

BUILDING A PRIVATE CLOUD

How Platform Computing's Platform ISF* Can Help

MARK BLACK, CLOUD ARCHITECT, PLATFORM COMPUTING

JAY MUELHOEFER, VP OF CLOUD MARKETING, PLATFORM COMPUTING

PARVIZ PEIRAVI, PRINCIPAL ARCHITECT, INTEL

MARCO RIGHINI, SOLUTION ARCHITECT, INTEL

Cloud computing is a paradigm shift in the way IT is developed, managed, and consumed. It provides infrastructure and computer resources as services. End users request IT services through a Web browser or a computer using an API. These services are provisioned from a pool of shared computing resources according to corporate standards and business policies. Each line of business (LOB)

SUPPORTING FLEXIBILITY AND CHOICE

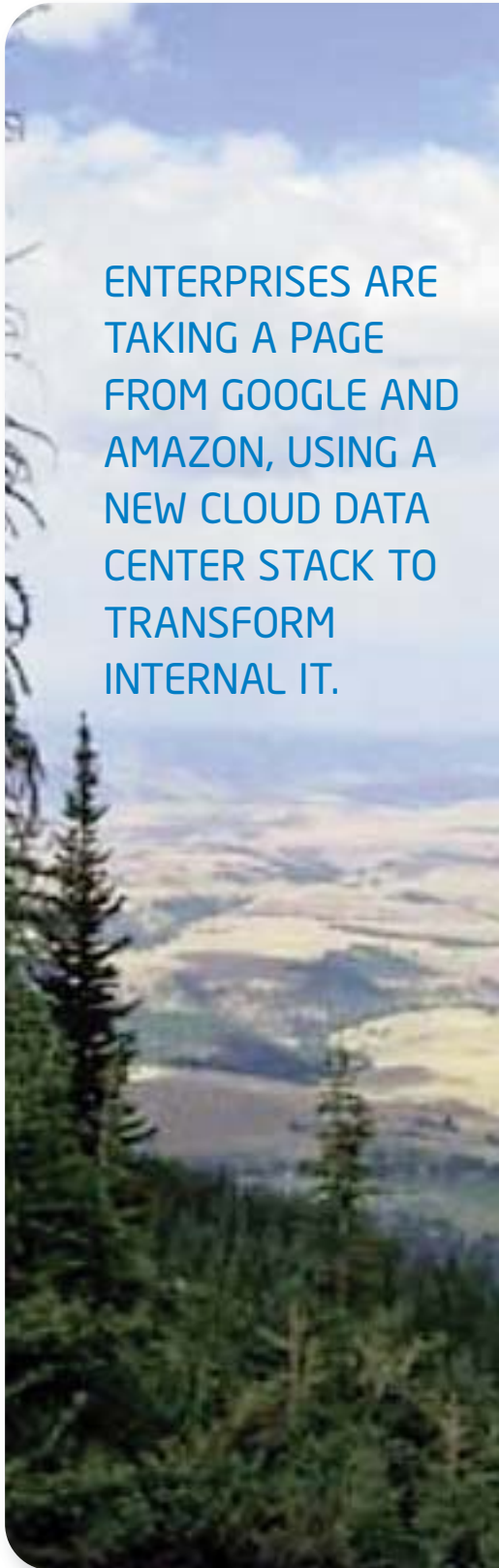
can have its own self-managed, virtual private cloud to get the benefits of IT consolidation without losing the ability to self-manage and optimize the cloud for their business. However, the private cloud administrator still maintains overall control and defines the top-level constraints for each LOB. The concept is a cloud within a cloud. Within each virtual LOB cloud, business policies optimize the cloud according to specific needs such as performance, efficiency, high availability, and scalability.

Enterprises looking to take advantage of the cloud do so for many reasons—chief among them to enhance their agility in response to changing business dynamics. Today's enterprise data center is facing tremendous pressure to both innovate with new cloud architectures and operate legacy applications and heterogeneous systems. With that reality, it's cru-

cial to adopt an open cloud management solution that supports flexibility and choice.

Large enterprises continue to recognize the need for a private cloud to meet regulatory, security, and performance requirements. To achieve agility and cost objectives, enterprises are taking a page from Google and Amazon, using a new cloud data center stack to transform internal IT.

Cloud uses your company's investment in virtualization—such as with VMware vSphere* and other hypervisor providers—and must have a deep integration with virtual machine (VM) technologies. However, the new cloud data center requires more than just virtualization and traditional IT practices. Cloud management is a layer, purpose-built for cloud infrastructure and processes, that co-exists with legacy and bridges to the future. Key capabilities need to include



ENTERPRISES ARE
TAKING A PAGE
FROM GOOGLE AND
AMAZON, USING A
NEW CLOUD DATA
CENTER STACK TO
TRANSFORM
INTERNAL IT.

MEETING ENTERPRISE DEMANDS

self-service and chargeback, policy-based automated provisioning of applications, dynamic scaling of applications to meet service-level agreements (SLAs), and unification of distributed and mixed-vendor resource pools for sharing.

Enterprises are currently demanding three more capabilities from private cloud management:

- **NO VENDOR LOCK-IN:** The ability to easily switch hypervisor and provisioning technologies and not be locked into any one major system vendor.
- **A COMPREHENSIVE PRODUCT:** A streamlined user experience from a single vendor instead of stitching together disparate offerings or multiple, complex tools.
- **A PATH TO PRODUCTION APPLICATIONS:** Enterprises recognize that infrastructure as a service (IaaS) offers tremendous benefits for development and

testing, but that clouds also need to support applications. Cloud management systems must deliver fully operational, multi-tier application environments, or application clouds.

To meet enterprise requirements, Platform Computing offers the Platform ISF* solution. This next-generation cloud management modular software product helps IT organizations build and manage enterprise clouds that span both internal and external resource pools. Platform ISF's application-centric approach automates the self-service assembly and runtime management of the IaaS platform (middleware) as services, up to complex, multi-tier applications on top of shared heterogeneous resource pools. Data centers benefit with a solution that can support the entire application lifecycle, from development and testing to production-ready application clouds, in as little as 30 days.

Platform ISF offers a single platform that delivers:

- **LOB SELF-MANAGED VIRTUAL CLOUDS:** Enables hierarchical definition of clouds for each LOB to self-manage according to resource quotas and business policies.
- **INFRASTRUCTURE TO APPLICATIONS:** Supports IaaS, a customer's own platform as a service (PaaS), applications, and instance-specific software as a service (SaaS).
- **DEVELOPMENT AND TEST TO PRODUCTION:** Defines service templates for simple to complex multi-tier applications that support the entire application lifecycle.
- **ALLOCATION AND RUNTIME MANAGEMENT:** Manages both the allocation of the environment and the dynamic flexing according to changing workload levels and SLA requirements.

With Platform ISF you can:

- **ELIMINATE OVER-PROVISIONING OF INFRASTRUCTURE** to meet peak demand, resulting in lower capital and operating expenses and higher utilization.
- **AUTOMATICALLY PROVISION APPLICATION ENVIRONMENTS** and place workloads on the right systems to meet service levels in a timely and cost-effective way.
- **KEEP VMWARE* ENVIRONMENTS OPEN** with support for other VMs, physical provisioning, and external cloud providers.

Key capabilities of Platform ISF include:

- **SERVICE MANAGEMENT.** Self-service portals, account management, unlimited levels of hierarchical administration for ease of management, chargeback, and reservation management.
- **ALLOCATION:** Service catalogs, allocation engine for policy management, and runtime management.
- **RESOURCE MANAGEMENT:** Deep VMware vSphere* integration and support for Citrix Xen* and Intel® KVM technology, mul-

iple physical provisioning tool integration, connectors to public clouds such as Amazon Elastic Compute Cloud* (Amazon EC2*), and an open API to other data center systems.

- **OPERATIONS MANAGEMENT:** A single cloud cockpit monitoring alarms and events.
- **ENTERPRISE-CLASS SUPPORT:** Global coverage and 24x7 hotline support.

Figure 1 shows how Platform ISF works. End users (at the top) are presented with a self-service portal from which they can request different offerings from the service catalog. Once the request is approved and within the user's allocation limits, a reservation is created for those resources. When it's time to start

the request, the allocation engine locates the appropriate resources to run the service and creates the service on those resources. These resources can be obtained from either an internal or a public cloud, or both. Performance metrics are gathered and fed to the reporting and monitoring tools. The data is available to both users and administration staff. A policy engine allows the service to be scaled up or down automatically. The self-service portal allows the user to see the application and monitor the machines in the application. The user can access the services once they are created. The whole process, from the user requesting a service to delivery, can complete in a few minutes with no need for administrators to get involved.

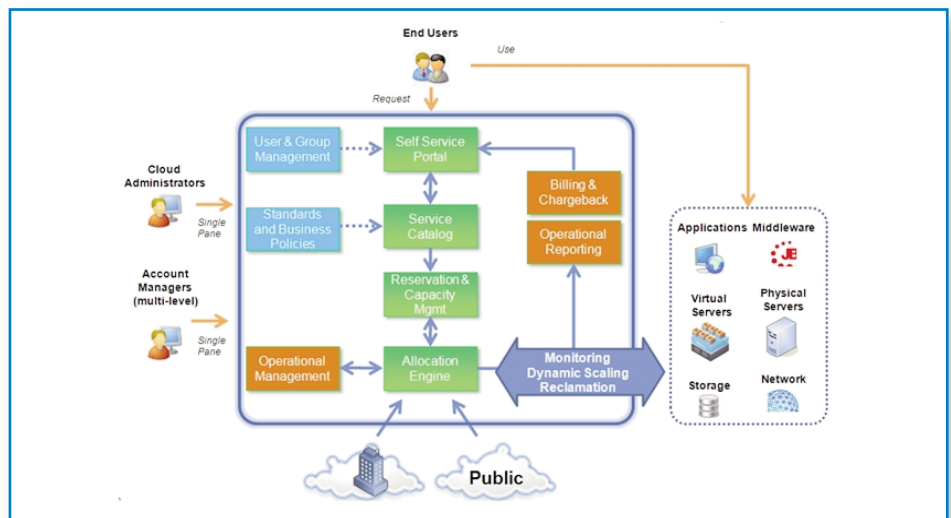


FIGURE 1. PLATFORM ISF USER FLOWS

MANAGEMENT FROM A SINGLE PANE

Cloud administrators can view and manage the cloud resources from a single pane. Different views in the user interface allow the administrator to quickly isolate fault locations.

Along with remote log file viewing, remote command execution, and remote consoles, the administrator has all the tools to manage the cloud resources. The cloud administrator is responsible for defining the accounts that will use the cloud and for creating the initial service offerings.

The accounts are hierarchical, so once they are defined their management can be delegated to account owners (at the top level, this could be a business unit). The account owners can create other accounts (such as departments), subject to the limits imposed on their account, and add users to the accounts. They also have access to the billing and charge-back reports. Account owners can also create service offerings. These, in turn, can be offered to different sub-accounts (such as projects within departments within business units).

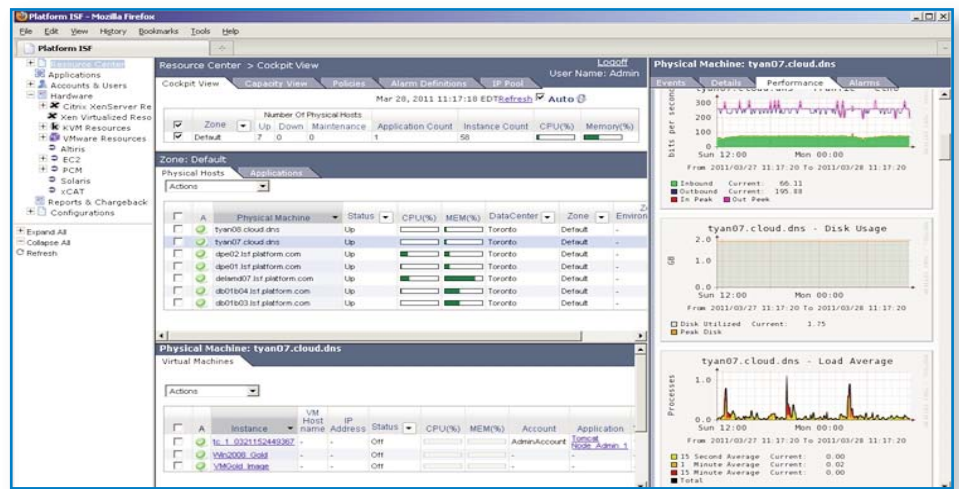


FIGURE 2. ADMINISTRATOR COCKPIT

Figure 2 shows the cloud administrator's view, with an interface optimized for managing a large-scale cloud without introducing unnecessary management complexity. The left frame shows a variety of virtualization and physical provisioning systems supported by Platform ISF. The top-middle frame summarizes the entire cloud including metrics organized by each data center. The middle frame connects the applications (services) in the cloud to the physical hosts. The bottom frame shows the VMs running on that physical host or as part of that application. This ties together the multiple layers of the stack in one

easy-to-browse management view. The right frame shows the performance metrics gathered on the physical or virtual hosts, including any events and alarms.

PLATFORM ISF SOFTWARE ARCHITECTURE

Platform ISF integrates with major hypervisor technologies including VMware vSphere, Citrix Xen, Red Hat Xen*, and Red Hat KVM*. Where a hypervisor presents a central management interface, such as VMware vCenter* or Citrix XenCenter*, Platform ISF executes, controls, and monitors status through that interface. In cases where the hypervisor

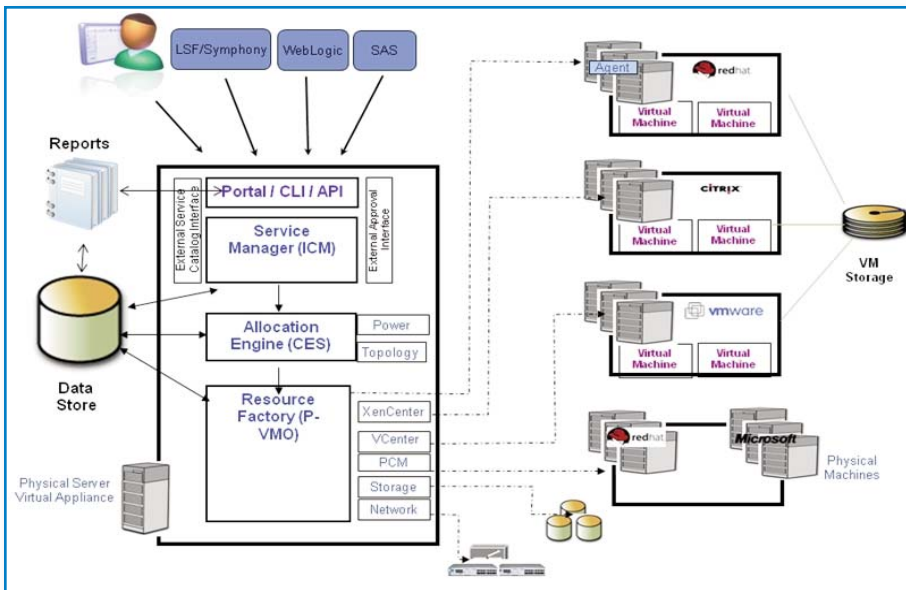


FIGURE 3. PLATFORM ISF SOFTWARE ARCHITECTURE

technology has no central manager, Platform ISF provides its own agent, which is deployed to each hypervisor node.

Platform ISF can manage and provision physical machines from bare metal using its adapter technology (Resource Interface Adapter*) with adapters to best-in-class provisioning tools such as those from Altiris, TPM, BladeLogic, and xCAT.

Platform ISF also provides its own provisioning tool, Platform Cluster Manager* (PCM*), which integrates with Platform ISF and can perform image- and packaged-based installs of the operating system and applications. PCM has also been adapted

to provision hypervisor hosts to support demand-based shrink and grow of VM capacity by, say, switching nodes between VMware and Red Hat KVM. Finally, Platform ISF can also manipulate storage and network configuration to suit a particular workload.

Once integrated, Platform ISF can deploy a workload across any resources available (virtual or physical) through its Allocation Engine*, which can create and execute complex policies governing how a workload needs to be initially deployed and how it will behave over the lifecycle of an application. The Allocation Engine also lets the user make current and future reserva-

tions on a given request. All requests for a workload are submitted through a Web portal, where users are given a service catalog, published by the cloud administrator, from which to choose. The Service Manager (ICM) manages the application lifecycle (application definitions and instances) as well as users and accounts.

Platform ISF tracks the applications' duration and produces chargeback and billing reports based on the price set for each resource (e.g., CPU, MEM) and the time for which the application ran. It also produces capacity and allocation reports to manage the overall system.

PLATFORM ISF WITH INTEL® TRUSTED EXECUTION TECHNOLOGY

Without a doubt, cloud security is a hot topic and a major concern for enterprises. Cloud security covers a number of important areas including identity management, access control, data protection, data loss prevention, and hypervisor security. Although cloud access and data protection have been at the center

of the security discussion, cloud infrastructure security and, specifically, hypervisor security have been getting special attention from enterprise IT. Pervasive use of virtualization technology among enterprises and cloud service providers, with the ability to move virtual machines between internal data centers or external to cloud service providers, raises the question of how enterprises ensure the security of their cloud infrastructures.

It isn't too difficult to imagine that one infected hypervisor or guest VM can spread the infection through virtualized infrastructure when moving from one host to another. While there are solutions to detect infected applications within guest VMs, there are far fewer solutions to detect infected hypervisors today. For this reason, Intel has developed a unique technology called Intel® Trusted Execution Technology (Intel® TXT).

Intel TXT helps prevent software-based attacks on currently unprotected areas, such as attempts to insert a non-trusted VM manager (VMM, or rootkit hypervisor), reset

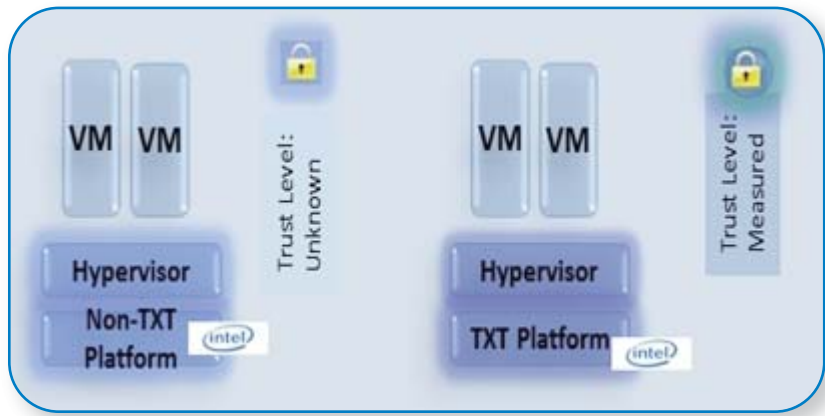


FIGURE 4. PLATFORM ATTESTATION AND SAFER VMM LAUNCH

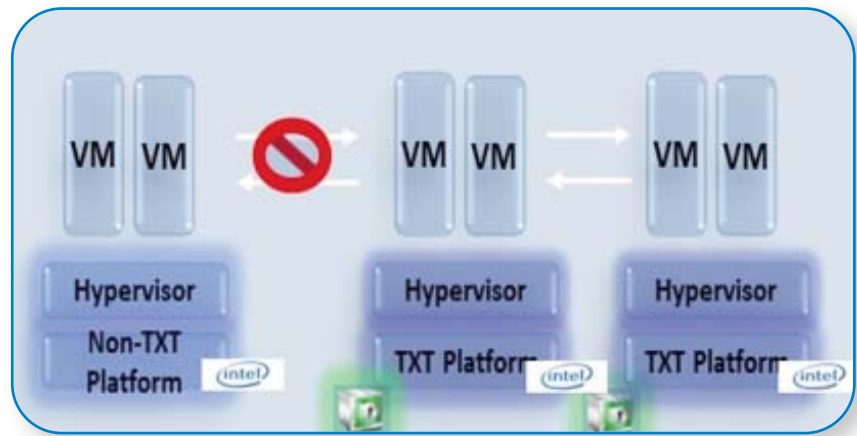


FIGURE 5. TRUSTABLE POOLS AND SECURE MIGRATION

attacks designed to compromise platform secrets in memory, or BIOS and firmware update attacks. To view it in a different way, Intel TXT enforces control through measurement, memory locking, and sealing secrets. To do this, it also works cooperatively with Intel® Virtualization Technology (Intel® VT).

An Intel TXT-enabled system requires all of the listed components—processor, chipset, TPM,

enabled BIOS, and enabled hypervisor (VMM) or operating system. Without a complete set of these components, a trusted launch is not possible (Figure 4).

Available on Intel® Xeon® processor 5600 series-based servers, Intel TXT is providing hardware-based protection in the processor, chipset, and third-party trusted platform modules (TPMs) that can better resist software attacks and make platforms more robust (Figure 5).

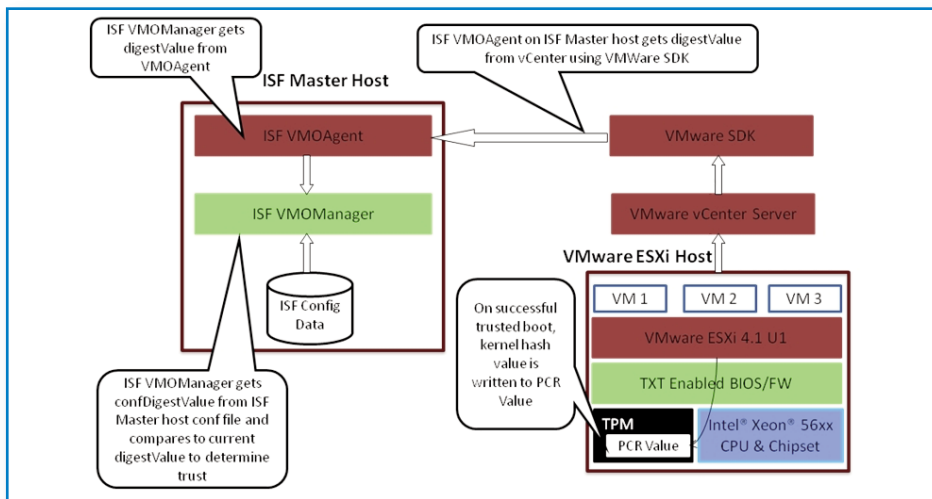


FIGURE 6. PLATFORM ISF HIGHLY SECURE ENVIRONMENT

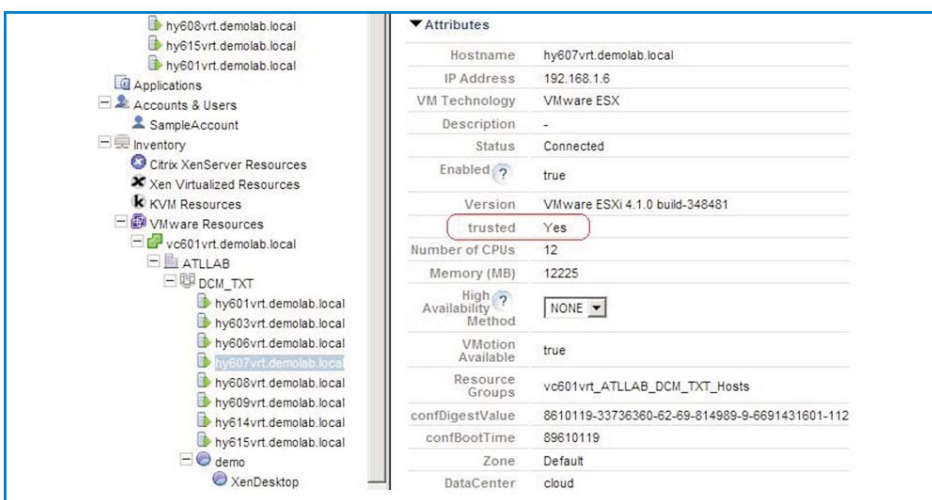


FIGURE 7. HOST MARKED AS TRUSTED

Platform ISF creates a highly secure environment for running applications in VMs through its integration with Intel TXT, which monitors changes to the BIOS and boot processes of a

hypervisor host to ensure it has not been tampered with. When a new host is added to the system, the administrator indicates it's a "trusted" host. Platform ISF then queries Intel

TXT for the host's digest value, a cryptographic hash value coded to a number of metrics that measures the unique characteristics of the host's boot sequence. The digest value remains constant as long as the hypervisor installed on the host is not modified. Platform ISF saves this good digest value in its internal database for later comparison (Figure 6).

Each time a host connects to Platform ISF (e.g., after rebooting), the VMOAgent component retrieves the host's current digest value and passes it to the VMOManager component to compare it to the known good value saved. If the values are equal, Platform ISF marks the host as "trusted" (Figure 7).

With this knowledge of trusted and untrusted hosts, Platform ISF enables a number of important policies. Applications can be easily restricted to running only on trusted

Actions						
<input type="checkbox"/>	A	Physical Machine ↓	Status ▼	CPU(%)	MEM(%)	Data
<input checked="" type="checkbox"/>		hy615vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy614vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy609vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy608vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy607vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy606vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy603vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud
<input type="checkbox"/>		hy601vrt.demolab.local	Up	<div><div></div></div>	<div><div></div></div>	cloud

FIGURE 8. RED FLAGS INDICATE A PROBLEM

hosts by specifying “trusted==1” in the application definition. This controls not only which hosts are initially chosen to start the application VMs on, but also which hosts VMs are allowed to migrate to. Platform ISF ensures only trusted hosts are used.

Platform ISF can also notify the administrator when a host becomes untrusted by using the configurable alarm feature of ISF. When Digest Values do not match, a red flag next to the host’s name indicates a problem (Figure 8). The administrator can

then drill down and find the cause of the issue.

It’s important to remember that in building secure cloud services, you need to incorporate multi-layer security architecture from the start. The Platform ISF and Intel TXT solution provides a foundation for building secure infrastructure while relying on other solutions to address requirements for data protection and data loss prevention.

BUILDING A PRIVATE CLOUD

In future articles, we’ll discuss how to build private cloud using Platform ISF.

For more information, visit the Platform Computing Private Cloud website at www.platform.com/privatecloud or contact the authors: Mark Black (mblack@platform.com), Jay Muelhoefer (muelhoefer@platform.com), Parviz Peiravi (parviz.peiravi@intel.com), or Marco Righini (marco.righini@intel.com).

