CITRIX®

Get the Most Value Out of Your Microsoft Applications with Citrix NetScaler

Modern application delivery controllers provide improved reliability, security and performance for Exchange, SharePoint and Lync

Fast, responsive servers make employees happy and productive. In organizations that rely heavily upon Microsoft enterprise applications, like SharePoint, Exchange and Lync, well-functioning applications drive the business forward. The flip side, though, is that when something goes wrong, misbehaving or poorly optimized servers kill productivity, damage morale and drive up support costs.

Employees notice problems at the back end when they experience slow response times, dropped VoIP calls, repeated requests for user authentication, and browser timeouts. From the IT administrator's perspective, back-end problems appear as high CPU utilization on application servers, the inability to consistently apply security policies, and misbalanced workloads.

The bad news is that IT can't simply ignore these problems and hope they'll get better over time. The good news is that there's an easy solution: Install an application delivery controller (ADC) to front-end your critical enterprise servers.

An ADC, which includes load balancing among its many features, offers benefits to employees by boosting productivity and improving the user experience. From an IT perspective, the ADC distributes workloads between servers and also offloads many CPU-intensive workloads from each server, making each machine more efficient, scalable, secure, cost-effective and resilient.

TechTarget Custom Media
A TECHTARGET WHITE PAPER

Architecturally, the ADC sits between the network router and the servers. Here is a typical workflow:

First, user traffic originating from the corporate LAN or public Internet is directed by the network router to the ADC. A full-featured ADC examines incoming traffic, decrypts that traffic if encoded using Secure Sockets Layer (SSL) encryption, and, optionally, authenticates the traffic against Active Directory. The ADC can also prioritize certain traffic—voice phone calls from Lync or streaming video through a SharePoint portal, for example, would often be given a higher priority than Exchange email retrieval.

Once authenticated, the ADC determines if the user's request is for common information or objects that can be cached on the appliance. If this is the case, the ADC handles the request directly, without requiring an additional server transaction. If the request can't be satisfied by the cache, the ADC sends the traffic to the server that is best equipped to handle the transaction based on response time, user or the type of content being requested, such as video or multimedia.

After the server processes the request, the response is sent back to the ADC, which can choose to cache this content, encrypt it or compress it, depending on the nature of the traffic. The plain, encrypted and/or compressed response is then sent out to the user.

At all times, the ADC monitors the health and responsiveness of each server. If a server becomes slow or unavailable, the ADC stops sending traffic to it, and seamlessly redirects any current sessions and workloads to an available server. Once the faulty server recovers, the ADC resumes sending traffic to it for processing. These actions are logged, and administrators may be alerted according to IT policies.

This paper explores the benefits of an ADC in an environment that runs on Microsoft enterprise applications, and digs deeper into how an ADC provides benefits for these applications.

Introducing Application Delivery Controllers

Load balancers have been around for decades. Some of the earliest load balancers were used to distribute Web traffic across front-end HTTP servers and mid-tier application servers in order to improve scalability and reliability. Hardware-based load balancers distributed workloads evenly between multiple servers, often in a round-robin fashion, and would monitor the response time of each server. If a server failed or exhibited slower-than-usual response times, the load balancer would simply allocate its work to other servers, thereby preventing users from experiencing browser timeouts, dropped sessions or lost data.

ADCs, which serve as modern load balancers, can still distribute workloads between servers and monitor server availability and responsiveness. They offer additional benefits for critical server environments. ADCs actively improve the user experience by compressing and caching data; monitoring performance; offloading CPU-intensive tasks such as SSL encryption and decryption; establishing and managing virtual private networks (VPNs); acting as web application firewalls; authenticating users; and defending against distributed denial-of-service (DDoS) attacks.

An ADC eliminates common pain points experienced by end users—that is, employees and customers—while offering cost savings and other benefits for the IT department. Let's look at the ADC from both perspectives.

Improving User Experience

Latency—long delays between initiating a request and receiving the results—frustrates users. Seeing the spinning hourglass when retrieving emails via Exchange, searching a SharePoint site, downloading documents, listening to a voice call or navigating through other corporate resources not only lowers productivity, but can cause of a lack of confidence in the organization's IT infrastructure. In some cases, users might even lose data. If Google or Facebook can be lightning fast, why is the company's network so slow? Why are there delays when scrolling through a message list? Today's employees expect everything to just work, and have a low tolerance for delays.

Although users may not know the word for it, they are also frustrated by jitter—that is, when latency varies from moment to moment. Jitter delays can ruin the usability of voice communications. It's hard to read documents when scrolling speeds up and slows down, or the cursor and characters being typed in an email message are out-of-sync with what's being typed on the keyboard.

Employees and other end users expect—no, demand—fast application performance with minimal latency and jitter, as well as seamless, invisible failovers when problems occur.

An ADC addresses these and other user experience issues by distributing workloads across multiple servers and by monitoring the latency and jitter of each session. Underutilized servers get their share of user traffic, while overloaded servers are freed up. As mentioned earlier, the ADC caches frequently requested information and compresses data that is sent to end users, meaning that fewer, smaller packets are transmitted over the network, resulting in faster response times.

Another area where an ADC helps is by offloading processor-intensive tasks that can bog down application servers, such as processing encryption and decryption of SSL-encoded messages. This frees up the server's resources to focus on running the application more efficiently.

Systems failures also affect the user experience. Servers can go down at any time, although in most cases this is rare in today's enterprise networks. The ADC keeps track of each server's work in progress. If a server fails or becomes non-responsive, the ADC can redirect its work sessions to another server with minimal delay. Because the ADC shares each redirected transaction's state with the new server, in many cases the end user is unaware that a different server is handling their request.

Finally, depending on the environment, an ADC can provide authentication for Windows users via Active Directory. Not only does this reduce the workload on servers, but user authentication can be shared across distributed servers and applications, reducing the number of times that the user needs to log in—and thereby improving productivity and satisfaction.

Optimizing Back-End IT Infrastructure

What's good for the end user is good for the IT department—happy employees with better user experiences mean fewer support calls. However, that's only a small portion of the benefit that ADCs offer server administrators and network support teams.

ADCs provide additional security for Microsoft enterprise servers. Because traffic and workloads are filtered through the ADC, it acts as a reverse proxy for these servers and applies consistent security and Active Directory control policies. The ADC can integrate with firewalls and intrusion detection/prevention systems (IDPS) to perform deep packet inspections as soon as SSL-encrypted packets are decrypted. Some full-featured ADCs can even perform this security scanning as part of their functionality.

An ADC provides system administrators with additional visibility into server workloads, user requests, sessions and application utilization through a single control point. In a farm with several servers, the front-end ADCs become the management interface for logging, management consoles, security incident response systems and administrative dashboards.

There are cost savings as well, both now and in the future. Many, if not most, ADCs have the ability to offload processor-intensive tasks, such as SSL encryption/decryption, from the application servers. This, in turn, reduces the processor load on each server, which means that it can scale to handle a great workload, such as voice calls over Lync, document management and messaging using SharePoint, and email processing and filtering over Exchange. This will allow existing hardware to handle more users, more loads and more data and to scale more efficiently, leading to savings on hardware, software licensing, racking, cabling, power, cooling and more. An ADC provides an efficient means of future-proofing your back-end infrastructure.

Front-Ending Microsoft SharePoint, Exchange and Lync

When load balancers first appeared on the scene, they were used primarily to distribute traffic across multiple web-hosting servers. While many load balancers and ADCs are still used to distribute web traffic across multiple servers, increasingly they

are used to front-end enterprise and cloud-based applications, such as those offered by Microsoft.

Consider a Microsoft Exchange environment where digital certificates are employed to validate users' identities when accessing the system through an Outlook client on a laptop, mobile device or via a web browser using Outlook Web Access.

Regardless of which client is used, the inbound request is sent to the ADC, which performs the appropriate Active Directory authentication and forwards the message to the Exchange server. The Exchange server would return the required information (such as an email repository search) to the ADC, which would secure the results with SSL and send to the user.

What's good for the end user is good for the IT department—happy employees with better user experiences mean fewer support calls.

In the case of Lync, Microsoft's unified communications server, an ADC could be deployed to serve multiple roles within the solution's architecture. The ADC could be leveraged to create a pool for managing communications endpoints, such as mobile phones, desk phones, Live Meeting videoconferencing systems, and even attendant consoles at a receptionist station. An ADC can be used to front-end multiple Edge Servers, which connect the Lync communications system to the public Internet, federated enterprise networks and the public switched telephone network (PSTN). The ADC augments and scales Lync to provide robust failover, load balancing and data compression as needed.

Microsoft SharePoint is another enterprise platform that benefits from using an ADC. Here, the ADC can perform content switching, which allows the appliance to inspect specific characteristics of the inbound traffic and direct the user to a specific SharePoint server based on the rules or policies created for different types of requests. The ADC can be configured with specific policies for optimizing traffic, such as having different compression rates for video and text documents, as well as setting up caching for frequently used objects, such as graphics files.

The ADC can rewrite packet headers and adjust security, for example, seamlessly switching plain-text HTTP to secure HTTPS while offloading SSL from the SharePoint servers. An ADC can handle Active Directory authentication, in addition to providing Layer 7 protection to protect against threats to SharePoint servers.

Citrix NetScaler Is the Best ADC for Microsoft

Citrix has been in the application delivery business since 1989, and through its popular desktop and server virtualization products, it has developed a deep understanding of how popular enterprise applications are consumed in the enterprise. Since the acquisition of NetScaler in 2005, Citrix engineers have worked extensively to build a more intelligent delivery controller that provides unmatched levels of performance, scalability and reliability for modern application environments. The effort has paid off, as NetScaler has consistently been rated as a leader in delivery controllers by several independent analyst firms.

Citrix NetScaler monitors, compresses, caches and optimizes Microsoft applications to meet or exceed end-user and IT requirements. NetScaler is certified to work with Microsoft, and several deployment guides are made available to assist administrators with configuring the appliance to support these applications.

Citrix offers a wide range of ADCs for all customer requirements—whether the customer is a large global enterprise organization, small business or branch office. NetScaler MPX is a hardware-based solution that can support throughput performance from 500 Mbps up to 160 Gbps. Smaller organizations should consider NetScaler VPX, a software-based virtual appliance that supports throughput from 10 Mbps to 3 Gbps. For organizations that require the versatility of a virtual appliance but need the on-board resources of dedicated hardware, NetScaler SDX is the best option, with

advanced virtualization that can consolidate as many as 80 independently managed NetScaler instances with up to 150 Gbps overall performance.

Tremendous Resources in Citrix Deployment Guides

To assist administrators with the installation and configuration of NetScaler, Citrix offers specialized deployment guides written specifically for Microsoft enterprise applications.

For example, the *Microsoft SharePoint 2013 with Citrix NetScaler Deployment Guide* explores the three modes for deploying SharePoint 2013: with the application server and database server on a single device; on a two-tiered architecture with separate application and database servers; or in a three-tier architecture that includes a web front end. The guide walks the administrator through Citrix's *NetScaler AppExpert Templates* and how to configure NetScaler to provide SharePoint-specific content switching, caching, compression, load balancing, authentication, SSL offload and application firewall functionality.

Citrix offers a number of other detailed deployment guides for Microsoft, including the *Guide to Deploying Microsoft Exchange 2013 with Citrix NetScaler, Citrix NetScaler and Microsoft SharePoint 2013 Hybrid Deployment Guide* and *Microsoft Lync 2013 and Citrix NetScaler Deployment Guide.*

Get the Most Value From Microsoft Applications With an ADC

Employees and other end users expect—no, demand—fast application performance with minimal latency and jitter, as well as always-on access, even when problems occur. The best way to meet those expectations is to front-end enterprise application servers with Citrix NetScaler. Not only will the user experience improve, but IT will benefit from better security, centralized authentication and security policy enforcement, and more scalable server performance.

If your organization already uses NetScaler to provide remote access to your XenApp or XenDesktop farm, consider extending the use of NetScaler to support your Microsoft enterprise environment.

If you are not already using the NetScaler ADC, learn more at citrix.com/netscaler or try it free for 90 days at citrix.com/trynetscaler.

At all times, the ADC constantly monitors the health and responsiveness of the app servers. If an app server becomes slow or unavailable, the ADC instantly stops sending traffic to it, and seamlessly fails its current work and sessions over to other app servers.