White Paper

Enhancing VMware Horizon View with F5 Solutions

VMware Horizon View is the leading virtualization solution for delivering desktops as a managed service to a wide range of devices. F5 BIG-IP devices optimize the user experience and help ensure maximum performance, availability, scalability, and security for View implementations.

by Simon Hamilton-Wilkes
Principal Solution Engineer - VMware Alliance

Contents

Introduction **3**

VMware End User Computing 3

Performance, Scalability, and Security **4**

Enhancing Security and Access Control 4

Simplified Authentication for Users 6

Local and Global Access Management **7**

Persistent and Non-Persistent Desktops 7

Username Persistence 7

Single Namespace 7

Conclusion **9**

Introduction

Desktop and endpoint device management has long been a challenge for IT organizations. End users demand flexibility, multiple access options, and desktop customization, while business units often require multiple desktop types based on their business and technical requirements: Windows 7 for sales and staff in the field, Windows XP for accounting, Mac for creative design, and Linux for technical staff. This kind of multi-level matrix can be a major management headache on its own. But add in support for all the different desktop needs, plus remote support for those on laptops, and desktop management can all but consume an IT organization's budget and time.

VMware End User Computing

VMware Horizon View—part of VMware's Horizon Suite of products—alleviates two significant management headaches: location and standardization. To solve the location problem, virtual desktop infrastructure (VDI) deployments virtualize user desktops by delivering them to individual clients over the network from a central location. Those desktops are stored and run in the data center, rather than having individual desktop and laptop machines in the field running localized operating systems. This seamless virtualization goes undetected by users.

To solve the standardization problem, VMware enables business groups that have specific desktop needs to be clustered together in the data center and managed as a unit. For example, when all the Windows machines need a new service pack, it can be installed to the master image in the data center and then delivered to users the next morning when they log in to their virtual desktops. Administrators can package applications with VMware ThinApp and manage access though Active Directory permissions rather than installing them on individual images. Because IT staff no longer have to visit each local system or push software installs down through remote tools, users aren't forced to reboot during the business day.

Virtual platform providers host VDI solutions, such as View, as part of their hypervisor platforms in the data center. This enables companies to deploy and manage virtual servers and virtual desktops at the same time and in the same place, which cuts down on management time and costs because IT can manage these two virtual technologies as a single solution.

Organizations consistently cite user experience as critical to the success of their virtual desktop deployments: performance has to compare favorably to a conventional desktop, while availability and security must be even greater.

F5 offers a variety of solutions to help organizations maximize the success of these critical elements in their View desktop deployments. As a VMware partner, F5 has thoroughly tested and documented the benefits of using its Application Delivery Networking solutions with View to address secure access, username persistence, load balancing, server health monitoring, and more.

Performance, Scalability, and Security

The larger the VMware Horizon View deployment, the more View Connection Servers are needed to handle the concurrent desktop connections. F5® BIG-IP® Local Traffic Manager™ (LTM) provides valuable load balancing and health monitoring, resulting in higher system availability and greater scalability—and ultimately, a better user experience. Additionally, an F5 iApps™ Template makes configuration straightforward by simplifying setup and preventing human error. View client connectivity utilizes multiple ports and protocols that must be directed at the same View Connection Server for a successful session, and while PC-over-IP (PCoIP), the View desktop streaming protocol, is UDP-based, SSL-wrapped TCP connections are utilized for authentication and USB. Administrators can save capacity on the View Connection Servers by offloading encryption to the BIG-IP devices.

Enhancing Security and Access Control

Ensuring secure remote access is critical to protecting corporate information. VMware satisfies this with its Security Gateway, a PCoIP proxy that is installed on multiple Windows Server 2008 R2 machines. To route incoming connections to the internal network, these need to be installed in an organization's DMZ. While this is very effective for zero clients (appliances that do not run a traditional operating system), organizations may prefer a more robust solution for thin clients based on Windows, OS X, Linux, Android, and iOS.

F5 addresses this with BIG-IP® Access Policy Manager® (APM), which performs pre-login checks to the endpoint device prior to allowing the login sequence to

begin. BIG-IP APM can determine if antivirus software or a personal firewall is running on the endpoint and whether it is up to date, and it can enforce a specific operating system patch level, View client installation version, and a host of other pre-login checks. BIG-IP APM can direct the user to a remediation page for further instructions or even turn on antivirus software or firewalls for the user. It can also enforce Active Directory group policies on corporate-owned and non-corporate-owned assets for the duration of the connection.

BIG-IP APM supports a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. Once authenticated, high-performance View PCoIP can be transported within the DTLS (Datagram Transport Layer Security) protocol. This provides the security organizations need to transport View communications without the performance degradation that a common SSL VPN solution suffers. There can be an automatic fallback to TCP SSL VPN if a high-performance UDP tunnel cannot be established. The BIG-IP® Edge Client® can also apply rate-shaping functions so PCoIP traffic receives priority over other UDP network traffic from the client. This ensures that even if the user is running other programs, the virtual desktop user experience remains a positive one.

For zero clients or where endpoint inspection is not desired, the PCoIP proxy functionality in BIG-IP APM can be used. This removes the requirement for VMware Security Gateways in the DMZ along with their 1:1 mapping to View Connection Servers. The BIG-IP APM appliance proxies the PCoIP connection, passing it internally to any available Connection Server within the View pod, which interprets the connection as a normal internal PCoIP session. This provides the scalability benefits of a BIG-IP appliance and gives BIG-IP APM and BIG-IP LTM appliances visibility of the PCoIP traffic so that more advanced access management solutions can be used.

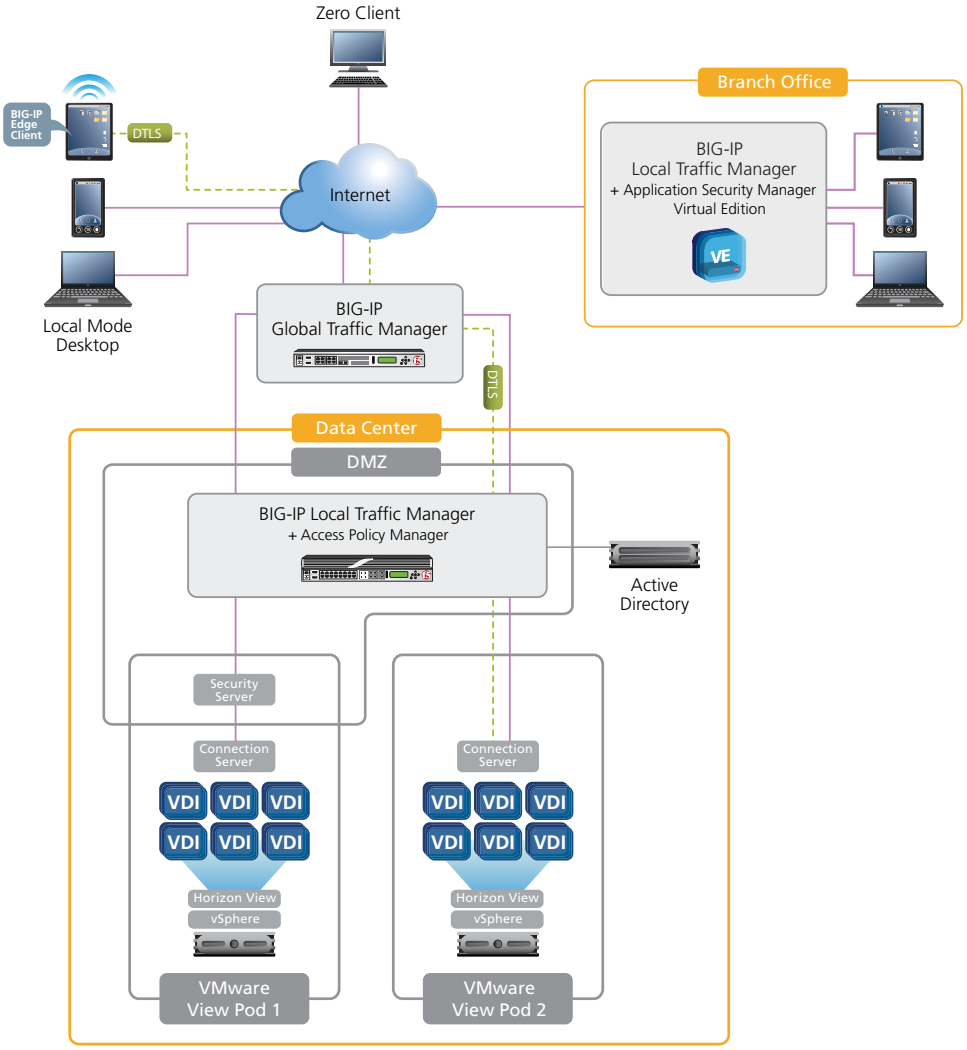

Figure 1: The F5 BIG-IP system and VMware Horizon View topology.

Simplified Authentication for Users

Streamlining the authentication process for remote workers is important to a good user experience. BIG-IP APM securely caches login credentials and enables authentication pass-through during the login process, so users can log in once, access their desktops immediately, and stay logged in as long as they are using the system. This single sign-on provides a seamless user experience, minimizes the security risk, and reduces password lockout calls to the help desk.

VMware Horizon View now supports multi-factor authentication with RADIUS, though without fallback to redundant authentication servers. BIG-IP LTM fills this void by load balancing and performing health checks on the RADIUS servers to ensure availability.

Local and Global Access Management

Persistent and Non-Persistent Desktops

VMware Horizon View has two types of desktops: non-persistent, in which a generic desktop image is given to users and upon logout returns to its initial state, and persistent, in which all user changes persist, just as they would on a physical PC. This is an important distinction when supporting mobile users, as those with persistent desktops will expect to be connected to their unique image wherever they may be, whereas non-persistent users can be directed to the nearest available source.

Username Persistence

VMware Horizon View scale-out is based on infrastructure "pods," each of which can host up to 10,000 source desktops. If administrators want to serve more users with multiple pods, or divide the infrastructure for management reasons, they must connect users to the correct pod. View's built-in persistence mechanism uses a J-session ID, which is baked into the client access device or client software, that could give the jarring experience of receiving a fresh desktop after a short move from one client device to another.

The F5 solution reconnects users to their existing sessions transparently. This persistence based on username is very powerful when users are moving between multiple devices and locations (such as medical staff in a hospital), but they want to retain access to a non-persistent desktop for a period of time.

Single Namespace

When many sites are possible desktop location sources, (and those sites are potentially in different geographies), using BIG-IP LTM in conjunction with

BIG-IP APM and BIG-IP® Global Traffic Manager™ (GTM) is ideal. Clients can be initially directed by BIG-IP GTM to their nearest site. If, post authentication, the BIG-IP system determines their desktop resides elsewhere, BIG-IP GTM can transparently redirect them. This permits active/active multi-site View deployments with an infrastructure that can dynamically direct connections to provide high availability and a seamless user experience.

The connection flow starts when a user launches the View client and it performs a DNS lookup; BIG-IP GTM receives this request and makes an initial decision on the correct destination for the session, based, for example, on the geographic IP lookup of the client's DNS server. The View client connects and authenticates with the View Connection Server IP address BIG-IP GTM has provided. BIG-IP APM monitors the Microsoft Active Directory (AD) authentication process by querying AD itself to look for a custom parameter that specifies the user's desktop location. If the initial connection is not to the correct site or pod, BIG-IP APM replays the authentication transaction to the correct location and establishes a PCoIP View session. The entire dynamic decision and redirection process is invisible to the user. This solution has the advantage of AD being a distributed replicated database, so the user's desktop location can be determined with a single lookup.

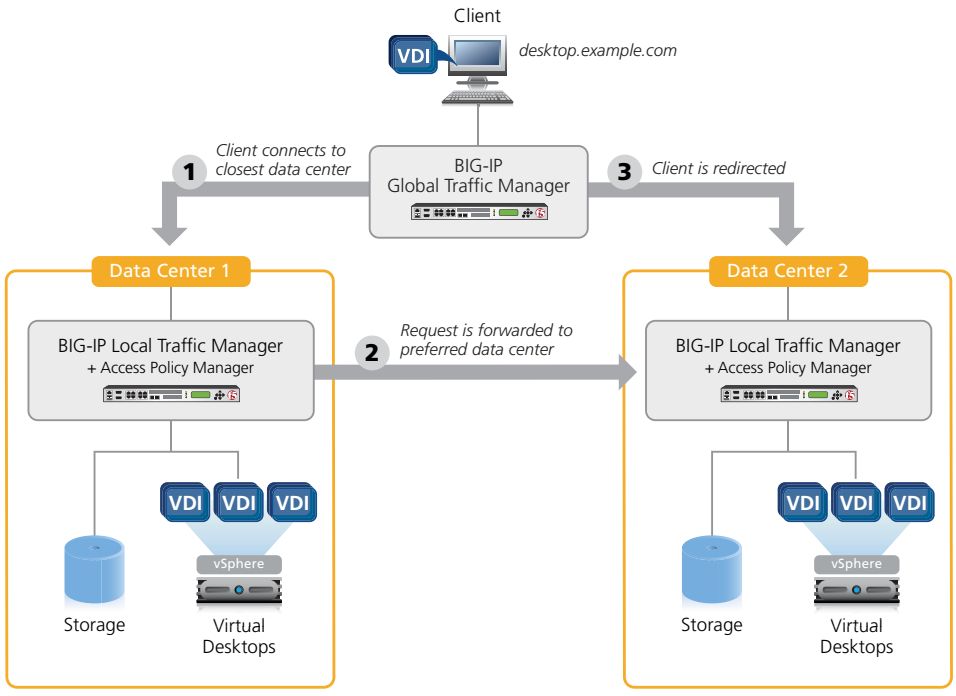

Figure 2: Single namespace logical connection flow.

Conclusion

The BIG-IP system provides secure remote access from a full selection of client devices, with endpoint inspection where appropriate and a full range of authentication options. BIG-IP LTM and BIG-IP APM improve the user experience by providing single sign-on and enhancing the reliability and performance of RADIUS or Active Directory. With the iApps Template for VMware Horizon View, administrators can configure these features accurately with minimum effort.

There's no doubting the advantages of deploying a virtualized desktop solution like View throughout the enterprise. By deploying the F5 BIG-IP system alongside it, organizations can achieve even higher availability and scalability. Leveraging BIG-IP LTM, BIG-IP APM, and BIG-IP GTM allows IT staff to integrate multiple View pods or physical sites for source desktops—all without disrupting the user. In enabling users to reconnect to their existing persistent desktop source when required, and providing a dynamic and agile infrastructure that can adapt to planned and unplanned events, the BIG-IP system is key to successful VMware Horizon View deployments.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com