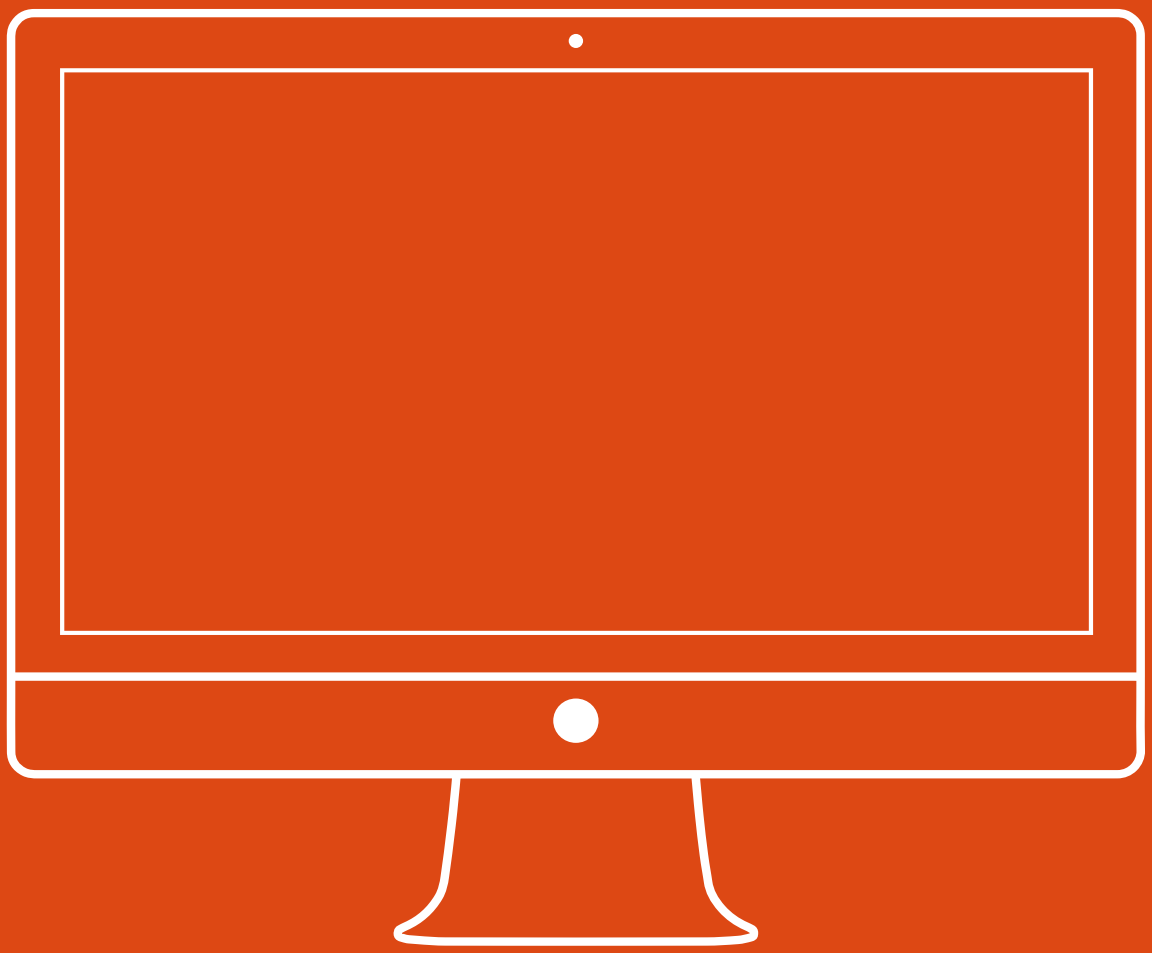
Jentu - The VDI Alternative

A secure latency free platform for IT Infrastructure Management



© 2015 Jentu Technologies

Jentu - The VDI Alternative

A secure latency free platform for IT Infrastructure Management

© 2015 Jentu Technologies

Contents

Challenges posed by VDI

Challenges posed by VDI

VDI isn't easy to deploy, and the challenges that come with VDI are well-documented: It's too complex, it costs too much, performance issues and admins are hard to find.

WITH SO MANY MOVING PARTS IN VDI DEPLOYMENTS, IT'S EASY FOR THINGS TO GO WRONG. PROBLEMS WITH REMOTE CONNECTIONS, STORAGE, MANAGEMENT AND LATENCY CAN KEEP YOUR TO-DO LIST FULL.

LATENCY

Remote displays are not throttled by VDI bandwidth considerations alone. The latency of the links from the client to the virtual desktop and the number of dropped packets also affects stability and usability.[1]

Users who experience this kind of latency may still be able to connect to the desktop but may suffer keyboard lag, where the screen is slow to update when they type. An average latency of 220 milliseconds (msec) is to be expected with most typical VDI installations.

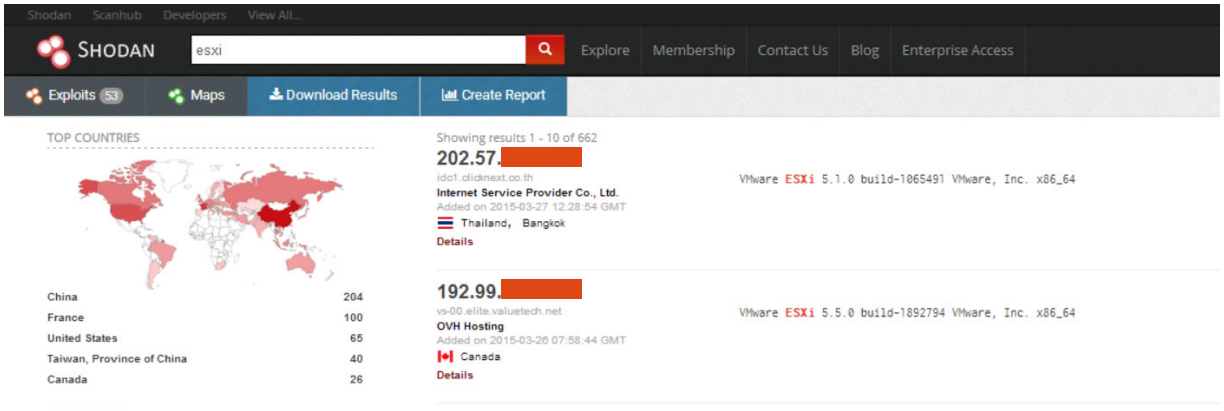
Latency becomes a real headache when it exceeds 350 msec, with intermittent spikes to 800 msec -- even if those latency spikes last only a few minutes each day and wouldn't be very disruptive for a single application. [2] Even as VDI performance increases (either by increasing the number of cores or buying more storage) there are still users for whom VDI is simply not a viable alternative.

For example, large files such as graphics and databases must be downloaded to the user's machine each time they begin work, and must then be uploaded back into the virtual infrastructure when the user is finished. Considering the large amount of network traffic generated by VDI, these users may find that they require a traditional, locally-installed desktop with local storage of user files to get their job done.[3]

HYPERVISOR VULNERABILITY

The hypervisor has the disadvantage of being potentially attacked in one of two ways, from either the network layer or from the host running on that hypervisor.[4]

The default behaviour of a hypervisor on a network is to respond to connections through standard TCP/IP, much the same as other desktop machines, devices and infrastructure. This results in the hypervisor being



» Shodan search reveals 662 eSXI hypervisors that are vulnerable to guest-host exploitation, connecting to the IP's brought up VMWare ESXi welcome pages.

locatable on the network and consequently susceptible to traditional network enumeration attacks. While enumeration tools are primarily used as a discovery mechanism, they are often able to extract further information about a system by analysing characteristics and information returned by the host. [5]

An example of this technique using the currently most utilised enumeration software (Nmap), which compares the host's packet response against a large database of software. With the response from Nmap an attacker is able to identify attributes such as patch levels and service packs.

Depending on the software that is found, using these approaches the attacker is then able to determine the appropriate CVE (Common Vulnerabilities and Exposures) that the host may be vulnerable to. After the vulnerabilities have been identified, the attacker is able to exploit the system using the exploit and insert a payload to further control the host and maintain access. Current examples of software that can be used to exploit systems and insert malicious payloads are Metasploit (Metasploit, 2012) and CORE Impact (Core Security, 2012). [6]

It is the second method used to attack the hypervisor from the guest or virtual machine that is even more dangerous and an unfamiliar concept, especially for companies invested in the cloud computing or hosting servers in large datacentres.

The term virtual machine (VM) escape is the concept of breaking out of an isolated VM in order to execute malicious code on the host. While the danger of 'Type 2' hypervisor escape is still a threat, the implications of breaking out of a guest, running on an enterprise 'Type 1' hypervisor such as ESXi or the Xen hypervisor would be much greater due to the environments that they are often employed in. [7]

In traditional networks, security can often be achieved through the segmentation of networks into either physical or virtual networks. This segmentation is still applicable within virtual networks; however this only offers security at the network layer, rather than this new layer of 'guest–host' exploitation. While this might sound like an unlikely threat, due to HA features found in VMMM such as VMware's DRS (Distributed Resource Scheduler) the movement of machines across hypervisors is determined by the management server rather than by a human. [8]

Challenges posed by VDI

Every VDI problem has a solution. But the solution is either give up something or pay more.

DATA CENTRE DENSITY

There's no getting around the fact that VDI is a resource hog in the data center. As the density of VDI racks and appliances continues to go up, so does the underlying need for power, cooling and network capacity in the data center. [9]

Implementing resource-intensive services such as VDI is really about chasing data center bottlenecks until you have some marginal balance between cost and performance. If the data center network connection to the Internet is a VDI bottleneck, you can always install 20 or 50 or 100 redundant Internet links, but that will likely cost more than the entire VDI project.[10]

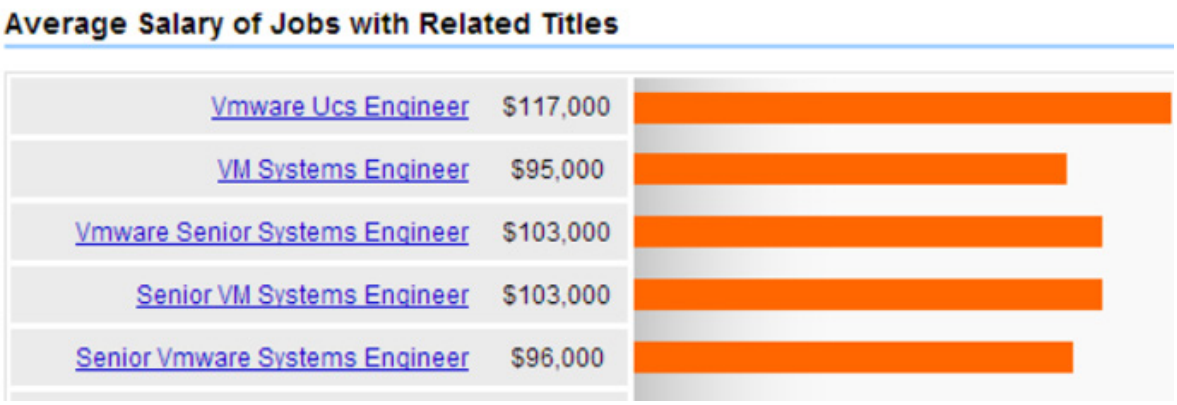
STORAGE HARDWARE

The type, location and performance of storage also affect desktop and application downtime. It's great to be able to centralize the storage of user data, but there is a big gotcha in using SAN or other network-attached mass storage devices for VDI: disk I/O latency. That's because operating systems read and write data to disk on a regular basis, even when the desktop appears to be idle.

As the user loads a new application or performs work in an open one, the amount and frequency of reading and writing to the disk storage can put a considerable burden on the network and storage arrays. Data read-ahead algorithms and disk buffering can typically keep up with read requests from virtual desktops, but writing to disk often involves a physical disk head touching a spinning disk platter in order to store the data. [11]

SOFTWARE

These tend to be the same issues that you get on a desktop PC: An application starts to use a lot of CPU or memory, and the desktop becomes unresponsive. The big difference is, with a VDI deployment, that affects the user's ability to see the desktop because the remote display protocol gets starved of CPU, with a desktop PC if an application saturates one CPU core, there's multiple other cores available. [12]



» *Indeed search for VDI salaries in Toronto, Ontario in USD as of Mar 27, 2015*

ADMIN CHALLENGES

VDI admins require a different skillset than traditional administrators because VDI is totally dependent on a tightly-integrated set of infrastructure technology and services. As your company considers transitioning to a VDI environment, your network, server, application and storage admins absolutely must work in unison for VDI to work as designed.

You can always hire someone with the requisite VDI admin expertise, right? In an ideal world, companies implementing VDI would simply search the vast pool of available IT talent for someone with VDI expertise, but VDI is still new enough that finding the right person can be expensive and exasperating.

The laws of supply and demand will likely keep salaries for VDI admins elevated for the foreseeable future. [13]

You can always hire someone with the requisite VDI admin expertise, right? In an ideal world, companies implementing VDI would simply search the vast pool of available IT talent for someone with VDI expertise, but VDI is still new enough that finding the right person can be expensive and exasperating.

CONSISTENT SPEND

One of the first advantages of VDI that pundits and vendors touted was that it can save companies money in much the same way that virtualizing servers has become a cost-saving standard. But the equation turns out to be quite different in the VDI world. Back-end infrastructure must be fully redundant, expandable and fault tolerant. That can be an expensive proposition, depending on how many end users you support.

If you pay $800 per physical desktop, then you can probably get a virtual desktop for about the same. Purchasing physical PCs is a pay-as-you-go investment, however. You can say the same about virtual desktop licenses, but an organization typically has to invest in hypervisors, connection brokers, load balancers, storage and more before it can deploy the first virtual desktop. [14] Quantifying these numbers, a Microsoft study showed that "VDI reduces hardware costs by 32% but increases software costs by 64% canceling any savings."

The study reported the additional licensing costs as "Additional licensing costs associated with virtualization, management and desktop software from VMware and Microsoft®."[14]

Jentu - The VDI Alternative

Server Based Hard Drive Provisioning with Centralized Desktop Management

An alternative with all of the benefits

All of the benefits of an expensive VDI solution without the significant challenges that come with VDI and at a fraction of the cost.

JENTU IS DISK BLOCK "STREAMING" WHERE YOU TAKE THE HARD DRIVE OUT OF A COMPUTER, DO A PXE BOOT, AND IT CONNECTS TO A CENTRAL IMAGE WHICH IS RUN LOCALLY ON THE DESKTOP. YOU GET BARE METAL (I.E. NO HYPERVISOR) PERFORMANCE ON YOUR DESKTOP, AND WITH 100MB OR 1GB NETWORKS AND A BUNCH OF DRIVES AND CACHE IN YOUR SERVER, YOU CAN ACTUALLY GET BETTER PERFORMANCE THAN A LOCAL DISK.

The real advantage though is the central management, security, and the ease of reverting back to a stable state (or swapping out an image) just by rebooting the desktop.

LATENCY FREE

Jentu uses the local machine to handle all processing. Software runs the way it's supposed to. You never have to worry about starving the CPU as a result of virtualization. As such, Jentu also does not use any sort of Hypervisor.

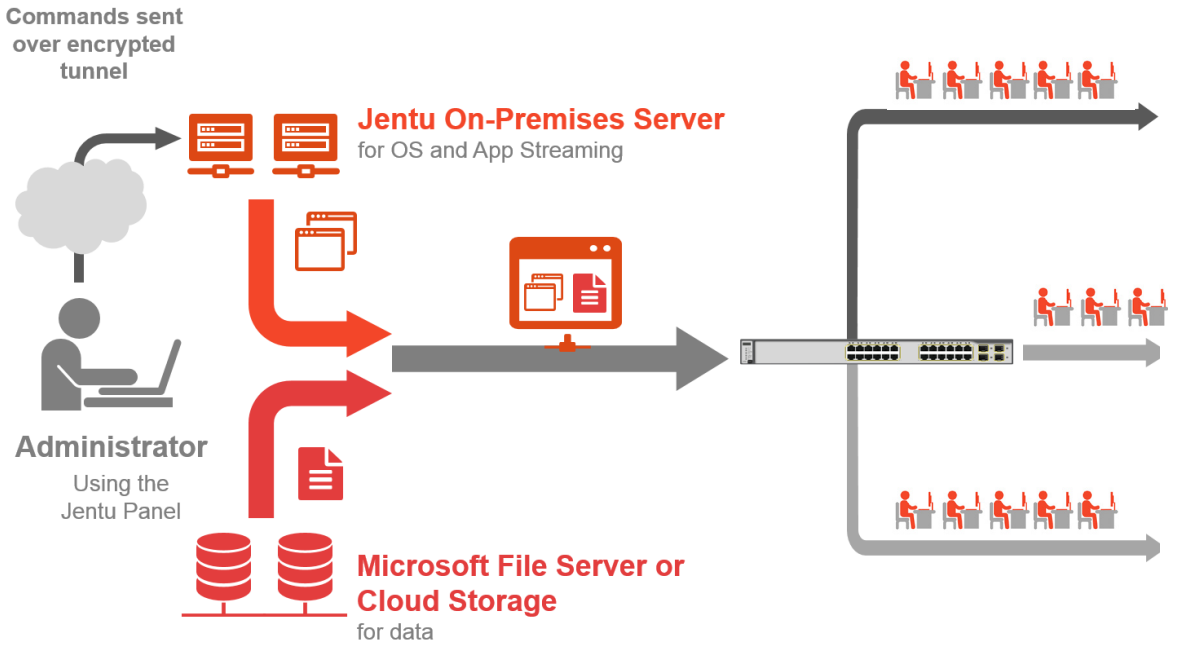
Jentu uses the local machine to handle all processing. Software runs the way it's supposed to. You never have to worry about starving the CPU as a result of virtualization. As such, Jentu also does not use any sort of Hypervisor.

To truly appreciate the performance capabilities of Jentu, a benchmark test was run. The amount of work performed by the benchmarking utility is equivalent to 6 different workstations doing 8 persons worth of extremely intense (32 transactions per IO) workload across a single 1Gb link, using very random data.

Software performs even better than natural hard drive performance. During the benchmark test, the hard drive booted workstation experienced very high latency, peaking at 1800ms and an average of 400-500ms response time leading to stalls and stuttering. It's notable that this latency is around 430ms greater than the desired 20ms maximum. On the other hand, Jentu's hard drive-free machines were latency-free, never spiking above 20ms response time with an average of 7ms (millisecond) during peak load. Without running the benchmark, servers have an average .022 ms response time with 30 active workstations during real office day operations.

All results show that Jentu diskless workstations experience far greater performance than virtualized systems. This allows administrators to implement Jentu for large groups of workstations without compromising user experience.

In the past, the only way to maintain pristine operating environments centrally has been through virtualization, which has added cost and exceptionally



» *Jentu Architecture*

complex server requirements, oftentimes still, user experience suffers and productivity drops because underlying subsystems in the centralized virtual PC structure will always be limited by the overall performance of the one server, which may still suffer contention and bottlenecks in different software systems.

By design, Jentu has avoided all of these issues by choosing an elastic storage infrastructure, keeping all processing distributed across workstation nodes, resulting in zero-load servers (even during peak loads).

With no Hypervisor on the server and no Hard Drive at the end point malware has a hard time finding anywhere to establish a breach. With reboot to restore any unauthorized changes to the OS are eliminated upon each boot.

ENHANCED SECURITY

Jentu allows administrators to mark an entire group of workstations as locked or unlocked. When locked, a user may refresh their own operating system by merely rebooting. All OS changes are reverted, and folder redirection keeps documents safe on your own data server. A side-effect of this is security, as any unauthorized changes to the OS are eliminated upon each boot.

Jentu has three distinct communication paths, which can be easily monitored and maintained using standard network tools:

Panel to Server communications occur through an SSH tunnel that originates from your server automatically during boot-up.

By default, an SSH public key is generated during the server install, and is stored in a tunnel endpoint server. An existing SSH+VPN tunnel infrastructure can also be used.

Alternatively, the server can be directly exposed to the web to avoid tunnels or VPN, and use a standard firewall to deny public access to the RPC structure.

An alternative with all of the benefits

All of the benefits of an expensive VDI solution without the significant challenges that come with VDI and at a fraction of the cost.

Server to Panel communications occur through a standard HTTPS connection every time a workstation boots up on your network.

- Checks for new configuration details at the panel during each boot-up and saves it locally
- Local settings cache allows for continuous operation without internet access once all settings are finalized and transferred

Workstation to Server

- DHCP connection to retrieve temporary IP address, which terminates early. DHCP doesn't need to be provided by the Jentu server, but this is the default mode of operation
- TFTP connection to download JentuPXE bootloader binary, which also terminates early
- HTTP connection to local Jentu server which discards the DHCP address and assigns a static IP according to the machine's configuration in the panel
- iSCSI connection to the local Jentu server. This connection must be maintained, whether it is through ethernet or on a wifi bridged virtual machine.

Jentu does not interfere with external intrusion detection systems such as snort, which keep track of local network devices and alert administrators upon changes. In addition, Jentu's SSH tunnel (Panel -> Server) and HTTP connection (Server -> Panel) are not required to run constantly.

Jentu does not interfere with external intrusion detection systems such as snort, which keep track of local network devices and alert administrators upon changes. In addition, Jentu's SSH tunnel (Panel -> Server) and HTTP connection (Server -> Panel) are not required to run constantly. A Jentu network administrator could disable either connection and the system would continue to run allowing total control of security.

LOWER TOTAL COST OF OWNERSHIP vs VDI

As Jentu does not require the significant up front investment that VDI requires it also does not require a specific type of education. A network administrator can be easily trained to be a Jentu professional. As Jentu uses regular software licenses there's no need to invest in costly virtual licenses for the entire enterprise. Without hard drives at the stations machines have a significantly extended lifespan (double that of a traditonal desktop with an HDD). As a result of using Jentu an MSP saw a 90% reduction in desk side support calls resulting in significant savings for both the client and the MSP.

Works Cited

[1] http://searchvirtualdesktop.techtarget.com/tip/Eliminating-VDI-network-bottlenecks-and-latency-issues

[2] *ibid*

[3] http://searchvirtualdesktop.techtarget.com/tip/Top-seven-most-griped-about-VDI-challenges

[4] https://johncouzins.wordpress.com/2013/11/27/attacking-the-hypervisor/

[5] *ibid*

[6] *ibid*

[7] *ibid*

[8] *ibid*

[9] http://searchvirtualdesktop.techtarget.com/tip/Top-seven-most-griped-about-VDI-challenges

[10] *ibid*

[11] http://searchvirtualdesktop.techtarget.com/tip/Top-5-causes-of-virtual-desktop-and-application-downtime

[12] http://searchvirtualdesktop.techtarget.com/tip/QA-How-to-troubleshoot-common-VDI-problems

[13] http://searchvirtualdesktop.techtarget.com/tip/Top-seven-most-griped-about-VDI-challenges

[14] http://www.brianmadden.com/blogs/brianmadden/archive/2010/11/19/microsoft-tco-study-vdi-is-11-more-expensive-than-traditional-pcs.aspx

JENTU TECHNOLOGIES
WWW.JENTU.CA