



White Paper
Intel Information Technology
Computer Manufacturing
Client Virtualization

Virtualizing the Client PC: A Proof of Concept

To determine whether virtualizing client PC operating systems could lower total cost of ownership (TCO) while offering users more flexibility, Intel IT conducted a client virtualization proof of concept (PoC). We found that client virtualization could reduce TCO by streamlining PC client builds. Concerns included performance, security, and data migration. These issues may be resolved as client virtualization technology matures and faster processors with hardware-assisted virtualization technology become available.

Julian Braham, John Dunlop, Michael Flores, Efi Kaufman, and Daniel Shukrun, Intel Corporation

July 2008

IT@Intel

Executive Summary

To determine whether virtualizing client PC operating systems could lower total cost of ownership (TCO) while offering users more flexibility, Intel IT conducted a client virtualization proof of concept (PoC) in late 2007.

Intel's traditional rich-client architecture delivers a full suite of powerful user applications. However, the PC build process is time-consuming, and the tight integration between applications, OS, and hardware inhibits change and limits user choice and flexibility.

To determine whether we could streamline the build process and provide a viable virtualized solution, we created a PoC virtualized client environment and delivered it to users. We used PC-based hypervisor software, along with management software to address potential manageability, security, and integration issues.

- We deployed the environment on DVD to 13 users, who completed the installation themselves.
- We found that client virtualization could potentially reduce TCO because fewer resources would be required for PC builds.
- Concerns included performance, security, application installation, and data migration.

Existing concerns may be resolved as virtualization technology matures. Key developments include hypervisors expected to deliver near-native performance as they begin to take advantage of faster processors with Intel® Virtualization Technology (Intel® VT). These developments may enable enterprises to reap the benefits of client virtualization, reducing client PC TCO while providing users with a greater choice of platforms and applications.

We found that client virtualization could potentially reduce TCO because fewer resources would be required for PC builds

Contents

Executive Summary	2
Business Challenge	3
Proof of Concept	5
Improving the Build Process.....	5
Virtual Environment Design Goals.....	5
Solution.....	6
Delivering the PoC Environment.....	7
Results and Analysis.....	8
Conclusion	10
Authors	11
Contributors	11
Acronyms	11

Business Challenge

Intel IT client PC architecture has evolved over time without fundamentally changing. It is a classic rich-client architecture with a tightly coupled solution stack based on Microsoft Windows*, as shown in Figure 1.

This PC platform delivers a powerful set of enterprise, line-of-business, productivity, and collaboration applications to our users. Over the years, Intel IT has streamlined the process of creating builds and provisioning PCs with this solution stack, reducing client total cost of ownership (TCO) as a result.

However, the current architecture limits our ability to realize further savings. It also limits our ability to meet business and user demands for greater functionality, personalization, and flexibility at lower cost.

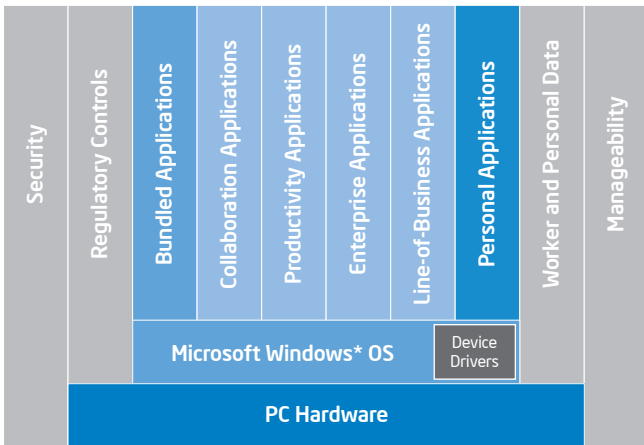


Figure 1. Current Intel rich-client PC architecture.

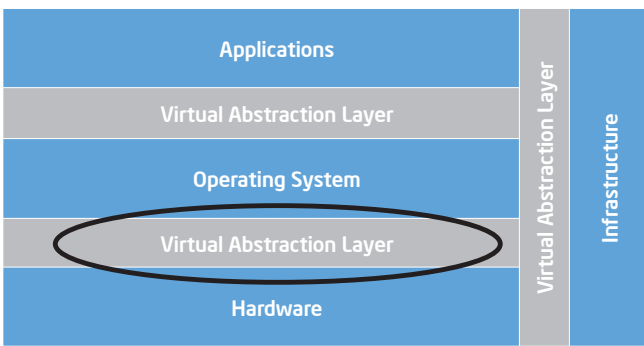


Figure 2. OS virtualization abstracts the client IT environment from the hardware.

Many applications and services are tightly coupled to the OS, and the OS is tightly coupled to the hardware platform. This makes it difficult and costly to change or upgrade the platform. The effect is to inhibit change and limit user choice. Cost pressures and security considerations are forcing Intel IT to exert even more control over the client platform. However, users want the same widely available capabilities, such as Internet phone applications, that they have on their PCs at home.

Though we have streamlined our traditional client build process, it is still complex and time-consuming. We create builds consisting of a package of hardware, OS, drivers, services, and applications. In order to maximize reuse, we design each build to work on all IT-supported desktop and laptop computers. Developing the builds includes lengthy engineering, quality assurance (QA), and certification processes. Intel IT specialists need to be involved in provisioning every client PC and deploying it to users.

In 2007, we began exploring a new way to reduce TCO while providing users with greater flexibility. We identified virtualization as a key technology that could help us achieve these goals by allowing us to abstract the client IT environment from the hardware platform.

We determined that the most potentially compelling, disruptive yet achievable approach was to focus on OS virtualization (see Figure 2). We could create a virtualized IT client environment based on a virtualized OS. Ideally, we would quickly deploy this within a virtual machine (VM) onto any capable off-the-shelf client PC. This would provide a more loosely coupled, flexible platform, potentially letting us introduce and upgrade capabilities more quickly.

We decided to undertake a proof of concept (PoC) study to examine the viability of this approach.

Proof of Concept

Our fundamental goal was to determine whether we could reduce client TCO by reducing the cost, complexity, and time required for the build process. We also wanted to analyze the usability and performance of the virtualized client, as well as security and other potential issues.

Improving the Build Process

Today, our build process consists of a set of chained scripts that provision the PC, preparing it for data migration and user personalization. The scripts first identify the platform model type, then provision the BIOS, Microsoft Windows OS, and platform drivers. The next step is the installation of security, manageability, and connectivity applications and services. Finally, we install core and business-specific applications. The build process also sets the machine name and joins it to Intel's centralized directory service.

This complex and platform-dependent process requires an IT technician and involves multiple machine shutdowns and restarts.

We perform additional engineering and QA tasks each time we introduce a new type of PC platform into our environment. Our engineers configure and customize the OS services and parameters so that we can use the same build on all our client platforms. Then we perform QA tests to validate that the new build functions on all these platforms.

In summary, we perform the following steps for each new type of hardware platform:

1. We obtain the PC platform from the hardware manufacturer.
2. We verify the new platform's specifications and features.
3. The platform is handed over to our engineering team.
4. Engineers install the most recent known build on the new platform, record all issues and deviations, and then resolve any issues.
5. Our QA team tests the new platform. The QA team may test and return the platform to the engineering team several times before all issues are fixed.
6. Our PC services team takes over the new platform and the build for large-scale deployment.
7. The PC services team deploys the new platform build, transferring each user's data and personal settings to the new machine.
8. The PC services team delivers the platform to the user.
9. The user provisions any additional software and refines personal settings.

In our PoC, we set out to determine whether client PC virtualization could reduce the process to just steps 1, 2, 8, and 9. This could substantially reduce the cost, complexity, and time needed to deploy new platforms.

Virtual Environment Design Goals

We wanted a solution that provided a secured and manageable virtual IT environment and supported other specific design goals, including:

- **Separate IT and personal environments on the same PC platform.** We wanted to run two environments on one physical platform. One would be our manageable, secure, virtualized IT environment. The other would be the user's personal environment; this would be unmanaged, and the user would be free to run any personal applications.

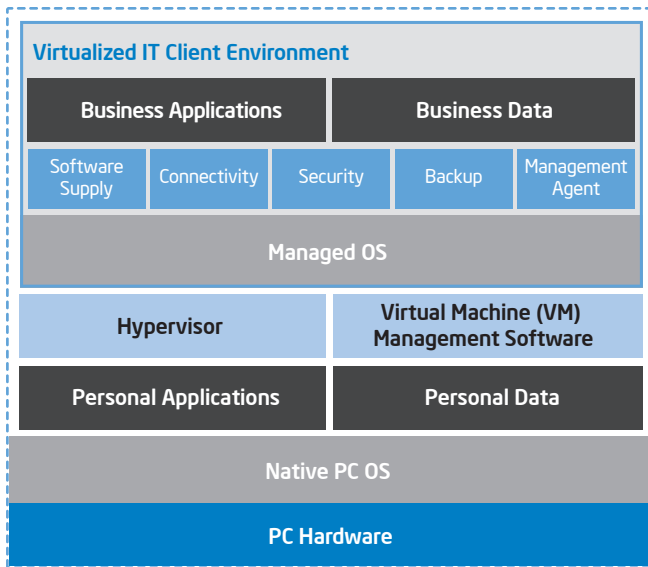


Figure 3. PC running a virtualized client.

- **User acceptance and experience.** A virtualized client environment needs to be acceptable to users and meet defined human factors engineering (HFE) criteria.
- **Allow policy differentiation.** We needed to be able to set different policies for the managed and the unmanaged environments.
- **Reduce build customization.** We wanted to support different client builds and platforms.
- **Portability and mobility.** The solution needed to run on a variety of platforms and OSs.

Solution

We selected software from two suppliers to implement our solution.

We used a hypervisor software product from an established virtualization software supplier to create virtual client builds and free hypervisor software from the same vendor to run each virtualized client. Like most available products, our hypervisor used Type 2 virtualization, in which the hypervisor runs as a service on an existing OS, rather than Type 1 virtualization, in which the hypervisor runs directly on the hardware.

We added management products from a second supplier to manage our virtualized environment and create an integrated user interface. We used the VM desktop management software to manage build images, ease provisioning, enforce policies, integrate the client with our corporate directory, change configuration settings, create VM templates, and install applications. Our solution is shown in Figure 3.

Key Features

Our solution attempted to address several key concerns about client virtualization including VM encryption, manageability, connectivity, and usability.

VM encryption

With virtualization, the IT environment no longer runs on dedicated hardware; instead, it exists as a virtual client image that shares a system with other applications. To provide additional protection for the client environment, our desktop management software encrypts the VM using strong encryption based on the Advanced Encryption Standard (AES) algorithm.

Manageability

Deploying desktop virtualization to Intel's large user population would require strong manageability. Potentially, we might deploy and manage tens of thousands of client VMs. Our selected desktop virtualization management software supported this goal by

using a centralized server to provision policies, configurations, and security features for each VM, as well as controlling access permissions and authentication using our corporate directory.

This also could help deliver customized IT environments for different business groups within Intel. Our management software has the ability to provision different VMs to different users, based on groups defined within our directory.

Connectivity

With Type 2 desktop virtualization, the VM can potentially connect to the network in two different modes:

- **Bridged mode.** The VM is a network entity at the same level as the host. The VM sets up a virtual switch and, using the host's physical network interface card (NIC), negotiates an Internet Protocol (IP) address from the physical network infrastructure.
- **Network address translation (NAT) mode.** In this mode, the VM sets up a private network and allocates an IP address for the host and for itself from the private network. The VM uses a virtual switch to route all its traffic to the host through the host's private IP address. The host then routes the traffic to the Internet.

We used NAT mode because of our wireless networking requirements. Intel IT is enabling all laptop clients to connect wirelessly to the enterprise network within Intel facilities using 802.1x authentication. Our hypervisor software does not currently support the ability to manage wireless access profiles from the virtualized client environment, so wireless connection and authentication must take place through the host. This required us to choose NAT mode, which routes all traffic through the host.

To enable remote access, we installed virtual private network (VPN) client software in the virtualized environment. When the host connected to the Internet, the VPN client established a secure connection that provided intranet access only from within the virtualized environment.

The disadvantage of using NAT and VPN is that packets are encapsulated as they traverse the different network layers; as a result, we anticipated performance degradation.

Usability

To ease user adoption, we looked for a solution with an intuitive user interface. With the classic model of implementing a hypervisor, the user toggles between two isolated and independent desktops. To create a more intuitive interface, we used our desktop management software to integrate the two desktops into one.

Delivering the PoC Environment

Thirteen users participated in the PoC, which was conducted in late 2007. We initially selected users from within Intel IT after interviewing them and explaining the program's goals. Then we added users from other organizations within Intel to obtain a cross-section of different users and application use cases. This resulted in a diverse mix of users with differing levels of computing expertise—some were very experienced IT professionals, while others had much less computing knowledge.

We provided each user with a new client machine. We copied the virtual client image setup files onto each system in order to accelerate the installation process. This also ensured that each client contained a backup copy of the virtual image, in case the user needed to re-run the virtual image installation process in the future.

Users performed the rest of the installation process themselves. We provided the new systems to users along with a user guide to help them perform the installation as well as post-installation activities such as migrating data, installing applications, and connecting to printers. We also scheduled training sessions with users after they received the machines, to help them overcome any issues encountered during the install process and to identify ways that we could improve the system delivery process in the future.

Results and Analysis

We analyzed the virtualized client environment from several perspectives. We analyzed how improving the build process could deliver business value by reducing client TCO. We measured user satisfaction by surveying PoC participants and conducted tests to measure the performance of the environment.

Business Value

We estimate that client virtualization could substantially reduce costs by streamlining build preparation and client provisioning. We analyzed this potential cost reduction based on the steps we could eliminate in the build process and by using resource estimates from Intel engineering and PC services groups.

Because client virtualization could reduce the need to customize builds for each hardware platform, we estimated that we could potentially reduce engineering resources required for each new platform by 33 percent. We also assumed a 24 percent reduction in the resources required for provisioning each client.

In our analysis, these benefits more than offset additional costs associated with the virtualized environment. We assumed that users' client platforms would use free client hypervisor software, but we assumed a management software license cost of about USD 75 per user. This figure will vary depending on the product and the IT organization; our estimate is conservative because we anticipate that in the future, some management capabilities may be provided at lower cost or free to companies with existing enterprise licensing agreements.

Based on this analysis, client virtualization could result in a 19 percent increase in cash flow over five years, compared with our current approach to client build preparation and provisioning.

User Experiences

To analyze users' experiences with client virtualization, we surveyed seven PoC participants

at the end of the study. We combined the survey data with feedback the participants had previously given during the study.

System deployment and data migration

Most participants reported no issues with delivery of the systems. However, most experienced some problems migrating data to the virtualized systems, and three were not able to migrate all of their data. Participants also reported software and OS installation issues, including slow installs.

We believe that to deploy virtualization successfully, additional engineering work would be needed to automate these data migration and system setup tasks. Intel IT has developed a mature process for data migration in our traditional non-virtualized client environment, and that has raised users' expectations. Users' comments indicated that we might be able to resolve installation issues by clarifying expectations or improving communication. This could help users understand that configuring and installing software in a VM model requires different processes.

Everyday use

Participants actively used the systems during the study—26.3 hours per week on average. They liked the ability to install non-work applications on their systems. One user felt that being able to install a personal version of an Internet phone application was the biggest benefit of the system.

This highlight should be considered when evaluating the model as a whole. Users can introduce risk by installing software that is not compliant with IT security policy; however, if they are prevented from installing software, they may not be as excited about moving to the new type of platform.

Performance was an issue. Users have expectations that a new system will perform as well as their existing system. Six participants were "neutral" to "not satisfied" with system performance, and five said they were "not satisfied" with the system overall.

When prompted for specific feedback, most participants said installing and subsequently finding applications were the biggest obstacles to their productivity. Other considerations were copying files, system slowness, reboots, system freezes, and network issues. Five users said these problems would critically affect their ability to perform their work when using the virtualized environment.

Other themes reported by users included poor training, system error messages, and confusion between the virtualized and personal environments on the platform.

Clearly, a deployment team would have to address these issues in order to successfully deploy client virtualization.

Performance Testing

We conducted two sets of performance tests. We performed the tests using laptops equipped with the Intel® Core™2 Duo Mobile Processor T7300 (2 GHz) with 2 GB RAM, 80 GB 5400 RPM hard disk, Mobile Intel® 965 Express Chipset, Intel® 82566 Gigabit Ethernet Controller, and Intel® Wireless WiFi Link 4965AG. The OS was Microsoft Windows XP*.

Results, shown in Figure 4, confirmed the performance issues identified by users.

File transfer

We compared file transfer speeds using two identically configured laptop PCs connected by a switch to a standard Intel IT server. One PC ran only the native environment; the other ran our virtualized environment. Each downloaded a 500 MB file from the server. We repeated the test more than 100 times, within multiple LAN zones and at different times of day. We compared the average time that each laptop needed to complete the transfer. The file transfer took 66 percent longer in the virtualized environment compared with native Microsoft Windows XP.

Productivity software

We created a test representing typical user activities. It included opening a suite of typical office productivity software and a Web browser, manipulating a table in a document, performing spreadsheet calculations, and shutting down the system. It took about 66 percent longer to complete the task in the virtualized environment compared with the native environment.

Design Challenges

While designing the PoC, we encountered several challenges that we would need to resolve or mitigate before deploying client virtualization in a production environment.

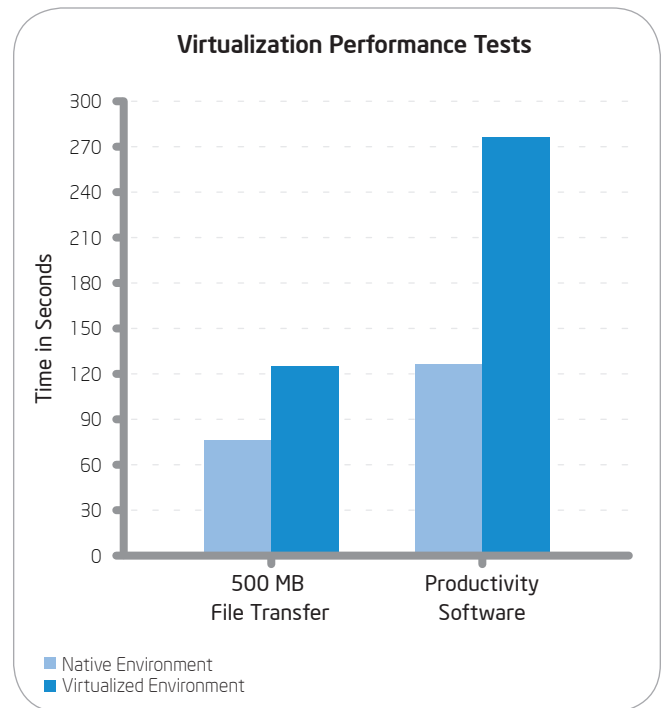


Figure 4. Results of virtualization performance tests.

Security

At about the same time we started exploring our desktop virtualization PoC, Intel's information security group began an analysis of potential virtualization security issues. The analysis showed that compromise of hypervisors, host OSs, or management software could expose our enterprise network to risk. The group stated that systems must be protected against the aggregate risks of all VMs installed on the physical system.

Because we needed to comply with this policy, we could not evaluate a managed virtualized client running on a system that was not an Intel-managed PC. However, we did develop a script to help ensure that the host OS complied with Intel security standards, including domain membership, security compliance agent, and personal firewall and anti-virus applications.

OEM builds

Our solution's cost model is based partly on an assumption that the virtualized environment can run on any hardware platform and manufacturer-supplied Microsoft Windows OS. We would not need to provide an Intel IT build customized for every platform. However, the OS and applications delivered by PC manufacturers typically did not meet Intel security requirements.

Double patching

Updating systems is the largest task for our manageability teams, as it is for most other IT organizations. This includes delivering security patches, OS updates, and application updates.

In our PoC, we ran two workspaces on one PC: the virtualized client and the host. From a manageability standpoint, we appeared to be running two separate platforms—each of which may have different security levels and security patch requirements.

This can lead to the problem of double patching. When we update to the two OSs on a machine, a patch may be installed twice—once on the host and once on the guest. This can negatively affect the user experience and decrease productivity.

One idea for avoiding this problem in the future could be a VM-aware patching capability. Once downloaded, each patch could scan all OSs on the same machine and update any OSs that require the patch. In this way, a patch would be downloaded only once.

Support for native peripherals

Our VM software was not able to recognize peripherals such as a trusted platform module (TPM) chip, a fingerprint reader, and peripherals connected to the platform using non-standard interfaces.

Conclusion

Our PoC showed that OS virtualization combined with a managed virtualized desktop could let us simplify the way we provision new desktop and laptop PCs for employees. This creates opportunities to reduce TCO and provide new systems more quickly.

However, we also found several issues due to that fact that the technology is still maturing. Core virtualization capabilities are not guaranteed to be hardware-platform agnostic, and it is still necessary to test platforms and applications to confirm that a virtualized environment will indeed run on multiple platforms.

Our solution included software for managing virtualized clients; however, because existing corporate manageability services do not yet comprehend virtualization, extensive work would be required to integrate a large number of virtual clients into the existing infrastructure. Virtualization is considered an emerging

information security threat; though we used products that include strong security, testing would be required to validate their capabilities.

We also found that not all users liked integration of host and guest workspaces into a single desktop; some found it confusing.

Performance was an issue for users. Several factors contributed to lower virtualization performance, including the computational overhead introduced by a Type 2 hypervisor; the fact that the hypervisor lacked support for Intel VT; the addition of desktop management software; and the need to run multiple enterprise agents to provide security and patching for both the host and guest OS.

New and anticipated products may address these performance concerns. For example, Type 1 hypervisors are expected to introduce significantly less overhead, run at near-native performance, and take advantage of Intel VT support included in faster processors.

As client virtualization technology matures, it may overcome the obstacles we encountered in this early client virtualization PoC. This will enable enterprises to deploy client virtualization to reduce TCO, provision client platforms more quickly, and provide users with additional choice and flexibility.

Authors

Julian Braham is a product engineer with Intel IT.

John Dunlop is an enterprise architect with Intel IT.

Michael Flores is a senior human factors engineer with Intel IT.

Efi Kaufman is a product engineer with Intel IT.

Daniel Shukrun is a program manager with Intel IT.

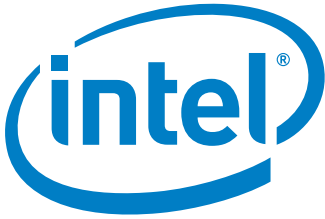
Contributors

Dvir Ben-Ari, Cheryl Mascaro, and Tomas McInerney, Intel IT

Acronyms

AES Advanced Encryption Standard
HFE human factors engineering
Intel® VT Intel® Virtualization Technology
IP Internet Protocol
NAT network address translation
NIC network interface card

PoC proof of concept
QA quality assurance
TCO total cost of ownership
TPM trusted platform module
VM virtual machine



www.intel.com/IT

Performance tests and ratings are measured using specific computer systems and / or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit www.intel.com/performance.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF


ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel, the Intel logo, Intel. Leap ahead. and Intel. Leap ahead. logo, and Intel Core are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2008 Intel Corporation. All rights reserved.

Printed in USA
0708/REM/KC/PDF

 Please Recycle
319837-001US