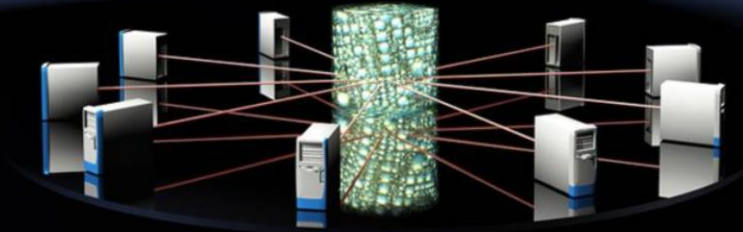



Virtualization & Cloud Computing

Module 6



Systems Security Management

Eller / MIS 
Copyright © 2015, Arizona Board of Regents



Module Objectives

- Virtualization
- How Virtualization Works
- Virtualization for Code Execution
- Benefits of Virtualization
- Negatives of Virtualization
- Virtualization Products
- Virtualization Security
- Cloud Computing
- Benefits of Cloud Computing
- Negatives of Cloud Computing
- Private Cloud Products
- Hosted Solutions
- The Industry
- Security of the Cloud
- Digital Forensics in a Virtual Environment
- Next Module...

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents


At the end of the module, you should be able to:


- Understand the concept of virtualization and how it works.
- Understand how virtualization can be used in your organization.
- Have a basic understanding of how virtualization can be used to test application code.
- Describe both the positive and negative aspects of virtualization.
- Understand some of the security issues related to the use of virtualization.
- Understand the concept of cloud computing.
- Understand how cloud computing and virtualization are similar yet different.
- Describe the positive and negative aspects of cloud computing.
- Understand how private clouds differ from hosted solutions.
- Understand how the industry views cloud computing.
- Describe some of the security issues related to the use of cloud solutions.
- Understand the basics of digital forensics in virtual environments.

Virtualization

- x86 & x64 Hardware
 - Designed to Run a Single OS
 - Leaves Server Resources Severely Underutilized
- Virtualization
 - Allows for Running Multiple Operating Systems
 - On a Single Server
 - Utilizes Server Resources More Effectively
 - Can Run Multiple Operating Systems on Same Server
 - Windows, UNIX, or Linux

Systems Security Management



Eller/ MIS 
Copyright © 2015, Arizona Board of Regents


What is Virtualization?

Virtualization is an operating system platform used to host other operating systems. Now this may sound a little confusing at first, but it really is a neat concept and one that is gaining increasing popularity within IT. Here is some general information regarding virtualization:

Virtualization software is designed to run on both x86 (32-bit) and x64 (64-bit) based hardware platforms. This means most virtualization software products take advantage of your existing hardware, without the need to purchase new servers. In general, when you have a server you install an OS such as Windows Server or a Linux variant and that server is used for a specific purpose. What this does is leave a large amount of server resources unutilized when the server is idle or if the server has more power than is necessary for its original purpose. For example, if you have a server with a dual core processor and 4 gigabytes of memory, that would likely be more than sufficient for a simple file storage and print server. In fact, more often than not you will see minimal usage of the hardware. This means that this server will have a lower ROI than it might otherwise have based on actual resource utilization.

Why Virtualization?

Taking the previous example, how do you deal with the fact that your server is underutilized? The answer is virtualization! Virtualization technology allows a system administrator to install a “host” operating system on the server and then create one or more “guest” operating systems through the use of virtual machines. In other words, you can install multiple operating systems and have them all run at the same time on a single server. The virtualization software is designed to manage the resources of each guest operating system, ensuring each one has the resources it needs at a given time. And since you can run multiple operating systems at once, it is important to note that you can run Windows, UNIX, or Linux, or any combination therein at the same time with no problems. The bottom line is a dramatic improvement in ROI that will reduce the number of physical servers necessary to operate while ensuring needs are met.



How Virtualization Works

- Virtual Server OS
 - Inserts a Small Layer of Software for Server to Boot
 - Hypervisor
 - Virtual Machine Monitor
 - Allocates Hardware Resources Dynamically
 - Encapsulates Entire Server
 - Transforms or “Virtualizes” Server Resources
 - Into Resource Pools
 - Includes CPU, Memory, Hard Drive, & Network
 - Allows Creation of Virtual Machines
 - Can Run Separate Operating Systems
 - Utilize Shared Server Resources

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

How Virtualization Works

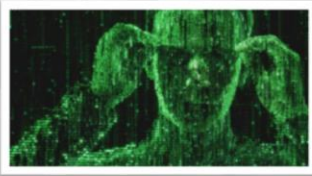
When you install a virtual server operating system, what you are installing is a small piece of software that is used to provide a conduit between the server’s physical hardware and the virtual machines. This software allows the server to boot up and become usable by guest operating systems and is called a hypervisor. This hypervisor acts as a virtual machine monitor, allocating hardware resources dynamically as each virtual machine requests resources. The benefit of the hypervisor is that it encapsulates the entire server, meaning each of the virtual machines is running separately and none of them can cause another to crash unexpectedly.

The hypervisor is designed to take existing physical resources and “virtualize” them into resource pools. These resource pools will include the server’s CPU, memory (RAM), hard drive space, and network interface card. Multiple guest operating systems will share these resources and only use what they need when they need it.

The hypervisor also allows for the creation of one or more virtual machines (VMs), each of which can run separate operating systems using a different amount of resources. For example, let’s assume the previous server we discussed with the following physical resources: 2 processing cores and 4 gigabytes of memory. You can create a VM specifying only one processor and 1 gigabyte of memory and then create a second with 2 processors and 2 gigabytes of memory. Now you may ask how is it possible to specify a total of 3 processors when only 2 are available. The answer to this is easy, the virtual server itself will manage the processor usage and will dynamically allocate the resources as needed. This is referred to as overutilization and is a concept we will discuss in a few slides.

How Virtualization Works

- Virtual Machines
 - Compatible with x86 & x64 Operating Systems
 - Including Drivers
 - As Far as the OS is Concerned
 - Each Machine is a Physical Server
 - Each Machine Isolated
 - Allows Multiple Machines to Run Multiple Operating Systems
 - Prevents a Single Machine from Crashing Other Machines
- Virtual Infrastructure
 - Ability to Utilize Multiple Servers & Resources
 - Each Virtual Server Contains Multiple Virtual Machines



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

How Virtualization Works, continued

Each virtual machine is compatible with both 32-bit and 64-bit operating systems. The caveat with 64-bit OSes is that the physical server must include 64-bit hardware. Otherwise the server will only be capable of running 32-bit OSes. In addition, virtual machines provide compatible hardware drivers for both variants to help the VMs run smoothly. Once an OS has been installed into a VM, the OS believes it is a physical server and not a virtual one. As far as the OS is concerned the server only has the hardware specified when the VM was created. The nice thing with VMs is that should the sysadmin find it is underperforming, he or she can increase the resources provided to the server simply by shutting down the VM, modifying the number of processors, memory, or disk space needed, and then restarting the VM. This usually takes no longer than a simple reboot and it can dramatically improve the VM's performance.

Another benefit with virtual machines involves how the hypervisor isolates each VM. This allows each VM to run a different guest OS, including multiple copies of an OS and prevents any of these individual VMs from causing others to crash. So, for example, if you were running a Windows OS in a VM and some issue caused the server to crash, only that one VM would be affected. The other VMs running on the same physical server would continue operating as normal.

Virtualizing an Infrastructure

When you think of a server infrastructure you are likely thinking of giant rooms filled with servers, all performing different tasks. In many cases this is a fairly accurate (and common) picture of a server infrastructure. With virtualization, a system administrator can take that room full of servers and physically reduce the number of servers necessary. In other words, if your server hardware is powerful enough, you could theoretically take a room filled with 100 physical servers and reduce that number down to 10 or 20, while still running all 100 servers on the network as VMs (5-10 VMs per physical server). This is huge!

Virtualization for Code Execution

- Binary Translation
 - Used without need for a VM
 - Can be done statically or dynamically
- BT with Direct Execution
 - Faster than binary translation alone
 - Only translates code executing in Ring 0



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Virtualization for Code Execution


The previous slides discussed when you want to virtualize an entire machine, but sometimes you don't want to do that, maybe you just need to test some code out for a program you're writing and don't necessarily need an entire testing platform. That's where code execution virtualization can come in handy. Other examples are for inspecting code for malware and/or viruses before executing them on your machine.

Binary translation is a concept that's been around for a while, but isn't often implemented. The idea is that a hypervisor is created that can examine a piece of guest code before it runs, find the sensitive but unprivileged instructions, translate them into something privileged, and then run the translated code. This can be done statically on a full program, or dynamically, on-demand just before a chunk of code is executed. This negates the need for a full system-level hypervisor.

The only problem with binary translation is that in traditional binary translation all code is translated, which can slow implementation and code execution down. Modern operating systems use what's called "protected mode" to separate operating system code from regular program and application code. Intel processors define four different "rings" of security: ring 0 is privileged code and is reserved for the OS kernel, ring 3 is where application code is run, this way it's not possible for an application to execute sensitive instructions. In order to implement a hypervisor based on binary translation, we only need to translate code that is executing in ring 0. Usually this is just a fraction of the total code being executed, so by using direct execution along with the binary translation, most code will actually run straight on the CPU without need for translation. This allows high performance with binary translation.

Benefits of Virtualization

- Get More Out of Existing Resources
- Reduce Datacenter Costs
 - Reduces Physical Infrastructure
 - Improves Server to Admin Ratio
 - Less SysAdmins Necessary to Manage Virtual Infrastructure
 - Reduces Power & Cooling Requirements
- Increase Availability of Hardware & Apps
 - Improves Business Continuity
- Gain Operational Flexibility
- Improve Desktop Manageability & Security



Systems Security Management Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Benefits of Virtualization

So far we have discussed a few general benefits for adopting virtualization and here are a few more specific ones. As we just discussed, it is very easy to get a much higher resource utilization out of existing server resources than ever before. However, running multiple VMs on one or more single servers has a number of benefits beyond resource utilization. Virtualization can be used to reduce the size of the physical server infrastructure. This means the job of maintaining all of the machines and servers becomes much easier for the system administrator. This is because virtualization actually changes the physical server to sysadmin ratio, making it possible to manage all resources with fewer sysadmins. In addition, the reduction in physical servers means there is a significant cost savings when it comes to power and cooling requirements. Which, of course, means that fixed costs for server infrastructure can actually be reduced over time.


Virtualization also helps to increase the availability of different hardware and applications necessary to operate on a day-to-day basis. This is because virtualization software supports a feature that allows VMs to be moved from one physical server to another with zero downtime should a particular server need maintenance or the hardware actually fails. This improves business continuity because servers remain active and on the network despite physical hardware issues.

In addition, virtualization provides the means by which an organization can gain operational flexibility. If a new server is needed for a particular project or department, a new VM can be created and configured within a few hours, providing the necessary resources when they are needed most.

Virtualization can also be used outside of the server infrastructure as well. Desktop virtualization is becoming an increasingly popular option among large companies. This is because the software, tasks, and data are all stored on the network and not on any specific computer (desktop or laptop). By assigning users what is known as a “dumb” terminal (meaning their computer has minimal processor and memory) they can boot an OS from a virtual server on the network and operate as if they were working locally. The major benefit to this technology involves the use of “dumb” laptops. If someone took a laptop on a business trip and it was stolen, all the thief took is a machine incapable of doing anything. No data is stored on this type of laptop as everything is accomplished through a network connection. This makes the loss of the laptop a non-issue with regard to security and a minimal cost for replacement.

Negatives of Virtualization

- Hardware Support
 - Most Servers Supported
 - External Storage & RAID Hardware
 - Must Appear on Supported Hardware Lists
 - Occasionally 3rd Party Vendors Can Provide Solution
- Up-Front Costs
 - Shared Storage Hardware
 - To Support Live VM Migrations
 - Can be High for Software Licenses
 - Also Support Contracts
- Learning Curve



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Negatives of Virtualization

Despite all of the benefits of virtualization, there are some negative aspects that should be acknowledged. The largest of which involves the hardware supported by virtualization software vendors. In general most servers are supported (e.g. Dell, HP, etc.); however, the main issue involves the use of external storage and RAID-level hardware solutions (we will discuss RAID more in-depth in a later module). When it comes to adding external disk storage solutions, it is vital the sysadmin takes the time to research whether or not a particular solution will work with the software. Each software vendor will have an officially supported list of hardware (known as a Hardware Compatibility List) which will list the specific types of hardware that will work with their software. On occasion it is possible to find a third-party hardware vendor who can provide the necessary drivers to make the hardware work with virtualization software; however, it is important to note this is not officially supported by the software vendors and may cause unknown issues. In general, it is a best practice to use only officially supported hardware products to minimize risk.

Another major detractor will include up-front costs associated with adopting the technology. The largest cost will involve the physical hardware. If you have the necessary physical servers then this is reduced; however, disk storage solutions can be quite pricey, especially when it comes to the speed of the hard drives (faster is more expensive). In addition, if you plan to use multiple servers sharing the disk storage solution, then you need to ensure you are using a Storage Area Network (SAN) or Network Attached Storage (NAS), both of which can be expensive; however, this is necessary if you need to support an environment where VMs must be able to be moved from one physical server to another to minimize downtime.

The virtualization software can also come with a high cost as well. While all virtualization software vendors offer a free version of their software that works very well, paying for licensing allows access to support resources as well as features such as live VM migrations (moving VMs from one server to another).

Finally, as with any new software, the learning curve can be quite high. Depending on the sysadmin's experience, this could mean a high learning curve. Users, however, will not notice any difference in how a VM reacts on the network versus a physical server.

Overutilization of Resources

- Virtual Servers Allow for Overutilization
 - Assign More Resources than Physically Available
 - Overutilization of RAM
 - 16GB Total RAM
 - 5 Virtual Machines
 - Each VM Assigned 4GB
 - $5 \times 4 = 20!$ Huh?
 - Not All VMs will Use all 4GB at the Same Time
 - Therefore All 5 VMs can Run Despite Not Enough RAM
 - Can Overutilize RAM, CPU, & Hard Drive Space
 - HD Space Overutilization Known as Thin Provisioning



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Overutilization of Resources


One very interesting feature of virtualization involves the concept of overutilization. We have talked previously about underutilization, but overutilization is the exact opposite. The question becomes, how can you use more resources than you physically have available? The answer is actually very simple.

Let's say you have a virtual server with 16 gigabytes of memory (RAM) available. On this server you are hosting 5 different guest virtual machines. What is the maximum RAM you can assign to each VM? This is fairly simple math: 16GB divided by 5 VMs = 3.2GB per VM. So, in order to fully utilize this server's memory resources you can assign each VM 3GB without a problem, but what if one VM needs more than another? Or all 5 need more than 3GB? The answer is simple: assign each VM the amount of memory it needs (that is less than the total amount physically available). So, let's say we assign each VM 4GB of RAM. With 5 VMs this means we are using 20GB of RAM. The idea here is that not all VMs will utilize all 4GB at one time. Think of it as the server is a casino and each VM is a person gambling. The house is betting that not everyone will win at the same time, meaning they can take in money from the losers while still giving it out to the winners.


One important thing to note about overutilization is the risk that more than one VM will be demanding resources at the same time. If all of the available memory is used at once, there will be a noticeable decrease in system performance, so when planning to overutilize resources, the sysadmin must take this into account and plan accordingly. In addition to overutilization of server memory, it is also possible to overutilize CPU processing power as well as hard drive space. The overutilization of hard drive space is referred to as thin provisioning.

Thin Provisioning

- Overutilization of HD Space
 - Server Has 2TB Physical HD Space Available
 - 5 VM Servers, Each Need 1TB of Disk Space
 - Can Allocate 1TB Hard Drives During VM Config
 - Specify (Check) Option for Thin Provisioning
 - When Running VM OS
 - Hard Drive Appears to be 1TB
 - Actual Usage Determines Physical Usage
 - » So...
 - » If the HD only Contains 25GB in Files
 - » Only 25GB Storage Used
 - » Still Shows Remaining Space up to 1TB Free



Systems Security Management

Eller/ MIS 
Copyright © 2015, Arizona Board of Regents




Thin Provisioning

Thin provisioning is the overutilization of hard drive space in a virtualized server environment. This works in a manner similar to memory and CPU overutilization. Let's start with a server that has 2 terabytes (TB) of physical hard drive space available. When hosting 5 VMs, you can specify each VM to have a hard drive with a maximum size of 1TB. Now, simple math shows that $1\text{TB} \times 5\text{ VMs} = 5\text{TB}$ which is larger than the available 2TB. This does not matter. When creating a VM, you can specify the size of the hard drive available to the VM, and specify this drive is thin provisioned. This means the hard drive on the VM will appear to be 1TB in size to the guest OS; however, the actual size will start small and grow as files are saved to the hard drive up to a maximum size of 1TB. So, in reality, a VM may only start by using 25 gigabytes (GB) of disk space, but could potentially grow to the 1TB limit over time.

As with overutilization of RAM and CPU, the sysadmin must carefully plan when using thin provisioning. If the 2TB physical limit is reached between all 5 VMs in this case, it will mean degraded performance of all VMs and users will be unable to save any additional data until the space issue is resolved.

Virtualization Products

- Citrix XenServer
 - Essentials for XenServer
 - Provides Advanced Management of Servers
- VMWare vSphere
 - Free Version: VMWare ESXi
 - Uses VMWare vCenter Server
 - For Centralized Management of Multiple Servers
 - Not Freely Available, Must be Licensed
- Microsoft Hyper-V Server 2008 R2
 - Available Free from Microsoft

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Virtualization Products

There are a number of different virtualization products available in the market. We will briefly discuss the three most commonly used in industry.


Citrix XenServer – XenServer is a free offering from Citrix which allows organizations to easily virtualize their infrastructure; however, the free version has limited capability. You can host multiple VMs per server, but cannot do any advanced management features such as migrating VMs to another server automatically. Citrix offers a paid version called Essentials for XenServer, which includes these missing features and includes support contracts for assistance and free updates.

VMWare vSphere – VMWare is one of the biggest names in virtualization today. They offer a free server version called VMWare ESXi which operates similar to XenServer's free version. For cost, an organization can upgrade to VMWare vSphere server which includes more features and can also choose to license VMWare's vCenter Server. This add-on allows for centralized management of multiple servers, including the ability to do live migrations of servers from one physical machine to another or from one set of hard drives to another, all while the system is up and running, with minimal degradation of system performance. Support and free updates are also included with the paid version.

Microsoft's Hyper-V Server 2008 R2 – This version is available free from Microsoft with most of the options offered by the competition. As always with Microsoft, support services require a contract or pay-by-the-incident support.

Virtualization Security

- Hypervisor is Software
 - Can Have Software Vulnerabilities
 - Will Require Updates to Firmware
 - If Client Tools are Used
 - These May Also Require Reinstallation on VMs
- VMs Separated from Hypervisor
 - Memory for Each VM Isolated
 - Prevents Hacking of Individual VMs through Hypervisor
- Possible to Breach Individual VMs
 - However, Hypervisor not Susceptible through VMs



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Virtualization Security


It is important to remember that with a virtualization solution, the virtual hypervisor is software developed by people. As such, the hypervisor software can have software vulnerabilities. From time to time, each virtualization software vendor will provide updates or patches for the hypervisor software and the system administrator should learn about each update and evaluate it prior to upgrading the server. Updates should happen in a test environment in order to minimize the potential risk for system failure due to a bad update. This should sound familiar to you. Sysadmins must take the same precautions with updating a virtual server as they would with patching a Windows or Linux OS. Testing is vital.

In addition to the server updates, many of the virtualization server software options require guest OSes to have a set of tools installed. These tools are usually used to provide driver support for the guest OS as well as provide a means for the hypervisor to control the VM if necessary (such as for shutting down the server if the hypervisor is shutting down). Client tools receive updates regularly as well to fix bugs or provide better stability within the VM environment. Sysadmins should take the same precautions as patching the guest OS when updating the tools.

One great security feature in virtualization involves a separation between the VMs and the hypervisor. The memory used for each VM is isolated from other VMs, which helps with stability issues, and also prevents the hacking of individual VMs through the hypervisor itself. While it is possible to breach the guest OS within a VM, the hypervisor and other VMs are not vulnerable through the hacked VM. In other words, a hacker would need to break into each VM separately, they could not use the hypervisor as a conduit to breach each VM.

Cloud Computing

- The “Cloud” Refers to the Internet
- Some Define Cloud Computing as
 - Virtual Servers Available over the Internet
- Others More Broadly Define Cloud Computing
 - Anything Consumable Beyond the Firewall
- Cloud Computing Comes into Focus
 - Only when you Think About what IT Always Needs
 - A Way to Increase Capacity or Add Capabilities on the Fly without Investing in New Infrastructure, Training New Personnel, or Licensing New Software



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents


Cloud Computing

Cloud Computing is one of the biggest IT buzz words today. In general, the “Cloud” in Cloud Computing refers to the Internet. Some people define Cloud Computing as virtual servers that are available over the Internet. Others more broadly define Cloud Computing as anything that is consumable beyond the firewall. So, what does this mean? Well, from a broad perspective, any server you might interact with that lies beyond your local network (e.g. your workplace or your home) could be considered Cloud Computing. From this thought perspective, you might consider any company that provides a web-based service to be a Cloud Computing provider. Some examples could be an e-mail service (such as Gmail or Hotmail) or an online backup service (such as Carbonite).

In a more traditional IT environment, Cloud Computing is considered to be a solution that can be hosted either externally or internally (Private Cloud) and is available from anywhere in the world from the Internet. However, Cloud Computing really comes into focus when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.

Cloud Computing Examples

- At an Early Stage
 - Few Providers Delivering Services
 - Applications, Storage, Spam Filtering
 - Includes Utility-Style Infrastructure & Software as a Service
- SaaS
 - Delivers a Single Application through the Browser
 - Clients: No Upfront Investment
 - Servers or Software Licensing
 - Providers: One App to Maintain, Low Costs
 - Salesforce.com, Google Apps, HR, ERP, etc.



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Cloud Computing Examples

Despite the fact that Cloud Computing has been in existence for years, the concept is still at an early stage. There are few major providers delivering the kind of services organizations need. Typical offerings include applications, storage, spam filtering, utility-style infrastructure, and software as a service.


Software as a Service (SaaS)


Software as a Service providers aim to deliver a single application through a web browser. This is by far the most common form of Cloud Computing available to organizations. From a client perspective, there is no upfront investment, meaning the initial cost of adopting a SaaS solution is very low as there are no servers or software licensing required. SaaS typically is a month-to-month or contract-based payment process, making it easier for an organization to justify adopting a SaaS solution.

For providers, there is typically only one application to maintain. This means providers only need to update or patch one application over time, allowing them to focus on a core product offering. This also equates to a lower cost for providing services to clients. Examples of SaaS products include Salesforce.com, Google Apps, Human Resource Applications (PeopleSoft), and Enterprise Resource Planning (ERP) applications.

Cloud Computing Examples

- **Utility**
 - Includes Storage & Virtual Servers
 - Accessible on Demand
 - Amazon, Microsoft, IBM
 - Used for Supplemental, Non-Mission Critical Needs
 - May Eventually Replace Part of the Datacenter
- **Web Services in the Cloud**
 - Closely Related to SaaS
 - APIs Enable Developers to Exploit Functionality over the Internet Rather than Delivering Full-Blown Applications
 - Google Maps, ADP Payroll Processing, Bloomberg, USPS



Systems Security Management Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

Cloud Computing Examples (continued)

Utility

Utility Infrastructure offerings include storage and virtual servers. Storage vendors usually offer one of two different services: online data storage space or online backups. Charges for either kind of storage can either be a flat rate for a specific amount of data, a per-gigabyte or per-terabyte charge, or even be based on how much bandwidth is used to store and access a specific amount of data.

Virtual server providers are looking to give organizations some flexibility by providing server capacity without the need to invest in internal infrastructure. Virtual servers can be managed either by the Cloud provider or the organization's internal IT department, this will depend on the specific service chosen.


The primary benefit with Utility Cloud providers is the services are accessible on demand, exactly when the organization needs them. Some providers of this type of service include Amazon.com, Microsoft, and IBM. It is important to note that Utility Cloud solutions should be used primarily for supplemental, non-mission critical needs. Despite this recommendation, Utility providers may eventually replace part of an organization's datacenter.

Web Services in the Cloud


Web Services in the Cloud are closely related to Software as a Service. The primary idea here is the Web Services provider provides application programming interfaces (APIs) to organizations so the organization's software developers can exploit functionality over the Internet rather than delivering a full-blown application. This is also referred to as a Service Oriented Architecture (SOA), and allows developers to provide application features without the need to develop their own code. Some of the main providers include Google Maps, ADP Payroll Processing, Bloomberg, and the United States Postal Service.

Cloud Computing Examples

- Platform as a Service
 - Another SaaS Variation
 - Delivers Development Environments
 - Build Your Own Apps, Run on Provider's Infrastructure
 - Delivered to Users over the Internet
 - Constrained by Vendor's Design & Capabilities
 - Force.com, Google App Engine, Yahoo Pipes
- Managed Service Providers (MSP)
 - Oldest Form of Cloud Computing
 - Application Exposed to IT Rather than Users
 - Virus Scanning for E-mail, Application Monitoring



Systems Security Management

Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

Cloud Computing Examples (continued)

Platform as a Service

Platform as a Service is another SaaS variation delivering development environments to organizations. The idea here is to provide your application developers with the means to build the necessary applications and run them on the providers infrastructure. Developed applications are designed to be delivered to users over the Internet. The primary caveat here is the developers will be constrained by the vendor's design and capabilities. In other words, vendors may only be able to provide a specific set of development languages, software or infrastructure, so your application developers must be able to code in specific languages, using specific software, and within a specific server environment. Examples of PaaS providers include Force.com, the Google App Engine, and Yahoo Pipes.

Managed Service Providers (MSP)

Managed Service Providers are the oldest form of Cloud Computing. The idea with MSPs is the application is exposed only to IT departments rather than the users. For example, MSPs would provide capability for scanning e-mails for viruses or spam, application monitoring (licensing for example), or even help desk-based applications.

Cloud Computing Examples

- **Service Commerce Platforms**
 - Hybrid of SaaS & MSP
 - Offers Service Hub Users Interact With
 - Common in Trading Environments
 - Expense Management Systems
 - Allows Users to Order Travel & Secretarial Services then Coordinates Service Delivery & Pricing
 - Rearden Commerce
- **Internet Integration**
 - Integration of Cloud-based Services
 - Designed to Consolidate all Services Under one Roof



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents


Cloud Computing Examples (continued)

Service Commerce Platforms

Service Commerce Platforms are a hybrid variant of SaaS and Managed Service Providers. These systems provide a service hub for users to interact with while also providing the back-end functionality needed by service groups. Service Commerce Platforms are common in trading environments, where users can interact with professional day traders. Another type of SCP commonly available to organizations are expense management systems, which allow organizations to order travel and secretarial services, then coordinate service delivery and pricing. Rearden Commerce is an example of a vendor specializing in Travel, Management, and Finance Service Commerce Platforms.

Internet Integration

The final example of Cloud Computing we will take a brief look at is known as Internet Integration services. The concept behind this type of cloud computing service is the integration of Cloud-based services, consolidating all services used by an organization under one roof to help simplify management and contracting. This type of cloud provider does not specialize in any one application, but acts as a third party IT department, managing all of the organization's Cloud services.



Benefits of Cloud Computing

- *Reduced Cost*
 - Cloud Technology Paid Incrementally, Saving Organizations Money
- *Increased Storage*
 - Organizations Can Store More Data than on Private Computer Systems
- *Highly Automated*
 - IT Personnel do not Need to Worry about Keeping Software Up-to-Date

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Benefits of Cloud Computing

Cloud Computing can provide a number of benefits to organizations looking to adopt these options. Keep in mind these benefits are generalized. Specific offerings from different vendors can provide other benefits than those discussed here (or some of these may not be a benefit with the chosen solution) .

Reduced Cost - In general, providers boast a reduced cost to clients. The expectation here is that cloud technologies are paid for incrementally, negating the need for a large up-front investment for hardware and software. This alone will save organizations money.

Increased Storage – While it is true that hard drive storage space is cheap, there is a limit to the amount of storage space that can be placed in a local server. This is mostly due to the amount of space and access speed needed. Providers can supply as much storage space as is necessary, increasing storage allotments on demand, making the process seamless to clients.

Highly Automated – By adopting a cloud solution, the typical onus of responsibility for maintaining servers and applications is on the service provider, so IT personnel do not need to worry about keeping software up-to-date, nor worry that an update will break the application.

Benefits of Cloud Computing

- *Flexibility*
 - Cloud Computing Offers much more Flexibility than Past Computing Methods
- *More Mobility*
 - Employees can Access Information wherever they are, Rather than Having to Remain at their Desks
- *Allows IT to Shift Focus*
 - No more Worrying about Constant Server Updates and Other Computing Issues, Government & Organizations Free to Concentrate on Innovation

Systems Security Management

Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

Benefits of Cloud Computing (continued)


Flexibility – Another benefit with cloud computing involves the flexibility the platform provides. Cloud vendors are able to dynamically add or remove resources as necessary to provide the best possible performance to their clients. Past computing methods were fairly rigid, restricting resources based on the physical configuration of the server, especially if virtualization technology was not being used. Adding resources typically involved a potentially high one-time cost with downtime necessary to achieve results.

More Mobility – By shifting to the Cloud, an organization can make its applications available to employees from anywhere in the world. All the user needs is a connection to the Internet, so whether an employee is at their desk, on a business trip in another city, or at an off-site meeting, they can still access the organization's data when necessary.

Allows IT to Shift Focus – Perhaps the most significant benefit to adopting a cloud solution is that it allows the IT department to shift its focus from the constant need for maintaining systems. System administrators no longer would need to worry about constantly updating servers or other computing issues related to system maintenance. This leaves governments and organizations free to concentrate their IT resources on innovation and improving business processes with technology.

Negatives of Cloud Computing

- **Loss of Control**
 - By Handing over Data to a Cloud Computing Provider, the Organization Loses Overall Control of the Data and Information
- **Dependence on Third Party**
 - The Organization will Depend on the Third Party Provider to Ensure their Systems are Secure so Data and Information Remain Confidential
- **If the Cloud Host Disappears, where Does the Organization's Data & Information Go?**



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Negative of Cloud Computing

Despite all of the positive aspects to cloud computing, the platform is not without some negative aspects. How problematic these issues are is something left to the organization to decide and mitigate.

Loss of Control – When an organization contracts for cloud services, they are handing their data over to the cloud computing provider. From that point forward (until the contract ends) the data is stored and manipulated on the provider's hardware. By handing over data to the third party, an organization is, for all intents and purposes, losing direct control over that data and information. This is not to say the organization could not get the data back, but it will be depending on that vendor to maintain its data. This leads us directly into the dependence aspect.

Dependence on a Third Party – By adopting a cloud computing service, your organization is contracting with a third party to provide specific services. As such, the organization will be depending on the third party provider to ensure their systems are secure so the organization's data and information will remain confidential. What about backups?

Quite possibly the biggest risk to cloud computing involves the threat that a cloud vendor could go out of business. The question then becomes: if the cloud host disappears overnight, where does the organization's data and information go? Organizations choosing to step out into the cloud arena absolutely must have an answer to this question. The risk of losing data is far too great to not know how things would be handled if this kind of event were to occur.

Private Cloud Products

- VMWare vSphere Server
 - Built on Virtualization Platform
 - Adaptable Hybrid (Public/Private) Systems
- Microsoft Windows Azure
 - Operating System for the Cloud
 - Microsoft SQL Azure – Cloud Databases
 - Azure AppFabric – Connect Cloud & Applications
- Ubuntu Enterprise Cloud
 - Grow/Shrink Computing Capacity to Meet Needs
 - Same APIs as Other Prominent Providers (Amazon)

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Private Cloud Products

Up to this point we have focused primarily on the public side of cloud computing; however, private clouds are also becoming a popular solution. The primary idea behind private clouds is to give organizations all of the benefits of cloud computing without being at the mercy of a third party provider. Organizations can host their own cloud platforms using a variety of operating system platforms and applications. This type of cloud service will have a much higher up-front cost than third party products, but many of the risks can be more easily mitigated internally than externally. There are several private cloud products available; however, we will just briefly discuss three provided by VMWare, Microsoft, and Ubuntu.

VMWare vSphere Server – VMWare’s specialty is virtualization software and the vSphere platform is its premier product. As we previously discussed, one of the benefits of the cloud is flexibility, and more often than not that flexibility comes from the use of virtualization products. The vSphere platform allows system administrators to adapt to changing needs and provide cloud systems that can be both used for private and public purposes.

Microsoft Windows Azure – In order to compete in this growing market, Microsoft has developed what they call the operating system for the cloud with Windows Azure. In addition, Microsoft has adapted the company’s SQL database server for cloud use. The final piece to Microsoft’s cloud solution is what they refer to as Azure AppFabric. AppFabric is designed to allow developers adapt their applications to the cloud.

Ubuntu Enterprise Cloud – The Ubuntu Linux team has worked to develop a version of the Ubuntu server for use in the cloud. As with other private cloud products, the Ubuntu Enterprise Cloud is designed to grow or shrink computing capacity in order to meet demand. The system takes another step and provides standardized APIs for developers that mimic similar hosted offerings by companies such as Amazon.com.

Hosted Solutions

- Google Checkout/PayPal
 - Online Payment Processing Aimed at Simplifying the Process of Paying for Online Purchases
- Amazon Elastic Compute Cloud (EC2)
 - Designed to Make Web-Scale Computing Easier for Developers
 - Pay Only for Capacity that you Actually Use
- Various Cloud Providers
 - IBM, Yahoo, Microsoft, Adobe, Amazon, Google
 - Rack Space Cloud, GoGrid, Hosting.com, Many More

Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents


Hosted Solutions

There are a number of hosted cloud solutions providing a wide array of services. Some types of hosted services you may have heard of include:

Google Checkout or Paypal – These are online payment processing solutions that are aimed at simplifying the process of paying for online purchases. While Paypal became a popular payment method through eBay, the payment system is being used by more and more individuals and organizations for collecting payments for items or services rendered.

Amazon Elastic Compute Cloud (EC2) – Amazon's EC2 cloud platform was designed to make web-scale computing easier for developers to create the applications your organization needs. This platform has gained some popularity in recent years, especially due to the company's increasing record of reliability for maintaining the availability of services to its clients. The primary benefit to Amazon's cloud solution is that you will pay only for the capacity your organization actually uses, instead of paying for capacity never used or needed.

Now, these are just the tip of the iceberg for hosted cloud solutions. Some of the major players in the Cloud Computing arena include IBM, Yahoo, Microsoft, Adobe, Amazon, and Google. While these big names might be enough of a deterrence for new companies to enter the Cloud fray, there are still plenty of small, upstart companies looking to make an impact in this area. Some of these include Rack Space Cloud, GoGrid, Hosting.com, and many more.



The Industry

- Business Processes Accounted for 83% of the Cloud Services Market in 2008
- Gartner Predicts Worldwide Cloud Computing Market will Reach \$150.1B by 2013
- Not Exclusive Domain of Tech Companies
 - Manufacturers & Supply Specialists Incorporate the Technology
 - Deal with Increased Complexity of Global Supply Chain
- Microsoft, IBM, Google & AT&T have Invested in the Technology & Adopted It

Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

The Industry

Just to give you an idea as to how Cloud Computing is viewed in the industry, here are some interesting facts that have been obtained by Gartner.

- Business processes (such as accounting and HR systems) accounted for 83% of the cloud services market in 2008.
- Gartner's research on Cloud Computing is predicting that the CC market will reach \$150.1 billion by 2013.
- Cloud Computing is not the exclusive domain of tech companies. Other companies specializing in manufacturing and supply specialists are also incorporating the technology in order to better respond to the increased complexity of the global supply chain.
- Many big companies, including Microsoft, IBM, Google, and AT&T have all invested in the technology and adopted it for various purposes.

Security of the Cloud

- How Secure is Cloud Computing?
- Potential Security Issues
 - Privileged User Access
 - Regulatory Compliance
 - Data Location
 - Data Segregation
 - Recovery
 - Long-Term Viability
- Do You Trust the Cloud Provider?
 - Learn About the Hosting Company...



Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Systems Security Management

Security of the Cloud

How secure is Cloud Computing? The answer is complicated and it varies depending on the cloud service selected. Here is some general information to help understand the security risks with cloud computing services.

Privileged User Access – Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

Regulatory Compliance – Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

Data Location – When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

Data Segregation – Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

Recovery – Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

Investigative Support – Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

Long-term Viability – Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says.

The bottom line with Cloud Security is the question: do you trust the cloud provider? Organizations absolutely must do their due diligence and research the vendor prior to making any contractual agreements for Cloud services.

Digital Forensics in a Virtual Environment

- Benefits

- A single forensic image can be cloned multiple times
 - Allows for numerous tests to be run
 - A clean image is always used
- Need for hardware support is mitigated
 - Provides live viewing of the OS



- Challenges

- Different formats exist, complicating searches
 - VMware, Parallels, VirtualBox, etc.
 - All use different files
- VMs easily stored on external media
- Because the VM is stored in a flat file it's much harder to examine

Systems Security Management


Eller / MIS
Copyright © 2015, Arizona Board of Regents

Digital Forensics in a Virtual Environment

Digital forensics in a virtualized environment is a fairly new playing field; virtualization can not only benefit forensic analysts by providing new tools, but can also create unique challenges when an investigation needs to be done in a virtualized environment.

A great thing about virtualization is the ability to create a clone of a machine that can be investigated using numerous methods, each time creating a new image, while maintaining an untouched “golden” image for evidentiary purposes. This helps maintain the chain of custody and allows for certain activities that, in traditional forensic investigations, would be all but verboten: powering on the machine to inspect it live. Using clones of a target machine allows for deeper investigation without fear of compromising or damaging the initial operating system or associated files.

Unfortunately, along with the benefits come some unique challenges when conducting an investigation in a virtual environment. Now that computers have become powerful enough to allow even a modest desktop computer to run a hypervisor in the OS, the need for gathering evidence that may be in a virtual environment creates a need for new techniques and tools. Home virtualization products such as VMware Player, Parallels, and VirtualBox allow for virtual machines with many different file formats, some proprietary, meaning they can only be read with the software that created them. Another issue is that the operating system in a virtual machine is now a flat file, rather than something installed on a hard disk, meaning the user can delete the file and the machine along with all its contents, making finding the evidence that much harder. Add to this the fact that storage devices have greater capacity in smaller form factors, so finding tiny jump drives in a suspect's house just got a lot harder.



Next Module...

- Viruses
- Virus Classification
- Worms
- Trojan Horses
- Malicious Software & Automated Tools
- Botnets
- Keystroke Monitoring
- Brute Force & Dictionary Attacks
- Social Engineering
- Awareness, Training, & Education (AT&E) as Countermeasures
- Data Mining
- Database Inference
- Protecting Systems
- Risk Management Concepts

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

In the next module we will be discussing threats, vulnerabilities, and the countermeasures used to protect systems, including:

- Viruses, Worms, & Trojan Horses
- Malicious Software & Automated Tools
- Botnets
- Keystroke Monitoring
- Brute Force & Dictionary Attacks
- Social Engineering
- Awareness, Training, & Education (AT&E) as Countermeasures
- Data Mining & Database Inference
- Protecting Systems
- Basic Overview of Risk Management Concepts

References

- Brodikin, J. (2008, July 2). Gartner: Seven Cloud Computing Security Risks. *InfoWorld*. Retrieved from <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0.0>.
- Cloud News Desk. (2008, November 3). Six Benefits of Cloud Computing. *Web 2.0 Journal*. Retrieved from <http://web2.sys-con.com/node/640237>.
- Gnorr, E. & Gruman, G. (2009). What Cloud Computing Really Means. *InfoWorld*. Retrieved from <http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031>.
- Leybovich, I. (2009, August 4). Can Cloud Computing Help Your Business? *ThomasNet News*. Retrieved from <http://news.thomasnet.com/IMT/archives/2009/08/cloud-computing-in-the-supply-chain-distribution-networks-online-resources-it.html>.
- Virtualization Basics. (2010). *VMWare, Inc.* Retrieved from <http://www.vmware.com/virtualization/what-is-virtualization.html>.
- Ware, C. (2009, April 24). The Pros and Cons of Cloud Computing. *Ezine Articles*. Retrieved from <http://ezinearticles.com/?id=2264422>.
- What is a Virtual Machine? (2010). *VMWare, Inc.* Retrieved from <http://www.vmware.com/virtualization/virtual-machine.html>.
- Windows Azure Platform. (2010). *Microsoft Corporation*. Retrieved from <http://www.microsoft.com/windowsazure/>.
- Why Your Company Should Virtualize. (2010). *VMWare, Inc.* Retrieved from <http://www.vmware.com/virtualization/why-virtualize.html>.