Intel® Cloud Builders Guide
Intel® Xeon® Processor Servers
Enhanced Cloud Security with HyTrust* and VMware*

Intel® Cloud Builders Guide: Cloud Design and Deployment on Intel® Platforms

Enhanced Cloud Security with HyTrust* and VMware*

Intel® Xeon® Processor 5500 Series

Intel® Xeon® Processor 5600 Series

AUDIENCE AND PURPOSE

This reference architecture explains a secure cloud infrastructure deployment and operation. It describes a cloud built with VMware vSphere*, Intel® Xeon® processor 5600 series-based server platforms, and a HyTrust Appliance* designed to enforce cloud security policies, including those based on platform trust attestation provided by Intel® Trusted Execution Technology (Intel® TXT).

This reference architecture is tailored to aid security administrators responsible for design, implementation, validation, and utilization of cloud implementations. Hardware configuration, software configuration, and results from the implementation of specific test cases that demonstrate basic operational capabilities are covered in this document. This reference architecture is intended to complement product documentation and is provided as a starting point for the actual development of an enterprise cloud.

Copyright® 2011 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are 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.

Table of Contents

Executive Summary

Cloud computing encompasses an on-demand, self-managed virtual infrastructure, which is provided as a service. This approach makes applications available, independent from the underlying infrastructure, allowing IT personnel to focus on delivering support and value. Increasingly, cloud computing architectures are built on virtualization technology. VMware* is a proven leader in virtualization and is helping to establish and standardize cloud computing. Working with Intel and other industry leaders, VMware helps businesses of all sizes migrate to cloud computing, with the goal of addressing IT costs and complexities.

Recent cloud computing customer surveys unanimously cite security, control, and IT compliance as primary issues that slow the adoption of cloud computing. These survey results denote concerns about change management, configuration management, access controls, auditing, and logging. Many customers have specific security requirements that must assure data location and integrity, and use legacy solutions that rely on fixed hardware infrastructures. Under current cloud computing conditions, the means to verify a service's security compliance are labor-intensive, inconsistent, and non-scalable. For this reason, many businesses only deploy non-core applications in the public cloud and restrict sensitive applications to dedicated hardware.

Comprehensive security requires an uninterrupted chain of control from the application user's interfaces to the underlying hardware infrastructure. Any gaps in this trust chain render them vulnerable to attacks. Today, security mechanisms in the lower stack layers (for example, hardware and firmware are almost absent. In this reference architecture, the trusted compute pool (TCP) concept, which is a collection of physical platforms known to be trustworthy, is described. This solution utilizes Intel® Trusted Execution Technology (Intel® TXT), a Intel® Xeon® processor 5600 series-based hardware platform, a cloud policy definition and enforcement engine from HyTrust*, and virtual infrastructure via VMware vSphere*.

Introduction

Cloud architectures separate the physical hardware from logical compute units consumed by the user. As virtualization proliferates throughout the data center, the IT manager can no longer point to a specific physical node as belonging to any one critical process or detail; virtual machines (VMs) may move to satisfy policies for high availability, performance, or resource usage. Regulatory compliance for certain types of data has also become increasingly difficult to enforce. Public cloud resources usually host multiple tenants concurrently, which increases the need for an isolated and trusted compute infrastructure.

IT administrators must balance security requirements with efficiency. Cloud computing only increases security challenges, and many of the downsides of conventional architectures still exist. The shared, multi-tenant environment, combined with the concentration of IT assets, increases the tension between operational efficiency and security, which makes deployments high-value targets for attacks.

Cyber Attacks

The data center has seen a rise in cyber attacks over the past several years, and these attacks continue to grow in volume, complexity, and sophistication. Today's attackers are better resourced and more determined. According to the *Symantec Internet Security Threat Report*, the release rate of malicious code and other unwanted programs "may be exceeding that of legitimate software applications."[1] To make matters worse, the cost of each data breach increases as well: the average organizational costs of a data breach have gone from $4.7 million in 2006 to $6.75 million in 2009[2], with lost revenue and potentially disastrous impact to a company's brand.

Trust in the Cloud

One of the pillars of security in the cloud is trust. A trusted computing system will consistently behave in expected ways, and hardware and software will enforce these behaviors. Trusted computing uses cryptography to help enforce a selected behavior because it authenticates the launch and authorized processes. This authentication allows someone else to verify that only authorized code runs on a system. Authorization covers initial booting and may also cover applications and scripts. Usually, the establishment of trust of a particular component implies the ability to establish the trust for that component with respect to other trusted components.

This trust path is known as the "chain of trust", with the first component known as the "root of trust". It is implied that the root of trust be a trusted set of functions that are immune from physical and other attacks. Because an important requirement for trust is to be tamper-proof, cryptography or some immutable unique signature that identifies a component is used. For example, the hardware platform is usually a good proxy for a root of trust, because for most attackers, the risk and cost of tampering directly with hardware exceeds the potential benefits. With hardware as the initial root of trust, software can then be measured (such as a hypervisor or operating system) to determine whether unauthorized modifications have been made to it. In this way, a chain of trust relative to the hardware can be established.

Trust techniques include hardware encryption, signing, machine authentication, secure key storage, and attestation. Encryption and signing are well-known techniques, but these are hardened by the placement of keys in protected hardware storage. Machine authentication provides users a higher level of assurance, as the machine is indicated as "known and authenticated". Attestation means firmware and software are validated as they are loaded. This is particularly important to cloud architectures based on virtualization.

Establishment of a Trusted Cloud

In order to minimize security risks, IT administrators must protect and validate the integrity of the infrastructure on an ongoing basis. This requires the implementation of the right tools and processes for protection and validation of all compute resources. Each server must have a component that reliably behaves in the expected manner, and that contains a minimum set of functions that enable a description of the platform characteristics and its trustworthiness. This reference architecture describes policy-based controls and infrastructure segmentations implemented by HyTrust Appliance* on top of the VMware* stack (VMware vSphere*). Policies implemented by HyTrust Appliance can be based on one the following categories:

- Workload.
- Role of the user.
- Configuration and audit requirements driven by the external compliance requirements and local governance.
- Server trustworthiness.

The later is established by relying on the Intel® Trusted Execution Technology (Intel® TXT) as the foundation to establish a chain of trust. This chain extends from the platform as a root of trust through measured firmware up to hypervisor. Furthermore, the system trust can be re-verified at any time during its life-cycle as a foundational element of the cloud, and the policies will automatically adjust on the basis of the trust status of the individual hypervisors / hosts.

Intel® TXT Overview

The value of Intel® TXT is in the root of trust establishment, which provides the necessary underpinnings for reliable evaluation of the computing platform and the platform's protection level. This root is optimally compact, extremely difficult to defeat or subvert, and allows for flexibility and extensibility to measure platform components during the boot and launch of the environment including BIOS, operating system loader, and virtual machine managers (VMM). Given the current nature of malicious threats prevalent in today's environment and the stringent security requirements many organizations employ, a system cannot blindly trust its execution environment.

Intel® TXT reduces the overall attack surface for individual systems and compute pools. Principally, Intel® TXT provides a launch environment signature to enable a trusted software launch and to execute system software. Launch environment protection ensures that the cloud infrastructure as a service (IaaS) has not been tampered with. Additionally, security policies based on a trusted platform or pool status can then be set to restrict (or allow) the deployment or redeployment of VMs and data to platforms with a known security profile. Rather than reliance on the detection of malware, Intel® TXT works because it builds trust into a known software environment and thus ensures that the software being executed hasn't been compromised. This advances security to address key stealth attack mechanisms used to gain access to parts of the data center in order to access or compromise information. Intel® TXT works with Intel® Virtualization Technology (Intel® VT) to create a trusted, isolated environment for VMs.

Enforce Trusted Pools

Policies and compliance activities that use platform attestations are required for enforcement of trust and security in the cloud. In this reference architecture, attestations and policy enforcements are managed by HyTrust Appliance*. After trust is established at the time the hypervisor is launched and added to HyTrust Appliance for protection, appropriate policy and compliance activities can be applied to make migration and deployment decisions to manage the operation and control the migration of workloads within the cloud.

Architectural Overview

Intel® TXT is a set of enhanced hardware components designed to protect sensitive information from software-based attacks. Intel® TXT features include capabilities in the microprocessor, chipset, I/O subsystems, and other platform components. When coupled with an enabled operating system, hypervisor, and enabled applications, these capabilities provide confidentiality and data integrity in the face of increasingly hostile environments. Intel® TXT incorporates a number of secure processing innovations, including:

- Trusted extensions integrated into silicon (processor and chipset).
- Authenticated code modules (ACM): platform-specific code is authenticated to the chipset and executed in an isolated environment within the processor and the trusted environment (authenticated code mode) enabled by AC Modules to perform secure tasks.
- Launch control policy (LCP) tools

Some of the required components for the Intel® TXT secured platform are provided by third parties, including:

- Trusted Platform Module (TPM) 1.2 (third party silicon)[3]: A hardware device defined by the Trusted Compute Group* that stores authentication credentials in platform configuration registers (PCRs), which are issued by Intel® TXT.
- Intel® TXT-enabled BIOS, firmware, operating system, and hypervisor environments.

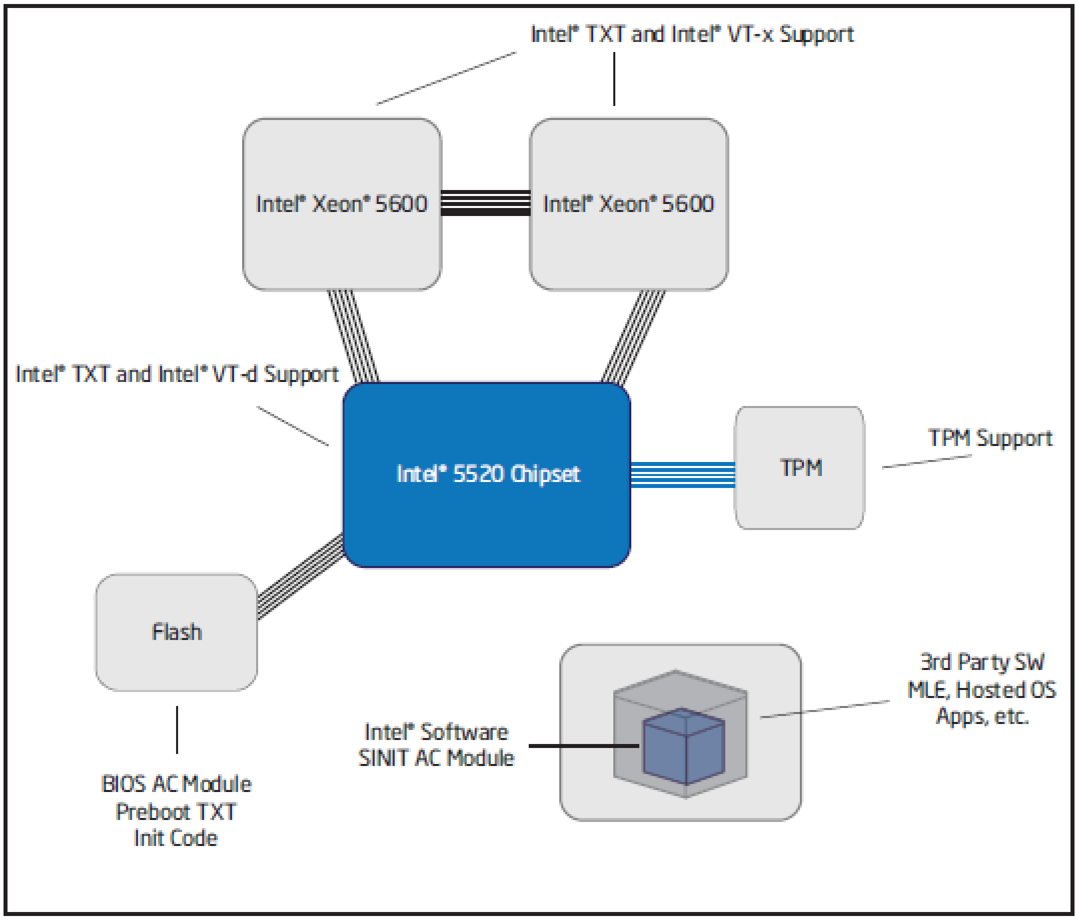


Figure 1 - Intel® Trusted Execution Technology Components

Intel® TXT Capabilities

The capabilities of Intel® TXT include:

- Protected execution: Lets applications run in isolated environments so that no unauthorized software on the platform can observe or tamper with the operational information. Each of these isolated environments executes with the use of dedicated resources managed by the platform.
- Sealed storage: Provides the ability to encrypt and store keys, data, and other sensitive information within the hardware. This can only be decrypted by the same environment that encrypted it.
- Protected input: Protects communication between the input hardware (keyboard/mouse) and the execution environment so that the communication cannot be observed.
- Protected graphics: Enables applications to run within the protected execution environment to send display information to the graphic frame buffer without being observed or compromised by any unauthorized software on the platform.
- Attestation: Enables a system to provide assurance that the protected environment is correctly invoked and to take a measurement of the software running in the protected space. The information exchanged during this process is known as the "attestation identity key credential" and is used to establish mutual trust between parties.
- Protected launch: Provides the controlled launch and registration of critical system software components in a protected execution environment.

Intel® Xeon® processor 5600 series support Intel® TXT, which is designed to address such software-based attacks. For more information on Intel® TXT, please visit http://www.intel.com/technology/security.

Intel® TXT: Operation Principles

Intel® TXT works through the creation of a measured launch environment (MLE) that enables an accurate comparison of all the critical elements of the launch environment against a known good source. Intel® TXT creates a cryptographically unique identifier for each approved launch-enabled component and then provides hardware-based enforcement mechanisms to block the launch of unauthenticated code. This hardware-based solution provides the foundation IT administrators can build trusted platform solutions on to protect against aggressive software-based attacks.

Figure 2 illustrates two different scenarios. In the first, the measurements match the expected values, so the launch of the BIOS, firmware, and VMM are allowed. In the second, the system has been compromised by a root-kit hypervisor, which attempts to install itself below the hypervisor to gain access to the platform. In this case, the Intel® TXT-enabled, MLE-calculated hash system measurements will differ from the expected value because of the root-kit insertion. Therefore, the measured environment will not match the expected value and, based on the launch policy, Intel® TXT could abort the launch of the hypervisor.

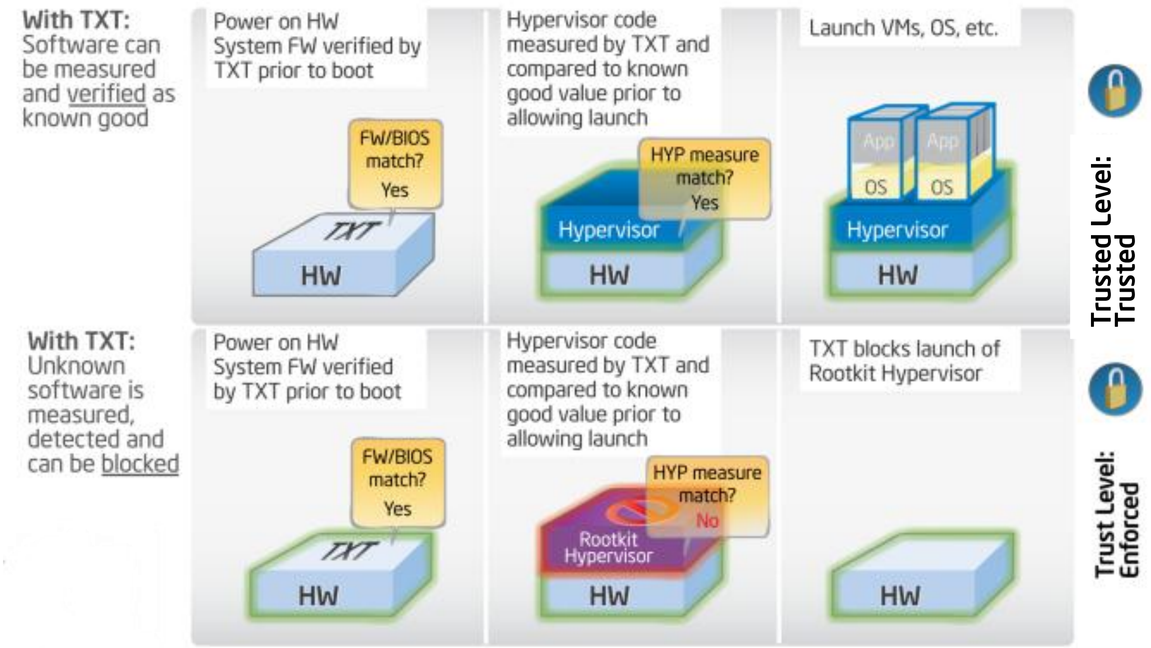

With TXT: Software can be measured and verified as known good
Power on HW System FW verified by TXT prior to boot
FW/BIOS match? Yes
TXT
HW
Hypervisor code measured by TXT and compared to known good value prior to allowing launch
HYP measure match? Yes
Hypervisor
HW
Launch VMs, OS, etc.
App
App
OS
OS
Hypervisor
HW
Trusted Level: Trusted
With TXT: Unknown software is measured, detected and can be blocked
Power on HW System FW verified by TXT prior to boot
FW/BIOS match? Yes
TXT
HW
Hypervisor code measured by TXT and compared to known good value prior to allowing launch
HYP measure match? No
Rootkit Hypervisor
HW
TXT blocks launch of Rootkit Hypervisor
HW
Trust Level: Enforced

Figure 2 - How Intel® Trusted Execution Technology Protects a Virtualized Environment

Implementation Overview

HyTrust Appliance* is a network-based policy management solution for virtual infrastructure that provides administrative access control, hypervisor hardening, and audit-quality logging. HyTrust Appliance empowers organizations to fully leverage their investment in virtualization by delivering enterprise-class controls for access, accountability, and visibility. HyTrust Appliance offers system managers and administrators an end-to-end virtualization security platform to manage access, standardize and control configuration, and protect virtual infrastructure within a customer's environment. HyTrust Appliance is designed to fit easily within the configuration and architecture of most data centers and is installed as a virtual appliance. Features include unified access control, virtual infrastructure policy, hypervisor hardening, and audit-quality logging.

HyTrust* introduces production support of Intel® TXT technology in HyTrust Appliance* 2.2. HyTrust Appliance attests to the hypervisor trust status and enforces on-boarding and migration policies for virtual machines that require platform trust. HyTrust Appliance obtains the platform trust status from the VMware vSphere* application program interface (API) which makes the server TPM digest value available to higher level applications. VMware implemented support for Intel® TXT so that when VMware ESXi* undergoes a trusted launch, it is able to attest to the server TPM's platform configuration registers (PCR) values locally.

HyTrust Appliance allows administrators to configure expected TPM digest values for every build/patch of the VMware ESXi*. Subsequently, if a hypervisor with a bootable image with a TPM digest value known to HyTrust Appliance is added to HyTrust for protection, the hypervisor acquires a "Trusted" status. This is evident in the HyTrust Appliance by the policy label on the hypervisor used in the policy definition as well as by the lock icon in the host dashboard. For hosts where the actual TPM digest values mismatches the known value for the bootable image, it is labeled as "Untrusted". Where a TMP digest value is unknown or unsupported, no labels or icons are applied.

Supported Recipes from Intel® ESAA

The HyTrust Appliance* Installation and Configuration recipe and the VMware vSphere 4.1 ESX/ESXi 4.1 Installation recipe are available on the Intel® Server Board S5520HC and the Intel® Server Board S5520UR from the Intel® Enabled Solutions Acceleration Alliance (Intel® ESAA)

- HyTrust Appliance* Installation and Configuration:
  - Intel® Server Board S5520HC
  - Intel® Server Board S5520UR
- VMware vSphere 4.1 for ESX/ESXi* 4.1:
  - Intel® Server Board S5520HC
  - Intel® Server Board S5520UR

Design Considerations

Features include:

- Intel® TXT supported systems.
- 1 GbE and 10 GbE networks to achieve optimal performance during VM migrations.
- Multiple virtual local area networks (VLANs) to simulate cross-site VM migrations.

Hardware Description

System	Processor Configuration	Detailed Configuration
1 Management Server • Microsoft Windows8 2008, IIS*, .NET* 2.0 • VMware vCenter* Server 4.1 • VMware vSphere Web Services* SDK	Intel® Xeon® Processor L5630 See processor details at http://ark.intel.com/Product.aspx?id=47927	Form Factor: 2U Rack Mount Server Processor: Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM storage: 100GB HDD 10Gb Ethernet network
1 Management Client • Microsoft Windows* 7 • VMware vSphere* Client 4.1	Intel® Xeon® Processor L5630 See processor details at http://ark.intel.com/Product.aspx?id=47927	Form Factor: 2U Rack Mount Server Processor: Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM)Storage: 100GB HDD 10Gb Ethernet network
1 ESXi* Host (x2) • VMware ESXi* • HyTrust Appliance* 2.2 implemented as a virtual machine • Microsoft Windows* 2008 server configured for use as a domain controller implemented as a virtual machine	Intel® Xeon® Processor L5630 See processor details at http://ark.intel.com/Product.aspx?id=47927	Form Factor: 2U Rack Mount Server Processor: Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM)Storage: 100GB HDD 10Gb Ethernet network
3 ESXi* Host (x2) • VMware ESXi*	Intel® Xeon® Processor L5630 See processor details at http://ark.intel.com/Product.aspx?id=47927	Form Factor: 2U Rack Mount Server Processor: Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM)Storage: 100GB HDD 10Gb Ethernet network
1 iSCSI Data Store Server	Intel® Xeon® Processor L5630 See processor details at http://ark.intel.com/Product.aspx?id=47927	Form Factor: 2U Rack Mount Server Processor: Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM)Storage: 12TB HDD 10Gb Ethernet network

Table 1- Hardware Configuration Details

Physical Architecture

Figure 3 illustrates the test bed deployment architecture. Two different VLANs are configured:

1. VMware vSphere* Client virtual machine guest traffic resides on one VLAN which corresponds to a generic corporate network.
2. Two Intel® Server Boards, with VMware ESXi*, management ports and VMware vCenter* Server reside on a separate VLAN protected by HyTrust Appliance*.

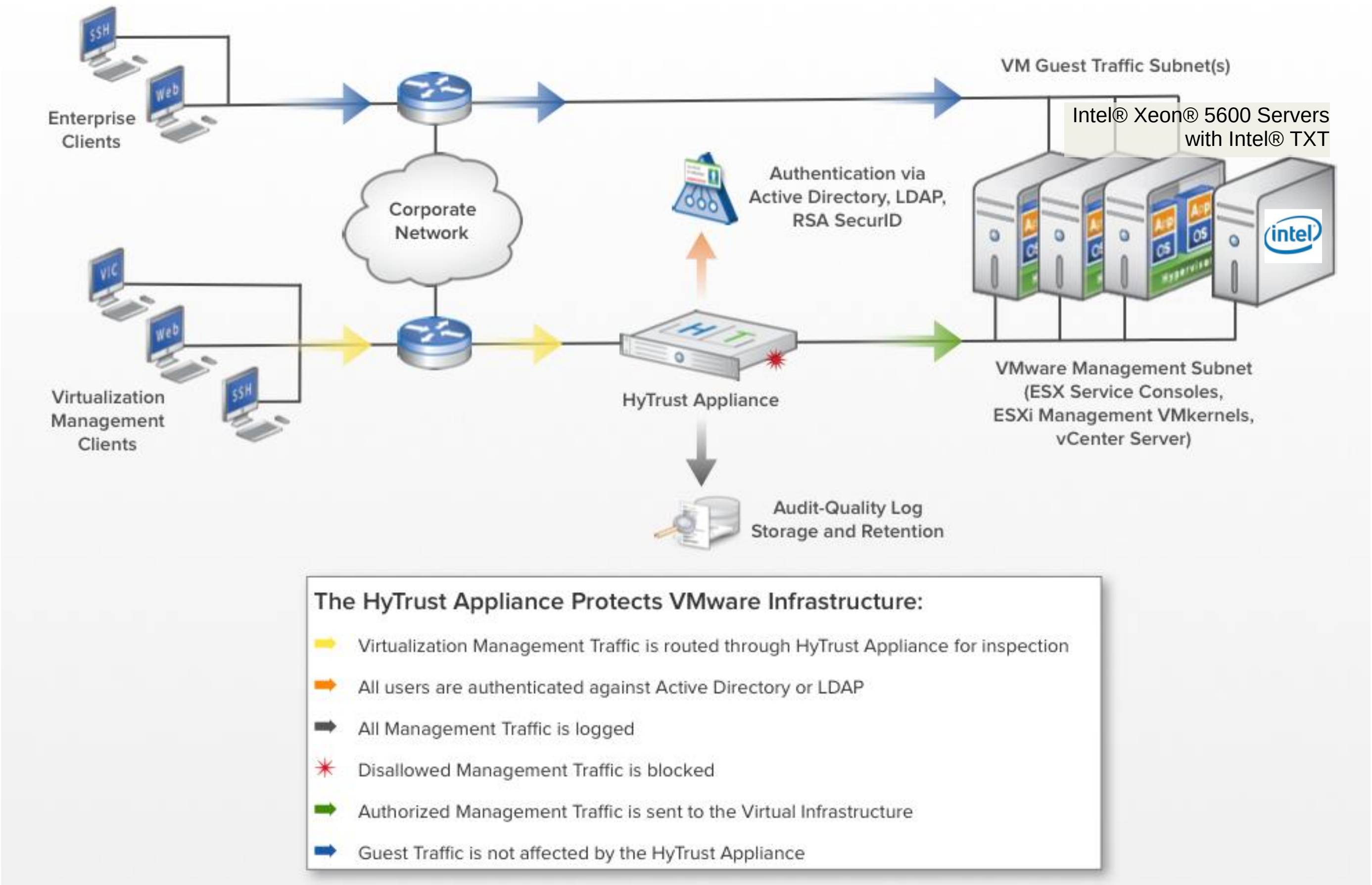

SSH
Web
Enterprise Clients
Corporate Network
VM Guest Traffic Subnet(s)
Intel® Xeon® 5600 Servers with Intel® TXT
Authentication via Active Directory, LDAP, RSA SecurID
VIC
Web
SSH
Virtualization Management Clients
HyTrust Appliance
VMware Management Subnet (ESX Service Consoles, ESXi Management VMkernels, vCenter Server)
Audit-Quality Log Storage and Retention
The HyTrust Appliance Protects VMware Infrastructure:
Virtualization Management Traffic is routed through HyTrust Appliance for inspection
All users are authenticated against Active Directory or LDAP
All Management Traffic is logged
Disallowed Management Traffic is blocked
Authorized Management Traffic is sent to the Virtual Infrastructure
Guest Traffic is not affected by the HyTrust Appliance

Figure 3 - Physical Implementation Architecture

Installation and Configuration

BIOS Changes

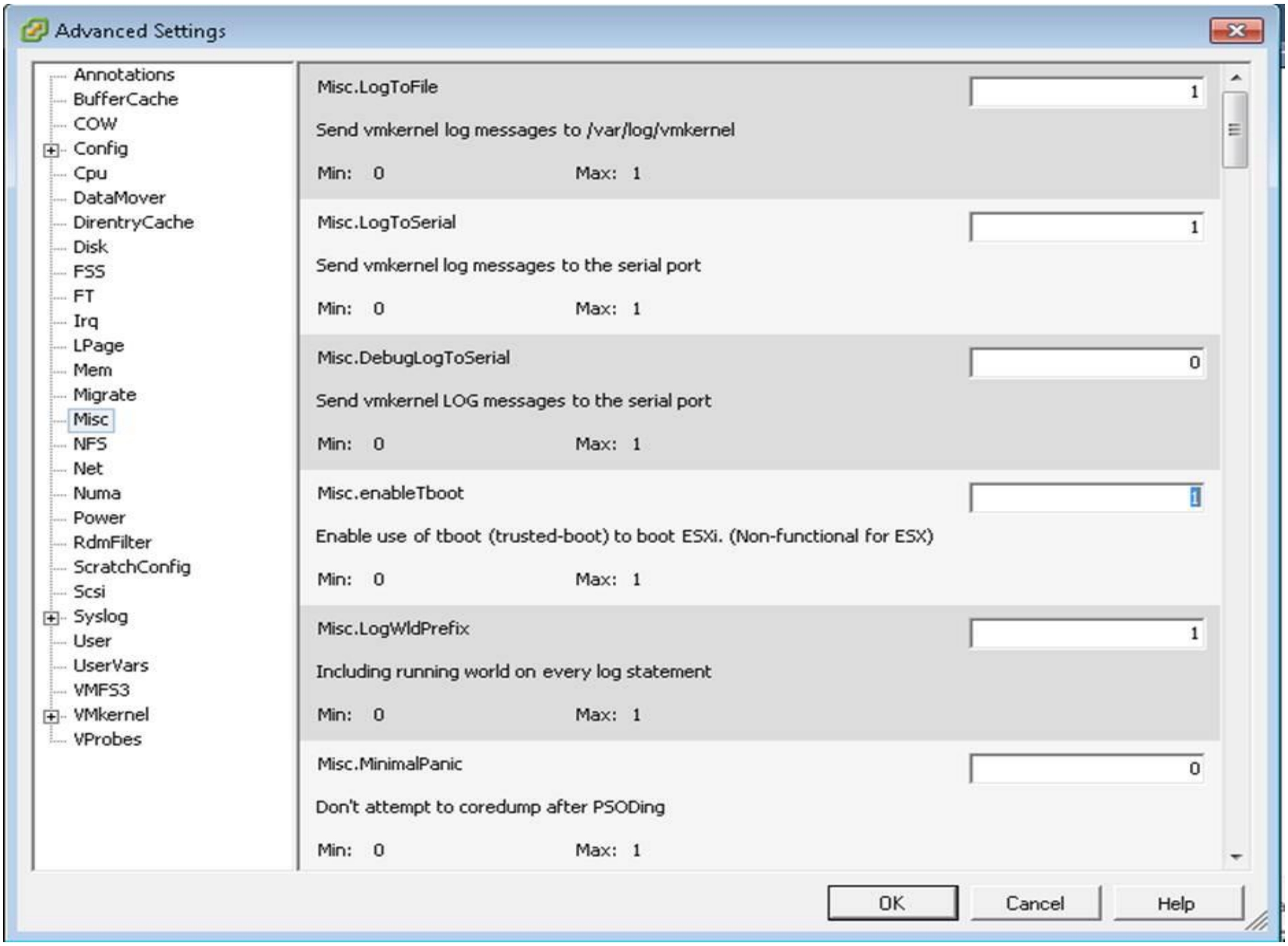
The following changes are required in the BIOS settings:

- Intel® TXT set to “Enabled”.
- Intel® Virtualization Technology (Intel® VT) set to “Enabled”.
- Intel® VT for Directed I/O set to” Enabled”.
- Set “Administrator Password” and reboot prior to enabling the TPM
- Change TPM Administrative Control” to “Turn On” - TPM state will show as “enabled and activated” after reboot.

VMware* Components

The high-level installation and configuration steps for the infrastructure setup required to employ the Intel® TXT capabilities supported by the platform are listed below. These setup steps assume a basic understanding of how to install and configure Windows Server* 2008 R2 Enterprise, VMware vCenter* Server, and VMware vSphere* Client.

1. Install Windows Server* 2008 R2 Enterprise on compatible hardware.[4]
2. Install the VMware vCenter* Server:
   - Depending on the scalability needed, an appropriate database should be used. A default SQL Server Express* edition is sufficient for a small database instance.
3. Set-up the vSphere* client machine:
   a. Install Windows* 7 on compatible hardware.
   b. Launch a browser and point it at the machine where vCenter* Server is installed to download the vSphere* client.
   c. Install the VMware vSphere* client.
4. Install the VMware ESXi* hosts:
   a. Install VMware ESXi* on the hosts. This version supports both Intel® TXT
   b. Ensure that the installation of the hypervisor is initiated after required BIOS settings are configured.
5. After the hypervisor installation completes, add the host to a Cluster via the vSphere Client.
6. One completed, ensure t-boot is enabled. Do this by selecting the hosts *Configuration* tab > “Software” > “Advanced Settings” > “Misc” and set the option “Misc.enableTboot” parameter from “0” to “1”.



Misc.LogToFile 1
Send vmkernel log messages to /var/log/vmkernel
Min: 0 Max: 1

Misc.LogToSerial 1
Send vmkernel log messages to the serial port
Min: 0 Max: 1

Misc.DebugLogToSerial 0
Send vmkernel LOG messages to the serial port
Min: 0 Max: 1

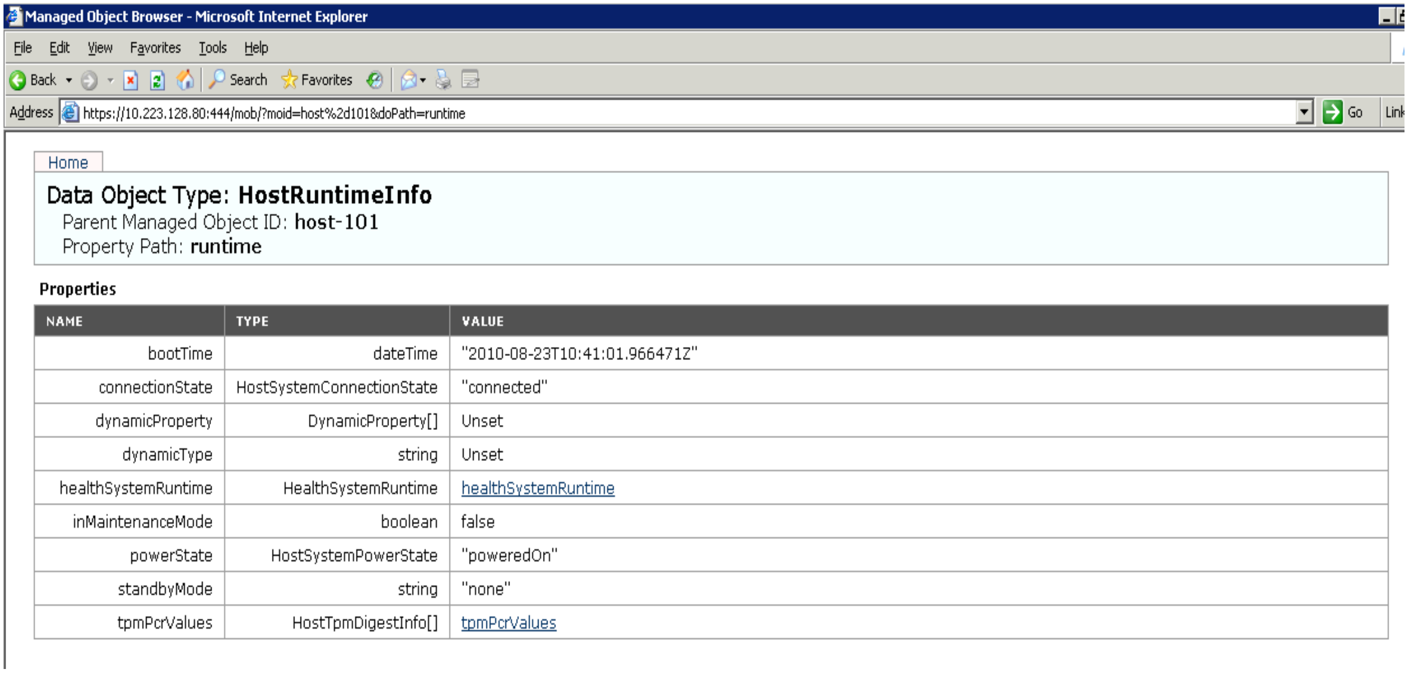
Misc.enableTboot 1
Enable use of tboot (trusted-boot) to boot ESXi. (Non-functional for ESX)
Min: 0 Max: 1

Misc.LogWldPrefix 1
Including running world on every log statement
Min: 0 Max: 1

Misc.MinimalPanic 0
Don't attempt to coredump after PSODing
Min: 0 Max: 1

Figure 4 – Enable Misc.enableTboot

7. Reboot the host and check that it has booted into trusted mode: Use the Managed Object Browser tool to verify that the "vmware-vmkernel" object's "HostTpmDigestInfo" is present under the "HostRunTimeInfo" of the ESXi* host. Figures 5 and 6 show how to verify these values.


Managed Object Browser - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
Home

Address https://10.223.128.80:444/mob/?moid=host%2d101&doPath=runtime

Data Object Type: **HostRuntimeInfo**

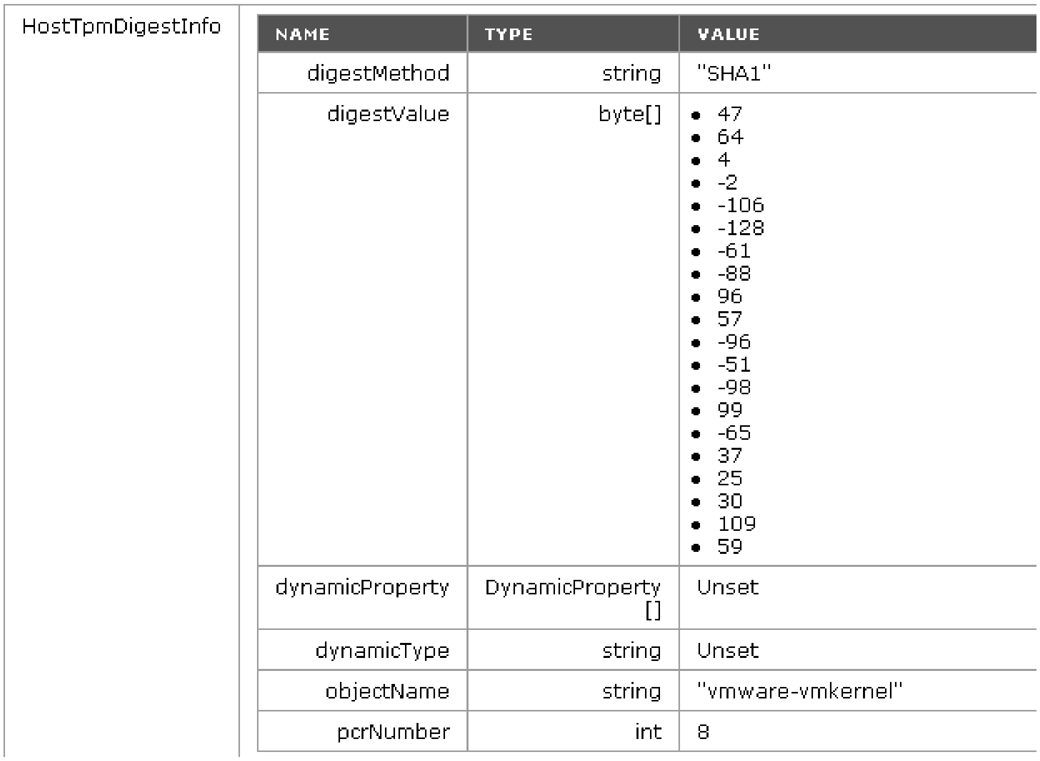
Parent Managed Object ID: **host-101**

Property Path: **runtime**

Properties

NAME	TYPE	VALUE
bootTime	dateTime	"2010-08-23T10:41:01.964671Z"
connectionState	HostSystemConnectionState	"connected"
dynamicProperty	DynamicProperty[]	Unset
dynamicType	string	Unset
healthSystemRuntime	HealthSystemRuntime	healthSystemRuntime
inMaintenanceMode	boolean	false
powerState	HostSystemPowerState	"poweredOn"
standbyMode	string	"none"
tpmPcrValues	HostTpmDigestInfo[]	tpmPcrValues

Figure 5 - Data Object Type: HostRuntimeInfo



HostTpmDigestInfo

NAME	TYPE	VALUE
digestMethod	string	"SHA1"
digestValue	byte[]	• 47 • 64 • 4 • -2 • -106 • -128 • -61 • -88 • 96 • 57 • -96 • -51 • -98 • 99 • -65 • 37 • 25 • 30 • 109 • 59
dynamicProperty	DynamicProperty []	Unset
dynamicType	string	Unset
objectName	string	"vmware-vmkernel"
pcrNumber	int	8

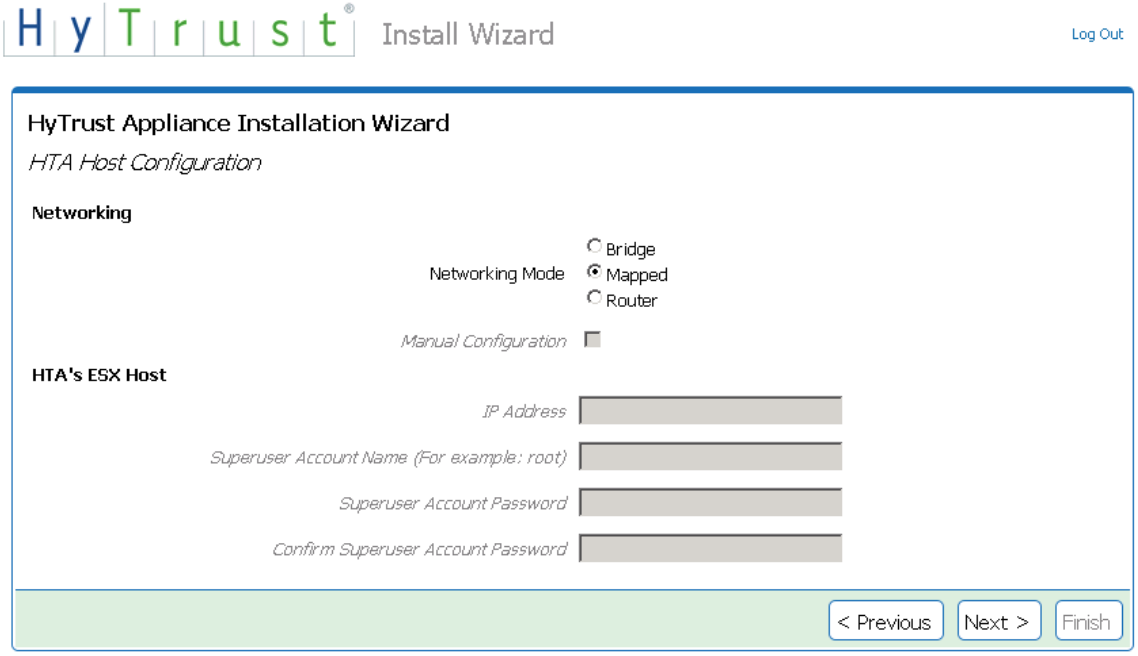
Figure 6 - HostTpmDigestInfo: Verify Digest Value

8. Configure VMware vCenter* Server.
   - Create a single cluster and add all VMware ESXi* hosts.

HyTrust Appliance* Installation and Configuration

HyTrust Appliance* installation and configuration steps:

1. Deploy HyTrust Appliance* from the OVF Template:
   a. Download the HyTrust Appliance* OVF to the vSphere* client machine.
   b. Launch the vSphere* client and connect to the vCenter*. In the VI Client, select "File" > "Virtual Appliance" > "Import" or in vSphere Client, select "File" > "Deploy OVF Template" and in the wizard, select the location to install/import the HTA OVF file.
2. Once the import is complete, HyTrust Appliance* appears in the VMware vSphere* Client inventory hierarchy for the selected VMware vCenter* or ESX* host. To power-on the HTA virtual machine:
   a. From the vSphere* Client *Summary* tab display click the "Power on" command. Once the boot process is completed, the management network interface for HTA (eth0) must be manually configured.
   b. At the console window, login as the user "htadminuser" with the password "Hytrust123!"
   c. Type "setup" to walk through the setup procedure.
   d. Type "n" to indicate a separate license.iso file is not available and to use the community license. Proceed to assign a static IP address, netmask, gateway and the DNS service to the appliance.
   e. Type "y" to save the configuration.
   f. Open the HyTrust Appliance* GUI by typing "https:<IPaddress>/hytrust/login" into the browser
   g. Ignore security warnings associated with self-signed SSL certificates, if any. Later Enterprise or 3rd party issued certificates can be installed.
   h. Proceed through the installation wizard. Select the Networking Mode "Mapped" radio button under HTA Host Configuration.



HyTrust Appliance Installation Wizard

HTA Host Configuration

Networking

Networking Mode ○ Bridge ● Mapped ○ Router

Manual Configuration □

HTA's ESX Host

IP Address

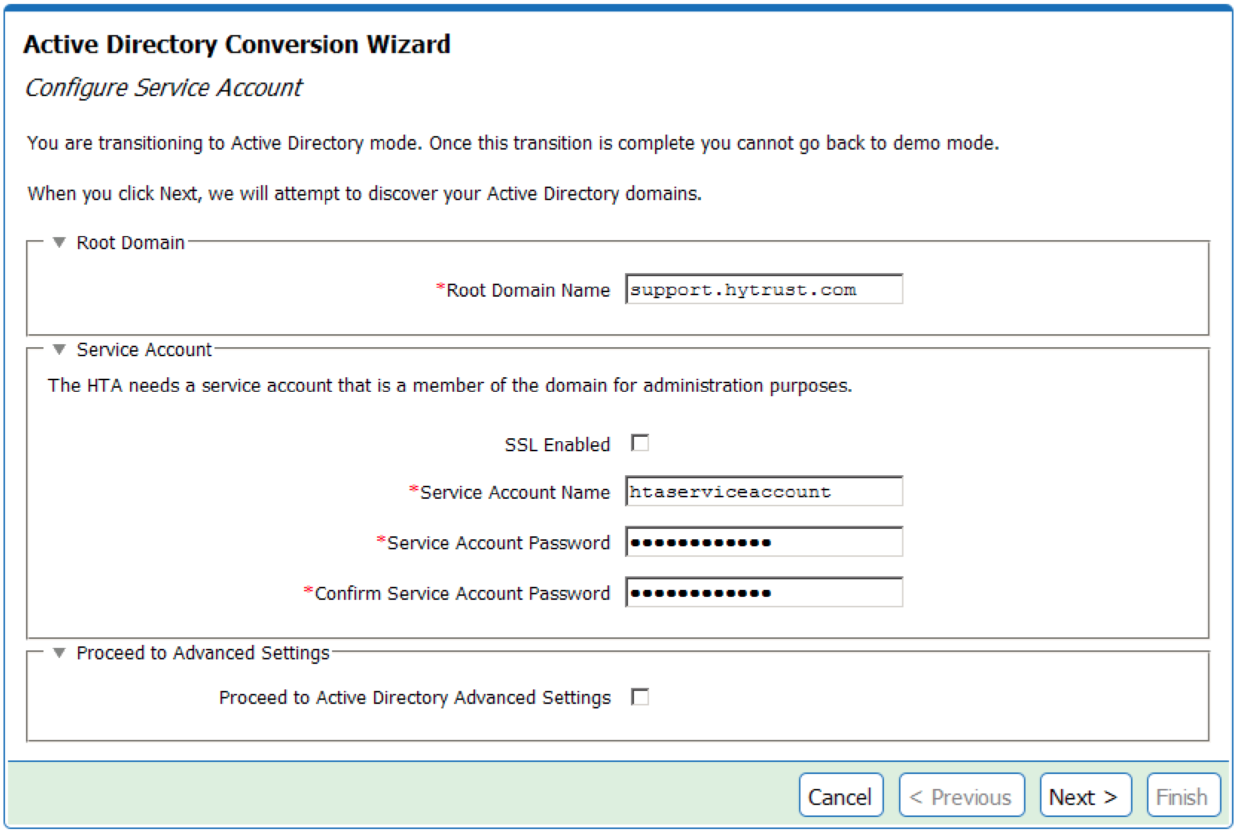
Superuser Account Name (For example: root)

Superuser Account Password

Confirm Superuser Account Password

Figure 7 – HyTrust Appliance* Installation Wizard HTA Host Configuration

3. Using the command line, change the "htadminuser" password from the default "HyTrust123! " to "HyTrust 1234!" (or a different password). Click "Finish" to complete the installation wizard.
4. Log into the Active Directory and create the following AD security groups: "HT_SuperAdminGroup", "SSLA_Administrators", "HT_PowerUserGroup". For each of the groups, create a user who is a member of this group.
5. Create a service account for HTA as a standard domain user account. Use "htaserviceaccount" or another user name.



Active Directory Conversion Wizard

Configure Service Account

You are transitioning to Active Directory mode. Once this transition is complete you cannot go back to demo mode.

When you click Next, we will attempt to discover your Active Directory domains.

▼ Root Domain

*Root Domain Name: support.hytrust.com

▼ Service Account

The HTA needs a service account that is a member of the domain for administration purposes.

SSL Enabled □

*Service Account Name: htaserviceaccount

*Service Account Password: •••••••••••••

*Confirm Service Account Password: •••••••••••••

▼ Proceed to Advanced Settings

Proceed to Active Directory Advanced Settings □

Figure 8 – Active Directory Conversion Wizard

6. Select "Configuration" > "Authentication". From the menu, deselect the "Demo" radio button and select the "Directory Service" radio button. Provide information on the root domain name and the service account, as required.
7. Map "HT_SuperAdmin" role to "HT_SuperAdminGroup" previously created.
8. Complete the conversion wizard.
9. Add VMware vCenter* Server and VMware ESXi* hosts to HyTrust Appliance* for protection:

   a. First add VMware vCenter* Server. From the menu select "Compliance" > "Hosts", then click the "Add" button. Follow the wizard to provide the host name, administrative credentials and public IP address.

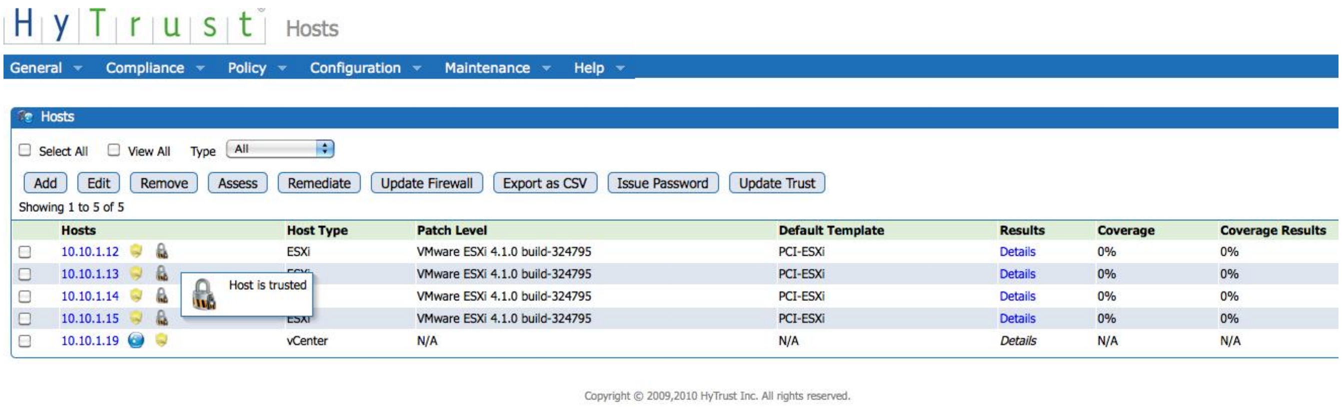
   Note: In mapped mode, HyTrust policies are only enforced when the protected resources are accessed through the public IP address. To improve security, a firewall may be installed to block access to the private IP address around HyTrust Appliance*.*

   b. After VMware vCenter* Server is added, all hosts managed by it appear in a "blocked" state. To add the hosts, click the checkboxes next to them, click the "Add" button, then follow the wizard.

10. Select "Configuration" > "IntelTXT" from the menu to configure TPM digest values for the hosts in the system.

    Note: If the current TPM digest values are unknown and if unsure of the trust status of the hosts at the moment, the last HyTrust-read TPM value can be retrieved from the hosts by inspecting recent HyTrust logs under "Maintenance" > "Log Viewer".

11. Now that the installation is complete, the attestation of the hosts trust status can be verified.



Showing 1 to 5 of 5

	Hosts	Host Type	Patch Level	Default Template	Results	Coverage	Coverage Results
□	10.10.1.12	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.13	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.14	[illegible]	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.15	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.19	vCenter	N/A	N/A	*Details*	N/A	N/A

Copyright © 2009,2010 HyTrust Inc. All rights reserved.

Figure 9 – HyTrust* Hosts Page

12. At any time the trust status of the individual hypervisor can be updated by checking the box next to the server, then by clicking "Update Trust".
13. If desired, the HyTrust Appliance* UI can be configured to appear as a plug-in in VMware vCenter* Server. To do so, select "Configuration" > "vCenter PlugIn" from the menu, then supply the VMware vCenter Server private IP address or fully qualified domain name.

Intel® TXT Usage Model

Trusted Compute Pools

In today's increasingly virtualized environment, security concerns are amplified because of security management complications through:

- Multi-tenancy, employed to increase density and efficiency in the data center.
- Software trust requirements combined with physical abstraction.

The objective of the trusted compute pools usage model is to demonstrate how to establish and maintain high-security SLA for sensitive workloads in the cloud, with the hardware maintained in "Trusted" status with the help of Intel® TXT.

First, how to define the policy for scheduled configuration monitoring and remediation, resource segmentation based on the hypervisor trust attestation, and least-privilege access is described. Second, policy enforcement for two key use-cases will be described.

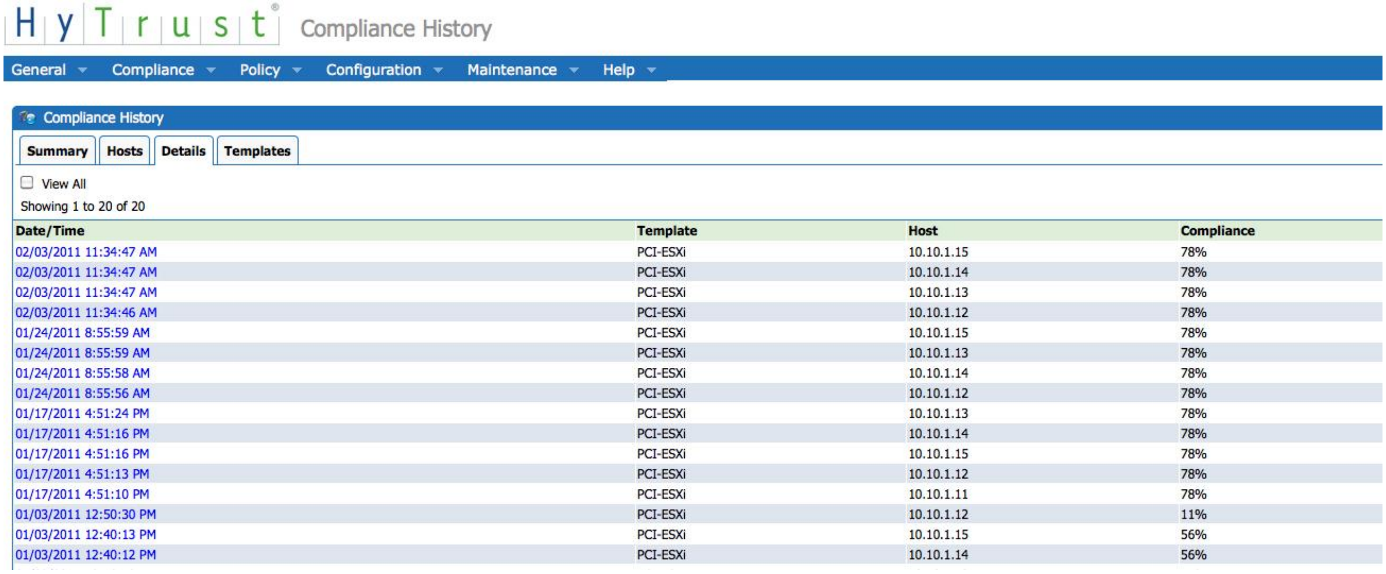
- Enforce security SLA during VMotion*.
- Enforce security SLA during VM on-boarding.

The following policies use cases will show the use of infrastructure segmentation and the TPM platform trust attestation to define and enforce policies for the workloads that need to comply with Payment Card Industry (PCI) data security requirements.

Host Configuration and Trust Status

In this use case, the hypervisors are added to HyTrust Appliance* for protection, their configuration assessed and remediated, and their TPM trust status established. This information becomes the basis of the infrastructure segmentation.

1. From the "Hosts" > "Hosts" menu, select the host to segment by clicking the host link and confirm that the PCI template is assigned to the host. If there are multiple hosts that need to be segmented, the PCI template needs to be assigned to each host individually.



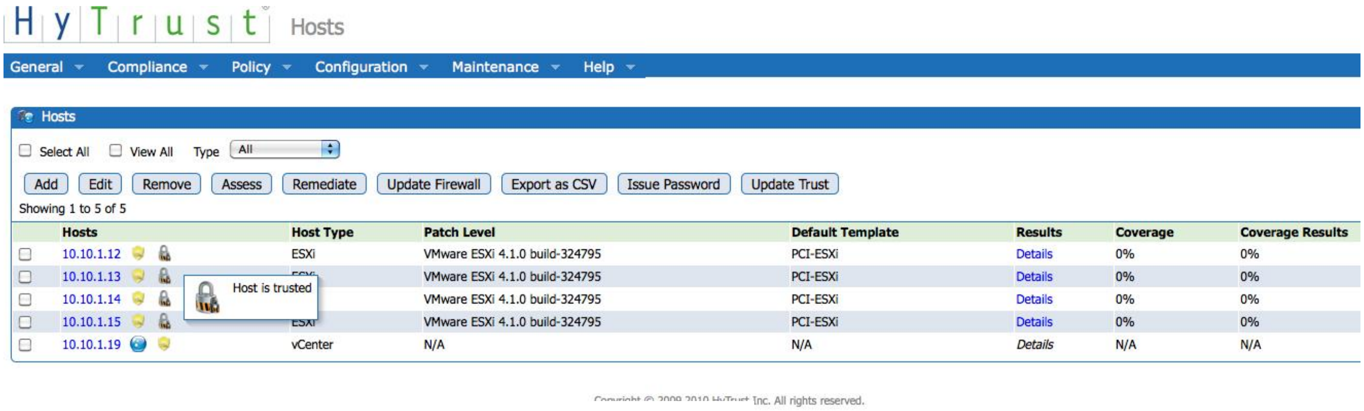
□ View All

Showing 1 to 20 of 20

Date/Time	Template	Host	Compliance
02/03/2011 11:34:47 AM	PCI-ESXi	10.10.1.15	78%
02/03/2011 11:34:47 AM	PCI-ESXi	10.10.1.14	78%
02/03/2011 11:34:47 AM	PCI-ESXi	10.10.1.13	78%
02/03/2011 11:34:46 AM	PCI-ESXi	10.10.1.12	78%
01/24/2011 8:55:59 AM	PCI-ESXi	10.10.1.15	78%
01/24/2011 8:55:59 AM	PCI-ESXi	10.10.1.13	78%
01/24/2011 8:55:58 AM	PCI-ESXi	10.10.1.14	78%
01/24/2011 8:55:56 AM	PCI-ESXi	10.10.1.12	78%
01/17/2011 4:51:24 PM	PCI-ESXi	10.10.1.13	78%
01/17/2011 4:51:16 PM	PCI-ESXi	10.10.1.14	78%
01/17/2011 4:51:16 PM	PCI-ESXi	10.10.1.15	78%
01/17/2011 4:51:13 PM	PCI-ESXi	10.10.1.12	78%
01/17/2011 4:51:10 PM	PCI-ESXi	10.10.1.11	78%
01/03/2011 12:50:30 PM	PCI-ESXi	10.10.1.12	11%
01/03/2011 12:40:13 PM	PCI-ESXi	10.10.1.15	56%
01/03/2011 12:40:12 PM	PCI-ESXi	10.10.1.14	56%

Figure 10 - Host with Assigned PCI Security Template

Note that some of the hosts appear in the host dashboard with a "lock" item (Figure 10), indicating that HyTrust Appliance* has obtained a TPM digest value for those hosts when they were added to HyTrust Appliance* for protection and that the TPM digest value matched the TPM digest value configured for the hypervisors boot image running on those hosts. Based on the Intel® TXT measured launch, HyTrust Appliance has automatically assigned "Trusted" label to those host which will subsequently be used to enforce VM on-boarding and trusted VM migration policies.



□ Select All □ View All Type All

Showing 1 to 5 of 5

	Hosts	Host Type	Patch Level	Default Template	Results	Coverage	Coverage Results
□	10.10.1.12	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.13	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.14	[illegible]	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.15	ESXi	VMware ESXi 4.1.0 build-324795	PCI-ESXi	Details	0%	0%
□	10.10.1.19	vCenter	N/A	N/A	*Details*	N/A	N/A

Copyright © 2009 2010 HyTrust Inc. All rights reserved.

Figure 11 - Select Hosts to Remediate for PCI Compliance

2. Now that the PCI security template is assigned to each host, from the "Hosts" > "Hosts" menu, check the box next to the desired hosts, then click the "Remediate" button to harden each host according to the HyTrust Appliance* PCI compliance benchmark. The main purpose of this usage model is to enable the migration of VMs from a multi-tenant, cloud-based environment that runs on a trusted host to another trusted host. This model restricts the migration of these tenant workloads to an un-trusted host. Restriction around the tenant workloads ensures that a VM that runs on the trusted host will only be allocated to another trusted host. This usage model is an extension of the first, where a pool of trusted hosts was established. Figure 11 below depicts the migrations are controlled based on the host trust status. The diagrams with a small box at the bottom indicate trusted hosts, while the diagram without a small box indicates the un-trusted host.

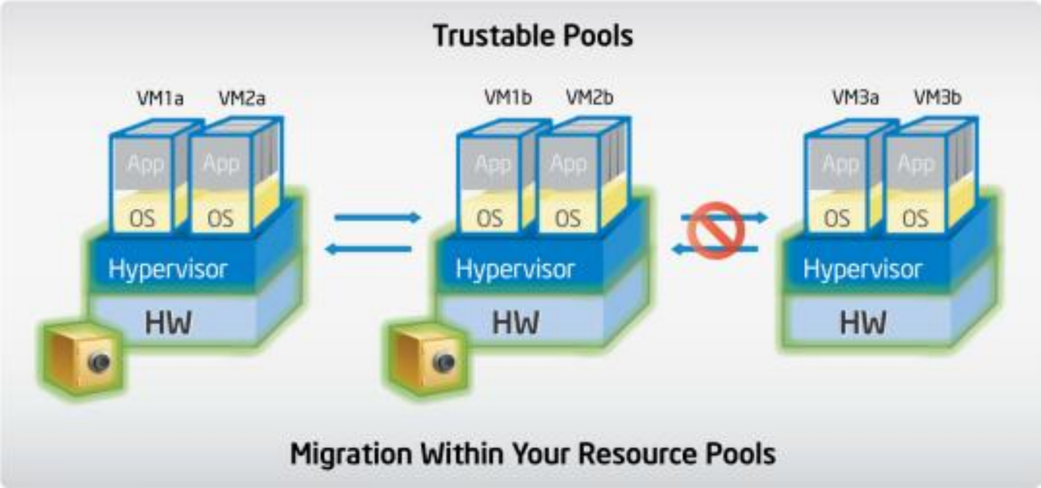
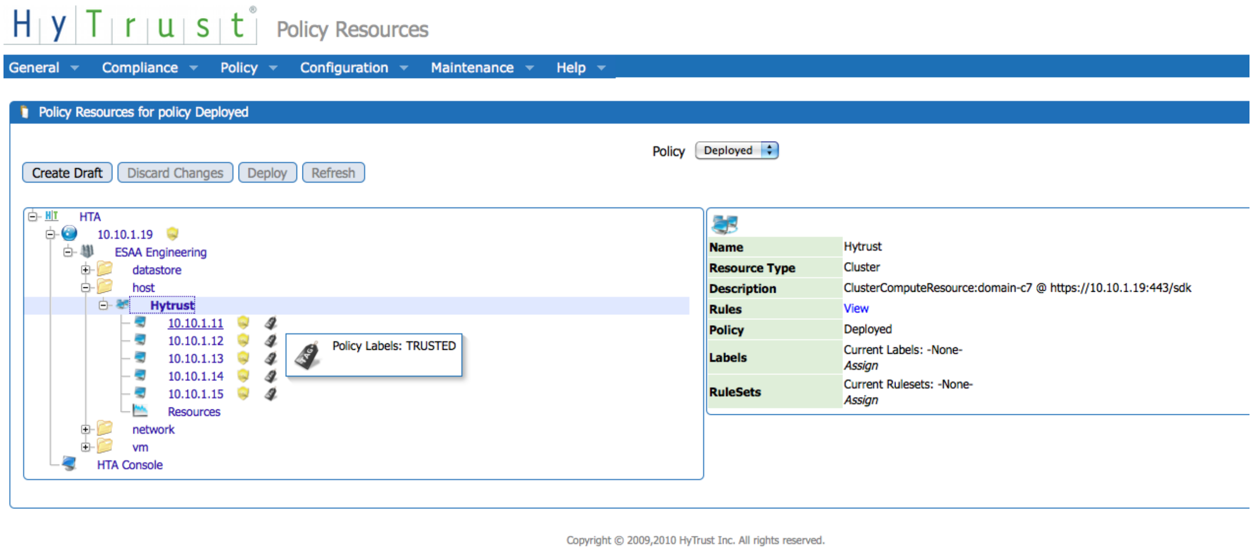


Figure 12 - Ensuring Safe Migration Between Hosts Through Trustable Pools Created Using Intel® TXT

Security Policy During VMotion*

1. From the "Policy" > **RuleSets** page, click the "Create Draft" button. This will copy the "Deployed" policy to a "Draft" policy. Next, define a policy for handling workloads with high security SLA. Go to the "Policy" > "RuleSets" menu, click the "Add" button, enter "Sec_SLA" into the name field, then click "OK".
2. Click the "Add" button to define a rule that matches "SSLA_administrators" security group to the "HT_VIAdmin" role.
3. Now that the rule is added, click the "Add" button and define a constraint. Select the "VM Move or Clone" constraint where both the "Move To" and "Move From" labels are indicated as "Trusted".



Name	Hytrust
Resource Type	Cluster
Description	ClusterComputeResource:domain-c7 @ https://10.10.1.19:443/sdk
Rules	View
Policy	Deployed
Labels	Current Labels: -None- *Assign*
RuleSets	Current Rulesets: -None- *Assign*

Figure 13 – HyTrust* Policy Resources Page

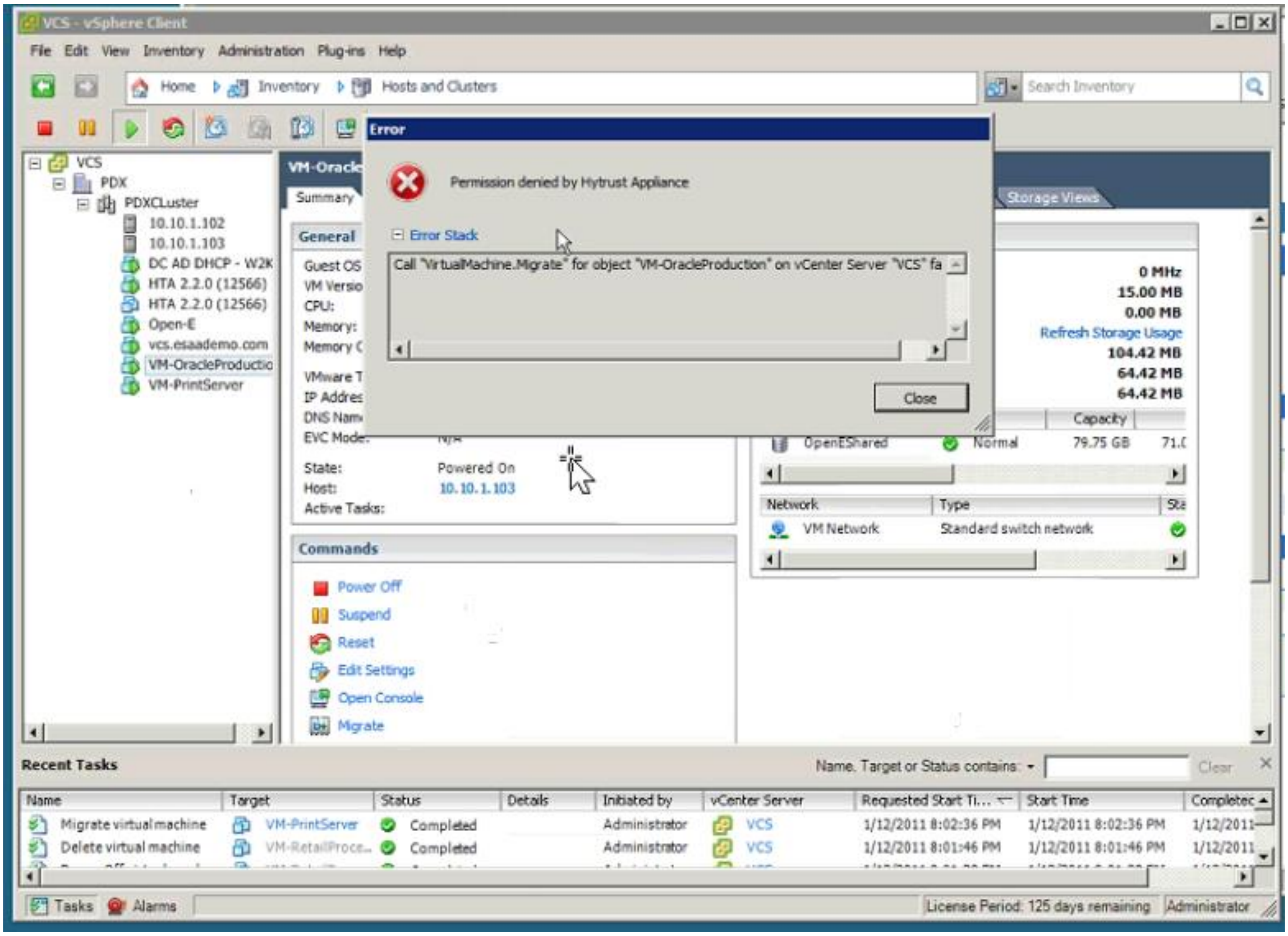
4. Click the "OK" button to save the settings. This constraint will ensure that VMs can only be moved to and from hosts that have Trusted status based on TPM attestation.
5. The next step is to assign the "Sec_SLA" RuleSet to the virtual machines that contain PCI data. Go to the "Policy" > **RuleSets** page, check the box next to the "PCI_workload" RuleSet, then click the "Assign" button. From the **Assign Policy RuleSets to Policy Resources** page, select the virtual machines that contain PCI data, then click the "OK" button.
6. "SSLA_administrators" also need to be granted basic login privileges. To grant those privileges, create a new rule with the default object assignment (HTA) which will grant the "SSLA_Administrators HT_BasicLogin" role.
7. To activate the policy, click the "Deploy" button; the policy will change from "Draft" to "Deployed".

Security Policy During VM On-Boarding

Similarly, the above policy can be extended to require that the workloads with PCI compliance requirements are only allowed to power-on on hosts with Trusted status and verified based on TPM measurement. To do that, a second constraint on the rule is also required:

1. Click the "Add" button again.
2. From the "Policy" > **Rules** page, click the "Create Draft" button again.
3. Check the box next to the rule for SSLA_Administrators added in the previous use-case, then click "Edit"
4. In the "Constraints" area select "Add".
5. In the wizard, select the "Host Label Match" constraint along with the "Trusted" box. Click the "OK" button to save the settings.
6. To activate the policy, click the "Deploy" button; the policy will change from "Draft" to "Deployed".
7. This constraint will enforce the on-boarding policies; high-security SLA workloads will only be powered-on in a Trusted environment.

Trust Policy Enforcement in the Infrastructure



Error

Permission denied by Hytrust Appliance

Error Stack

Call "VirtualMachine.Migrate" for object "VM-OracleProduction" on vCenter Server "VCS" fa

Guest OS
VM Versio
CPU:
Memory:
Memory C
VMware T
IP Addres
DNS Nam
EVC Mode: N/A

State: Powered On
Host: 10.10.1.103
Active Tasks:

0 MHz
15.00 MB
0.00 MB
Refresh Storage Usage
104.42 MB
64.42 MB
64.42 MB

			Capacity	
OpenEShared		Normal	79.75 GB	71.(

Network	Type	Sta
VM Network	Standard switch network	✓

Recent Tasks

Name, Target or Status contains:

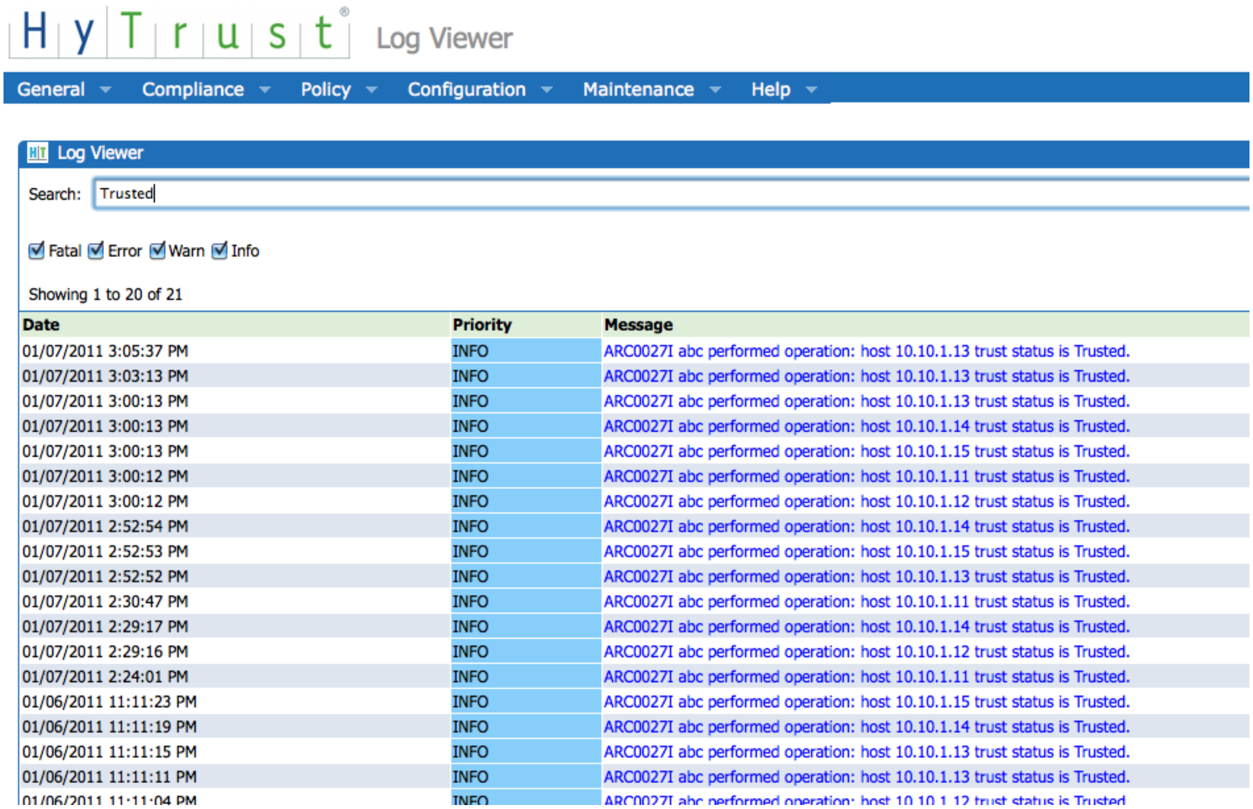
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completec
Migrate virtual machine	VM-PrintServer	Completed		Administrator	VCS	1/12/2011 8:02:36 PM	1/12/2011 8:02:36 PM	1/12/2011
Delete virtual machine	VM-RetailProce...	Completed		Administrator	VCS	1/12/2011 8:01:46 PM	1/12/2011 8:01:46 PM	1/12/2011

License Period: 125 days remaining | Administrator

Figure 14 – vSphere* Client Permission Denied by HyTrust Appliance* Message

To verify the policy is enforced, launch the vSphere* client from the client machine and connect to a VMware vCenter* Server public IP address. Attempts to power on a "Sec_SLA" VM on a host where the trust status was not verified or to migrate a VM to such a host will be blocked, and a message "Permission denied by HyTrust Appliance" will display.

An additional result of the policy enforcement is granular audit logging, which allows the Trust status of the platform, based on the hypervisor launch measurement taken by Intel® TXT to be reviewed and reported (See Figure 15). By searching the logs for "untrusted" labels, all possible violations of the chain of trust can be quickly identified. In addition, by using the logs side-by-side with the compliance and history dashboards, the remediated hosts can be verified that they are in good standing relative to their default template, and that the trust status was maintained.



Search: Trusted

☑ Fatal ☑ Error ☑ Warn ☑ Info

Showing 1 to 20 of 21

Date	Priority	Message
01/07/2011 3:05:37 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/07/2011 3:03:13 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/07/2011 3:00:13 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/07/2011 3:00:13 PM	INFO	ARC0027I abc performed operation: host 10.10.1.14 trust status is Trusted.
01/07/2011 3:00:13 PM	INFO	ARC0027I abc performed operation: host 10.10.1.15 trust status is Trusted.
01/07/2011 3:00:12 PM	INFO	ARC0027I abc performed operation: host 10.10.1.11 trust status is Trusted.
01/07/2011 3:00:12 PM	INFO	ARC0027I abc performed operation: host 10.10.1.12 trust status is Trusted.
01/07/2011 2:52:54 PM	INFO	ARC0027I abc performed operation: host 10.10.1.14 trust status is Trusted.
01/07/2011 2:52:53 PM	INFO	ARC0027I abc performed operation: host 10.10.1.15 trust status is Trusted.
01/07/2011 2:52:52 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/07/2011 2:30:47 PM	INFO	ARC0027I abc performed operation: host 10.10.1.11 trust status is Trusted.
01/07/2011 2:29:17 PM	INFO	ARC0027I abc performed operation: host 10.10.1.14 trust status is Trusted.
01/07/2011 2:29:16 PM	INFO	ARC0027I abc performed operation: host 10.10.1.12 trust status is Trusted.
01/07/2011 2:24:01 PM	INFO	ARC0027I abc performed operation: host 10.10.1.11 trust status is Trusted.
01/06/2011 11:11:23 PM	INFO	ARC0027I abc performed operation: host 10.10.1.15 trust status is Trusted.
01/06/2011 11:11:19 PM	INFO	ARC0027I abc performed operation: host 10.10.1.14 trust status is Trusted.
01/06/2011 11:11:15 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/06/2011 11:11:11 PM	INFO	ARC0027I abc performed operation: host 10.10.1.13 trust status is Trusted.
01/06/2011 11:11:04 PM	INFO	ARC0027I abc performed operation: host 10.10.1.12 trust status is Trusted.

Figure 15 – HyTrust* Log Viewer Page

Things to Consider

Architectural Issues

- Security: Security is one of the key considerations in server deployments, either virtualized or bare-metal. In a cloud deployment scenario, from both the perspective of the service provider and consumer, it is highly recommended to use platforms that support Intel® TXT, such as Intel® Xeon® processor 5600 series, along with supporting software platforms to create a trusted cloud environment that enjoys strong protection against compromise.
- Storage: For cost effectiveness and simplicity, a single NFS store was used as a shared storage for VM images. For production deployments, other alternatives may be chosen based on performance, cost and other factors.
- Scalability: The scalability of the VMware vSphere* test bed infrastructure has been greatly enhanced. Details on their performance enhancements can be found at http://www.vmware.com/files/pdf/vsphere_performance_wp.pdf.
- Networking: For the infrastructure test bed, 1 GbE connections were used for service console and VM networks, and a 100 Mbps link was used for the connection to BMC for out-of-band (OOB) power management. Depending on the customer requirements and usage, production environments might benefit from using 10 GbE or 100 GbE networks for VM networks.
- Hardware: It is beyond the scope of this document to fully discuss processor and overall server performance considerations. However, it is important to note that the performance of VMs that runs on virtualized platforms is heavily influenced by the processor architecture and specific feature sets available in the processor. The use of high performance server processors equipped with virtualization and I/O support feature sets, such as those provided by the Intel® Xeon® processor 5600 series, inclusive of Intel® Intelligent Power Node Manager and Intel® TXT, are strongly recommended. For more details on Intel virtualization technologies, please refer to www.intel.com/technology/virtualization/ and http://download.intel.com/business/resources/briefs/xeon5500/xeon_5500_virtualization.pdf.

Additional Usage Models Under Development:

- Trusted Boot of Virtual Machines: In this reference architecture, the trusted boot of the servers that runs a VMware ESXi* with HyTrust Appliance* is demonstrated. Intel continues to work to extend this usage to VMs as well. Because there is a limited number of hardware registers to store the digest information of the VMs that run on the host, a different architecture has to be developed. Also, storage of the VM digest information in the hardware registers greatly increases the complexity of the resource distribution algorithm. Security status on individual virtual machines would allow definition and enforcements of rich additional categorically policies in HyTrust Appliance.

- Tenant Visibility into Infrastructure: While a tenant is not in physical control of their infrastructure, trusted clouds must provide visibility to assess the security within the infrastructure. The management layer must report on the configuration of the virtual infrastructure the VMs use, tie these to a verifiable measurement of trust in the hardware and hypervisor, assess the actual security posture in the infrastructure, and provide provenance for auditing. HyTrust Appliance* enables tagging of tenant assets which in turn can be used for per-tenant reporting by the tenant and to enforce policies on the individual asset, such as requiring that a virtual machine runs only on the TPM-enabled platform with a Trusted status once it moves into the provider cloud.
- Secure Access Gateway: This model is similar to the Secure Services Transmittal. Based on their map of TCPs in the data center, a governance, risk and compliance monitor, and/or configuration manager reflects the service trust profile. If all TCPs that support workloads for the service are trusted, the service itself is stated to be trusted. Devices that attempt to access the trusted service based on policy management are only granted access to the service if the device hardware can attest to its integrity. A trusted device sends information that reflects its trust state as part of its service request. The service will grant access to the trusted services for that device based on policy management. If the policies indicate that an un-trusted device should not access a trusted service, that un-trusted device is not granted access to the service.

Summary and Conclusions

Usage models that use Intel® TXT to build an initial foundation for trust in the cloud are described in this reference architecture. The capabilities of Intel® TXT can form a basis to protect software from malware, which prevents unauthorized access of data, and halts unauthorized systems from booting. Specifically, protected execution, sealed storage, and protected launch harden a platform against emerging attacks on the BIOS, firmware, operating system, and hypervisor.

Intel® TXT is a technology to enable cloud eco-system security solutions. Through enabling trust attestation and machine authentication, Intel® TXT allows cloud providers to enforce strict security policies and provides trustworthiness to their services and platforms. Inside the servers that make up a cloud, Intel® TXT, in conjunction with hypervisors such as VMware vSphere*, can check each node's installation and verify the machine's health. When a problem is detected, further booting of a system can be prevented or other remediation steps implemented.

This reference architecture provides a guide to Intel® TXT and its integration to create a trusted cloud environment through the use of Intel® Xeon®, HyTrust Appliance* and VMware* products. The reader should be able to set-up and test a trusted attestation and machine identity model and prove the usefulness to their particular environment. Together, Intel® TXT, HyTrust Appliance, VMware vCenter* Server, VMware vSphere, and VMware ESXi* can provide a platform for a trusted cloud.

Glossary

Intel® Trusted Execution Technology (Intel® TXT): A hardware solution that validates the behavior of key components within a server or PC at startup.

Authenticated Code Modules (ACM): Platform-specific code that is authenticated to the chipset and that is executed in an isolated environment within the CPU. This term is also used to denote Authenticated Code Mode that is a trusted environment enabled by an AC Module to perform secure tasks.

Measured Launch Environment (MLE): The environment measured and launched as a result of the GETSEC [SENTER] instruction. This can be an operating system, virtual machine manager, or any trusted code that supports Intel® TXT.

PMBus 1.1: The Power Management Bus (PMBus) is an open standard power-management protocol. From: http://pmbus.org/specs.html.

Trusted Platform Module (TPM) 1.2 (third party silicon): A hardware device defined by the Trusted Compute Group* that provides a set of security features used by Intel® TXT.

Secure Initialization (SINIT): A trusted process that measures, validates, and launches an MLE.

Safer Machine eXtensions (SMX): The capabilities added to Intel processors that enable Intel® TXT.

Trusted Computing Group (TCG)*: Industry initiative for advancing computer security (http://www.trustedcomputinggroup.org)

Virtual Machine Extensions (VMX): A set of processor instructions defined by Intel® Virtualization Technology (Intel® VT) that software uses to provide isolation and protection for virtual environments (part of VT-x).

Intel® Virtualization Technology for Directed I/O (VT-d): Hardware support component of Intel® VT for management of DMA and interrupts generated by I/O devices.

Intel® Virtualization Technology for Execution™ (VT-x): A set of processor instructions (VMX) and capabilities defined by Intel® VT that software uses to provide isolation and protection for virtual environments.

Endnotes

1. Symantec Internet Security Threat Report, July-December 2007

2. "Data-breach costs rising, study finds," Network World, February 2, 2009.

3. Trusted Platform Module (TPM) Specifications, Trusted Computing Group*, http://www.trustedcomputinggroup.org/resources/tpm_main_specification

4. Windows* Hardware Compatibility List, http://www.microsoft.com/whdc/hcl/default.mspx

To learn more about deployment of cloud solutions, visit http://intel.com/cloudbuilders

Disclaimers

Δ Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

? Hyper-Threading Technology requires a computer system with an Intel processor supporting Hyper-Threading Technology and an HT Technology enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. See http://www.intel.com/info/hyperthreading/ for more information including details on which processors support HT Technology.

◊ Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security

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. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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 information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, Xeon, Xeon inside, Intel Data Center Manager, Intel Cloud Builders Test Bed, Intel Trusted Execution Technology, Intel Advanced Encryption Standard-New Instructions, and Intel Intelligent Power Node Manager are trademarks of Intel Corporation in the U.S. and other countries.

Copyright® 2011, HyTrust, Inc.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

325044-001US