren't delivered efficiently, users can suffer from a degraded quality of experience (QoE), resulting in a tarnished brand, negatively affecting customer loyalty and lost revenue.

Application delivery controllers (ADCs) are ideally situated to ensure QoE, regardless of the operational scenario, by allowing IT to actively monitor and enforce application SLAs. The key is to understand the role ADCs play and the capabilities required to ensure the digital experience across various operational scenarios.

OPTIMIZE NORMAL OPERATIONS

Under normal operational conditions, ADCs optimize application performance, control and allocate resources to those applications and provide early warnings of potential issues.

For starters, any ADC should deliver web performance optimization (WPO) capabilities to turbocharge the performance of web-based applications. It transforms front-end optimization from a lengthy and complex process into an automated, streamlined function. Caching, compression, SSL offloading and TCP optimization are all key capabilities and will enable faster communication between the client and server while offloading CPU intensive tasks from the application server.

Along those same lines, an ADC can serve as a "bridge" between the web browsers that deliver web-based applications and the backend servers that host the applications. For example, HTTP/2 is the new standard in network protocols. ADCs can serve as a gateway between the web browsers that support HTTP/2 and backend servers that still don't, optimizing performance to meet application SLAs.

PREVENT OUTAGES

Outages are few and far between, but when they occur, maintaining business continuity is critical via server load balancing, leveraging cloud elasticity and disaster recovery. ADCs play a critical role across all three and execute and automate these processes during a time of crisis.

If an application server fails, server load balancing should automatically redirect the client to another server. Likewise, in the event that an edge router or network connection to the data center fails, an ADC should automatically redirect to another data center, ensuring the web client can always access the application server even when there is a point of failure in the network infrastructure.

MINIMIZE DEGRADATION

Application SLA issues are most often the result of network degradation. The ecommerce industry is a perfect example. A sudden increase in network traffic during the holiday season can result in SLA degradation.

Leveraging server load balancing, ADCs provide elasticity by provisioning resources on-demand. Additional servers are added to the network infrastructure to maintain QoE, and after the spike has passed, returned to an idle state for use elsewhere. In addition, virtualized ADCs provide an additional benefit, as they provide scalability and isolation between vADC instance at the fault, management and network levels.

Finally, cyber-attacks are the silent killers of application performance, as they typically create degradation. ADCs play an integrative role in protecting applications to maintain SLAs at all times. They can prevent attack traffic from entering a network's LAN and prevent volumetric attack traffic from saturating the Internet pipe.

The ADC should be equipped with security capabilities that allow it to be integrated into the security/DDoS mitigation framework. This includes the ability to inspect traffic and network health parameters so the ADC serves as an alarm system to signal attack information to a DDoS mitigation solution. Other interwoven safety features should include integration with web application firewalls (WAFs), ability to decrypt/encrypt SSL traffic and device/user fingerprinting.

REDUCE TCO; IMPROVE QoE

You can't manage what you don't measure. Once application SLAs are established, it's the role of the ADC to provide improved automation and monitoring capabilities. It makes perfect sense, as the ADC is the only device that interfaces with both the user devices on the frontend and application servers on the backend. It allows the ADC to easily monitor server delays and network issues negatively impacting QoE via in-depth reporting and root cause analysis.

Ultimately, finding the right ADC means discovering a vendor that addresses all these considerations and more, in addition to understanding how the market is evolving. By finding a solution that fully addresses those considerations, your organization can reduce TCO while improving QoE for customers.

LEARN MORE ABOUT RADWARE'S ALTEON APPLICATION DELIVERY CONTROLLER