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

Secure Cloud On-Boarding over Distance for Mission-Critical Applications

Intel® Xeon® Processor 5600 Series

EMC²

Audience and Purpose

The purpose of this document is to provide IT professionals with an overall understanding of technologies that simplify cloud on-boarding and cloud bursting operations. The paper will discuss migrating business critical applications between private and public clouds to take advantage of elastic compute resources as part of cloud on-boarding. This document will also review considerations for on-boarding securely across cloud environments leveraging Intel® Trusted Execution Technology (Intel® TXT).

September 2011

Table of Contents

Executive Summary

As companies look to migrate application workloads between cloud environments or between private and public (Service Provider) clouds, they are looking to simplify the migration or on-boarding process.

As server virtualization enabled hardware resources to be pooled into resource groups and dynamically allocated for application workloads, storage has also evolved beyond a point of simple consolidation into virtual storage, which allows storage resources to be aggregated and virtualized to provide a dynamic storage infrastructure to complement the virtual server infrastructure.

EMC VPLEX Metro delivers a virtual storage solution which builds on Fully Automated Storage Tiering (FAST) to address the need for cloud on-boarding through federation—delivering cooperating pools of storage resources. Federation enables IT to quickly and efficiently support the business through pools of resources that can be dynamically allocated. This flexibility elevates the value IT offers within the business, as application and data movement is possible for better support and higher quality of service (QoS). Together, cooperating pools of server applications and storage enable a new model of computing—IT-as-a-Service (IaaS).

As customers on-board applications between cloud environments, they must ensure that the hosts that they are migrating virtual machines to are secure. Intel® Trusted Execution Technology (Intel® TXT) allows you to validate the launch status of the host, thereby enabling the on-boarding of virtual machines onto trusted hosts while preventing virtual machines from being migrated to un-trusted hosts.

Introduction

Customer Cloud On-Boarding and Security Challenges

Today IT organizations are challenged with supporting a wide range of mission-critical applications across their extended enterprise. Organizations need to quickly and reliably optimize the performance of applications such as SAP, Microsoft SharePoint*, Microsoft Exchange*, and Oracle databases across geographically dispersed data centers. As more companies deploy hybrid cloud environments, IT organizations are challenged with migrating application workloads to utilize elastic compute resources in public clouds. This migration needs to happen quickly and seamlessly with no impact to the underlying storage that supports your applications.

Before server virtualization technologies, IT administrators could easily identify which physical servers that their application workloads ran on. As IT professionals embrace virtualization and build out cloud environments, it is crucial to validate that their applications workloads are being migrated between trusted hosts in trusted pools. Customers need to implement a solution that can attest to the identity of a host within and between cloud environments.

Preparing to On-Board Applications

There are several different methods to on-board virtual machines and virtual appliances (vApps) to service provider clouds, including the import of vApp templates. In the scope of this paper, we will review the benefits of federated storage to accelerate the cloud on-boarding process. Throughout the paper, the assumption is made that the Service Provider has presented the customer with compute, network, and storage resources before any on-boarding begins.

Traditional Application Migration

Traditionally, customers were tasked with the challenge of migrating data and applications between geographically-dispersed data centers through a series of manual, error-prone tasks and activities. Customers would either make physical backups or use data replication services to transfer application data to the alternate site. Applications had to be stopped and could not be restarted until testing and verification was complete.

In today's virtualized data centers, migrating a virtual machine from site to site requires a stretched storage area network (SAN). A downside to this type of configuration is that both VMware VMotion and VMware Storage VMotion are required to make the storage available at the distant site. This significantly adds to the time needed for failover, which limits the ability to easily move virtual machines from site to site.

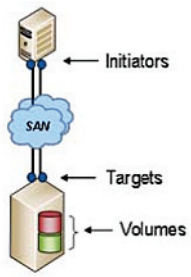


Figure 1: SAN-based storage access

The following image illustrates traditional SAN-based storage access.

Simplifying Cloud On-Boarding with EMC VPLEX Metro

Federation enables IT to quickly and efficiently support the business through pools of resources that can be dynamically allocated. This flexibility elevates the value IT offers within the business, as application and data movement is possible for better support of services. Together,

cooperating pools of server applications and storage enable a new model of cloud on-boarding. To address the need for mobility and flexibility to support cloud on-boarding and cloud bursting, EMC has developed federation-based storage solutions to provide cooperating pools of storage resources built on FAST.

EMC VPLEX Metro Overview

EMC VPLEX Metro is a SAN block local and distributed federation solution that allows the physical storage provided by traditional storage arrays to be virtualized, accessed, and managed across the boundaries between data centers. This new form of access, called AccessAnywhere*, removes many of the constraints of the physical data center boundaries and its storage arrays. AccessAnywhere storage allows data to be moved, accessed, and mirrored transparently between data centers, effectively allowing storage and applications to work between data centers as though those physical boundaries were not there.

EMC VPLEX Metro's unique scale-up and scale-out architecture along with advanced data caching and distributed cache coherency provides workload resiliency, automatic sharing, balancing, and failover of storage domains while enabling both local and remote data access with predictable service levels.

With EMC VPLEX Metro, these migration challenges can be resolved quickly and easily. Once the distributed RAID 1 device (DR1) is established, applications can be started immediately at the remote site, even before all the data has been copied over.

EMC VPLEX Metro provides companies with a more effective way of managing their virtual storage environments by enabling transparent integration with existing applications and infrastructure, and providing the ability to migrate data between remote data centers with no interruption in service.

Storage Access through a Storage Virtualization Layer

The following image illustrates storage access through a storage virtualization layer.

Figure 2: Storage access from VPLEX virtualization layer

The role of EMC VPLEX Metro in a SAN environment is both as a target and an initiator. From the host perspective, EMC VPLEX Metro is a target and from the back-end storage array perspective, EMC VPLEX Metro is an initiator. Through SAN zoning, hosts can have logical unit numbers (LUNs) presented from VPLEX, from the back end storage array directly, or both. This flexibility allows for easy migration from a standalone storage array to a VPLEX LUN using VMware Storage VMotion.

Using EMC VPLEX Metro, IT departments can migrate and relocate virtual machines, applications, and data within, across, and between data centers. EMC VPLEX Metro works in conjunction with VMware VMotion and Storage VMotion to support cloud on-boarding and cloud bursting operations.

Non-Disruptive Migration

VMware Storage VMotion can be used to non-disruptively migrate from a directly-accessed storage array to a LUN presented through EMC VPLEX Metro. This is accomplished by presenting both the original LUN and the new EMC VPLEX Metro LUNs to the hosts at the same time and then executing VMware Storage VMotion from the original LUN to the EMC VPLEX Metro LUN. Assuming there is no need to revert to the original LUN, that original LUN can then be reclaimed by the storage array and the disk capacity made available for other purposes.

This approach to cloud on-boarding and cloud bursting is based on VMware vSphere and Intel x86-based servers. This virtual infrastructure is shared across applications and clustered to achieve redundancy and failover capability. EMC VPLEX Metro can be utilized to present shared data stores across from the customer's virtualized data center and the service provider cloud, enabling VMotion migration of application virtual machines (VMs) between the cloud environments.

Solution Architecture

Overview

In the below scenario, the company contracts with their Service Provider for IaaS services that can be used to support the company's expansion initiatives. As the company continues to grow, compute, storage, and network resources can be leveraged from the Service Provider's IaaS offering.

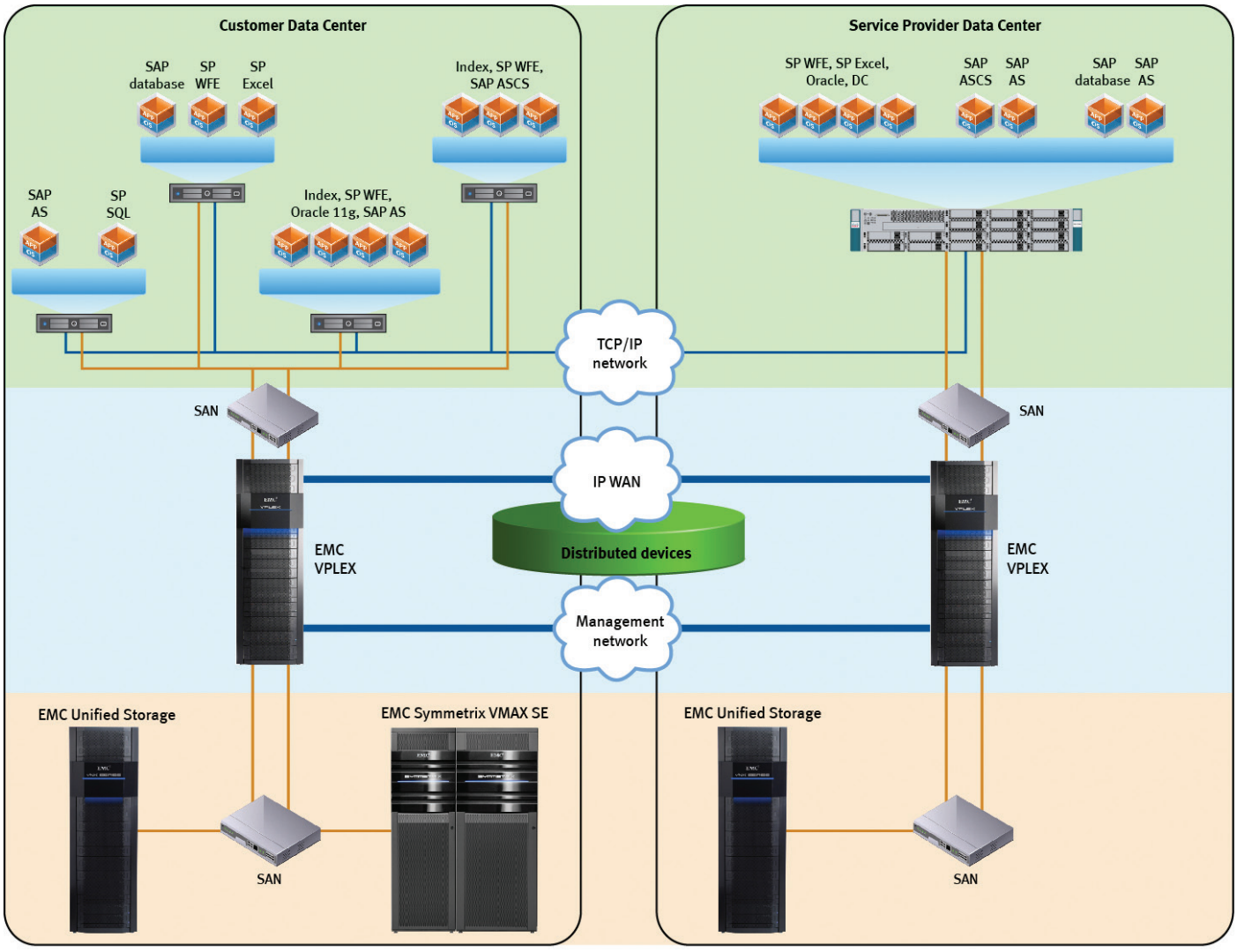


Figure 3: Solution architecture map

Hardware Configuration

Site A – Microsoft and Oracle application environment

The virtual infrastructure at Site A for Microsoft and Oracle consists of the following enterprise-class servers (two in total) running VMware vSphere 4 Update 1:

Configuration 1	
Part	**Description**
Memory	128 GB RAM
CPUs	4: 6 core, 2.659 GHz Intel® Xeon® X7460processors
SAN and network connections	▪ 2: 10 GB Emulex LightPulse LP21000 CNAs for Fibre Channel and Ethernet connectivity ▪ 2: Broadcom 5708 GbE adapters
High Availability networking	▪ 2: 1 Gb/s physical connections for the VMware service console ▪ 2: physical 10 Gb/s connections on a VLAN for virtual machine application connectivity and VMotion
VMDKs	Virtual machine disks were used for the virtual machines' boot LUNs, as well as the application data LUNs

Configuration 2	
Part	**Description**
Memory	96 GB RAM
CPUs	2: Quad core, 2.67GHz Intel® Xeon® E5650processors
SAN and network connections	2 x 10 GB Emulex CNA adapters
VMDKs	Virtual machine disks were used for the virtual machines' boot LUNs, as well as the application data LUNs

Site B – Microsoft, Oracle, and SAP application environment

The virtual infrastructure at Site B for all applications consists of the following enterprise-class Cisco UCS blade servers, running VMware vSphere 4 Update 1:

Configuration 1	
Part	**Description**
Memory	48 GB RAM
CPUs	2: Quad core, 2.526 GHz Intel Xeon E5540 processors
SAN and network connections	2: Cisco UCS CNA M71KR-E-Emulex FCoE CNAs for Fibre Channel and Ethernet connectivity
High Availability networking	2: Physical 10 Gb/s connections for virtual machine application connectivity, VMotion, and VMware Service Console
VMDKs	Virtual machine disks were used for the virtual machines' boot LUNs, as well as the application data LUNs

Configuration 2	
Part	**Description**
Memory	96 GB RAM
CPUs	2: Quad core, 2.67GHz E5650 Intel Xeon processors
SAN and network connections	2 x 10 GB Emulex CNA adapters
VMDKs	Virtual machine disks were used for the virtual machines' boot LUNs, as well as the application data LUNs

The solution architecture depicted above represents the typical production environment of customers with multiple server models. For the first use model, we featured Cisco UCS systems. For the secure on-boarding usage model, another set of servers powered by Intel® Xeon® 5600 series processors supporting Intel TXT were used. While the test hardware used for this paper changed, the cloud on-boarding and secure cloud on-boarding are complimentary usage models.

Introduction to the Common Elements

The virtualized data center environment described in this white paper was designed and deployed with a shared infrastructure in mind. From server to local and distributed federation to network consolidation, all layers of the environment were shared to create the greatest return on infrastructure investment, while achieving the necessary application requirements for functionality and performance.

Using server virtualization, based on VMware vSphere, Intel x86-based servers were shared across applications and clustered to achieve redundancy and failover capability. VPLEX Metro was used to present shared data stores across the physical data center locations, enabling vMotion migration of application VMs between the physical sites. Physical Site A storage consisted of a Symmetrix VMAX Single Engine (SE) for the SAP environment, and an EMC Unified Storage for the Microsoft and Oracle environments. Vblock 1 was used for the physical Site B data center infrastructure and storage.

For detailed step by step setup information please refer to the following whitepaper: http://www.emc.com/collateral/hardware/white-papers/h6983-vmotion-distance-apps-vblock-vmax-clariion-vplex-wp.pdf

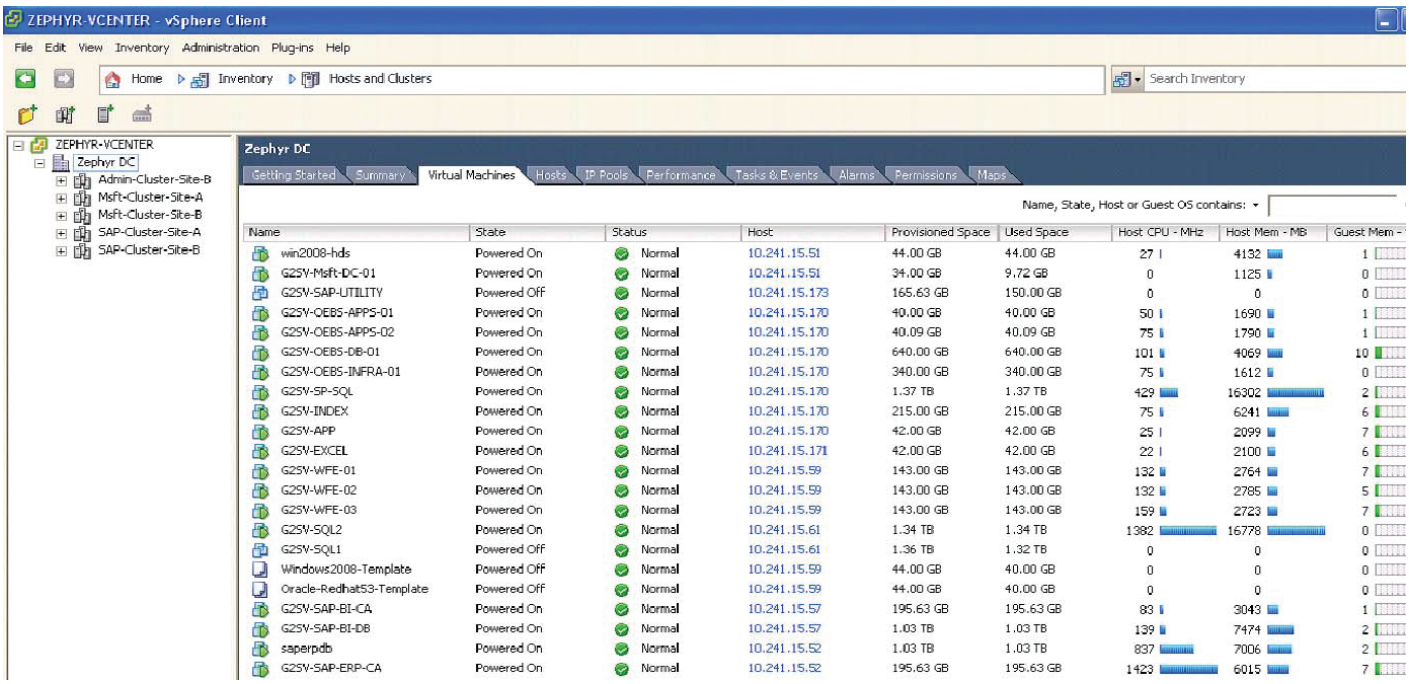
VMware vSphere

VMware vSphere is the industry's most reliable platform for data center virtualization of the IT infrastructure. It enables the most scalable and efficient use of the x86 server hardware in a robust, highly-available environment.

VMware ESX Server:

- Abstracts server processor, memory, storage, and networking resources into multiple virtual machines, forming the foundation of the VMware vSphere 4 suite.
- Partitions physical servers into multiple virtual machines. Each virtual machine represents a complete system with processors, memory, networking, storage, and BIOS.
- Shares single server resources across multiple virtual machines and clusters ESX Servers for further sharing of resources.
- VMware vSphere Configuration
- In this portion of the solution, VMware vSphere was configured as follows:
- Site A—Microsoft and Oracle application environment
- Site A—SAP application environment
- Site B—Microsoft, Oracle, and SAP application environment

The following image shows the Site A and Site B clusters.



EMC Symmetrix VMAX

Overview

The EMC Symmetrix VMAX series provides an extensive offering of new features and functionality for the next era of high-availability virtual data centers. With advanced levels of data protection and replication, the Symmetrix VMAX system is at the forefront of enterprise SAN technology. Additionally, the Symmetrix VMAX array has the speed, capacity, and efficiency to transparently optimize service levels without compromising its ability to deliver performance on demand. These capabilities are of the greatest value for large virtualized server deployments such as VMware virtual data centers.

The Symmetrix VMAX system is EMC's high-end storage array that is purpose-built to deliver infrastructure services within the next-generation data center. Built for reliability, availability, and scalability, Symmetrix VMAX uses specialized engines, each of which includes two redundant director modules providing parallel access and replicated copies of all critical data.

Symmetrix VMAX's Enginuity* operating system provides several advanced features, such as:

- Auto-provisioning groups for simplification of storage management
- Virtual Provisioning* for ease of use and improved capacity utilization
- Virtual LUN technology for non-disruptive mobility between storage tiers

Configuration

The SAP application environment deployed in this solution used a Symmetrix VMAX array for the primary storage at Site A. Boot and data LUNs were provisioned as detailed in the following table.

Note: See the SAP section of this white paper for the breakdown detail of the LUN allocation by virtual machine.

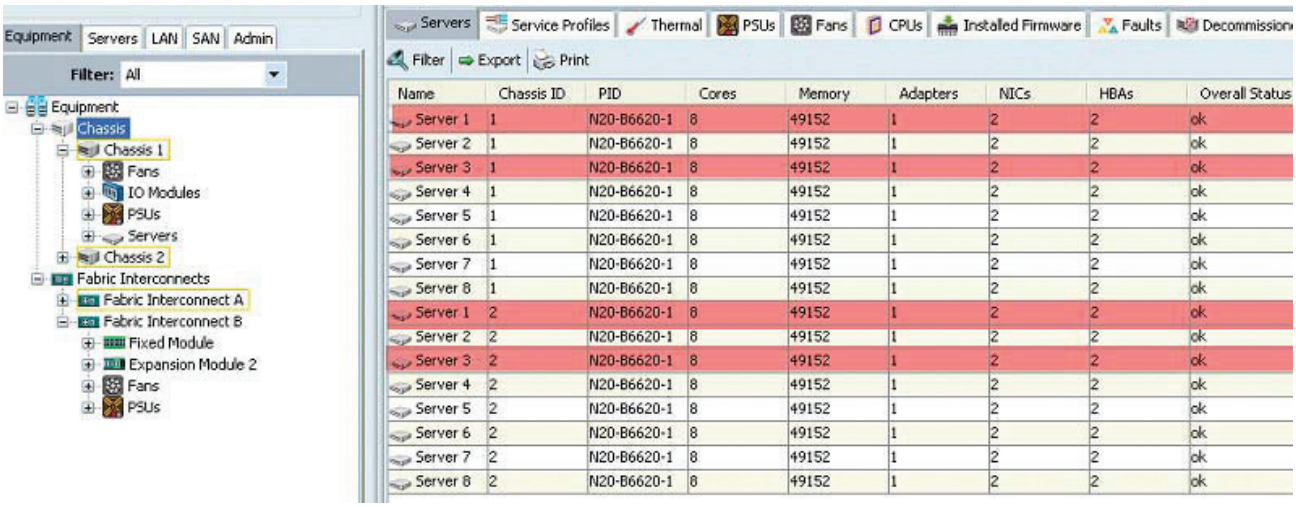
Capacity	Number of LUNs	RAID type
500 GB	2	RAID 5 (7+1)
250 GB	6	RAID 5 (7+1)
85 GB	8	RAID 5 (7+1)
65 GB	2	RAID 5 (7+1)
32 GB	4	RAID 1/0

All drives were 400 GB 15k FC drives. LUNs were presented from the Symmetrix VMAX through two front-end adapter (FA) directors for redundancy and throughput. After encapsulation into VPLEX Metro, devices of the same size and type were presented as DR1s.

At Site B, the computer resources were provided by Cisco UCS B-Series Blade Servers and the storage resources from EMC Unified Storage. Each Cisco UCS chassis contains B-200 series blades, six with 48 GB RAM and two with 96 GB RAM. This offers good price and performance and supports memory-intensive applications. There are no hard disk drives in the B-200 series blades as all boot services and storage are provided by the SAN and the EMC Unified Storage.

Four of the 16 server blades were used in the testing of this environment, as illustrated in the following image.

Two two-node ESX clusters were created at Site B: one to host Microsoft and Oracle applications, and one to host the SAP application. The storage was sized to duplicate the primary site environment. Devices were configured as part of the DR1 devices created in VPLEX Metro, being paired with the primary site LUNs.



EMC Unified Storage

Overview

EMC Unified Storage brings flexibility to multi-protocol environments. With EMC Unified Storage you can connect to multiple storage networks using NAS, iSCSI, and Fibre Channel SAN in an integrated package. EMC Unified Storage leverages advanced technologies like EMC FAST VP and EMC FAST Cache to optimize performance for the virtual desktop environment, helping support service level agreements of mission critical applications

Customers can leverage EMC Fully Automated Storage Tiering for Virtual Pools (FAST VP) and FAST Cache to optimize storage performance for virtual desktop environments. EMC FAST VP works at the storage pool level, below the LUN abstraction at a far more granular level than previous versions of FAST. As an example, rather than move an 800 GB LUN to Flash drives, FAST VP now identifies and monitors the entire storage pool in 1 GB chunks. As shown in the figure below, when data becomes active, then FAST VP automatically moves only these "hot" chunks to a higher tier like flash.

As data cools, FAST VP also correctly identifies which chunks to migrate to lower tiers and proactively moves them. With such granular tiering, it is now possible to reduce storage acquisition while at the same time improve performance and response time.

EMC FAST Cache, a part of the VNX FAST suite, enables flash drives to be used as an expanded cache layer for the array. FAST Cache has array-wide features available for both file and block storage. FAST Cache works by examining 64 KB chunks of data in FAST Cache enabled objects on the array. Frequently accessed data is copied to the FAST Cache and subsequent accesses to that data chunk are serviced by FAST Cache. This allows immediate promotion of very active data to the flash drives. This dramatically improves the response time for very active data and reduces the data hot spots that can occur within the LUN.

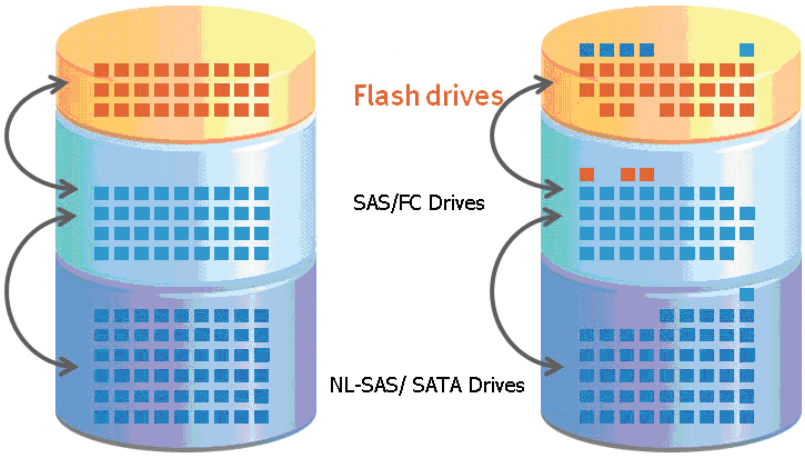


Figure 4: FAST VP data movement

Configuration

The application environments deployed in this solution used EMC Unified Storage for the primary storage. Boot and data LUNs were provisioned as detailed in the following tables.

Capacity	Number of LUNs	RAID type
200 GB	2	RAID 5 (4+1)
150 GB	2	RAID 5 (4+1)
125 GB	4	RAID 5 (4+1)
100 GB	16	RAID 5 (4+1)
75 GB	24	RAID 5 (4+1)
50 GB	3	RAID 5 (4+1)
20 GB	12	RAID 1/0
15 GB	4	RAID 5 (4+1)
500 GB	1	RAID 5 (4+1)
150 GB	2	RAID 1/0
80 GB	4	RAID 5 (4+1)
50 GB	1	RAID 5 (4+1)

All drives were 400 GB 15k FC drives. LUNs were presented from the Unified Storage through four storage processor (SP) ports for multipathing support (providing redundancy and throughput). After encapsulation into the VPLEX Metro, devices of the same size and type were presented as DR1 devices.

On-Board Securely with Intel TXT

As companies on-board their applications into multi-tenant environments, IT professionals must be able to verify that they are migrating virtual machines onto hosts that are located within a trusted pool. Intel TXT allows you to validate the launch status of the host, thereby enabling the on-boarding of virtual machines onto trusted hosts. Intel TXT provides the necessary underpinnings for reliable evaluation of the computing platform and the platform's level of protection. For a detailed overview of Intel TXT please refer to "Intel Trusted

Execution Technology: Hardware-based Technology for Enhancing Server Platform Security." [05]

Intel TXT 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 integrity of data 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): A hardware device defined by the Trusted Compute Group that stores authentication credentials in platform configuration registers (PCRs), which are issued by Intel Trusted Execution Technology
- Intel TXT-enabled BIOS, firmware, operating system, and hypervisor environments

The full 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.
- **Attestation**: Enables a system to provide assurance that the protected environment has been 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. Rather than relying upon the detection of malware, Intel TXT works before malware can be launched as it builds trust into a known software environment, thereby ensuring 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 your cloud. Intel TXT works with Intel® Virtualization Technology (Intel® VT) to create a trusted, isolated environment for VMs.

The launch time protection that Intel TXT provides for a host becomes all the more important and powerful when you consider the deployment of such hosts in virtualized and cloud-based implementations. As these implementations abstract the physical hardware and because of multi-tenancy movement across shared infrastructure, they require more than traditional perimeter-oriented security techniques.

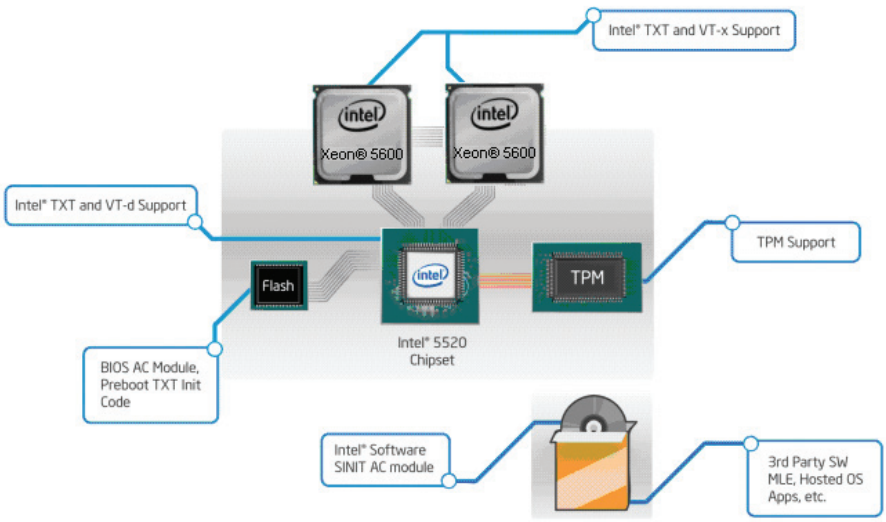


Figure 5: Intel TXT Components

When a VM that is compromised because of a compromised host is migrated to another host, there is a possibility of impacting the new host along with the other VMs running on that host. Intel TXT can help address this issue by creating something known as "trusted compute pools". In this model, Intel TXT is used to create a pool of trusted hosts, each with Intel TXT enabled and by which the platform launch integrity has been verified. A policy is then created that restricts the migration of VMs such that only those on trusted platforms can be migrated to other trusted platforms and vice versa. Fig below shows how VM migration can be controlled across resource pools using trust as control instrumentation for migration policy. A small box icon at the bottom indicates a trusted host.

Installation and Configuration

In this test environment, a prototype Intel plug-in to VMware vCenter for Enhanced Platform Security was leveraged to support trusted migration. As highlighted in the figure below, Intel TXT functionality integrates directly with VMware Center to simplify cross-cloud migrations and cloud on-boarding. Throughout this environment the IntelpPlug-in to VMware vCenter for Enhanced Platform Security appears as the Cloud 2015 TXT tab.

Below are the high level steps for the setup and configuration.

ESXi Hosts

- BIOS changes
  - Update the BIOS and firmware to the latest version supporting TXT
  - Setup the BIOS password
  - Enable VT, VT-D and set TPM to enabled and activated for storing measurements
  - Enable TXT
- Install VMware ESXi 4.1 U1 or higher build on the hosts

VMware Components

The high-level steps for the installation and configuration of the infrastructure setup required to exercise the Intel TXT capabilities supported by platform are listed below.

These setup steps assume that the reader has a basic understanding of how to install and configure Windows Server* 2008 R2 Enterprise, VMware vCenter Server, and VMware vSphere Client.

- To set up Windows Server 2008 R2 Enterprise:
  - Install Windows Server 2008 R2 Enterprise on compatible hardware.
  - Configure the web server (IIS) role, choosing WebDav Publishing, Application Development, Basic Authentication, Windows Authentication, and II6 Management Compatibility services.
  - Check that IIS is configured to process the ASPX pages. Confirm that they are among the MIME types supported. If not configured, create a new MIME type for ASPX pages.
  - For Intel plug-in we need to setup a backward compatibility with ISS 6.0. Open up the "Server Manager" and click on the "Web Server (IIS)" Role. Scroll down to "Role Services" section and click on "Add Role Services" option on the right side and enable the "IIS 6 Management Compatibility" option as shown below. Please select all the sub options under "IIS 6 Management Compatibility."
  - Also since the plug-in uses Windows Authentication, open up the "Server Manager" again and click on the "Web Server (IIS)" Role. Scroll down to "Role Services" section and click on "Add Role Services" option and enable "Windows Authentication" service as will under the "Web Server (IIS)" role.
- Install the vCenter Server prototype and vSphere Client
  - Install the VMware vCenter 4.1 U1 or higher build. Set the HTTP port to 81 and HTTPS port to 444 (another port number could be used as well), as the IIS runs on the same system. If you choose to use a different system for vCenter, the default ports need not be changed.
  - Depending on the scalability needed, an appropriate database should be used. A default SQL Server Express* edition is sufficient for a small database instance.
  - Install vSphere Client 4.1* with default settings.
- vCenter configuration
  - First create a "Datacenter" & "Cluster." For the cluster configuration, turn on "VMware DRS" option with "Automation Level" set to "Manual." Keep the default values for the "Power Management" configuration. Depending on the configuration of the ESXi hosts built choose appropriate "VMware EVC" mode.
  - For example: If the cluster will have only Intel ® Xeon® 5500 and 5600 servers, choose "Intel® Core™ i7" as your EVC Mode configuration. This mode will support flex migration of VMs between Intel Xeon 5500 and 5600 systems.
  - Add the ESXi host to the vCenter Server and complete all the required configurations for live migrations.
  - For each of the TXT enabled hosts added to the vCenter server, set the "Misc.enableTboot" to 1, which is located under Configuration->Software->Advanced Settings->Misc option. Finally reboot the ESXi host.

- After the reboot, verify the trusted boot of the ESXi host using the Managed Object Browser tool. After the login to the tool follow the below hierarchy to verify that the host is trusted.
- Content -> rootFolder -> childEntity -> hostFolder -> childEntity -> host -> runtime -> tpmPcrValues -> PCR[20] (vmware-vkernel)

▪ Intel Plug-In

- Install the plug-in on the server configured with IIS. Change the default virtual directory where the plug-in needs to be installed.
- After the successful installation, update the following attributes of the Web.Config file located in the installation directory:
  * The URL for VMware vCenter Server
  * The URL for the plug-in installation & other attributes that use the value.
- Edit the ESXHosts.XML file and ensure that there are entries for each of the hosts configured in the VMware vCenter Server. Clear the values of "digest" and "bootTime" fields.
- Modify the physical security settings of the ESXHosts.XML file so that Windows IIS account would have read/write privileges.
- Edit the URL fields of MOB_ExtMgr.xml & TXTPlugIn.xml files to point to the right installation folder. Register the plug-in with the contents of the MOB_ExtMgr.xml using the Managed Object Browser (MOB) tool provided as part of the vCenter Server installation.
- Log in to the vCenter Server through the vSphere Client. Click on the data center name created during the configuration of vCenter Server. A new tab corresponding to the plug-in installed will appear on the right-hand side of the vSphere Client
- Create a VM custom attribute called "TrustedBoot" by going to the VM's summary tab and clicking on the edit option of "Annotations." This value would be used to decide whether a VM would need a trusted host for execution or not.

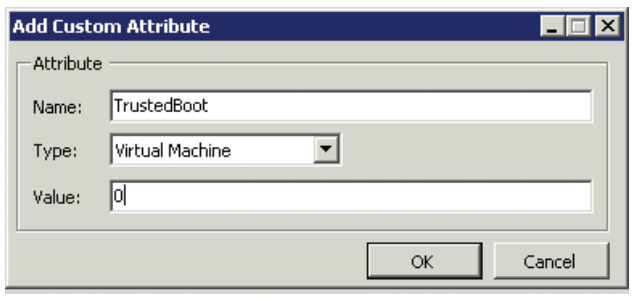
Data Object Type: **HostRuntimeInfo**
Parent Managed Object ID: **host-182**
Property Path: **runtime**

Properties

NAME	TYPE	VALUE
bootTime	dateTime	"2011-05-31T04:27:52.04918Z"
connectionState	HostSystemConnectionState	"connected"
dasHostState	ClusterDasFdmHostState	Unset
dynamicProperty	DynamicProperty[]	Unset
dynamicType	string	Unset
healthSystemRuntime	HealthSystemRuntime	healthSystemRuntime
inMaintenanceMode	boolean	false
powerState	HostSystemPowerState	"poweredOn"
standbyMode	string	"none"
tpmPcrValues	HostTpmDigestInfo[]	tpmPcrValues

[20] HostTpmDigestInfo

NAME	TYPE	VALUE
digestMethod	string	"SHA1"
digestValue	byte[]	-28, -83, -25, -9, -31, -121, 83, -87, 71, -64, -40, -80, 31, -118, 10, 40, -108, 100, -24, 125
dynamicProperty	DynamicProperty[]	Unset
dynamicType	string	Unset
objectName	string	"vmware-vmkernel"
pcrNumber	int	20



Secure Cloud On-Boarding Usage Models

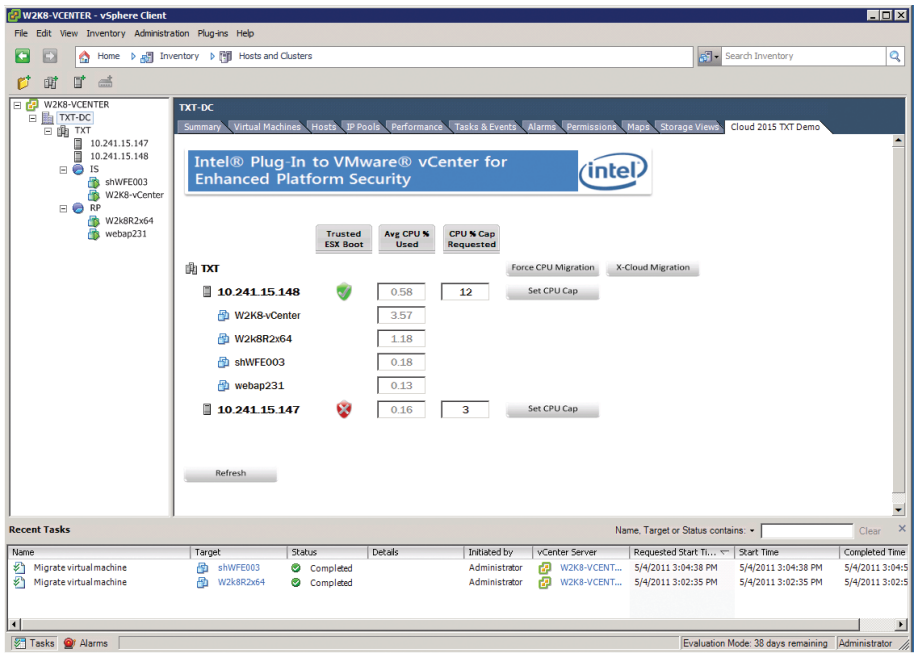
Trusted to Un-Trusted Host

Customers can leverage the integration of Intel TXT with VMware vCenter to attest the platform's launch status.. In this prototype environment, the Intel plug-in to VMware vCenter for Enhanced Platform Security was leveraged to support trusted migration. As highlighted in the figure below, Intel TXT functionality integrates directly with VMware Center to simplify cross-cloud migrations and cloud on-boarding. In the tested environment the Intel plug-in to VMware vCenter for Enhanced Platform Security appears as the Cloud 2015 TXT tab.

As shown in the above figure, Intel TXT functionality has been enabled within the BIOS of host 10.241.15.148, but has not been enabled yet on host 10.241.15.147. Here in this VMware vSphere environment, host 10.241.15.148 is supporting the following virtual machines:

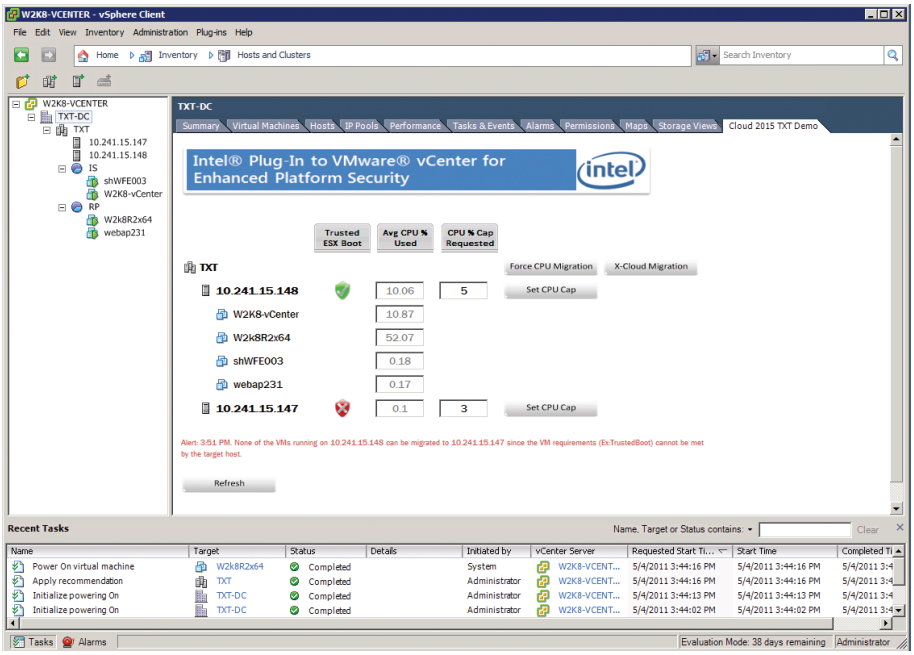
- Microsoft SharePoint 2010 Web-Front End server
- Microsoft 2008R2 Server
- Web Application Server
- Microsoft 2008R2 Server running VMware vCenter

Also all the VMs configured in this prototype environment were enabled for "TrustedBoot" policy as described in the setup and configuration section. To test the Intel TXT functionality, a VMotion of the Microsoft 2008R2 virtual machine to the un-trusted 10.241.15.147 host is attempted.



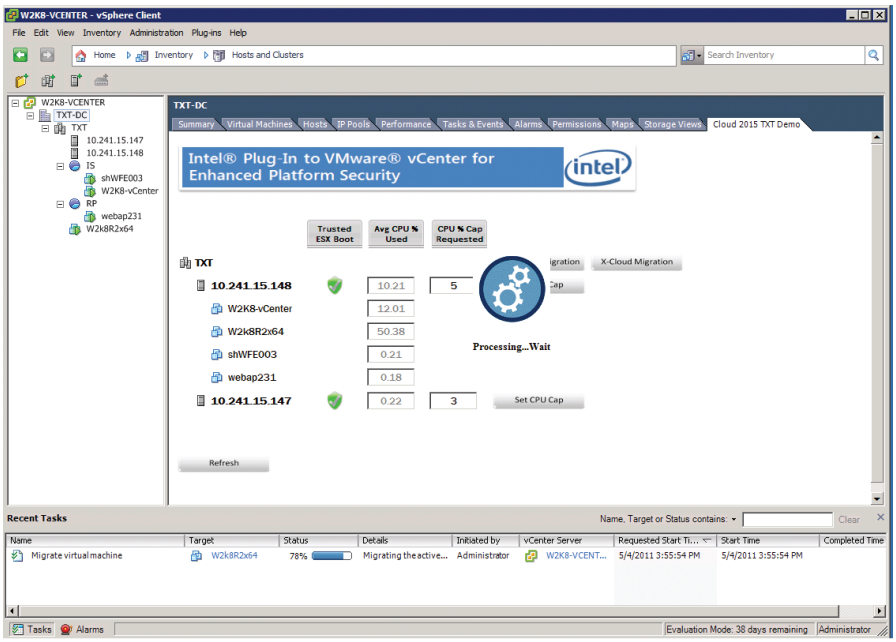
Results

Intel TXT ensures that VMs can only be migrated onto trusted hosts between cloud environments. As shown below, Intel TXT prevented the VM from migrating onto the un-trusted host within the Data Center. At 3:51 PM, an alert appeared within the plug-in tab, informing the user that no virtual machines were migrated as the trusted boot requirements were not met.



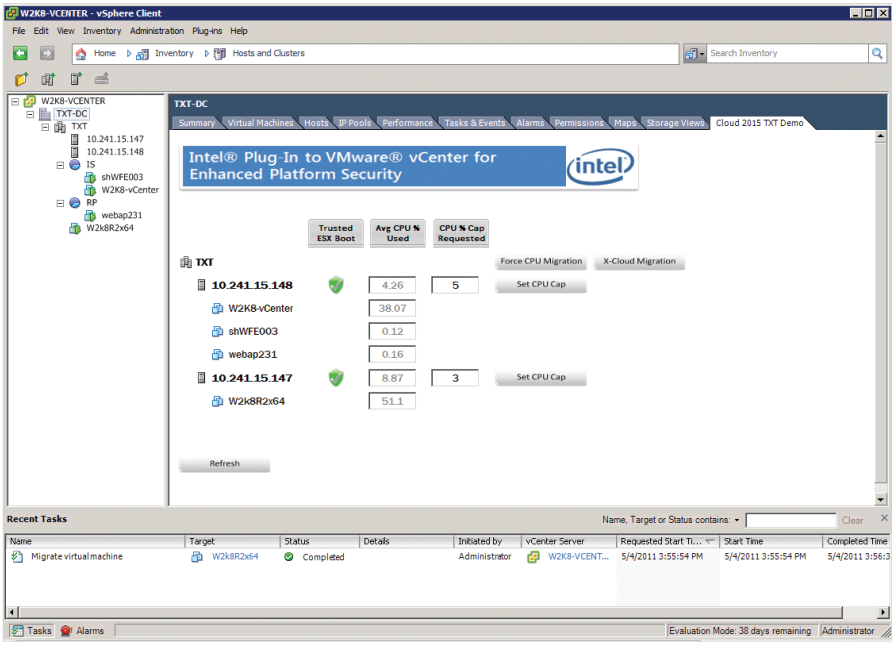
Trusted to Trusted Host

To test a successful VMotion between trusted hosts, Intel TXT functionality was enabled on the BIOS of host 10.241.15.147. Once the Intel TXT functionality was enabled on the10.241.15.147 host, a VMotion of the Microsoft 2008R2 VM was attempted in the figure below.



Results

As shown by the below figure, the VMotion operation was successful as the target host (10.241.15.147) met the trusted boot requirements.



Summary

EMC and Intel can help accelerate cloud on-boarding with EMC VPLEX Metro and advanced technology such as Intel TXT. EMC VPLEX Metro allows you to migrate active application workloads between cloud environments with latencies up to 5ms, simplifying the cloud on-boarding process with its AccessAnywhere technology. As you migrate application workloads across cloud environments you can validate that the target hosts are located within a trusted pool with support from Intel TXT. This attestation process is simplified as Intel has developed the Intel Plug-in to VMware vCenter for Enhanced Platform Security allowing you to leverage the familiar VMware interface. Regardless of where you are in the cloud building process, EMC and Intel can help you ensure a quality application experience for your end users while increasing business agility across your enterprise.

Appendix A: VMware Infrastructure Client Plug-Ins

In an abstract sense, a cloud plug-in is a pre-packaged technology building block that implements a new capability. The plug-in is inserted into a pre-existing application, preferably through a published interface to enhance the application with the new capability. The Intel TXT plug-in gives the application an ability to enforce a measured hypervisor launch.

The framework to achieve enhanced platform security in a virtualized cloud environment relies on the careful orchestration of a set of collaborating technologies. The orchestration is loosely coupled, mainly through the use of Web services. The loosely coupled nature of the solution is an essential characteristic to enable rapid integration of mature, pre-fabricated, and working solution components. A green field environment and a blank slate for development are no longer practical luxuries, and time-to-market requirements would make more traditional tightly coupled solutions equally impractical.

Technology plug-ins are integrated through pluggable technology building blocks architected for extensibility with well-defined Web services interface points. The architecture supports very late binding of new components. These components can essentially be inserted in a running system with minimal effect on the pre-existing capabilities.

In this paper, we provided a constructive proof of how it is possible to set up migration policies for a set of VMs to stay within the confines of a trusted pool with operating rules enforced by the hardware. Likewise, hardware mechanisms prevent extraneous VMs from landing in a pool that has been designated as trusted. The trusted pools effectively define a secure, sanitized enclave, where only VMs with known properties are allowed to run. This capability is known as a measured launch in Intel TXT parlance. This property is useful for support in multi-tenant environments. The support in the hardware makes it much more difficult for the environment to be subverted.

Additional Resources

- **EMC Solutions for VMware**: http://www.emc.com/solutions/application-environment/vmware/index.htm
- **VMotion Over Distance for Microsoft, Oracle, and SAP Enabled by VCE Vblock 1, EMC Symmetrix VMAX, EMC CLARiiON, and EMC VPLEX Metro**: http://www.emc.com/collateral/hardware/white-papers/h6983-vmotion-distance-apps-vblock-vmax-clariion-vplex-wp.pdf
- **Intel Cloud Builders**: www.intel.com/cloudbuilders
- **Virtualizing Information Infrastructure**: http://www.emc.com/solutions/business-need/virtualizing-information-infrastructure/index.htm
- **Intel® TXT**: Hardware-based technology for enhancing server platform security: http://www.intel.com/content/www/us/en/trusted-execution-technology/trusted-execution-technology-security-paper.html
- **Creating a new MIME type for ASPX processing**: http://support.microsoft.com/kb/326965
- **VirtualCenter VMotion Requirements**: http://pubs.vmware.com/vi3/resmgmt/wwhelp/wwhimpl/common/html/wwhelp.htm?context=resmgmt&file=vc_create_cluster.7.4.html
- **Registering VI Client Plug-in without a single line of code**: http://communities.vmware.com/docs/DOC-9203

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.