



IT in Transition:

Security and Compliance in a Virtual Data Center

707 SW Washington, 7th Floor

Portland, Oregon 97205

Telephone: 503.227.2207

www.signacert.com

Introduction

In today's complex enterprise server environments, rack space is at a premium, energy costs are rising, and there is an increasing desire to make modern data centers more efficient. Pressure is on today's CIO to drive performance up, costs down, and increase the capacity and scalability of existing operations and infrastructure. For many, the application of virtualization across computing and storage resources is an attractive solution.

Forrester Research Inc. reported that, on average, large enterprises have virtualized 31% of their operating instances, adding that in the next two years the average would rise to 54%. Why? Server hardware utilization in a highly efficient, non-virtualized data center is considered best-in-class at levels above 30%. The majority of data centers have much lower resource utilization averages, running at less than 15%. This low utilization, combined with costly power and rack space, are the primary targets for cost reduction and improved efficiencies.

This paper will briefly describe how virtualization is being used to increase the efficiency of the modern data center, and will discuss some of the problems which arise with the use of virtualization, such as asserting regulatory and IT policy compliance, and how SignaCert solves these problems.

Enterprise Computing Trends

There is a rapid shift occurring from monolithic computing¹ to virtual computing, where the same platforms can host and operate multiple virtual machines (VMs). This shift within the enterprise is inevitable and is driven by two interrelated factors:

- Cost of IT deployment and systems management
- Demand for greater business agility

Many benefits can occur as this shift progresses. Security and reliability can be improved by reducing the persistence and exposure of monolithic computing architectures and environments. Therefore, properly architected and implemented VMs and grid environments may add benefits relating to:

- IT system and network security
- IT privacy and compliance issues

¹Monolithic Computing is defined for the purposes of this paper as one hardware configuration mapped to one memory pool where one operating system and a single set of applications are present.

Server Consolidation

The most basic use of virtualization involves reducing the number of servers by increasing the utilization levels of a smaller set of machines. Virtualization enables the administrator to perform this consolidation by treating each physical machine as two or more virtual machines. For instance, if a server's average utilization is only 15%, deployment of multiple virtual machines onto that server has the potential to increase the overall utilization of that resource by a factor of five or more.

This consolidation has the following benefits:

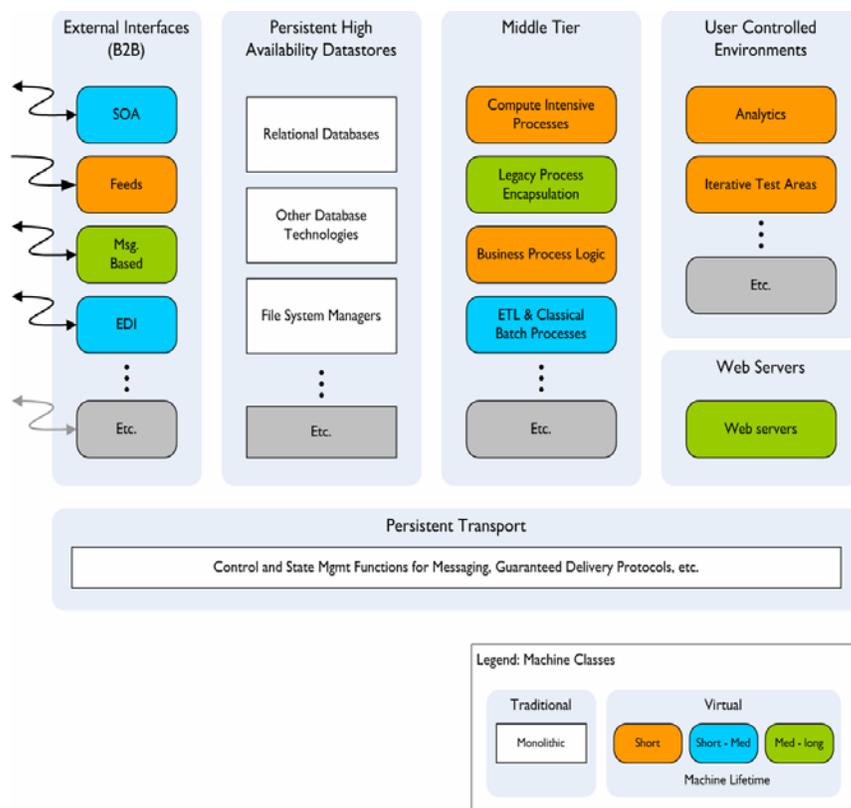
- Fewer physical machines to support (redundant back-up servers, networking, etc)
- Reduced power and rack space costs
- Increased utilization levels across physical resources
- The opportunity to homogenize your hardware platforms while continuing to run disparate legacy operating systems and applications
- The freedom to quickly re-purpose existing hardware without modifying the underlying platform
- A simplified disaster recovery plan.

Enterprise systems required for business continuity can be deployed into any data center built on virtualized resources, regardless of whether the hardware platforms are identical

Virtualized environments often enable another important benefit: encouraging IT to develop a standard set of tested virtual machine images that represent the goals of the business. This further introduces the ability to scale a business system by deploying these standard images onto existing physical machines.

Virtualization is also being used to standardize desktop and front-end systems, allowing workers to have a consistent

Figure 1: Persistent Transport



experience regardless of which physical desktop they are using. For the IT desktop administrator, this is a means to a more efficient use of resources, as it begins to consolidate a large number of geographically dispersed systems into the data center where centralized control, maintenance, and remediation can take place. Virtualization provides IT agility, allowing customers to quickly configure machines tailored to their dynamic needs. For example, a virtualized analytical model could be deployed across several servers for a single financial calculation then shutdown.

Figure 1 represents typical servers and their expected life cycle based on function.

Dynamic Systems

There are many issues that can arise from enterprise business systems in a virtualized environment. A few examples are below:

- How does an IT administrator ensure that when an image is deployed it is in a known state?
- When a virtual machine is suspended or un-deployed, how does the IT administrator know whether it has drifted from its original state?
- When virtual machines are no longer deployed, where do auditors go to review the systems responsible for a set of business transactions?

One price for higher utilization through virtualization is that business systems become more transient. However, these systems and their transactions are still subject to the same regulatory, compliance, and audit requirements as their physical counterparts. For these reasons the integrity of virtual machines must be verified at key points in their lifecycle and an audit trail produced.

SignaCert and the Value of Software Measurement in the Virtual Environments

One audit and compliance issue that IT faces is the need to express the configuration of each virtual machine in such a way that the integrity of its configuration can be verified at key points in its lifecycle, and an audit trail of that configuration integrity be created.

SignaCert enables the capability to ensure integrity at all of the following key points in the lifecycle of virtual machines:

- **Standard Virtual Image Creation:** Once a standard virtual machine image has been created and is ready to be deployed, SignaCert can capture software measurements for both the image as a whole, as well as the runtime environment, and store those images to be used for comparison at a later time. Each time a standard virtual image is pulled from the IT library for deployment, SignaCert can then verify that the measurements of either the whole image, or the runtime environment within, match the known good reference. If the measurements do not match, an alert is generated before the virtual machine is started, allowing IT to proactively avert problems. Either way, this information becomes part of the business system's audit record.

- **During Runtime:** When a given virtual image is found in a trusted state, it can be started on a given physical resource. Once a virtual machine is running, periodic configuration assessments can be performed, gathered, and compared against the reference set. Discrepancies may indicate unauthorized or unintended changes to the virtual machine. Regardless of the outcome, this information contributes to the business system's audit record.
- **Host System:** Virtual machines rely on the host system to provide a reliable and trusted platform on which to execute. SignaCert provides the tools to measure the host systems to ensure that a known and trusted foundation is provided for all virtual machines across the enterprise. By measuring the host systems against a standard reference, consistency in the runtime environments will become standard across the enterprise.
- **Shutdown:** Once a given virtual machine has completed its tasks, it will either be suspended or un-deployed to free up physical resources for other business systems. SignaCert Enterprise Trust Server (ETS) can provide a critical piece of audit information: whether or not the virtual machine was in the expected state when it completed the tasks. The virtual machine image is scanned offline and verified against the original reference set that was initially captured, thereby, creating an auditable record of the event.
- **Migration:** When a virtual machine is migrated from one physical platform to another, it is important to create an audit record that proves the virtual machine moved unchanged onto the new platform. Physical to virtual systems could be potentially tapped as a source of measurements for image capture and management.
- **Compliance:** Utilizing software measurements, an audit trail can automatically be created throughout this lifecycle. This audit trail then becomes a clear source of information when asserting regulatory and IT policy compliance. This is particularly important when dealing with the transient nature of the stack and business process.
- **Mirroring and Disaster Recovery:** Creating and storing reference software measurements enables the CIO to trust that a set of disaster recovery resources, virtual or not, are configured exactly the same as the currently running business system resources.

Conclusion

The current evolution toward virtualization is the next step in migrating business systems from a set of applications running on a single piece of hardware to sets of self-contained, hardware-neutral virtual machines ready to be instantly deployed to whatever physical hardware has available capacity. This will increase server utilization levels and the portability of the software business systems that today's enterprises rely on.

With these new freedoms comes the need to ensure that virtual machines start, maintain, and end in a known and trusted state. This information also needs to be readily demonstrable to a CIO or external auditors in absolute and meaningful terms.

SignalCert's ETS extends this capability into virtual environments at many levels, by providing the capability to capture, store and compare to a known trusted state.

About SignalCert

SignalCert is the leading provider of next-generation IT compliance solutions allowing organizations to rapidly achieve and prove continuous compliance for the systems that deliver critical business services. SignalCert's patented technology can be quickly deployed and provides immediate visibility into the actual state of IT infrastructure. The SignalCert architecture is designed to seamlessly integrate with existing change processes and continuously monitor critical business services without disruption.

Founded in 2004 by 34-year IT security and compliance industry veteran Wyatt Starnes, SignalCert has assembled a world class team of industry leaders with hands-on IT experience for its executive team, board of directors, and advisory board. SignalCert's customers span a wide variety of industries, including financial services, government, and healthcare.

For more information visit: www.signacert.com.

References

Garfinkel, Tal, et al. "Data Lifetime is a Systems Problem." Stanford University Department of Computer Science. September 2004.

"The State Of Emerging Enterprise Hardware Trends: 2008 To 2009", Forester Research