Why Ivanti for VDI – How User Virtualization Performs and Adds Value

More and more enterprises are turning to desktop virtualization as a solution to rising IT costs and security concerns combined with user demands for a personalized desktop experience and the ability to work from anywhere, at any time, from any device. Ivanti and Citrix are working together to integrate the market-leading user virtualization solution with the world's most widely deployed desktop virtualization platform.

In 2012, Ivanti spent two weeks at Microsoft's Enterprise Engineering Center (EEC) with Citrix and Microsoft to validate the compelling integrated value and impact of Ivanti Environment Manager 8.2 on XenDesktop 5.6 platform and density. This paper demonstrates the joint value of Ivanti with XenDesktop 5.6 on Microsoft Hyper-V 2008 R2 SP1.

Our joint customers attain similar performance gains using current versions of these products.

Ivanti and Citrix bring together the worlds of user and desktop virtualization via XenDesktop and provide a joint value in three core areas:

User Onboarding and Personalization

Ivanti supports the migration process, from Windows XP through to Windows 10 and from physical to virtual desktops on XenDesktop or XenApp. We ensure that the customer's first experience logging on to their new desktop, irrespective of physical or virtual, is a good one that doesn't create a post-migration support issue. The user's first impression will be that nothing changed—their desktop and application settings look the same as when they left them on their physical desktop. As part of this, Ivanti supports the dynamic composition of pooled XenDesktop images (via Machine Creation Services or Provisioning Services[1]) with Windows 7 SP1 and above, utilizing best-of-breed application virtualization technologies such as App-V. This removes the need to use tools such as Windows roaming profiles, thus saving IT from potentially significant architectural, support, and management issues.

Post deployment, Ivanti ensures that as users move from a physical desktop to their XenDesktop environment (both forwards and back and in real time, without logoff) the user experience remains a consistent and positive one irrespective of whether the customer is using native or virtualized application technologies. Citrix further supports the onboarding process with Citrix AppDNA, which helps to transition applications that previously worked in their Windows XP platform and move them to Windows 7, 8, or 10 on XenDesktop.

Environment Optimization and Security Management

Users become frustrated when the system feels slow. This can be compounded by inefficient security policies and restrictions. Additionally, at times, production pilots have faced external challenges simply because the user experience—from the moment the user logs on—was inconsistent with the previous physical platform.

Ivanti streamlines the XenDesktop and Windows logon process by replacing scripts and only delivering the settings and policies the user needs when they need them—on application launch. Ivanti also minimizes the network traffic through the granular storage of application settings in a database. Ivanti also takes full advantage of multicore processors by running logon activities in parallel rather than in serial-like traditional logon script. The net effect is that logon is quicker and the user benefits from being able to work from the moment they first log on to XenDesktop.

Ivanti also adds a security layer that provides granular management of user rights. In combination with Citrix AppDNA's assessment, this helps with application compatibility situations, especially on Windows 7, with the default implementation of User Account Control (UAC).

Ivanti also increases security with a layer called Trusted Ownership™ that blocks any malware from being executed that the user downloads onto their desktop, allowing you to minimize antivirus functions in the XenDesktop VMs and XenApp servers while not increasing the risk profile. This helps provide a secure and usable user experience, delivering quick logon performance that allows the user to do what they need to do but at the same time delivering the security that enterprise IT demands.

Density and Response Improvement

Scale and maintaining a low cost per user are critical factors in VDI deployments. In particular, capital expenditure can be a significant portion of the overall expense.

While XenDesktop is already a proven, scalable, and responsive platform for desktop virtualization, with excellent TCO metrics, Ivanti delivers a further significant drop to XenDesktop and XenApp TCO models.

Typically, antivirus and Adobe Flash products create a significant density impact, with reported losses of up to 30% user density and a corresponding increase in the cost per user. Other poorly designed and written applications can have a similar negative impact on density. Ivanti can significantly minimize and constrain these and other performance-hogging tools and technologies, while improving security and allowing you to significantly improve the cost per user. The net effect is also providing a user experience that is both responsive and consistent.

Test Scope and Purpose

Ivanti engaged a customer validation test in the Microsoft Enterprise Engineering Center (EEC) to complete performance and density testing with Citrix and Microsoft on a large- scale joint VDI project. [2]

The customer had a specific target density in mind for the test work and needed to understand how Ivanti could add value to this density metric. The metric chosen for the test was based loosely around the memory constraints of the IBM blade of 128GB of RAM. The target was a maximum dynamic allocation

of 1GB RAM per Windows 7 SP1 32-bit virtual machine, plus some headroom for the Windows Server 2008 R2 SP1 parent partition itself to work in. This placed the target density at 115 VMs, though from the testing it is obvious we probably could have achieved higher to completely exhaust the blade.

The goal of the test work was to understand how the end-to-end Ivanti software stack could:

- Add tangible and measurable joint value to XenDesktop, XenApp, and Microsoft platforms
- Ensure that the joint solution stack performed or exceeded performance baseline expectations

The testing evaluated the performance impact of two of the three components of Ivanti DesktopNow to benchmark their impact, positive or negative, in a test environment.

The scope of the test was not aimed at testing every feature of the Ivanti software suite for a value-add to XenDesktop. The features mentioned throughout this paper represent a small amount of its total capability.

As a note, it should be appreciated that while test work can demonstrate potential scalability and impacts, these impacts can and will vary greatly in a real-world production scenario. These variations can be caused by a variety of issues such as software and hardware platform choices, applications in use, and the workstyles and use cases of the user populations.

Test Framework

The test framework that was used for the evaluation is the industry-leading LoginVSI 3.5 produced by Login Consultants, based in the Netherlands.

At its core, this industry-standard test framework is designed to emulate how a user works by starting and executing work with applications such as Microsoft Office, Internet Explorer, and Adobe Flash among other applications to simulate web browsing activity, creating and editing Microsoft Office documents, printing documents, and finally including pauses to simulate coffee breaks and pauses that users typically make in their workplace.

This has the effect of generating load on the whole system, end to end, with the goal of determining a maximum VM density that could be achieved in production. It is arguably even more severe than a typical user would push the system, especially in aggregate, as it executes many tasks both in the foreground and background, measuring both concurrently. It certainly does provide a very solid estimate that can be used to project user loads and thereby cost-per-user models that a business could reasonably use to budget with.

LoginVSI has several modes of operation that simulate different use case profiles such as light, medium, and heavy profiles, which additionally have either Adobe Flash switched on or off. Adobe Flash (like antivirus products) in particular places extreme load on a densely deployed VDI host and can push the total system—inclusive of processor, memory, disk, and network—to its extreme limits.

In all tests, we chose the Medium profile with Flash enabled as many vendors such as Microsoft, Citrix, HP, and Cisco all use this profile to test their reference architectures exhaustively.

During the test, LoginVSI 3.5 measures the overall system responsiveness via various applications and operations. It calculates a measure of response known as VSIMax, usually occurring when the average system response hits a single 4000ms threshold and representative of the maximum number of VMs that can be delivered successfully by the system. If 4000ms is not hit on average during the test pass, VSIMax is considered not reached and the target density met. The implication of this is that further density could be potentially achieved.

For more information on this framework, please consult www.loginvsi.com

Hardware

As a top line, the hardware used for this test was a combination of:

- IBM BladeCenter H series chassis with IBM Hx5 blade servers .
    - Each blade was configured with a dual socket Intel® Xeon® CPU E7-4870 @ 2.40GHz (10 core hyper-threaded) with a total of 20 CPU threads per processor.
    - 128GB of RAM.

    - Each blade was also configured with local SSD storage for write caching.

- EMC VNX 7500 SAN with 138 600GB SAS disks and 27 200GB SSD disks. In addition, it had a 47GB cache. This was connected via 10GB iSCSI to the BladeCenter chassis.

Software

The base platform software used throughout the testing was a combination of Citrix XenDesktop and Microsoft Windows and System Center platform products.

Consistently throughout the tests the following software stack was used:

- Citrix XenDesktop 5.6 Beta
- Microsoft Windows Server 2008 R2 SP1
- Hyper-V
- System Center Virtual Machine Manager 2012
- Windows 7 SP1
- Office 2010

There was one software component tested a single time. System Center EndPoint Protection 2012 (antivirus) was implemented in the last test to determine whether Ivanti could minimize the impact of its input/output (IO) overhead.

Overlaid onto this software environment were the Ivanti components:

- Ivanti Environment Manager 8.2
- Ivanti Performance Manager 8.1

While Ivanti Application Control was also in scope of the overall value proposition, it was not included in the testing itself. It does not generate any significant or even measureable load that justified its inclusion into the testing. This component will be handled in the results section further on, discussing how it adds value and why it's an important part of the overall software build.

More information on each of these product areas can be found in the Appendix.

Core Infrastructure

The core infrastructure and application services for the test were hosted on separate IBM blades to the VDI blade host and launchers. This included individual VMs for:

- Citrix XenDesktop 5.6 Beta Desktop Delivery Controller
- Citrix XenDesktop Provisioning Services 6.0
- Windows Server 2008 R2 hosting Active Directory and DNS roles
- Microsoft System Center Virtual Machine Manager 2012
- Microsoft SQL Server 2008 R2

Windows 7 VDI Blade

A single IBM blade was used to host the 115 Windows 7 VMs that would run the test, running on Hyper-V with dynamic memory enabled. To represent this better as a hypervisor stack, please refer to figure 1.0 (overleaf).

Each Windows 7 SP1 Virtual machine was configured with 512MB RAM as startup memory, with dynamic memory allocating memory to the virtual machine as required.

The Windows 7 SP1 VM is diskless, booting an image and streamed from a Citrix Provisioning Services virtual machine via PXE. The Provisioning Services virtual machine was directly connected to the EMC VNX SAN storage and reading the image from there. The write cache for each Windows 7 SP1 VM was pointed to the blade's local SSD storage for maximum performance.

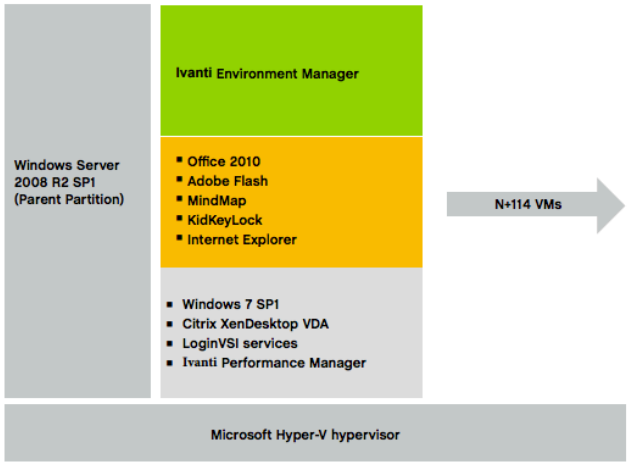

Figure 1.0

LoginVSI launchers

The LoginVSI launchers, which launch each session in succession, were all hosted on a single blade.

The launcher software was installed on 10 Windows Server 2008 R2 virtual machines, each configured to launch a maximum of 15 XenDesktop sessions. The launch for each test was performed in parallel rather than sequential. This means that as each launch window occurs, a session is executed on the next launcher rather than sequentially on the same launcher before moving to the next launcher. The launch (and subsequent logon) window for each test was set at 30-second intervals.

Commentary on parallel vs sequential launching can be found at: www.loginvsi.com/en/admin-guide/performing-tests#h0-2-1-sequential-vs-parallel-launching

Results

How does Ivanti Application Control add value?

Even though Application Control is not included in this test pass, it adds significant value to the software stack. Not having it present would have a significant impact on security and density.

Antivirus products in particular create a significant impact on VDI and session virtualization density. In fact, some whitepapers report as much as a 30% impact on density caused by antivirus overhead[3].

Independent and unpublished testing indicates Forefront antivirus overhead is a minimum of 13% using the same test methodology with LoginVSI as these tests are using. Either way, a 13% loss at best is still a loss in cost-per-user models that can ultimately make or break a VDI business case.

Due to the significant impact, many customers dangerously choose to ignore antivirus products in their VDI implementations.

The rationale is that the VDI image is usually only “alive” for a maximum of eight hours due to the use of pooled VDI technologies such as Citrix XenDesktop with Provisioning Services. All other documents and data that they are using from file shares are scanned at the file server, thus minimizing risk at the data level.

To explain this concept better, as the user logs on to XenDesktop, the image is dynamically composed with the operating system, data, applications, and user information. After the user has finished their work and logs off, this XenDesktop image is discarded completely. The next time the user logs on, they receive an entire newly composed desktop, yet because Ivanti Environment Manager plays a key part in the user experience, it feels the same as the way they left it.

Therefore, the argument is that given the image is only “alive” for eight hours and completely discarded, then how can malware persist beyond eight hours?

This is a very risky view that ignores the danger of other malware that can then infect other systems that are not VDI based, such as physical PCs, XenApp servers, and core server infrastructure. The VDI implementation now becomes the weak link to security and the entry point for malware.

There are now two problems to be balanced: 1) the loss of density (and increased cost per user) caused by antivirus; and 2) the potential for a higher risk of infection into peer systems. And Application Control helps to solve both issues.

Application Control provides a layered security capability, among other features in granular Windows

privilege management, called Trusted Ownership. This serves to place a “trust layer” over the operating system whereby the IT administrator can add identities to the Windows 7 SP1 VM that are trusted. Examples of these identities are Trusted Installer, the system installation account, and the Domain Administrator account. Other examples could be the System Center Configuration Manager service account that installs corporate-managed software.

However, we may not choose to trust executable code that the user downloads from the Internet. We do this by checking who owns the executable code. If the interactive user is the owner, then that code is blocked from execution.

Trusted Ownership effectively blocks user-downloaded software, which can be infected with Trojans or other types of malware, or at the least could severely impact system performance.

The net effect of this is that antivirus can now be implemented in a much-reduced feature state. Antivirus technologies such as heuristic scanning and scheduled scans, which can impact performance significantly, can be switched off now that malware is being blocked altogether from execution by the untrusted interactive user. Instead, only real-time scanning now needs to be implemented to provide the last “catch all” to anything not interactively executable.

This still maintains a very solid risk management profile that minimizes potential impacts due to antivirus overhead.

In the testing performed, we assumed this antivirus configuration state and tested performance impact based on the assumption that Application Control was present.

Baseline Testing

Before we started with Ivanti software testing, it was important to gain a baseline test of XenDesktop running without any influence of Ivanti software or System Center Endpoint Protection.

This test was run at 30-second intervals in parallel with a target density of 115 VMs.

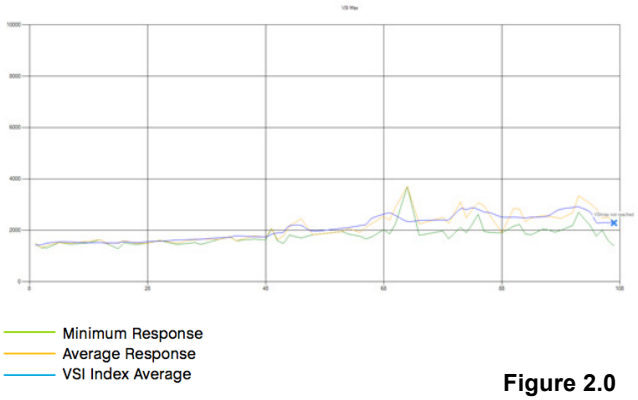

Figure 2.0

In figure 2.0 we see that the test passed as expected. VSI Max, an indicator of maximum usable density, was not reached. This indicates that some headroom is still present.

Overall this system showed very good results.

The baseline software for this test was the combined Citrix and Microsoft software stack only in order to enable the core solution to function, inclusive of Provisioning Services. As per the guidance in the LoginVSI documentation, Microsoft’s inbuilt roaming profiles were used.

Ivanti Environment Manager Test

While the LoginVSI documentation recommends the use of roaming profiles for test purposes, this isn’t practical in production. Many customers find that roaming profiles synchronized as a large chunk only at logon and logoff simply doesn’t scale in the enterprise and the technology itself is fraught with corruption issues. This is especially manifested in multi-desktop scenarios such as a mix of VDI and physical PC environments. Additionally, to maintain acceptable performance with roaming profiles and VDI it’s critically important to ensure that the roaming profile server is near the VDI delivery platform. The

combination of support factors and the lack of practicality around proximity ensure that the use of roaming profiles is not an enterprise solution.

This is where Ivanti Environment Manager comes in. It provides the capability to deliver personalization (along with policy, both application and operating system) per application in a granular and scalable way that eliminates the support issues of roaming profiles. Plus it delivers a multi-master solution that can be replicated from data center to data center, utilizing the power of Microsoft SQL Server. What's more, onboarding into XenDesktop and XenApp from older platforms such as Windows XP and Windows Server 2003 (or Metaframe) can be solved easily without even worrying about the concept of user migration.

For more information on Environment Manager and Personalization, please consult: https://www.ivanti.com/products/environment-manager, or the appendix.

The goal of this test was to determine any performance impacts relating to real-time personalization. This test simply replaced Microsoft's Roaming Profiles from the baseline test with Environment Manager's Personalization Server. This can capture and deliver settings to any application, irrespective of whether the application is a natively installed application or a virtual application such as App-V, without violating the App-V isolation "bubble" as competitive solutions do.

In this instance, Ivanti personalized the user desktop and associated settings into the standard local profile of the VM, along with any Office 2010 applications, since these are used significantly during the test pass.

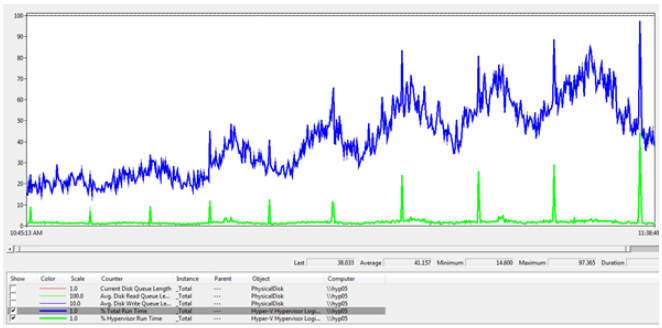

Figure 3.0

Figure 3.0 demonstrates the Performance Monitor trace of this test, focusing purely on processor counters. The two processor counters highlighted are:

- **% Total Run Time** (blue) – measures the aggregate utilization across the parent partition and child VMs
- **% Hypervisor Run Time** (green) – indication of how the parent partition itself is performing, managing the load of the individual VMs

At the top of the test, the total aggregate processor utilization was 97%, with an average utilization of 41% throughout the test pass.

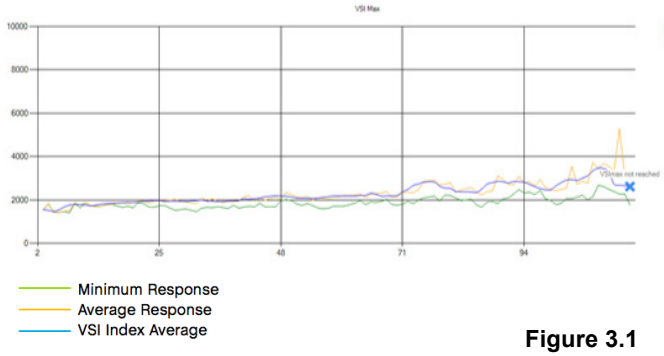

Figure 3.1

As with the baseline test, in Figure 3.1, looking at the LoginVSI response trace, VSIMax was also not reached.

In fact, it's observable that there is a relatively neutral overhead to Environment Manager's Personalization compared to the baseline testing, even though each client performs a roundtrip back to the Personalization Server in real time to retrieve settings that are delivered on demand (application launch) to each application.

Ivanti Environment Manager + Performance Manager Test

The goal of this test was to demonstrate Performance Manager's ability to manage and constrain performance-sapping processes such as Adobe Flash from impacting overall performance and thus creating a failure to achieve target density.

Each Windows 7 SP1 VM had the Performance Manager Agent installed and a configuration applied. This configuration was designed to prioritize LoginVSI processes and related applications that it measures, and to constrain Adobe Flash with a hard processor limitation of 30% on the Adobe Flash and Internet Explorer processes for both foreground and background tasks.

The reason for this specific configuration concerns the nature of LoginVSI's test profile. It executes both foreground and background processes and measures responses in both while generating load inside the VM with Adobe Flash-based media.

Thus, our configuration for this specific test platform focused on the behavior of the testing workload.

In practice however, this would likely be different. The configuration would probably still cap IO-expensive processes such as Adobe Flash due to the extremely negative nature of it on performance, though we would likely change the prioritization. Users in general care the most about what they are working on at present. Applications that are in the background are of less importance and Performance Manager can ensure that this user experience is met.

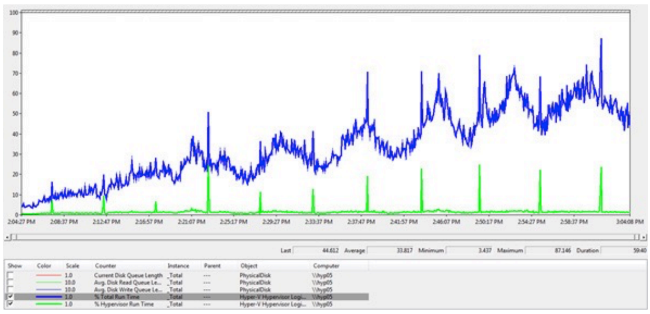

Figure 4.0

In Figure 4.0 we see the results of this test in Performance Monitor. Performance Manager has effectively constrained the Adobe Flash process within each Windows 7 SP1 VM and reduced the total processor utilization.

The two processor counters highlighted are:

- **% Total Run Time** (blue) – measures the aggregate utilization across the parent partition and child VMs
- **% Hypervisor Run Time** (green) – indication of how the parent partition itself is performing, managing the load of the individual VMs

At the top of the test, the total aggregate processor utilization was now reduced to 87%, with an average utilization of 33% throughout the test pass. This represents a reduction of 10% at the top of the test and an average reduction of 8%.

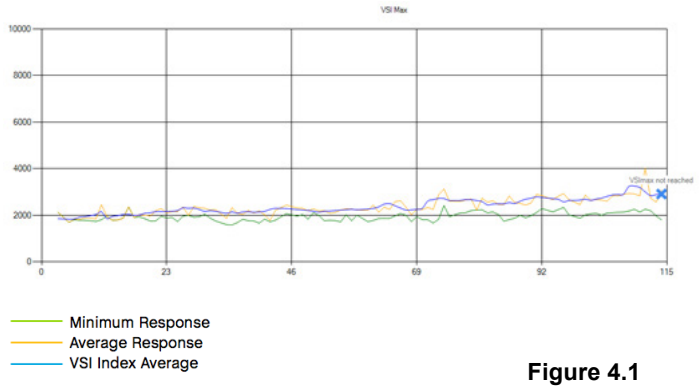

Figure 4.1

The LoginVSI trace in figure 4.1 shows a similar story to the Performance Monitor trace with a reduction in response time at the top of the test and a smoother response curve.

The net effect of a reduction in both response time and processor utilization directly correlates to an

increase in density and thus a reduction in cost per user.

Ivanti Environment Manager + Performance Manager + System Center EndPoint Protection Test

The goal of this test was to determine whether the use of Performance Manager can effectively constrain System Center EndPoint Protection antivirus in combination with the risk mitigation approach discussed in Ivanti Application Control's value.

The configuration for this test adds System Center EndPoint Protection. Both heuristic scanning and scheduled scans were disabled and a full antivirus scan (not quick scan) was run on the base Windows 7 SP1 VM before it was cloned via Provisioning Server. This allows SC EndPoint Protection to build up a cache of known files that are not scanned again in real time, unless they are modified.

The Performance Manager configuration was then updated to place a hard-processor limit of 40% on the MsMpEng.exe executable; the SC EndPoint Protection engine itself in combination with existing controls on Adobe Flash via Internet Explorer.

Figure 5.0

In figure 5.0 we see that the processor counter increased marginally. To recap again, the two processor counters highlighted are:

- **% Total Run Time** (blue) – measures the aggregate utilization across the parent partition and child VMs
- **% Hypervisor Run Time** (green) – indication of how the parent partition itself is performing, managing the load of the individual VMs

But the processor only marginally increased. As mentioned previously, typically antivirus creates an impact of up to 30% depending on antivirus vendor, and as low as 12%.

In this test, Ivanti Performance Manager managed to keep this loss to 3% both at the top of the test with a total processor utilization of 90% and an average of 36%.

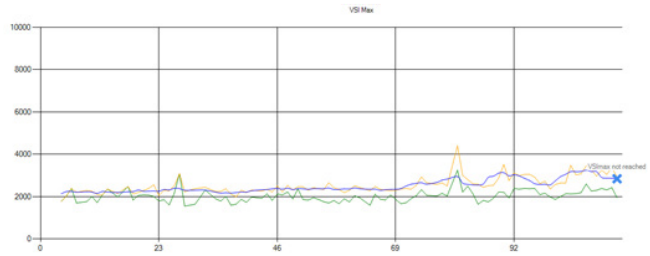

Figure 5.1

In figure 5.1 we see the final LoginVSI response test result. Again, VSImax was not reached and although the test started a little higher than usual (correlating to the slightly higher average processor result), performance overall stayed within acceptable response limits.

This test validates the approach of using a combination of Application Control to provide the concept of Trusted Ownership to block user downloaded executables from executing and creating a malware risk and Performance Manager to further constrain the process itself.

Conclusion

Ivanti adds significant value to virtual desktops using XenDesktop and XenApp. It helps with onboarding into XenDesktop, personalization of the user session, controlling security and malware issues, and managing density and user response.

Ivanti also adds value right across the XenDesktop and XenApp stack. It impacts how users first experience VDI and session virtualization and provides a rapid logon experience with a snappy and responsive environment to work anywhere in keeping with the FlexCast delivery models.

This testing underscores how Ivanti proved that we do provide this value. The integrated DesktopNow platform delivers solid performance, increased security, and an overall reduction of at least 10% in the cost per user.

As noted earlier, although these tests were conducted using Ivanti Environment Manager 8.2 and XenDesktop 5.6, Citrix customers running current versions of these products can expect similar performance gains.

An example

As an example,, consider a 5,000-user XenDesktop deployment. A 10% reduction in processor utilization (all other things being equal), which was achieved in this test, can mean a significant reduction in capital expenditure. In this example, 10% represents 500 users.

Considerations to note:

- As we have demonstrated, each tested blade can easily baseline scale to 115 VMs.
- To scale this to 5,000 users means purchasing approximately 44 IBM Hx5 blades.
- The IBM H Series blade chassis can hold a maximum of 14 blades
- 44 blades require 4 IBM H Series blade chassis (three fully populated chassis with one chassis holding two blades)

In this example, if the customer were to use Ivanti DesktopNow and save the minimum of 10%, they would not require four blades, and importantly, save on buying another whole blade chassis!

Final commentary on test work

As mentioned through the document, real production scenarios and use cases can be quite different from test scenarios, irrespective of different simulation modes.

LoginVSI works by automating a simulated user workload and duplicates this across the number of VMs that the customer needs to scale to. For what it's designed to do, which is to apply workload to push every part of the VDI solution inclusive of hardware and software, it does very well.

However, this is not how real users work. Some users start a lot of applications and switch among them. Other users start a few applications, but of those applications they do use, perform complex calculations. Each of these types of users pushes different parts of the system, some of which requiring more memory and some requiring more processor resources. Each user is different.

What Ivanti does in the real world is to help smooth out these diverse needs, deliver the right experience for all users, and deliver a secure workspace that meets the needs of the user without compromising the needs of others sharing the resources. This technology works across virtual desktops such as XenDesktop as well as physical PCs.

Ivanti has very large customers using this solution stack today with very real results. Our customers typically report much better results than the test results shown in this document, with many surprised with how good the user experience is they now have. Ivanti customer case studies can be found at: https://www.ivanti.com/resources/success-stories.

For more information, please visit us at: www.ivanti.com. For a demonstration or a call from one of our team please contact us at: contact@ivanti.com.

Appendix

The following sections cover overviews of each of the product areas of Ivanti DesktopNow, including capability areas not covered in the testing.

Ivanti Environment Manager

Environment Manager enables the delivery of fully configured and personalized desktops to all employees. This ensures a reduction in the complexity and risk associated with maintaining a large desktop estate and an ease of migration to a new Windows platform.

Used by thousands of companies around the world, Environment Manager provides users with a 'follow me' personality—providing the same managed yet personal experience regardless of how the desktop is delivered. Combinations of virtual, local, published, streamed, and provisioned desktop components are personalized dynamically as the employee uses them—enabling IT to use best-of-breed technologies without having to worry about consistency of user experience.

Environment Manager has two core capabilities:

1. Policy: It can deploy and manage policy—both operating system and application-level policy. Operating system policy utilizes regular Group Policy ADMX controls, though with a significantly more manageable interface and conditional targeting capability. The application policy is customizable per application and can contextually control individual application capabilities.

2. Personalization: It delivers granular personalization irrespective of operating system version or application deployment type. What this means is that settings can be delivered from one Windows platform to another, irrespective of whether it's XenDesktop or XenApp, Windows 7 or Windows 10, native or virtual application.

Ivanti Application Control

Regardless of how a user's environment is delivered, it is essential that users receive only the applications they require and cannot introduce unknown executable code into the environment.

The use of unauthorized software is a primary factor in destabilizing user environments, and the costs associated with rectifying a corrupt desktop can be significant.

The extent to which an employee has access to corporate applications can depend on the context of the accessing device. For example, a user in an Internet cafe will typically have a different level of application access than an employee within the secure confines of the corporate LAN.

Application Control can utilize information about the user's context to determine the level of entitlement necessary. Parameters such as location, firewall settings, and even time of day can be used to establish a necessary level of entitlement.

Application Control is also endorsed by Microsoft to enforce software licenses by controlling application usage on a per-device basis. Passive mode enables monitoring, auditing, and reporting to detail application access across the user and device base.

Lastly, the desire by enterprise IT departments to lock down corporate desktop environments to maintain security and reduce support costs is frequently at odds with end-user demands for greater flexibility and convenience through desktop customization. Windows privilege management solves this by enabling the elevation or reduction of user rights on a user, application, or business-rule basis. With Windows privilege management, the privilege level of a user, group, or role can be elevated or reduced for applications, individual processes, services, control panel applets, ActiveX controls, and tasks.

Consolidating 100 physical servers by 40% could save more than 120,000 kWh each year, cutting over 50 tons of CO2 emissions.

Ivanti Performance Manager

Any degradation in user experience reflects negatively on IT. No matter how a desktop or application is delivered to a user, ensuring that the environment reacts quickly to user actions is key to providing a high quality of service and meeting user expectations.

Ensuring a consistent quality of service is key to gaining user acceptance when trying out a new application delivery mechanism. Unresponsive environments are a major disruption and often lead to users rejecting a new system, making quality of service just as important as the overall hardware consolidation or desktop centralization project goals. For most organizations, there is a continuous trade-off between quality of service and server hardware cost reduction.

By allocating CPU and memory resources to applications and users and optimizing how user actions are processed, Ivanti Performance Manager provides a smoother, more responsive application experience. It also maximizes the value of server hardware investments through improved user density.

Many IT departments are tasked with consolidating their existing server infrastructure to simplify system management and reduce power consumption and carbon footprint. Significant savings in power, cooling, hardware, software licensing, and management can all be made by optimizing resource use and consolidating servers. Whether you plan to maximize user or application density, Performance Manager enables a substantial increase in server capacity by reducing the amount of resources required to run desktops on applications within a data center.

For example, consolidating 100 physical servers by 40% could save more than 120,000 kWh each year, cutting over 50 tons of CO^2 emissions[4]. These financial savings alone often provide return on investment within the first year of implementing Ivanti Performance Manager.

Finally, even though the testing discussed in this paper focuses around CPU performance management, Performance Manager also provides important memory-enforcement capabilities for Hyper-V. It enforces the upper limit memory configuration, thus preventing virtual machines using excessive memory and creating secondary paging issues.

Citrix XenDesktop

Citrix XenDesktop is a desktop virtualization solution that delivers Windows desktops as an on-demand service to any user, anywhere. With FlexCast™ delivery technology, XenDesktop can deliver individual applications or complete desktops to the entire enterprise quickly and securely, whether they are task workers, knowledge workers, or mobile workers. Users now have the flexibility to access their desktop on any device, anytime, with a high-definition user experience.

With XenDesktop, IT can manage single instances of each OS, application, and user profile, and assemble them dynamically to increase business agility and greatly simplify desktop management. XenDesktop's open architecture enables customers to easily adopt desktop virtualization using any hypervisor, storage, or management infrastructure.

www.ivanti.com

1.800
.982.2130

sales@ivanti.com

[1]http://support.citrix.com/proddocs/topic/technologies/ pvs-provisioning.html

[2]Microsoft EEC - http://www.microsoft.com/en-us/eec/default.aspx

3Cisco Unified Computing System, Citrix XenDesktop, and Atlantis ILIO, Summary comments on AV, November 2010, http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns944/cisco_ ucs_atlantis_citrix.pdf