WHITE PAPER

Securing Virtualized Environments and Accelerating Cloud Computing | May 2010

securing virtualized environments and accelerating cloud computing

Nimrod Vax

CA Security Management

table of contents

executive summary

Challenge

A well-meaning developer at a large insurance company made a clone of a production virtual machine and launched it in a test environment. The company had no controls on access, so the developer was allowed free access to test, development, and production environments. When he turned on the copy of the system, the machine behaved as though it was in production. The developer ran some claims scenarios in order to test functionality, and didn't realize that the system was actually cutting checks and kicking off the process to mail the checks to customers. One customer received two checks for a claim that was already in process and called to ask about which one they should cash. As enterprises adopt virtualization and cloud technologies, a new set of identity, access, and user activity reporting problems are introduced that increase the risk of exposure. Compromising the hosting virtualization platform puts all of the virtual guests at risk. Auditors are now beginning to ask the hard questions relative to these risks. When asked, 90 percent of enterprises name 'security and control' as the primary inhibitor to the wider adoption of virtualization and cloud computing.

Opportunity

To reduce virtualization security risks, independent access enforcement and monitoring technology must be employed in conjunction with native security measures. Some of the vulnerabilities that were traditionally controlled by the presence of physical security must now be mitigated through the implementation of granular access controls and user activity reporting on the virtualization platform. A comprehensive solution for privileged access management is required in order to mitigate the risks associated with the new breed of security considerations and satisfy auditors. Internal or external service providers delivering Infrastructure-as-a-Service will need to provide premium visibility and control features to their customers if they want to support the organization with next-generation technologies.

Benefits

By ensuring limitations on privileged users performing authorized operations on the virtualization infrastructure, the risk associated with over-privileged accounts or external intrusions which may compromise the virtual machines is dramatically reduced. Enforcing access to the virtual machines themselves supplements protecting the integrity of virtual machines through network isolation. Centralized management of security policies minimizes deployment and administrative costs incurred due to virtual machine sprawl. Finally, by securely logging and tracking all sensitive administrative activities on the virtualization infrastructure and guest virtual machines, reports are quickly created and compliance requirements are met.

Section 1: Virtualization technology overview

Virtualization technologies enable the execution of multiple operating system instances, or virtual machines (VMs), on the same physical piece of hardware. Each VM functions as if it is its own physical machine with a dedicated operating system and hosted applications. Each VM requires access control, sometimes different between different VMs on the same physical hardware platform. Some virtualization platforms require an external host operating system; others are embedded directly in the hardware. The layer within the virtualization platform that enables hardware resource sharing among VMs is called the hypervisor. For the purpose of this document, we will use the term 'hypervisor' loosely to relate to the system hosting the virtual machines.

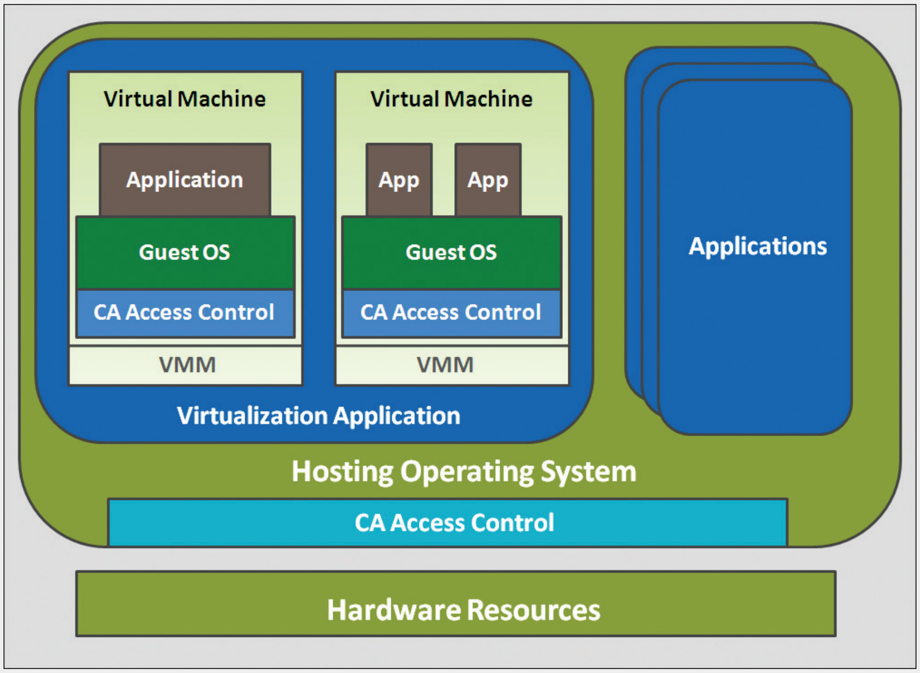
There are several common approaches to virtualization. The significant difference between the various approaches lies in the component that has visibility and control over the virtual machines. In some architectures, it is the hosting operating system and, in others, it is the privileged partitions.

Application-based virtualization

A virtualization application is hosted on top of the hosting operating system such as Windows, UNIX®, or Linux. This virtualization application then emulates each VM containing its own guest operating system and related applications; for example, VMware Server and Microsoft Virtual Server. This virtualization architecture is commonly used for testing, education, and demo purposes. It is not commonly used in production environments.

Figure A

Application-based virtualization

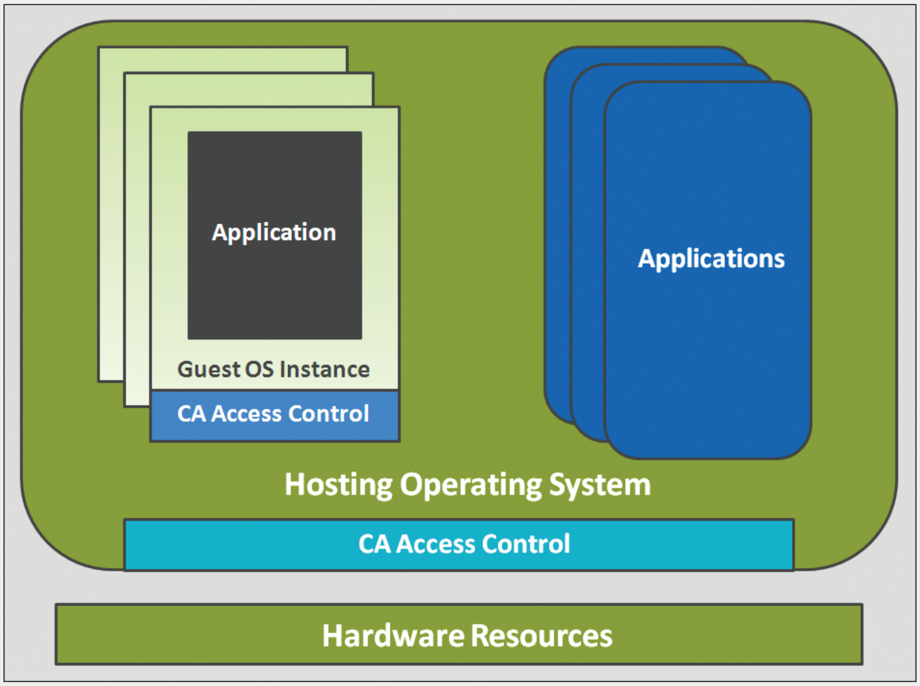


Operating system-based virtualization

Virtualization is enabled by a hosting operating system that supports multiple isolated, virtualized guest-operating system instances on a single physical server, all sharing the same operating system kernel. An example of this is Microsoft Hyper-V. Here, the hosting operating system has visibility and control over the virtual machines.

Figure B

Operating system-based virtualization.

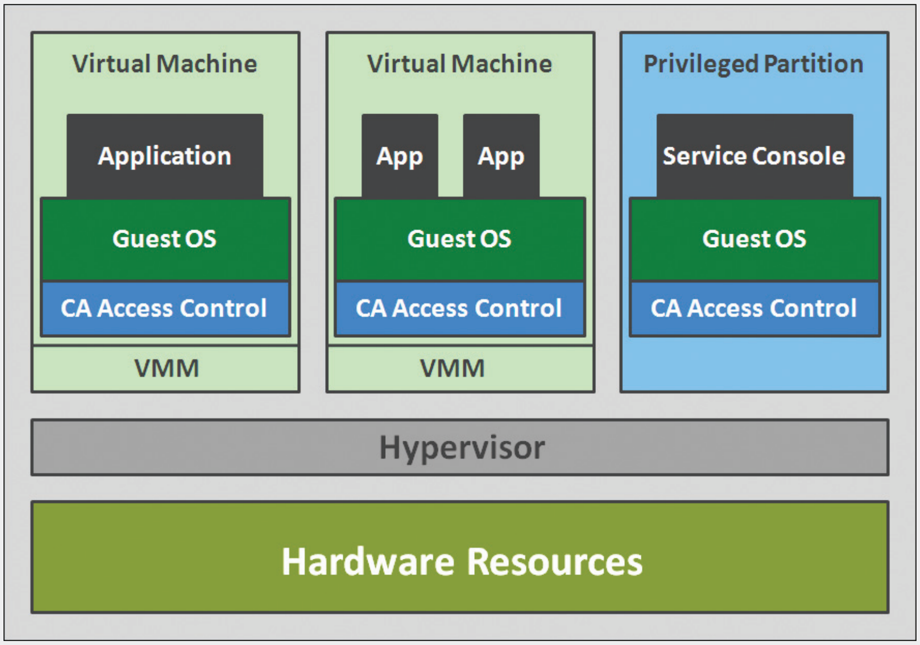


Hypervisor-based virtualization

A hypervisor is embedded in the hardware or implemented as the hosting operating system kernel. The hypervisor is available at the time of machine boot to control the sharing of system resources across multiple VMs. Some of the VMs (privileged partitions) are used to manage the virtualization platform and hosted virtual machines. In this architecture, the privileged partitions have visibility and control over the virtual machines. Examples include IBM AIX Logical Partitioning (LPAR), HP-UX Virtual Partitions (VPAR), and VMware ESX Server.

Figure C

Hypervisor-based virtualization



Virtualization security risks

When we want to identify the risks of virtualization we first need to understand how virtualization is different from the traditional physical environments. The virtualization host becomes more critical as it hosts many virtual machines, not just one. The hypervisor serves as a single management point to all VM images and a control for many critical services, creating a vulnerability leverage point. A person with hypervisor access is analogous to a root user in the UNIX world; this person can do anything to any of the hosted machines. Compromising the hypervisor to download an image or introduce a rogue VM is equivalent to bypassing physical security to break into a server room in order to steal a machine or introduce an external one. Virtualization management applications can be bypassed and the hosting operating system or virtualization console can be accessed directly by privileged users. Native operating system security does not provide protection for mission-critical data and resources at the level needed to meet regulatory compliance and security best practices.

The physical boundaries are dissolved. The server room is virtualized. You don't need to cross a server room door to enter.

Time is not deterministic—a VM can be suspended and then reverted back to a snapshot. Because of the decoupling of hardware and software, these environments become much more heterogeneous and dynamic.

Unstructured physical boundaries

The scenario presented in the abstract is real. A well-meaning developer at a large insurance company made a clone of a production VM and launched it in a test environment. The company had no controls on access, so the developer was allowed free access to test, development, and production environments. When he turned on the copy of the system, the machine behaved as though it was in production. The developer ran some claims scenarios in order to test functionality, and didn't realize that the system was actually cutting checks and kicking off the process to mail the checks to customers. One customer received two checks for a claim that was already in process and called to ask about which one they should cash.

We used to have servers stacked away in our server room with tight physical controls in place to control access to the boxes. In a virtual environment, servers are files that can be copied from the host. Copying a server image is equivalent to stealing a server from the server room. Furthermore, machine memory can be accessed from the hypervisor, compromising transit information like passwords and encryption keys. So any access to the virtualization host—even remote access—is critical. The modern virtual data center is highly distributed, unlike the traditional mainframe. Risks that were previously mitigated using physical security must now be handled by IT security.

Managing the fourth dimension: time

We all know the cool features of VMWare. You can take a snapshot of a VM, work on it, make configuration changes, and if something goes wrong, you can always revert back to the snapshot. This feature has great benefits in terms of ease of use and flexibility. But what happens when you revert back to the snapshot?

You lose any configuration changes you may have done.

If you have changed the security policy, data or configuration information that was previously protected might now be widely accessible because the policy reverts back to the prior version. Most importantly, you would lose all audit logs stored on the box, which means you might lose any record of these changes. How does that impact your compliance?

The privileged user and unrestricted privileged access

Normal users are identified and controlled by the operating system and application security. They may make mistakes or attempt misuse; however, provided the controls are correctly set, they cannot breach confidentiality or damage the system.

The privileged user has elevated privileges on the servers. This access is not controlled by the operating system security and is typically shared between administrators, making it virtually anonymous.

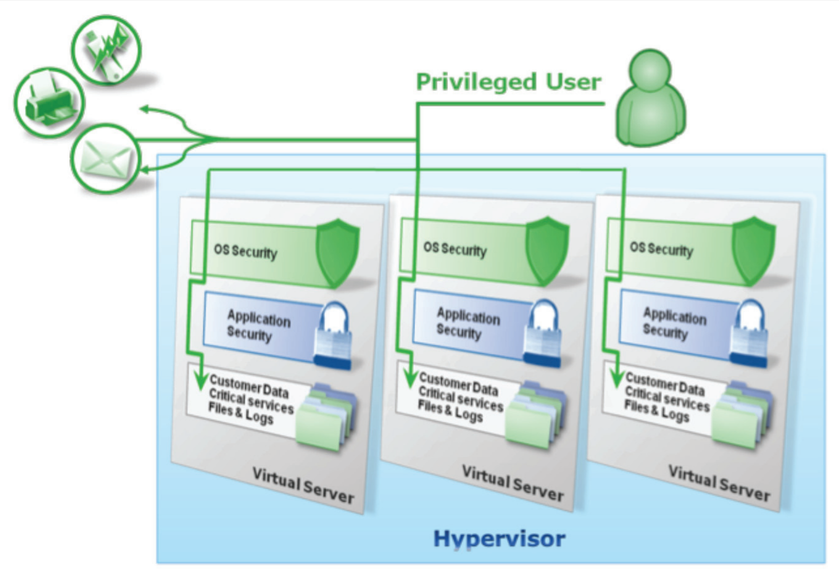
Virtualization makes the problem worse. The administrator not only has leverage over the physical host, but over all of the virtual sessions running on it. They can also have access to sensitive data and have an impact on business continuity. Without an independent access control solution, multiple privileged users in various roles have the ability to interact with numerous components of a virtualization deployment. This inadequately regulated access to the hypervisor presents the potential for significant damage to the enterprise through the compromise of valuable information and disruption of critical services. VM images can be copied, along with the data and applications that they hold. These images can be brought back online on an unsecured network, making it easier for an intruder to access the contents managed within the copied image.

In addition, critical VM images that are shut down or paused, intentionally or unintentionally, can significantly impact business continuity. Tampering with the virtualization platform configuration could lead to a denial of service or the compromise of data managed by dependent VMs. This compromise could affect configuration of local area networks (LAN) or virtual local area networks (VLAN) and shared disks or central processing unit (CPU) resource allocation.

Unsecured VMs can serve as back doors to the virtual data center or an entry point to inject viruses to the protected LAN. For example, on some virtualization technologies, a VM compromised by a keystroke monitor could allow the monitoring of server hardware resources on all other VMs hosted on the same machine. In such a case, by tracking keystrokes for all VM images, an intruder can compromise user passwords and other confidential data. Shared internal network traffic could also be sniffed from the hosting operating system, exposing other critical data.

Figure D

Hypervisor-privileged user



Insufficient security via isolation

A perceived security benefit of virtualization is that the isolation of services in dedicated VMs protects services from being affected by a compromised sibling service. Unfortunately, the assumption that VMs running on the same host are isolated and cannot be used to attack each other is not accurate. While technically separated, VM partitions still share utilization of resources such as network bandwidth, memory, and CPUs. Any partition consuming a disproportionate amount of one of these resources because of a virus or malicious change of configuration could create a denial of service for the other partitions.

Each VM on the virtualization host is also indirectly linked to the other images on that platform by its relationship to the managing host or privileged partition. A compromised privileged partition can be used as an entry point to attack the entire virtual data center.

Inadequate user activity reporting

Given the leverage the virtualization platform has on the stability of the entire data center and on integrity of the data it manages, it must be viewed as critical infrastructure. As a result, the virtualization platform is subject to tight regulatory requirements. Organizations must track the interaction that each user has with the virtualization platform and within each of the VMs it hosts. Native user activity reporting capabilities provided by operating systems are too coarse to be effective and are vulnerable to tampering and snapshot manipulation. Access to the hosting operating system must be monitored and verified to prove controls have ensured its integrity. Similarly, within each VM, access gained to each guest operating system is subject to the same regulatory compliance requirements. If you cannot implement enforcement, the minimum in many cases is user activity tracking and reporting.

Managing complexity

Virtualization makes the complex seem simple—but with it, the environment can become more complex. With the right management tools, virtualization vendors simplify configuration, network, storage, and resource management. But what about security and access management?

This complex environment introduces the need for a dynamic security policy. You have many types of operating systems, many VMs, and a highly dynamic and changing environment. When a VM comes up, how do you ensure that the access policy of that machine is compliant? How do you get visibility into the current state and any deviations caused by reverting to snapshots or legitimate exceptions? The same challenge applies to the physical IT infrastructure, but the dynamic nature of the virtual datacenter makes things worse.

While virtualization enables the consolidation of physical machines, it does not provide a native solution for the consolidation of security management. The challenge is how to enforce a consistent access control policy across this complex environment.

Compliance

When we talk about identity and access management, we cannot ignore the primary driver in this market: regulatory compliance.

Until recently, auditors have not been virtualization-savvy, and virtualization audit issues haven’t yet been flagged. But this is changing, as seen by the recent updates to some of the common regulations, such as PCI.

The primary concern raised is that the management environment can be bypassed through the virtualization console, such as the VMWare console OS or the hosting operating system of Linux XEN, Hyper-V, or Solaris.

Cloud computing

Cloud computing is defined in Wikipedia as “a paradigm of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet.” It relates to multiple aspects of IT services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). IaaS leverages virtualization technologies and their automation capabilities to provide a highly scalable IT infrastructure (i.e., servers and networks) that allow the organization dynamic capacity and flexible pay-per-use pricing that help reduce capital expenses on infrastructure and outsource some of the IT services for a lower cost. IaaS relies on virtualization technologies to achieve the low cost of management and economy of scale through automation, and thus inherits some of the security risks mentioned above.

Virtual Machine Sprawl generates huge complexity: due to the increased number of hosts to be managed and enforced—access control management will need an automatic identification of hosts and automatic deployment of access control agents. This is specifically due to the frequent changes that may occur in a utility computing environment.

Since deploying an image on the cloud requires access permissions that can remedy rollout, rollback, fail over, or other installation-related issues, cloud image security management services and remote API provided by the cloud vendors are essentially the same as regular administration permits, and thus require external enforcement. In other words, guarding the external management capabilities, such as enforcing integrity applied by the cloud vendors.

Protecting the physical boundaries of virtual machines is also critical. Since a virtual host (VH) image can be on any physical machine there is a need to restrict the physical boundaries of where a VH can run, as well as on which physical or virtual network section.

Since the “pay-per-use” model prohibits the IT security managers from accessing the root system that runs the cloud, the cloud vendor must accept and enforce security compliance needs, as well as report the status of the deployment and enforcement of the policy for reporting and monitoring.

Barriers to cloud adoption—security and control

IaaS is a new form of delivering managed IT services that is highly automated, off-premise, and commoditized. Its commoditization and automation make it virtually anonymous to the consumer, just like direct insurance services or online banking. Does anyone remember meeting an insurance agent or a bank teller?

Amazon is reporting exponential growth of their EC2 service. But we are not yet seeing wide adoption by the enterprises. Surveys show that 74 percent rate cloud security issues as “very significant.” Large enterprises avoid placing sensitive information in public clouds unless they can obtain strong assurances of appropriate protection from the cloud providers.

When asked, only 20 percent of enterprises are considering cloud computing, and most of them refer to internal cloud technology to manage and charge back for computing services within their enterprise.

Security and privacy concerns present a strong barrier-to-entry. To take full advantage of the power of cloud computing, organizations will need to attain assurances from the cloud’s treatment of security, privacy, and compliance issues

Section 2: Protecting the virtual environment

CA Access Control (AC) provides the critical layer of protection needed to effectively protect virtualization platforms. AC operates independently, both at the application level and at the operating system kernel level, without interfering with the kernel itself. By securing console access to the hypervisor, AC protects mission-critical information and services running in the virtual data center. It protects virtualization deployments at multiple levels: operating systems hosting a hypervisor, operating systems implementing operating system-based virtualization, privileged partitions managing hypervisor-based virtualization and the critical resources in VMs running on all of the above. Support of a wide range of operating systems makes AC ideal for protecting VMs, especially in a heterogeneous OS environment. AC also allows you to protect privileged users across IT environments beyond the virtualization host itself—on databases, network devices, and applications. It also helps simplify user management by consolidating the user management under a single authoritative source across all operating systems.

Segregation of duties

AC provides granular segregation of duties to limit each privileged user's privileges to the minimal set necessary to perform their job function. This mitigates the risk associated with unauthorized access to confidential information or critical services. This includes the containment of the superuser account by assigning permissions to specific roles and transparently enforcing these permissions. For example, AC can limit system administrators of a VMware ESX Server to root operations such as applying patches to the system while denying access to the VM file systems and daemons.

Starting and stopping of VMs can be tightly controlled and restricted to authorized administrators. This prevents unauthorized users from loading arbitrary software in security, management, and other critical partitions. AC also protects the configuration files for virtualization settings such as access controls, shared disks, VLANs, or CPU resource allocation. Organizations define which users can access which files and can even limit operation through approved administrative applications during defined calendar schedules.

Powerful control of privileged users

Like root users from the UNIX/Linux world, privileged users with hypervisor access need to be tightly controlled. As outlined above, a hypervisor admin has the potential to be able to do anything to a virtual environment. While these hypervisor accounts have passwords, these passwords can be shared or easily exposed to unauthorized people. These accounts may also be shared among many different operators, which make it impossible to hold them accountable for privileged activity. This activity could include an honest mistake such as moving and starting a virtual machine on a production server where it should not have been, or worse, malicious acts such as removing virtual machines and destroying data. Regulations are just as demanding in the virtual world as they are in the physical world. Passwords for these hypervisor accounts must be in compliance and their activities subject to tracking and reporting.

Improved isolation through operating system hardening

Advanced platform hardening features allow AC to provide the extra layer of security to protect VMs, hosting operating systems, and privileged partitions against Trojan or other malware attacks. Even in the event that one VM becomes compromised, it has features to prevent the propagation of negative effects to other VMs.

AC Stack Overflow Protection reduces the risk of stack overflow exploits that can break into privileged partitions, the hosting operating system, or the hosted VMs. AC can also regulate incoming and outgoing network traffic based on ports, connection methods, originating sources, network attributes, and time. This network protection can be utilized to restrict the communication between the VM images themselves, but more importantly between the images and the hosting operating system or privileged partitions.

User activity reporting and investigation

All management, servicing and security configuration sessions on the hosting and guest operating systems are fully logged by AC. It maintains the user's original ID even after the user performs a surrogate operation. Only those in the auditor role can access the log files and only in read-only mode, ensuring the forensic integrity of the files. Logging can be configured to log unauthorized access attempts as well as authorized access to critical virtualization resources.

AC employs a self-protecting mechanism to ensure logging services are not disrupted and logs cannot be tampered with. The integration with CA Enterprise Log Manager allows efficient validation of controls and effective user activity compliance reporting and investigation for identity, access, and data usage across physical, virtual, and cloud environments. Deployed as a virtual soft appliance, it delivers quick time-to-value. The product installs and is up and running quickly, providing pre-defined and easy-to-customize reports covering all user activities including those from hypervisors. Enterprise Log Manager accelerates and simplifies compliance and provides granular user and resource access reporting of virtualization host and guest. With hundreds of IT activity compliance reports and queries available right out-of-the-box and multi-dimensional log analysis tools, you can dramatically reduce the cost of proving compliance and improve efficiencies in performing user activity investigations.

Centralized cross-platform management

While virtualization enables the consolidation of physical machines it fails to provide a solution for the consolidation of security management. Through AC, user accounts, passwords, and security policies can be shared across all virtualization hosts and managed from a single administrative console. Through a unified policy-definition tool and syntax, organizations can consolidate not only physical assets but also management efforts.

AC allows organizations to take advantage of the breadth of virtualized operating systems including UNIX, Linux, and Windows operating systems as well as virtualization environments such as VMware ESX Server and Solaris 10 Zones. This broad support enables consistent management of all partition security regardless of the operating system.

The linkage between VMs and the managing host makes it even more apparent that the entire virtualization network is only as strong as the weakest link. AC brings all security up to the same level of parity, regardless of which operating systems are running.

While virtualization enables the consolidation of physical machines it doesn't provide a solution for the consolidation of security management. A typical virtual environment consists of heterogeneous operating system environments, and is often larger in quantity and highly dynamic. AC manages access to this environment through a centralized policy deployed and enforced across the entire environment. Once deployed, AC ensures an accountable change control process to manage changes and versions of the policy. This is especially important in an environment where images can be suspended, reverted, or cloned. AC tracks the versions of the policy and reports against the policy deployment status to identify any deployment errors or unavailability of services. The process manages deviations or exceptions to the policy by providing clear reports on exceptions. Auditors require proof of the controls enforced. This can be achieved by providing the reports mentioned.

CA Access Control supports a wide range of virtualization technologies. AC provides protection for all common operating system versions running as guests within a VM as well as the hypervisors.

CA Access Control virtualization support

VMware ESX	Solaris 10 Zones and LDOMs	Microsoft Hyper-V	Linux XEN
IBM AIX LPAR	HP-UX VPAR	Linux Xen	Mainframe x/VM
IBM VIO			

The complete CA security & management solution

To allow organizations the ability to completely secure their virtual environment, CA offers integration with other solutions like CA Identity Lifecycle Management. When Access Control is integrated with ILM, rapid provisioning and deprovisioning can be implemented, thus ensuring if a privileged user is terminated, they will lose their access immediately and are prevented from inflicting malicious damage.

In addition, when CA Access Control is operated in conjunction with other solutions like CA Spectrum® Automation Manager, key benefits extend to the virtual world as well. The integration of CA Access Control with CA Spectrum Automation Manager automates the deployment and configuration of CA Access Control agents. The agents manage access and entitlements of privileged users such as system, application, and virtualization administrators who need to operate on virtual machines or the hypervisor.

Enabling infrastructure-as-a-service

To take full advantage of the power of cloud computing, organizations will need to attain assurances from the cloud's treatment of security, privacy, and compliance issues. The primary barrier stated by corporate IT executives relates to 'security and control': "I cannot take my critical data and services out of my organization." This is changing. The best example of that is the success we see with cloud offerings like SalesForce.com that has revenues greater than $1 billion. Naturally, pressures for cost reduction will continue to push organizations into entering the cloud.

IT organizations need to change the way they manage their IT environment. As in any movement from an in-house to an outsourced model, the role of IT needs to change from management to audit. In essence, the IT organizations need to become the auditors of the service provider—much like their audit group is for them. They will need to demand the visibility from their cloud providers.

Providers will need to ensure that there is proper separation of administration access rights of the cloud management. IaaS vendors will need to provide organizations with the visibility into the infrastructure as if they were their auditors.

Cloud providers will need to provide controls over where VMs can run and who can run them—in other words, answer the question, "what's going to prevent someone on the cloud from copying my image and running it on their laptop at home?" This is a hard problem to address and might be resolved by proper user activity reporting above.

Organizations may want to control privileged access to their online images even when hosted by a third party. "Come through me to get root access, I want to know!"

Eventually, the economic business case will prevail. Especially in these times, we will see increasing pressure to reduce operational costs. If large enterprises can manage their entire customer portfolio on SFDC, they will eventually learn to accept the risks and controls in order to maximize the benefits of the cloud.

Section 3: Conclusions

There is no question that virtualization offers compelling tangible benefits for an IT organization. Virtualization is inevitable, and cloud computing is a new opportunity. It will mean entering your environment either from VMware or Microsoft, Intel or Cisco. If it is going to happen, the best thing you can do is develop a solid understanding of its security implications.

Understand the unique risks that are introduced with virtual environments, the fact that physical boundaries are changing and are much more volatile. VMs are more vulnerable to changes due to the flexibility offered by virtualization, such as snapshots. An additional layer of administration is introduced and the need for SoD is intensified. Finally, the virtualization host must be considered a critical infrastructure subject to strict regulatory controls. It has significant impact on your business.

In essence, the virtual environment is a shared and critical environment. Much can be done today. Start by utilizing the native controls provided by your virtualization vendors. Complement these controls with dedicated tools for enforcing privileged access management on the hosts as well as on the guests. Apply consistent policies centrally, and report on and remediate exceptions. Provide complete user activity reporting and investigation centrally, and remember that a VM can be reverted.

Finally, compliance regulations and security best practices dictate that organizations must be able to prove that appropriate access controls are in place. AC provides an independent security management system that can proactively control privileged users by enforcing, monitoring, and documenting their activities. Auditors are starting to ask the hard questions—be prepared.

If you are considering leveraging the benefits of cloud computing and Infrastructure-as-a-Service, demand the same level of assurance from your cloud provider as you are being asked by your auditors. Security and control is the number one inhibitor to cloud adoption by the enterprise. The auditor role is reversing. IT organizations are becoming the auditors of their providers. Cloud providers will need to reassure their enterprise customers (internal or external) and security will become a differentiator for cloud providers.

Section 4: About the author

Nimrod Vax has over ten years of experience in Software Development, including positions in R&D and Product Management. He is a member of the Product Management Team for the CA Security Management BU. As a security specialist, Nimrod designed and built cryptographic devices and access control mechanisms in various environments ranging from Windows Kernel to J2EE. As a development manager, he engaged in IAM deployments for major enterprises in North America and EMEA. Nimrod holds a B.Sc. in computer science and an MBA with a specialization in marketing management.

This document shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this document remain at CA's sole discretion. Notwithstanding anything in this document to the contrary, upon the general availability of any future CA product release referenced in this document, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. In the event of a conflict between the terms of this paragraph and any other information contained in this document, the terms of this paragraph shall govern.