

Intel® Virtualization Technology and Intel® Active Management Technology in Retail Infrastructure

Enabling a Robust, Reliable and Manageable Retail Infrastructure
Solutions at Low Total Cost of Ownership (TCO)

White Paper

December 2006

Revision 1.0



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

The Intel® Virtualization Technology and Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2006, Intel Corporation. All rights reserved.



Contents

1	Executive Summary	6
2	Background.....	7
3	Intel® Virtualization Technology on Retail Infrastructure	8
3.1	Intel® Virtualization Technology Background	8
3.1.1	Virtualization Challenges on Software-only Virtualization.....	9
3.2	Intel® Virtualization Technology - Hardware Assisted Virtualization	10
3.2.1	Hardware Enhancement on VT-x.....	11
3.2.2	VMX Operations	11
3.3	Intel® Virtualization Technology in Retail Server	11
3.3.1	Workload Isolation	12
3.3.2	Workload Consolidation.....	12
3.3.3	Workload Migration.....	13
3.3.4	Security	14
4	Intel® Active Management Technology Usage in POS Clients.....	15
4.1	Intel® Active Management Technology Background	15
4.2	Intel® Active Management Technology POS Usage Model.....	15
4.2.1	Asset Management	15
4.2.2	Remote Operations.....	16
4.2.3	SOL/IDER.....	16
4.2.4	Alerting and Sensor Configuration.....	17
4.2.5	Event Filtering and Logging.....	17
4.2.6	Network Interface	17
4.2.7	Authentication	18
4.2.8	Provisioning.....	18
4.2.9	Privacy	19
5	Conclusion	20
6	References.....	21

Figures

Figure 1 Point of Sales System.....	7
Figure 2 Virtualized vs Non Virtualized Platforms	8
Figure 3 T-x Ring Transition Block Diagram.....	10
Figure 4 VT Generic Usage Model	12
Figure 5 Sample of Workload Consolidation on Intel® VT-Enabled Retail Server	13



Tables

Table 1. Virtualized vs Non Virtualized Platforms8



Revision History

Revision Number	Description	Revision Date
1.0	Initial release.	December 2006

§



1 Executive Summary

This document illustrates the usage model of Intel® Virtualization Technology (Intel® VT) and Intel® Active Management Technology (Intel® AMT) in Retail Infrastructure Point of Sales (POS) Systems. This whitepaper explains the key features of these technologies and provides practical usage models to enhance the present retail solutions to be more manageable, robust and reliable at a low Total Cost of Ownership (TCO).

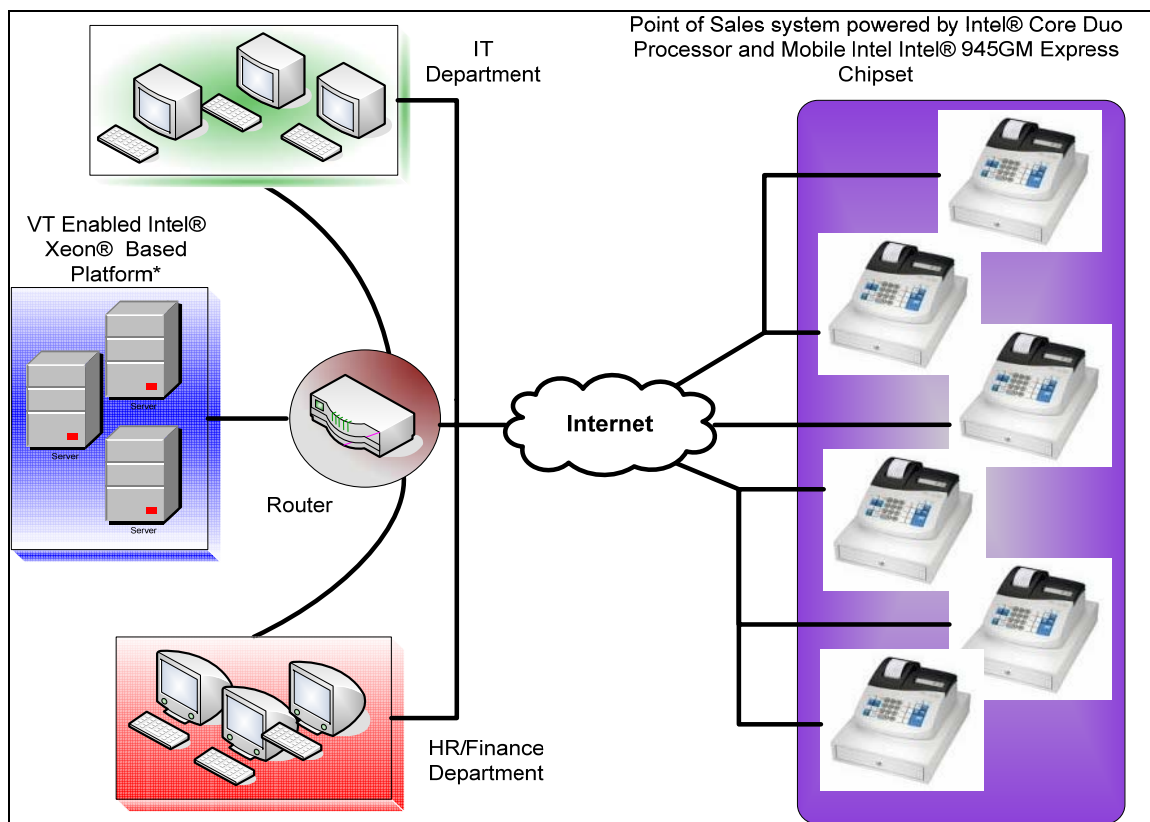


2 Background

A Retail Point of Sales (POS) system requires sophisticated information security and efficient data and asset management. A robust Operating System (OS) and executing environment is very important in the server environment, which is very important in the POS system. An intelligent network management is critical to manage a large and complicated client network. Intel® AMT helps the management console manage the activity of the client network out of band (OOB).

In addition, POS clients host many applications which could require multiple servers to provide network security, POS Database server, Customer Relationship Management Software and possibly even video streaming for advertisement. The advent of such requirements, coupled with the rising cost of operation, helped create the latest trend in server consolidation, virtualization technology.

Figure 1 Point of Sales System



- *NOTE: VT-x enabled Intel Processor for high performance platform:
- Dual Core Intel® Xeon® Processor LV and Intel® E7520 Platform
 - Dual Core Intel® Xeon® Processor 5100 series and Intel® 5000P Platform

3 Intel® Virtualization Technology on Retail Infrastructure

3.1 Intel® Virtualization Technology Background

Virtualization creates a level of abstraction between physical hardware and the OS that manages the computer processor(s) and other platform hardware.

Figure 2 Virtualized vs Non Virtualized Platforms

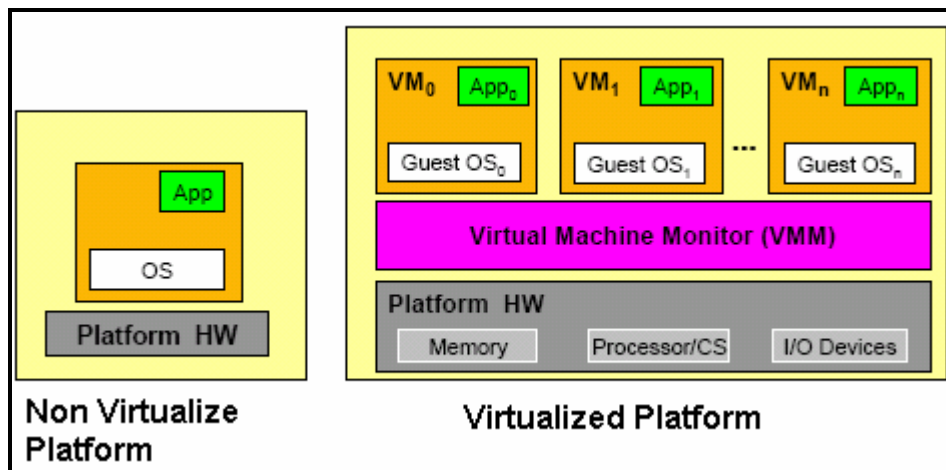


Table 1. Virtualized vs Non Virtualized Platforms

Non Virtualized Platform	Virtualized Platform
<ul style="list-style-type: none"> IA-32 architecture requires all software to run in one of the four privilege levels called “rings” OS typically runs on Ring0 – privileged access to the widest range of processor and platform resources Individual applications run in Ring3 – Limited privilege access to hardware resources 	<ul style="list-style-type: none"> The four privilege levels (rings) are still employed on VT platforms, but the VMM now runs on Ring 0 instead of an OS. Note that typically OS is programmed to run at Ring0 on a non virtualized environment. VMM runs in Ring0 and guest OS runs in Ring1 or Ring3.

Conceptually, without virtualization technology, a single operating system controls all hardware resources. Virtualization technology allows the VMM to present each guest OS a virtual machine (VM) environment that emulates the hardware environment



needed by the guest OS. Virtual-machine extensions define processor-level support for virtual machines on IA-32 processors. Two principal classes of software are supported under the virtual machine architecture:

- Virtual-machine monitor (VMM): A VMM acts as a host and has full control of the processor(s) and other platform hardware. VMM presents guest software with an abstraction of a virtual processor and allows it to execute directly on a logical processor. A VMM is able to retain selective control of processor resources, physical memory, interrupt management, and I/O.
- Guest software: Each virtual machine is a guest software environment that supports a stack consisting of the OS and application software. Each operates independently of other virtual machines and uses the same interface to processor(s), memory, storage, graphics, and I/O provided by a physical platform. The software stack acts as if it were running on a platform with no VMM. Software executing in a virtual machine must operate with reduced privilege so that the VMM can retain control of platform resources.

There are two options for software-only virtualization solution:

1. Runtime Modification of the guest OS: In this case the VMM monitors operation during runtime and takes control of the processor. When any of the 17 instructions controlling critical platform resources arises in the guest OS, the VMM manages the conflict and returns control to the guest OS.
2. Static modification on guest OS (Para-virtualization): In this case the guest OS is modified prior to runtime.

3.1.1 Virtualization Challenges on Software-only Virtualization

- When any of the 17 instructions controlling critical platform resource arises, but the OS is not running in Ring0, this could cause conflict resulting in system fault of wrong response.
- Runtime modification forces the VMM to provide complex workarounds during operations, which can impact performance and system reliability.
- Para-virtualization prevents VMM from hosting unmodified guest operating system
- Both runtime modification and para-virtualization require extensive software modification efforts from the VMM and the OS vendors. This increases the cost and complexity of IT support.

Today's virtualization solutions mainly involve virtual machines, which are implemented in software using techniques like ring compression and binary translation. This allows unmodified guest OS to run, at a slightly lower performance in the virtual machine. Para-virtualization requires changes to the guest operating system so it can surrender delicate system operations like page table memory and interrupt management to the VMM.



3.2 Intel® Virtualization Technology - Hardware Assisted Virtualization

Hardware support for processor virtualization enables system vendors to provide simple, robust, and reliable VMM software. VMM relies on hardware support to set policy and operational details for handling events, exceptions, and resources allocated to virtual machines. A hardware assisted processor must be able to avoid conflict caused by many guest operating systems running on top of the VMM software. This can be achieved if the processor can ensure that the VMM maintains control of critical platform resources and hands off limited control to each guest OS as appropriate. This efficiency and integrity of the hardware control switching between the VMM and guest OS are critical for optimal performance and reliability.

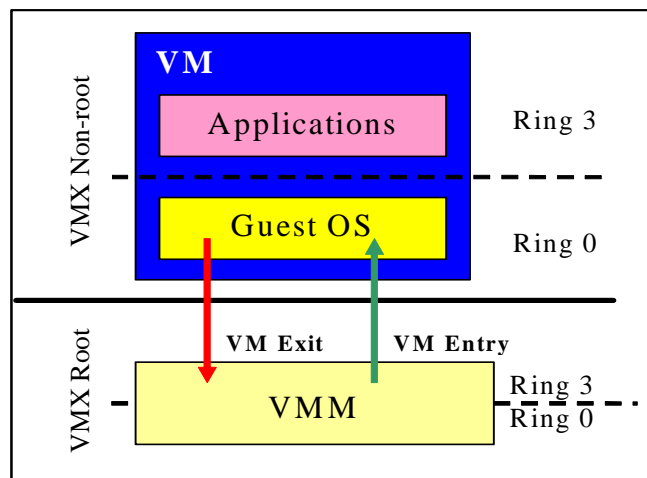
Intel® Virtualization Technology provides hardware support for IA-32 processor virtualization (VT-x) and directed IO virtualization (VT-d). VT-x consists of a set of virtual machine extensions (VMX) that support virtualization of processor hardware for multiple software environments using virtual machine. An equivalent virtualization technology to VT-x for Itanium processor architecture is defined and commonly referred to as VT-i. The scope of this whitepaper will focus solely on VT-x and will not cover VT-d and VT-i implementation.

A VMM written to take advantage of the Intel® Virtualization Technology runs the monitor in a new CPU mode called “VMX Root” mode and the guest OS in the “VMX Non-root” mode. The VMM will manage the virtual machines through the VM Exit and VM Entry mechanism.

Intel® Virtualization Technology is designed to enable high performance VMM without the need for para-virtualization changes or binary translation techniques. This enables the implementation of VMM that can support a broad range of unmodified guest operating systems.

VT-x introduces IA-32 architecture with two new forms of CPU operations: VMX root and VMX non-root operation. The following figure illustrates the software model for the VT-x architecture.

Figure 3 T-x Ring Transition Block Diagram





3.2.1 Hardware Enhancement on VT-x

1. Higher Privilege Ring for the VMM: This allows guest OS and applications to run on a reprioritized ring they were designed for, while ensuring VMM has privilege control over platform resources. This helps to eliminate potential conflicts, simplify VMM complexity and improve compatibility with unmodified operating systems.
2. Hardware based Transitions: Handoffs between the VMM and guest OS are supported in hardware, which reduces the need for complex software transitions.
3. Hardware based Memory Protection: Processor state details are retrained for the VMM and each guest OS in dedicated address spaces. This helps to accelerate transitions and ensure reliability of the process.

3.2.2 VMX Operations

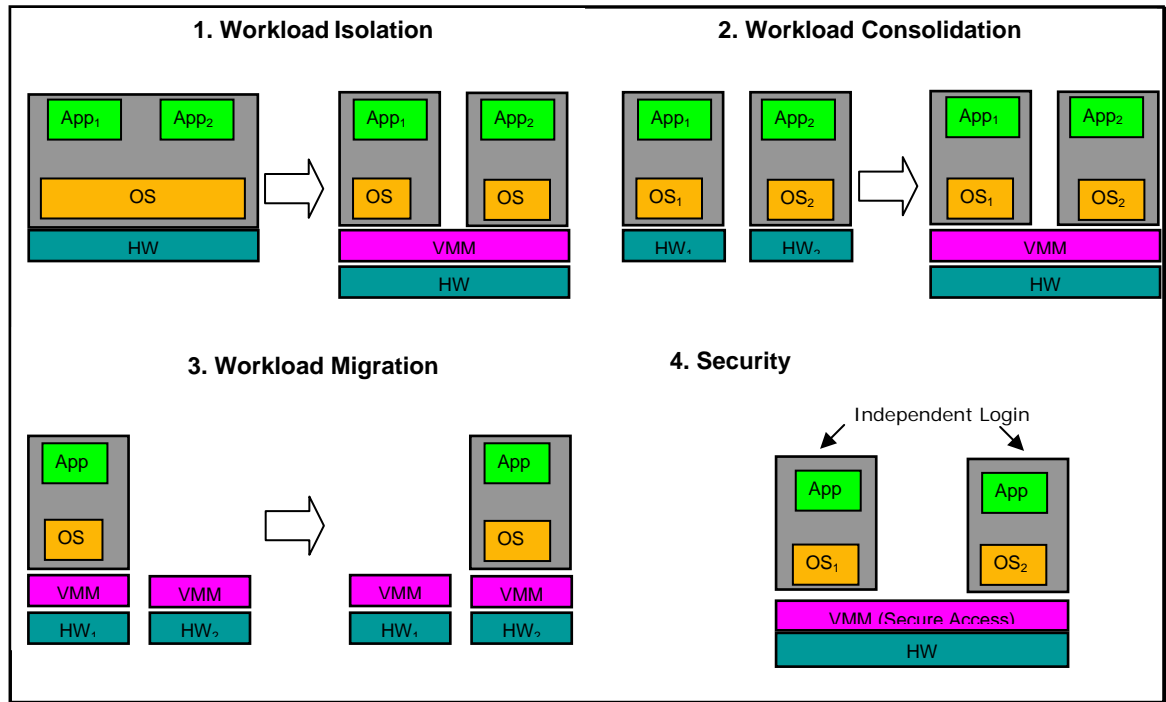
Processor support for virtualization is provided by a new form of processor operation called VMX operation. There are two kinds of VMX operation: VMX root operation and VMX non-root operation. In general, a VMM will run in VMX root operation and guest OS will run in VMX non-root operation. Transitions between VMX root operation and VMX non-root operation are called VMX transitions.

There are two kinds of VMX transitions. Transitions into VMX non-root operation are called VM entries. Transitions from VMX non-root operation to VMX root operation are called VM exits. Processor behavior in VMX root operation is very similar to its behavior outside VMX operation. The principal differences are that a set of new instructions (the VMX instructions) is available and that the values that can be loaded into certain control registers are limited. Processor behavior in VMX non-root operation is restricted and modified to facilitate virtualization. Instead of their ordinary operation, certain instructions (including the new VMCALL instruction) and events cause VM exits to the VMM. Because these VM exits replace ordinary behavior, the functionality of software in VMX non-root operation is limited. It is this limitation that allows the VMM to retain control of processor resources.

3.3 Intel® Virtualization Technology in Retail Server

There are various VT usage models which could be implemented to existing Retail Server to enhance the value proposition.

Figure 4 VT Generic Usage Model



3.3.1 Workload Isolation

Workload isolation implies that each VM is independent of the other. What this means is that:

- Each guest OS on the VMM could be used to host different operating systems and applications depending on their criticality and functionality. Customer Relationship Management software, Security Applications (such as Firewall, VPN etc) and POS Microsoft* SQL Server*, for instance, could be stored on separate guest OSes.
- Guest operating systems can also be replicated to provide failsafe functionality. For critical applications such as Retail POS database, downtime could translate into a showstopper. However, using VMs, if one VM with SQL Server application is down, the system could immediately switch to the second separate VM. The POS client could also be programmed to detect both proxy servers, since each VM has a unique IP address.

3.3.2 Workload Consolidation

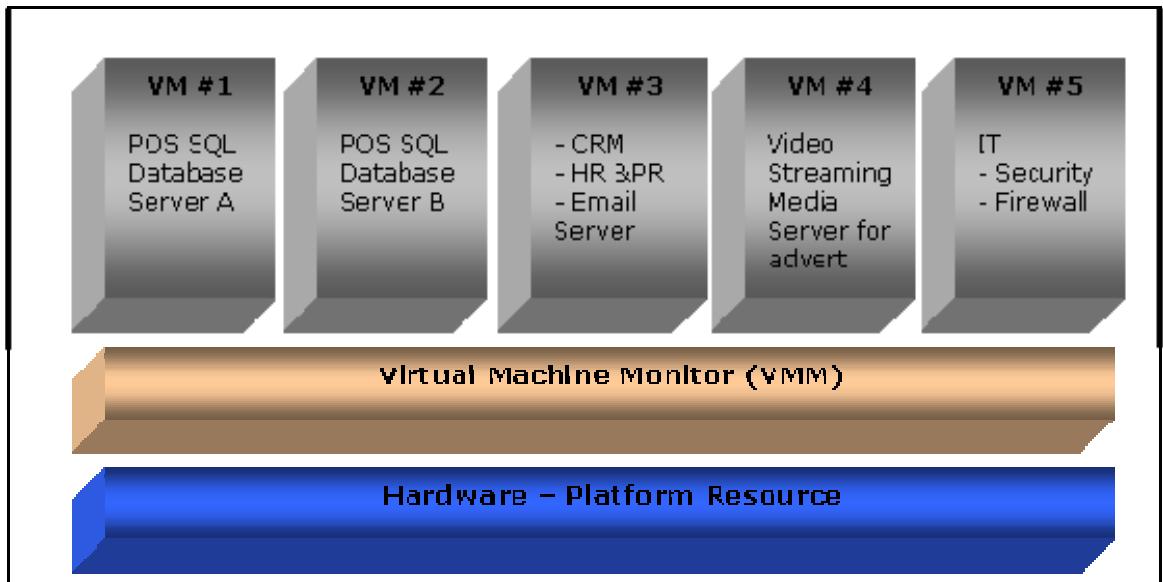
A few factors have driven the trend towards workload consolidation, primarily, the increasing cost of operations that comes with the higher number of servers required. This includes an increasing number people, space, power consumption and cooling solutions. Server consolidation is a key strategy for reducing these costs and today's virtualization software solutions make it easy to run multiple applications safely and securely on an Intel processor-based server. Companies are using virtualization software and associated management applications to:



- Manage and implement physical and VM resources efficiently from a common interface.
- Allocate server resources (CPU, memory and I/O) dynamically, and move running applications, workloads, and sessions very quickly from one VM to another. Initially this capability was used for zero-downtime maintenance. It is now beginning to be used as a method to automatically provision new capacity when a system fails or when the workloads threaten to exceed available resources.

Shown below are some of the applications that could be consolidated into a VT-enabled Intel® Xeon®-based platform:

Figure 4 Sample of Workload Consolidation on Intel® VT-Enabled Retail Server



- The Retail POS SQL database is replicated to provide automatic fail-over to the other VMM. The replicated server VMM can also be hosted on a separate platform. Other methods of utilizing the fail-over model is to ensure that the client can detect the IP address of VM #1 and VM # 2, and switch over to the healthy server if either server is down.
- Other VMs can be configured to host a variety of applications, such as Customer Relationship Management (CRM), human resource and payroll management(HRM & PRM), email server, firewall, and video streaming
- Media server can be hosted on a VM intended to stream video for advertisement at POS client or kiosk. This can be achieved by utilizing the dual independent display feature on Mobile Intel® 945GM Express Chipset on the POS system.

3.3.3 Workload Migration

Migrating VMs is akin to migrating an entire OS and all of its applications as one unit. This allows us to avoid many of the difficulties faced by process-level migration approaches. For instance, the narrow interface between a virtualized OS and the VMM makes it easy avoid the problem of dependencies in which the original host machine must remain available and network-accessible in order to service certain system calls or even memory accesses on behalf of migrated processes. With virtual machine



migration, on the other hand, the original platform that is hosting the VM may be shut down once migration has completed. This is particularly valuable when migration is occurring in order to allow maintenance of the original platform.

Migrating the virtual machine allows in-memory state to be transferred in a consistent and efficient fashion. This translates into a fast migration while the processes are still running on the operating system. This applies to kernel-internal state (for example, the TCP control block for a currently active connection) as well as application-level state, even when this is shared between multiple cooperating processes. In practical terms, for example, this means that it is possible to migrate an on-line advertisement via streaming media server without requiring clients to reconnect, using application level restart.

3.3.4 Security

Intel® Virtualization manages VMX transitions in hardware rather than software. This helps to strengthen the logical isolation of virtual partitions. Less complex VMMs also provide fewer opportunities for software based attacks.

In addition, each guest OS can be password protected separately, although they reside on the same VMM. This would be especially useful to prevent unauthorized access, since the consolidated server is shared between different functional groups in an organization.



4 Intel® Active Management Technology Usage in POS Clients

4.1 Intel® Active Management Technology Background

1. The Intel® AMT Agent provides a set of PC platform management capabilities and interfaces that work regardless of the operating system installed on the platform.
2. Intel AMT capabilities are fully available regardless of the hardware and OS states (S0-S5/H0-H5)
3. Intel AMT must be compatible with Preboot Execution Environment (PXE) Remote Boot Agent/BIOS. Intel AMT firmware must provide Alert Standard Format (ASF) Alert Device support to PXE Boot Agents. The Intel AMT firmware must not interface with PXE Boot Agent communication with a remote PXE Server.

4.2 Intel® Active Management Technology POS Usage Model

4.2.1 Asset Management

It is always a challenge to manage the client in a large Retail POS enterprise system. The system monitor always has a problem keeping track of all the assets of the POS client that are attached to the network in terms of hardware and software. The monitor would need to keep an updated inventory all the time, requiring additional manpower to manage it. Simultaneously, the system monitor would need to maintain software information about the clients attached to the network. This can only be done through periodic check on each client. Maintaining inventory and doing software audits are very time consuming and not always accurate. Intel® AMT can be used to solve these issues and provide a more sophisticated approach to tracking client inventory.

Intel® AMT keeps track of client information in the following manner:

1. Intel® AMT obtains asset information about media devices, Flash Recovery Utility (FRU), SMBIOS and ASF tables provided by the BIOS AMT module through the Keyboard Control Style (KCS) host interface. Intel® AMT stores asset information received from the BIOS in Non Volatile Memory (NVM) in the client and supports the operations mentioned below through OOB interface.
 - a. Enumerate Asset Types
 - b. Get Asset Data



- c. Remote Control – The remote control operations include Power-On, Power-Off, Reset, and Power-Cycle. Remote Control also accepts a Boot Options parameter describing actions for the BIOS to perform and boot source used by the BIOS.
 - d. Get Power State
2. Intel® AMT stores client system information, BIOS information, baseboard information, processor information, memory information, media information, and sensor information in NVM.

4.2.2 Remote Operations

Besides client asset management, the management console can use Intel® AMT for remote monitoring the client attached to the network without frequent desk visit. It helps to ease the time and manpower spent on health management of the POS client.

The management consoles can perform the following functions using Intel® AMT:

1. Change the system boot source with support of the BIOS to remote reboot the system.
2. Use remote control and diagnostic operations to do the following:
 - a. Return a value indicating the current system state of the client.
 - b. Set the current ASF Boot Option section.
 - c. Instruct the client to perform a hard power-on.
 - d. Instruct the client to perform a hard-reset.
 - e. Instruct the client to perform a hard power cycle.
 - f. Instruct the client to power-off.

Intel® AMT supports ASF remote control and Boot Option Control Signals.

4.2.3 SOL/IDER

Intel® Active Management Technology makes it possible to redirect serial and IDE communications from a managed client to a management console regardless of the boot and power state of the managed client. The client must have Intel® AMT capability, a connection to a power source and a network connection.

Serial-Over-LAN (SOL) is the ability to emulate serial port communication over a standard network connection. SOL can be used for most management applications where a local serial port connection would normally be required.

When an active SOL session is established between an Intel® AMT-enabled client and a management console using the Intel® AMT redirection library, the client's serial traffic is redirected through Intel® AMT over the LAN connection and made available to the management console. Similarly, the management console may send serial data over the LAN connection that appears to have come through the client's serial port.

In this case, the Retail POS management console may use the LAN connection to send commands or scripts through the LAN connection instead of manually modifying the client system. This reduces frequent desk visits to the client.

IDE Redirection (IDER) emulates an IDE floppy or CD drive over a standard network connection. IDER enables a management machine to attach one of its floppy or CD drives to a managed client over the network. Once an IDER session is established, the managed client can use the IDE device as if it were directly attached to one of its own IDE channels.



There is always the possibility of refreshing an unresponsive client system. This can be useful in the following scenario.

4.2.4 Alerting and Sensor Configuration

In a Retail Infrastructure POS system, the management console expects alerting from the client in order to respond on time. Intel® AMT handles the following signals:

1. System state signals, which help Intel® AMT to keep track of the current Advance Configuration and Power Interface (ACPI) state of the client.
2. Firmware progress and error signals.
3. Watchdog start and stop signals sent by the KCS driver through the host interface. If a watchdog expires, Intel® AMT sends an alert.
4. ASF sensor signals.
5. Polling and receiving events from the following sensors classes:
 - a. CPU sensor class
 - b. Temp sensor class
 - c. Volt sensor class
 - d. Fan sensor class
 - e. Intrusion class

The management console listens to and acts upon the following platform events with Intel® AMT:

- a. Environment event types, including CPU presence, CPU thermal, temperature, voltage, fan, chassis intrusion, etc.
- b. Firmware error event
- c. Firmware progress event
- d. System boot failure event
- e. OS event
- f. Power state event

4.2.5 Event Filtering and Logging

A Retail Infrastructure POS system monitor would like to keep track of all client events, so a mechanism in the network that will keep track of all the records is required. Intel® AMT provides the methods for filter and event log configuration available through the network interface and allows configuration of event filters through the OOB network interface to issue PET alerts or log for specific events.

Intel® AMT is capable of accepting up to 16 alert subscriptions and accepting up to a total of 16 event filters.

Clients with Intel® AMT enabled keep a log of events in non-volatile memory that can be queried remotely by a system management console. Each client maintains a log of at least the latest 256 entries.

1. Intel AMT maintains a set of overall event log parameters and enables access to them through the network interface.
2. Intel AMT event log stores events in records.

4.2.6 Network Interface

An Intel® AMT-enabled client executes an HTTP-based web service that provides both a user interface (HTML) and a programmatic interface Simple Object Access Protocol (SOAP). These interfaces allow remote access to system management events, data,



and controls provided from the Admin, Event manager, Asset manager, and Storage manager packages. The HTTP Server is compliant with HTTP/1.1 and provides supporting services for the Programmatic and User interfaces over the HTTP protocol. This includes support for HTTP basic authentication.

If SOAP is being used, the Intel® AMT client SOAP interfaces exonerating systems multiple management functions such as:

- a. Asset manager service
- b. Third party storage manager service
- c. Third party storage administrative service
- d. Event service
- e. Administrative service (Network administration, security administration, provisioning services)
- f. Remote control services

Intel® AMT supports the following web browsers:

- a. Microsoft* Internet Explorer* 6.0 SP1
- b. Mozilla* for Windows* 1.7
- c. Mozilla* Firefox* for Windows 1.0
- d. Mozilla* Firefox* for Linux* 1.0
- e. Netscape* 7.2 for Windows*

Intel® AMT Web User Interface provides direct user access to Intel AMT features via a standard Web browser. Interface includes the web pages described in the Intel Web UI specification.

4.2.7 Authentication

If a third party remote management application is used, it must authenticate its users using the HTTP Basic Authentication protocol if Intel® AMT is being used. The realms for HTTP basic authentication are:

- Intel® AMT Administrative Interface.
- Hardware Asset interface.
- Storage interface.
- Storage admin interface.
- Event manager interface.
- Remote control interface.

The third party data store, IDER, and SOL applications will use the authentication mechanisms built into their respective protocols. The local administrator authenticates itself using a separate username/password (local Access Control List (ACL)) through the BIOS configuration screen. User info is passed to Intel® AMT through the KCS interface and is authenticated using the admin ACL. Intel® AMT allows the configuration of the basic admin ACL by accepting a password setting through the local host interface. Intel® AMT maintains a general ACL in NVM that can be manipulated through remote user commands. Intel® AMT uses ACL (username/password pairs) to perform basic authentication of web service, SOL/IDER connections. The maximal length of the username and password is 16 characters, up to 32 bytes in UTF-8 encoding. Passwords must have at least one a-z, one A-Z (or Unicode+0x80) and one 0-9 character and at least one special character.

4.2.8 Provisioning

Intel® AMT provides two methods of provisioning the device: Enterprise mode and small business mode. Intel® AMT is not accessible from the network before the user changes the default username and password. In Small Business mode Intel AMT is



provisioned after the default username and password have been changed and the BIOS extension has updated Intel AMT with the system's UUID. In Enterprise mode, Intel AMT will be provisioned only after the following data was set:

- a. Host name if in DHCP mode.
- b. RSA Key pair and certificate if TLS mode is active
- c. RNG Key.

4.2.9 Privacy

An Intel® AMT-enabled POS client can be permanently disabled through a remote command(s) originating on a management console and protected by the security mechanism of the OOB network interface. As a result of this command, all secured Intel® AMT area in the flash will be erased, so that AMT cannot be re-enabled. This includes the ISV storage data and all Intel AMT Configuration information. Once these configuration changes have been made, a mechanism must be provided to permanently lock-out any additional configuration changes so that these manageability configurations cannot be re-enabled by the local or remote software running in the consumer's environment.



5 Conclusion

Intel® Active Management Technology (AMT) and Intel® Virtualization Technology (VT) enabled Retail Point of Sales systems serve as a retail management program that allows users to maintain absolute control over sales and inventory while utilizing an easy and professional customer checkout. As the retail business grows, businesses have little choice but to upgrade and upscale their IT infrastructure to cope with growing transaction terminals, as well as providing additional services such as streaming video advertisements to transaction terminals which could also earn them advertising revenue. Intel® VT-enabled Servers provide a scalable solution to add, remove, and consolidate applications into multiple virtual machines on the same hardware platforms.

Intel VT coupled with Intel's advanced server RAS capabilities help organizations meet the high uptime requirements for servers hosting multiple business-critical applications such as Retail Infrastructure POS Database Server, while providing application consolidation benefits of virtualized infrastructure. An Intel VT-enabled consolidated system results in reduced floor space for Customer Premise Equipment (CPE), improved management, flexible fail over, and low downtime platform migration, resulting in substantial savings.

Intel AMT on POS Clients enables IT personnel to utilize intelligent network management to manage a large and complicated client network. This technology also helps the management console manage the activity of the network and equipment at client premise by remote access. IT personnel can assess and fix typical downtime on transaction terminals without hands-on debugging, resulting in tremendous savings in cost and time to repair and higher uptime.



6 References

For more information on Intel® VT and Intel® AMT enabled platforms, please visit the links below:

- Intel® Core™ Duo Processors for Embedded Computing
<http://developer.intel.com/design/intarch/coreduo/index.htm>
- Mobile Intel® 945GM Express Chipset for Embedded Computing
<http://developer.intel.com/design/chipsets/embedded/945gm.htm>
- Dual-Core Intel® Xeon® Processor LV 2.0GHz for Dual-Processor Embedded Computing and Communications Applications
<http://developer.intel.com/design/intarch/dualcorexeon/overview.htm>
- Intel® E7520 Chipset for Dual-Core Intel® Xeon® Processor LV 2.0 GHz for Embedded Computing
http://developer.intel.com/design/chipsets/embedded/e7520_dcxeon_docs.htm
- Dual-Core Intel® Xeon® Processor 5100 Series for Dual-Processor Embedded Computing
<http://developer.intel.com/design/intarch/dualcorexeon/5100/index.htm>
- Intel® 5000P Chipset for Dual-Core Intel® Xeon® Processor 5100 Series
<http://developer.intel.com/design/chipsets/embedded/5000P.htm>
- Intel® 82573 Gigabit Ethernet Controller
<http://developer.intel.com/design/network/products/lan/controllers/82573.htm>
- Intel® Active Management Technology documentation
<http://www.intel.com/technology/manage/iamt/documentation.htm>
<http://www.intel.com/technology/manage/iamt/>
- Intel® Virtualization Technology Documentation
www.intel.com/technology/virtualization/index.htm