Deploying F5 Application Ready Solutions with VMware View 4.5

VMware View is the leading desktop virtualization solution built for delivering desktops as a managed service. F5 BIG-IP® devices optimize the user experience and help ensure maximum performance, availability, and security for VMware View implementations.

by Joe Malek
Product Management Engineer

and Alan Murphy
Technical Marketing Manager

Contents

Introduction

Corporate desktop management has long been a necessary evil for IT groups. Most employees need full desktops, and different business units usually require multiple types of desktops: Windows XP for accounting, Mac for creative design, Windows 7 for sales and people in the field, Linux for technical staff, and so on. This multi-level matrix can be a major management headache on its own. But when you add in supporting all the different desktop needs, and that you'll need to support some of those desktops remotely on laptops, desktop management can consume most of your IT management budget and time.

VMware View 4.5—part of VMware's complete Virtual Desktop Infrastructure (VDI) solution—alleviates two major management headaches: location and standardization. To solve the location problem, VDI deployments virtualize user desktops by delivering them to individual machines 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 that run localized operating systems. The end result is a better user experience and users don't notice that their desktops are now virtualized.

VMware View also helps solve the standardization problem: business groups that have specific desktop needs can be clustered together in the data center and managed as a unit. For example, when all the Windows XP machines for accounting need a new piece of software, it can be batch-installed to each desktop in the data center overnight and then delivered to users the next morning when they log in to their virtual desktops. IT staff no longer have to visit each local system or push software installs down through remote tools, which would force the user to reboot during the business day.

Most virtual platform providers bundle VDI solutions as part of their virtual server platforms in the data center, such as VMware with VMware View 4.5. Companies can now deploy and manage virtual servers and virtual desktops at the same time and in the same place. Integrating virtual servers and virtual desktops cuts down on management time and costs because IT can manage these two virtual technologies as a single solution.

One area where virtual servers and virtual desktops differ, however, is how they rely on the Application Delivery Network (ADN), both in usage and complexity. Virtual servers are typically focused on pushing small bits of data over the network: web pages, application data, and connection data. Virtual desktops, however, send much more GUI-based application data across the network.

VDI can strain network resources from the first deployment, and this strain is exacerbated in large-scale and remote-deployment architectures. Due to the unique placement of VDI—as users' primary daily work tool—users immediately see VDI performance issues. When a user's desktop moves from a physical machine to the data center, the user experience becomes paramount; a poor VDI deployment will result in IT being flooded with "My desktop is too slow" calls. Before VDI, those calls were typically prompted by old or sluggish hardware on the desktop. VDI moves the cause of the sluggishness to the network, placing the responsibility for a good user experience on the infrastructure rather than individual hardware.

Organizations consistently cite the following criteria as critical for measuring the success of their virtual desktop deployments:

• User experience

• Performance and availability of desktops

• Security of the end-to-end system

• Reduced desktop operating costs

F5 offers a variety of Application Ready Solutions to help organizations maximize the success of VMware View desktop projects. As a VMware partner, F5 has thoroughly tested and documented the benefits of using our Application Delivery Networks with VMware View 4.5. F5 solutions include secure access, single- sign-on, load balancing, and server health monitoring.

Deployment Benefits

F5 Value for Users

The F5 Application Ready Solution for VMware View ensures a secure, fast, and available deployment, which provides the following benefits to organizations.

Optimizing the Network

Ensuring a good user experience often means over-provisioning bandwidth to account for peaks in network traffic. F5's Application Ready Solution for VMware View uses advanced compression, deduplication, and TCP optimization to help reduce these bandwidth requirements while maintaining and even improving the user experience. Additionally, session persistence maintains stateful desktop

information between connections which can help users reconnect to their existing desktop for fast re-access, with no need for re-authentication.

One of the biggest challenges IT departments around the world face is network latency across the WAN. When deploying VMware View, this can be a major concern for organizations that have users who access desktops and applications from anywhere. Simply increasing bandwidth does not solve the problem.

F5 helps drastically reduce the impact of latency by optimizing application protocols, prioritizing traffic, optimizing TCP from clients to servers, and reducing the amount of data sent over the WAN, which helps prevent costly bandwidth upgrades. These measures ensure that critical or time-sensitive applications receive priority over others to maximize performance over the WAN. F5 provides granular control of traffic based on enterprise needs, enabling you to manage and prioritize bandwidth per application and improve quality of service for users over the WAN.

Application Performance and Availability

The larger the VMware View deployment, the more View Manager Connection Broker servers will be needed to handle the concurrent desktop connections. F5 devices provide valuable load balancing, health monitoring, and server resource offload functions (such as SSL processing) for the VMware Connection Brokers, resulting in higher system availability and greater scalability of the existing server infrastructure. This translates to a better user experience, lower server costs, and reduced monthly operating expenses (such as power and space).

One of the unique features of the F5 Application Ready Solution for VMware View is the ability to persist client-to-broker connections on a session-by-session basis. Other implementations commonly use simple/source address persistence, where all the connections from a single IP address are sent to one server. F5 can direct traffic with greater precision, resulting in a more uniform load distribution on the connection servers.

Enhancing Security and Access Control

Ensuring secure access is a critical component of protecting corporate information. F5 addresses this need with pre-login checks to the endpoint device prior to allowing the login sequence to begin. F5 can determine if an antivirus or personal firewall is running on the PC and whether it is up to date, or it can enforce a specific

operating system patch level, among a host of other pre-login checks. F5 can direct the user to a remediation page for further instructions or even turn on antivirus or firewalls for the user.

F5 also supports a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. F5 devices enforce Active Directory group policies on corporate-owned and non-corporate-owned assets for the duration of the connection. Finally, once authenticated, F5 guarantees the encryption of all VMware View transport protocols, whether natively encrypted or not, without compromising performance.

Starting with VMware View 4.5, VMware introduced the high-performance PCoIP (PC over IP) communications protocol. Unfortunately, most traditional SSL VPN devices are unable to properly handle this unique protocol and therefore run slow, which degrades the user experience.

F5 overcomes this issue with its Datagram Transport Layer Security (DTLS) feature. This transport protocol is uniquely capable of providing all the desired security for transporting PCoIP communications, but without the degradation in performance. In addition, F5 supports automatic fallback to TCP if a high-performance UDP tunnel cannot be established.

F5 devices can also apply quality-of-service functions so PCoIP traffic receives priority over other network traffic. This ensures that no matter how busy the network may be, the virtual desktop user experience remains a positive one.

Simplified Authentication for Users

Streamlining the authentication process for remote workers is important to the user experience. Users should be able to log in once and access their desktops immediately. Further, users should not have to manually re–log in every time their network connection gets temporarily interrupted. F5 securely caches login credentials and enables authentication pass-through during the login process. Log in once, and stay logged in as long as you are using the system. If your connection drops, it re-authenticates you automatically. This not only makes for a seamless user experience, but it minimizes the security risk and reduces password lockout calls to the help desk.

Attacks do not always come from outside of the network; internal users can gain sensitive information or sabotage applications with greater ease than external users. Because F5 devices can offload SSL encryption duties, organizations can encrypt traffic for entire transactions, without affecting performance for the end user. This allows

organizations to use SSL everywhere and prevents information from being sent in clear text over the internal network, so you can mitigate risks associated with internal users as well as comply with state and federal privacy regulations. This also simplifies administration by providing organizations a single location for certificate management.

Conclusion

There's no doubting the advantages and impact of deploying virtualized desktop solution like VMware View 4.5 throughout the enterprise. When deployed alongside F5's suite of BIG-IP Application Delivery Networking products, IT can enjoy the following benefits of VMware View 4.5 deployments as part of their complete ADN:

High Availability and Scalability

F5 provides valuable load balancing, health monitoring, and SSL offload for VMware Connection Brokers, resulting in higher system availability and greater scalability of the existing server infrastructure.

Reduced Bandwidth Usage

F5 enables organizations to reduce bandwidth requirements while maintaining, and even improving the user experience.

Secure Access

F5 provides a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services, as well as comprehensive pre-logon checks.

Convenient Single Sign On

F5 enables authentication pass-through during the logon process. Log in once, and stay logged in as long as you are using the system.

High Performance of PCoIP

F5 devices enable all the security for transporting PCoIP communications, but without the degradation in performance associated with many SSL VPN solutions.

Whether F5 BIG-IP devices are deployed in front of a small VMware View desktop environment—such as for use in a lab or kiosk environment—or if they manage an entire enterprise desktop deployment, offloading VMware View resources to BIG-IP devices can not only improve performance but also secure VMware View 4.5 desktop traffic and enable it to scale.