White Paper

Adaptable and Resilient VDI Deployments

As the impetus to begin a virtual desktop infrastructure (VDI) deployment has grown in recent years, VDI solutions have begun to proliferate in the market. These solutions range from new features and functionality offered by market leaders to point products from smaller players that cater to enterprises' VDI needs. A complete VDI solution should deliver a reliable, high-performing desktop user experience while taming complexity and supporting scalability within a secure, stable framework.

by Don MacVittie
Technical Marketing Manager

Contents

Introduction

Virtual desktop infrastructure (VDI) offers corporate IT a wealth of benefits, ranging from easier software license administration to simplified desktop rollout. For smaller organizations, VDI is just the tool they need to mobilize the entire company in one project; and for larger organizations, it offers mobility for the most demanding group of users while a larger rollout is planned. VDI enables enterprises to minimize the hours spent servicing machines, and to maximize cost savings by buying lower-end client machines. Offering clients to users outside the firewall is a good way to keep data internal while allowing people to work externally—if those connections can be adequately secured that is. Software license management—because with VDI, who is running what can be centrally administered and tracked—is a huge bonus in the event of an audit.

While VDI is still growing, IT organizations must consider many factors when constructing the architecture within which VDI deployments must reside. Not only is VDI going through its own growing pains but, in parallel, the target devices that host VDI clients are themselves changing at a rapid pace.

The pace of VDI adoption is closely tied to IT’s confidence in the level of performance, availability, and security that is ultimately delivered to users. Given this, it’s critical that IT approach VDI implementations strategically with these three traits at top of mind. With the right tools, IT organizations can develop a virtual desktop infrastructure that will adapt to changing enterprise needs.

Advantages and Disadvantages of VDI

There are many advantages to deploying a VDI. Centralized management; remote desktop management and fixes without labor-intensive processes; reduced restore time in the event of a desktop machine failure; streamlined software upgrades and license management; and provisioning machines to new and existing employees are all attractive business benefits.

However VDI deployments also come with problems. The burden on the corporate network is much greater than with fat-client solutions, simply because everything on the screen and each keystroke or mouse click must be transmitted to the remote server hosting the virtual desktop image. Managing network resources, optimizing communications, and increasing servers in the data center to host VDI instances means that much of the desktop management burden shifts from technical support to network and server teams. This burden is not insignificant.

Vendor lock-in is also a problem. VDI is a growing technology, and any interoperability among top-tier virtualization vendors to date is, at best, in its infancy. When organizations purchase infrastructure from a particular VDI vendor, the level of lock-in increases simply because that infrastructure is fine-tuned to work only with that vendor's products.

And yet, the appeal of supporting many devices from a single image is alluring. The ability to meet customer needs whether they prefer tablets, laptops, or desktops, without concern for which applications run where or how to get a new application deployed to all of the above, makes VDI a very attractive option for IT organizations.

Another attractive benefit is how easy it is to set up a new employee with a company-issued, IT policy–abiding personalized "machine" by creating a new virtual desktop instance and setting a user name and password. While the employee will still need hardware, that hardware doesn't have to be specially configured, since the software that makes up a unique user will be deployed in the server room, not on user or client-side equipment.

But from a network perspective, VDI is not terribly new. Rather than treating VDI as yet another application that needs to be accommodated by a set of special-purpose network devices, companies should turn to a tried and true infrastructure solution or platform that can support any application at any location at any time. F5® Application Delivery Controllers (ADCs) improve both the performance and the availability of apps that are centrally housed but delivered in a highly distributed environment. ADCs can play an ongoing, strategic role in accelerating the widespread deployment of VDI.

When they interact with enterprise applications, users generally expect the best-case scenario—that the VDI will run silently and invisibly in the background as hosted applications are delivered to any size endpoint device, serving up a seamless user experience. To preserve that experience, today's VDI solutions can apply the same technologies that improved the performance of application delivery to the physical desktop.

The same best-of-breed ADCs that provide security, high availability, and optimized network performance to VDI can be applied to networked applications, from databases to Exchange Server to server virtualization and beyond.

Desktop Virtualization Is About Servers and Network

All of the potential strengths offered by desktop virtualization can be watered down by adverse effects on servers and network utilization. When virtualizing a large number of desktops, the corporate network will see a significant increase in traffic due to the transfer of data between the client and the virtualized desktop in the data center. If clients must sometimes go over a WAN or log in from the road, this problem quickly becomes more acute, as the performance characteristics of WAN and Internet connections are definitely less appealing than those of the LAN.

The number of servers required to virtualize a significant number of desktops is also a critical factor, because increased server density results in increased man-hours for server and network administrators.

Finally, portability is a factor because it is a rare IT shop that uses one and only one virtualization product. For example, most use VMware for server virtualization and another product for desktop virtualization. Even if a shop uses a single vendor for all virtualization projects today, it may be only an acquisition away from being heterogeneous and needing an acceleration and security solution that is also heterogeneous.

Together, these three factors—the amount of traffic, the number of servers, and the level of portability—generate a list of issues that must be resolved when considering a partial or full move over to VDI. Can the infrastructure reliably support multiple virtualization toolsets? Is competition for virtualization something to keep on the table when negotiating with a VDI provider? And should the need arise, can the VDI be moved from one vendor to another?

In an attempt to relieve some of the most pressing issues surrounding VDI deployment, vendors have built partial solutions and toolsets into their products. For example:

- VDI vendors have tools to help determine how much bandwidth a given implementation will need.
- VDI vendors offer application delivery tools to optimize network traffic for an installation.
- VDI vendors offer compression capabilities to their customers—in the form of either software or hardware—to help with performance issues.

However, vendor application delivery and compression tools are a massive set of lock-in devices, trapping the enterprise in a given VDI implementation. While moving VDI vendors is never an easy task, moving VDI vendors while having to replace key parts of the infrastructure is even harder. So hard, in fact, that it may keep an organization from doing what's best in the long run. Additionally, VDI vendors are more focused on delivering the application than on making the network perform. In most cases, the net result is that more features are added to the VDI system without commensurate optimizations to maintain high performance.

Get More with Less

F5 ADCs—specifically, the BIG-IP® system—specialize in the performance of applications over a network. Running on F5's TMOS® operating system, BIG-IP® Local Traffic Manager™ (LTM) improves the performance of all networked applications. VDI installations use more network communications than most networked applications, so BIG-IP LTM does more to improve their performance. BIG-IP LTM also offloads encryption from VDI servers, lightening the workload and thereby increasing the processing power available to host virtual desktops on a given server. Adding in the advanced capabilities of BIG-IP add-on modules for security, WAN optimization, and web acceleration can significantly reduce the need for additional infrastructure. In some cases F5 products have reduced the need for more than 100 additional infrastructure elements—in this case servers for VDI supporting applications.

One key differentiator of the BIG-IP system is that it reduces the number or servers organizations need to support VDI applications. Infrastructure doesn't have to change, because the BIG-IP system includes customized settings to optimize each of the major VDI vendors' remote desktop protocols. This means that the vendor an organization chooses for server virtualization can be completely different from its desktop virtualization vendor—and yet both server and desktop virtualization will gain the benefits of a highly optimized infrastructure.

Naturally, the VDI market will change as it matures: new vendors will enter, old vendors will evolve, and new operating systems may even fold in (at the OS level) some functionality that is currently offered only by VDI vendors. F5 ADCs are vendor-agnostic, and will continue to support top-tier VDI vendors such as Microsoft, VMware, and Citrix with devices that are knowledgeable in the overall network and application ecosystem. And even as the market changes and grows, F5 will continue to support the features and functionality most needed to optimize content delivery for major VDI vendors.

Once F5 ADCs are in place in a VDI deployment, they can bring many additional benefits to the IT organization, including scalability, security, and availability.

Scalability

Just as server virtualization led inevitably to virtualization sprawl, so too can desktop virtualization. When an employee leaves the organization, there is no longer a supposition that their computer needs to be wiped. The virtual desktop can be saved indefinitely, and it generally will be unless there is a driving reason to delete it. Some employees will need multiple virtual desktops, and since this incurs no hardware expense, there will be great pressure on IT to provide them. Finally, mergers and acquisitions are commonplace in the modern business environment; IT organizations that can create plenty of room to scale out and absorb acquisitions give their companies an advantage.

VDI is scalable, but there are serious issues that must be overcome to scale successfully, from network saturation to systems management, and ROI must be examined. When scaling, do prices go down, or is cost constant across the project lifecycle? And is the cost low enough?

The overall architecture required for a VDI deployment is complex, but F5 ADCs simplify it by significantly reducing the number of servers required for some vendors. This reduction results in CapEx savings, while network optimizations that reduce the number of man hours required to operate the network provide OpEx savings.

With an F5 ADC, VM density per server increases, and network communications are optimized. Scaling becomes much less of an obstacle, and when new servers or clusters are required, the BIG-IP system gives IT the power to simply copy the important ADC functionality from existing servers and apply it to the new VDI servers, saving time and minimizing errors. In fact, F5 ADCs improve application deployment cycles by 10 to 100 times, and reduce configuration errors by 95 percent. By simplifying the allocation of network resources and viewing the network from the application's perspective, F5 ADCs make IT operations and deployment far more efficient.

And in a merger situation, where each company uses a different VDI vendor, F5 enables IT to create user pools that can map users to the correct VDI solution for them, regardless of where they're coming from in the network or which data center their VDI servers reside in.

This is the kind of flexibility that gives management leverage when negotiating with existing vendors. While it is never simple to change VDI vendors, having an architecture in place that will optimize not just today's infrastructure but whatever is chosen tomorrow makes it easier for IT management or procurement agents to potentially move to a new VDI vendor.

Security

When an organization deploys VDI with an external client element, for instance the ability to access applications from home or on the road, the security mechanism is exposed on the public Internet. This can have serious consequences for remote access if the authentication server is the target of a DDoS attack. It also places VDI outside the normal realm of security policy and protocol. This creates a scenario in which desktop images and physical desktops are not necessarily policed.

Moving large portions of network and application security to an ADC means that security policy can be centralized across all systems, whether virtual or physical. Enabling organizations to offload encryption for connections going out over the public Internet is one of the many ways F5 products increase VM density.

BIG-IP LTM is a solid platform for fending off DDoS attacks; it protected some of the most viciously assaulted sites during the Anonymous attacks of 2010.

But first and foremost, VDI should be part of an organization's central access and security policies. F5 ADCs help achieve this by handling security issues centrally. From two-factor authentication to one-time pad devices such as smart cards, F5 ADCs enhance the security of a VDI deployment while using the data center's AAA infrastructure. BIG-IP® Access Policy Manager™ (APM) can take security down to the level of "does this user, on this client device, have access to that resource." This gives IT unprecedented flexibility in meeting user needs and expectations while keeping attackers at bay.

Availability

Most VDI solutions offer much better recovery from machine-specific disasters than traditional desktops. This is because the VM can be dropped (or if necessary, deleted and a copy put in its place) and then restarted. This is far faster than sending a tech to troubleshoot or spending an hour on the phone trying to diagnose remotely.

Even if an organization has a disaster recovery (DR) plan, localized DR isn't enough. The ability to deal with an entire rack going dark, or even an entire data center, is more important in a VDI environment than a traditional environment.

The ability to move users from data center X to data center Y seamlessly, or from server X to server Y quickly, is important to productivity during outages. Most VDI solutions have only limited solutions in this space.

F5 ADCs, however, can switch users in an instant, from one server to another, or from one data center to another, nearly seamlessly. When BIG-IP LTM is combined with BIG-IP® Global Traffic Manager™ (GTM), users will notice only a slight blip when they're moved—whether it's across the data center or across the world. For VMware customers, F5 and VMware, working through their partnership, have a set of tools to accelerate and secure live migration events across data centers, so administrators can move VMs while they're being utilized.

VDI Is Resource Consolidation

VDI is, at the bottom level, an application layer protocol (or several application layer protocols) that transmits I/O between users and desktops at a remote location. When desktop processing is centralized, network protocols take up the burden of communicating I/O. F5 has years of experience optimizing networking protocols to make them reliable and efficient. And because all VDI traffic is additive to the network's burden—applications still have to make all the network calls they did before, but the results will also have to be transmitted to the client—efficiency is paramount.

No matter which VDI vendor an organization chooses, F5 brings these unique strengths to virtual desktop infrastructure:

- Custom application templates for each major VDI solution with specific configurations tested with each vendor, preconfigured to get VDI deployments up and running quickly.
- SSL offloading to increase VM density for VDI deployments.
- Heterogeneous support so organizations can support different vendors for desktop and server virtualization efforts with the same set of hardware.

- Support for other applications because once an F5 Application Delivery Controller is deployed, it can optimize, load balance, and secure any application running on the network. With specific F5 iApps™ for all of the major enterprise software products from Exchange to Oracle DBMS that enable quick configuration from the applications' perspective, the reach of the BIG-IP system goes far beyond VDI.
- External authentication portal protection, so VDI authentication does not become an attack vector.
- The user base of more than 80,000 peers on F5's DevCentral (devcentral.f5.com). DevCentral offers tools, techniques, and collaboration to help the F5 user community create and build upon solutions.
- SSL VPN support, with 500 user licenses bundled in the base product, with built-in support for iPad, iPhone, and Android devices.

Conclusion

VDI deployment is a worthy undertaking for lightening desktop footprint, centralizing application administration, and covering licensing concerns. But it is a complex system that shares many properties with server virtualization. VDI increases the network burden, and directing users to the appropriate server or data center requires configuration efforts beyond normal workloads. F5 offers a heterogeneous architecture to service all of an organization's virtualization needs, while helping to make VDI deployment secure, fast, and available. With tools to make deployment and network maintenance easier, loads of security features, and F5's award-winning ADC functionality, a VDI deployment can be easier and more adaptable.

And with a vendor-agnostic infrastructure rather than one sold by a specific VDI vendor, F5 will put IT organizations in a position to maximize the future, whether through mergers, change in VDI vendors, or support for different VDI and server virtualization vendors.

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