Getting the most out of your application and desktop virtualization solutions

Learn how NetScaler helps maximize the returns on your organization’s investments in application and desktop virtualization
Compared to traditional, distributed approaches for application and desktop deployment and management, virtualization solutions such as XenApp and XenDesktop promise significantly reduced operating costs, greater business agility, better data protection and improved compliance with industry and corporate standards. Fully achieving these gains, however, depend on ensuring the availability, security, performance and scalability of the associated infrastructure. As a result, leading IT organizations have developed the best practice of front-ending their application and desktop virtualization deployments with a dedicated solution that helps across all of these critical areas.

This paper explains why NetScaler is ideally suited to fulfill this role. By combining an extensive set of capabilities for ensuring the accessibility of essential components, enhancing the user experience, and protecting associated data, applications and infrastructure, NetScaler more than just preserves the benefits promised by XenApp, XenDesktop and other application and desktop virtualization solutions. It maximizes them.

**Critical requirements for success with application and desktop virtualization**

Enterprises that invest in full-featured application and desktop virtualization solutions such as XenApp and XenDesktop unlock the potential to:

- Sustainably reduce desktop ownership and operating costs
- Expand device compatibility by delivering Windows applications to both Windows and non-Windows devices
- Enable complete workplace flexibility, as well as workforce continuity in the event of a disaster or disruption
- Improve security and meet compliance mandates by having desktops, applications and data remain in the datacenter
- Increase business agility by rapidly and efficiently supporting strategic initiatives such as mergers and acquisitions, geographic expansion and dynamic partnership arrangements

However, the extent to which your organization can achieve these and other available benefits will depend on how well your implementation addresses the following set of critical requirements.
Critical requirement #1: Availability. Instead of users' desktop environments and associated applications residing on their local devices, with application and desktop virtualization these resources are hosted in the corporate datacenter and accessed over the network. Although this approach provides a tremendous degree of location and device independence, it relies on both network connectivity and centralized infrastructure. Furthermore, numerous users share the same application and desktop delivery infrastructure, from the front-end connection brokers to the back-end servers. This means that while a failure with a conventional desktop PC (or application) only impacts a single user, a failure within the shared infrastructure of a virtual application and desktop deployment has the potential to impact the entire user population. This is why you need to design your infrastructure to protect not only against the failure of individual components, but also from disasters that could cause site-level outages.

Critical requirement #2: Security. Robust security capabilities are especially important within a virtualized app and desktop environment, for several reasons. To begin with, many of your users are likely to access their apps and desktops remotely, over insecure public networks. Added to this is the need to support a rapidly expanding variety of client devices, each with its own distinct set of security capabilities and vulnerabilities. Complicating matters even further is the growing adoption of BYO practices, where many of these devices are no longer owned or controlled by the enterprise. Finally, with desktop virtualization in particular, it’s also important to recognize that what you’re giving users access to is an entire desktop, not just a sliver of functionality or data. In addition to their own applications and data, users can get to all of the downstream resources their desktops are entitled to access. The bottom line is that extra measures must be taken to adequately protect your organization’s critical assets against the challenges of this new environment.

Critical requirement #3: Excellent User Experience. Your users will insist on performance that’s comparable to that of a local desktop PC—and you’ll have to win them over with seamless logons, fast response times, quick issue resolution and a consistently enjoyable experience, even when access is occurring via disparate client devices and over a network. Otherwise, if users perceive or experience any shortcomings with the new environment, you will run the risk of their attempting to circumvent it—thereby eroding the investments you have made.

Critical requirement #4: Monitoring. Monitoring and visibility of the network and application traffic is very important when it comes to security and compliance and also for troubleshooting and providing better support SLAs. With users using any device from any location, performance can be an issue when it comes to accessing data over high latency networks such as mobile networks and on devices that do not have high performance hardware. Troubleshooting with tools that do not have knowledge about the underlying protocol can be a nightmare and can lead to finger pointing between server and networking teams leading to long SLAs and increased user frustration.

Critical requirement #5: Flexibility. Most organizations take a practical approach to app and desktop virtualization, starting out small and steadily growing their implementation over time. Also, they may shift from an initial deployment that is strictly on-premises to a hybrid-cloud model. The key point is that you should plan ahead to ensure the solution put in place has the flexibility to accommodate such changes without unduly impacting users or requiring forklift upgrades to the initial infrastructure investment.
**Optimize your app and desktop virtualization deployment with NetScaler**

A highly effective, best-practice approach to simultaneously address all of the critical requirements discussed above is to front-end your application and desktop virtualization infrastructure with NetScaler. A market-leading application delivery controller (ADC) and a remote access SSL VPN solution, optimized for security, mobility and hybrid-cloud use cases, NetScaler brings together in a single solution everything you’ll need to ensure a maximum return on your app and desktop virtualization investments. A powerful set of high-availability, security and performance-optimization capabilities are applicable and work equally well regardless of which virtual app and desktop products your organization has chosen to deploy. Not surprisingly, organizations using XenApp or XenDesktop will also benefit from a number of advanced features, made possible by the deeper level of integration achieved between NetScaler and those solutions.

**Ensuring availability**

NetScaler helps ensure the availability of critical components of your app and desktop virtualization infrastructure with a combination of robust server load balancing (SLB), health monitoring and global server load balancing (GSLB) capabilities.

**High availability for dependable access.** With NetScaler, you can configure and manage pools of essential resources. If a key component such as a connection broker fails, core load-balancing algorithms within the solution will dynamically route active user sessions to alternate servers within the corresponding resource pool. The result is the ability to automatically address both unanticipated failures and scheduled outages. These features can also help ensure high availability of other elements of a typical desktop virtualization deployment, including:

- Front-end components, such as Citrix StoreFront and essential security servers
- Supporting services, such as file transfer, licensing, provisioning and management servers
- Downstream components, such as the StoreFront and XML services of XenApp, that you can use to enable application virtualization

**Health monitoring for proactive failure management.** An extensive set of advanced health checks enable NetScaler to proactively avoid routing user sessions to unavailable or poorly performing components of the virtual app and desktop infrastructure. Although they confirm the availability of a network connection and that underlying server hardware is up and running, simple ping-based checks fail to establish the status of higher level services and software. This is why NetScaler includes extended content verification checks to further establish not only the availability but also proper operation of numerous software routines and system-level components that form part of the combined XenDesktop and XenApp solution, including ASP.net and essential logon, pool management, controller and database services.

The same degree of intelligent application-level monitoring can also be achieved for other app and desktop virtualization solutions, simply by taking advantage of NetScaler’s fully extensible management framework to configure a similar set of custom health checks.
Monitoring application and network traffic. The ability to observe, diagnose, and subsequently improve the performance of business-critical applications is essential to ensuring a positive user experience and maintaining the highest levels of employee productivity and customer satisfaction.

NetScaler offers HDX Insight as a part of NetScaler Insight Center, that allows end-to-end visibility of the XenApp and XenDesktop traffic. It not only provides real-time data to troubleshoot network and application issues but also provide historical data for planning and enhancements to the network in the future. Being the only solution that can decrypt ICA protocol traffic, this provides NetScaler a strong advantage over any other competitor offering.

GSLB for disaster recovery. NetScaler includes a robust GSLB capability that provides seamless disaster recovery for app and desktop virtualization. If a site becomes unavailable for any reason, NetScaler automatically directs users to an alternate datacenter, helping to ensure continuity of access to their apps and desktops.

IT can also configure intelligent monitors and policies to regularly route users to different sites based on pre-selected priorities, such as proximity, resource utilization levels, or overall performance. As a result, your organization can fully leverage secondary facilities all the time, even during normal operating conditions, while consistently providing users with the best available performance.
Strengthening security
Another way NetScaler helps maximize the return on your virtualization investments is by delivering additional protection for all involved data, devices and infrastructure. In particular, the Unified Gateway features of NetScaler not only help customers consolidate security at the network edge, but also deliver simplified, unified remote access to all types of business applications – including virtualized applications and desktops – for any user, in any location using any type of device.

Secure remote access from any location and device. To begin with, NetScaler with Unified Gateway provides numerous powerful capabilities for you to granularly control which users and devices are able to access which specific virtual desktops under different operating conditions. Related features include:

- **Identity based access control.** With this feature set, you can automatically block all inbound session requests until the identity of the corresponding user and their device is validated. Access can then be strictly confined to those parts of the enterprise network and the specific virtual desktops for which each individual user is authorized. To maximize compatibility with existing identity and access management tools and protect related investments, NetScaler with Unified Gateway provides SAML 2.0 federated identity and supports an extensive set of authentication mechanisms including local authentication, RADIUS, LDAP, TACACS, Digital Certificates, and NTLM delegation.

- **Dynamic access control.** The integral SmartControl feature set enables you to avoid the limitations and risks of rigid, one-size-fits-all policies by centrally configuring services for accessing virtual apps and desktops that automatically adapt to changing conditions, such as strength of authentication, the results of real-time endpoint analysis and the sensitivity of the resources being accessed. Because NetScaler with Unified Gateway includes in-depth knowledge of the ICA protocol, you can even control actions of XenDesktop and XenApp users that might be considered risky in certain situations, such as local print, copy, paste and save-to-disk operations.

- **Secure tunneling options.** All access sessions are protected from eavesdropping by standards-based SSL/TLS encryption. With the classic SSL VPN capability, the resulting network-level tunnel provides access to a broad set of resources, including a user’s virtual apps and desktop(s). Optionally, the innovative MicroVPN feature enables the use of tightly focused, per-application tunnels that inherently restrict the reach of client devices and thereby limit the impact of any that might be compromised.

Built-in infrastructure protection. NetScaler also provides protection for downstream virtual infrastructure components that it front ends through a combination of powerful network and application-layer shielding, extensive protocol validation, and multi-layer DDoS mitigation capabilities. For more information on NetScaler capabilities for protecting virtual apps and desktops, please refer to Securing virtual desktop infrastructure with NetScaler on www.citrix.com/gateway

Streamlining the user experience
NetScaler improves the usability of virtual apps and desktops, both by optimizing performance and consistently delivering a delightful user experience.
Performance optimization. Leading virtual app and desktop solutions employ optimized display protocols to help ensure adequate performance over wide area networks (WANs). ICA, the display protocol that both XenDesktop and XenApp use, is unmatched in this regard. Still, one or more of the NetScaler performance enhancement mechanisms can improve performance further, especially if your organization is using app and desktop virtualization solutions other than XenDesktop and XenApp.

Integral TCP optimizations – including advanced buffering and window scaling, intelligent packet retransmit, selected acknowledgement (per IETF RFC 2018) and enhanced congestion control (per IETF RFC 3742) – trim response times while making more efficient use of available bandwidth and back-end compute resources. In addition, innovative rendering technology ensures a smooth, highly responsive browsing and application navigation experience – even for graphics-rich content – when connecting over wireless and other types of networks subject to high latency and packet loss.

Then there’s HDX Insight, a native management capability that collects, correlates and displays extensive usage and performance data for XenApp and XenDesktop, both in aggregate form and down to the level of individual user sessions. Armed with this intelligence, you can not only triage ongoing issues in real-time, but also conduct regular capacity planning exercises to proactively avoid future performance problems.

Uniform, streamlined user experience. For XenApp and XenDesktop users, the Citrix Receiver user interface ensures a consistent access experience across disparate devices. Single sign-on (SSO) to back-end resources, company-specific branding and customizations, and a familiar app-store model for accessing, organizing and requesting virtual desktops and other available applications are just a few of the features intended to enhance usability and ensure a pleasing user experience.

Guaranteeing adaptability
Finally, NetScaler also provides the flexibility and capabilities needed to account for the growth and other changes likely to impact your app and desktop virtualization implementation over time.

Scalability to support growth. NetScaler server load balancing functionality does more than enable high availability. It also supports load distribution, which enables you to seamlessly scale up essential virtualization infrastructure components such as connection broker, security and management servers. If your organization needs to add capacity, all you need to do is deploy another instance of the desired component, and NetScaler takes care of the rest, automatically balancing the workload among all available instances.

As for NetScaler itself, unparalleled scalability is enabled by TriScale technology, a powerful triumvirate of Pay-As-You-Grow licensing, the NetScaler SDX multi-tenant platform, and advanced clustering technology for more details, see A revolution in cloud networking: Citrix Tri-Scale Technology.
Flexibility to support different architectures. Although many enterprises plan to take a private cloud computing approach to app and desktop virtualization, others will lean toward public or hybrid cloud configurations where an external service provider delivers all or some of the virtual apps and desktops. NetScaler easily and cost effectively supports all of these scenarios by providing you with a choice of platform: NetScaler MPX hardware appliances, the NetScaler SDX multi-tenant platform, and full-featured NetScaler VPX virtual appliances.

Cloud and branch office networking scenarios are further facilitated by NetScaler CloudBridge, a solution that conveniently combines WAN optimization and virtualization with L2 tunneling and GSLB technologies to ensure secure, high-performance delivery of virtual apps and desktops from both on and off-premises datacenters to wherever your users might reside.

Simple yet powerful management. Citrix Command Center is a centralized management console that eliminates the need to administer multiple, distributed NetScaler instances individually. Featuring an intuitive policy framework, it also includes several wizards for simplifying common configuration tasks, such as setting up SLB and GSLB for your app and desktop virtualization environment.

Another related tool, AppExpert Visualizer, helps manage the complexity of such environments by supplying an at-a-glance graphical view illustrating the full end-to-end virtualization infrastructure, including individual NetScaler delivery capabilities and the components they support. With AppExpert Visualizer at your disposal, you can easily monitor relationships, health status and configuration parameters, both for routine administration as well as detailed analysis and troubleshooting.

Maximizing the return on your app and desktop virtualization investment
Extracing the greatest value from your investment in app and desktop virtualization depends on ensuring the availability, security, usability and flexibility of the corresponding infrastructure, desktop environments and data. NetScaler, the industry’s leading application delivery controller, is the ideal solution for doing just that. By front-ending your app and desktop virtualization environment with NetScaler, you stand to benefit from:

• Increased availability, as NetScaler protects against both component and site-level failures
• Strengthened security that helps compensate for access over public networks and from client devices not controlled by IT
• A smooth and seamless user experience that helps ensure employees remain content and productive
• The ability to adapt to changing business conditions and ongoing technology trends without disrupting users or requiring forklift upgrades

Find out more about how NetScaler can enable you to realize the full potential of your organization’s preferred app and desktop virtualization solutions. Visit [www.citrix.com/netscaler](http://www.citrix.com/netscaler).