Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Business Continuity On A Stick

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2008, Author retains full rights.

Business Continuity On A Stick

GSEC-401 Gold Certification

Author: Patrick Kral, patrick.kral@gmail.com

Adviser: Leonard Ong

Accepted: March 28, 2008

© SANS Institute 2008, Author retains full rights.

Outline

1. Abstract..... 3
2. Introduction 3
3. Obtaining Business Requirements..... 4
4. Light-weight virtualization versus Full virtualization..... 6
5. Potential Pitfalls..... 7
   Common Compatibility & Performance Limitations..... 7
   Security..... 8
   User Acceptance..... 8
6. Cost Savings..... 10
   Licensing Costs..... 10
   Faster Recovery Time..... 11
7. Feasibility..... 12
8. Check Lists..... 13
9. References..... 14

© SANS Institute 2008, Author retains full rights.

1. Abstract:

Since the terrorist attacks of September 11th, 2001 it has been prudent for businesses and other organizations to implement business continuity and disaster recovery (BC/DR) plans as part of due diligence and/or compliance with state and federal statutes. The purpose of this document is to provide a technical analysis of using virtual machine technology and USB drives within business continuity and disaster recovery planning. The areas of focus are: obtaining business requirements, comparison between light-weight (aka desktop) virtualization versus full virtualization, potential pitfalls, and cost savings. This document is only intended to be part of BC/DR planning process or to be implemented within an existing BC/DR process; it can also be used as a guide for creating an inexpensive way to implement a mobile workforce.

2. Introduction:

Business continuity and disaster recovery or having a mobile workforce can be a costly endeavor, especially when one requires the procurement of laptops. The costs for laptops can become astronomical for some businesses to implement and therefore may not be feasible; however, improvements to a technology that has existed since the 1960s[1] can change all of that, its called virtualization. Virtualization is basically emulating a computer or computing environment on top of another (e.g. having a Linux operating system running inside a virtual

[1] http://en.wikipedia.org/wiki/Virtualization

© SANS Institute 2008, Author retains full rights.

machine on top of a Windows operating system). By utilizing virtual machine software or VM for short, and USB drives, one would be able to carry their workstation environment anywhere without the need for laptop, as long as they have access to a computer capable of running the VM client software.

The problem with using this concept would be performance versus compatibility, along with the security issues that could surface and user acceptance. It is extremely important to obtain the business requirements needed, before considering to implement or event pilot this technology. Without such information, it would be nearly impossible to obtain buy-in from management, let alone end-users.

3. Obtaining Business Requirements:

As with any endeavor one must be aware of what is required before starting a project. There are several questions that need to be answered before considering using USB drives and virtual machines:

1. What applications are needed to perform ones duties?

2. How will your users be able to access their data?

3. Do your users need VPN Clients or some other form of remote access?

4. If your users were to use their own PCs to run their virtual workstation, how will you obtain their system requirements to ensure compatibility?

- Also, (vendor/technology dependent) would your users mind

© SANS Institute 2008, Author retains full rights.

temporarily installing software on their home PCs?

5. What are the security risks?

The answers from those questions are meant to help one start to think and plan on the feasibility of using this technology. This will take not only management buy in, but also from your fellow employees as well; especially if a virtual client has been selected that temporarily installs software on their home computer. There are also security risks to consider that could result in security breaches if not planned carefully; this is especially true if a VM client does not have some form of encryption implemented to protect the data contained within them. It is important to note that there two types of VM technology: light-weight virtualization[2] and full virtualization both have advantages and disadvantages in regards to functionality and security.

4. Light-weight Virtualization vs. Full Virtualization:

The key difference between light-weight and full virtualization is the implementation of how the VM operates. Light-weight virtualization does not require a guest operating system (OS), whereas a full virtualization client does. Light-weight virtualization clients utilize the local operating system resources to run applications within its virtual container; this in of itself requires fewer system resources and drive space than the alternative. However, software compatibility can be an issue, especially those concerning proprietary or kernel mode

[2] Light-weight virtualization is not to be confused with Application Virtualization, such as Thinstall.

© SANS Institute 2008, Author retains full rights.

drivers, such as: IPSec VPN Clients. This will likely disappear as this technology matures over the course of time.

Full virtualization software can run an entire workstation image within a virtual container without relying on host operating system files for internal support; this in turn provides a higher level of compatibility, as software running inside of it would be no different then if it was running on a real workstation within the office environment. This compatibility comes at a cost of requiring more system resources and disk space, and therefore drives up costs.

Light-weight VM vs. Full VM

VM Technology	Advantages:	Disadvantages:
Light-weight	1. No guest OS needed 2. Small footprint 3. Requires fewer system resources 4. Compatible with major office applications	1. OS Dependent 2. VPN client compatibility is currently limited 3. Relies on host system for anti-malware protection[3]

[3] Vendor dependent: VM clients can scan host system for security programs before launching.

© SANS Institute 2008, Author retains full rights.

Full	1. Can utilize standard workstation images 2. Maximum Application Compatibility 3. Client may support multiple OSs	1. More resource intensive 2. Requires more drive space 3. Higher System Requirements 4. Requires guest OS

Keep in mind when deciding between the two technologies of compatibility versus performance. Full VM technology has been around for several decades and has proven itself useful within the corporate world[4]. At the time of this writing Light-weight VM technology has yet to have the level compatibility needed as a replacement to Full VM.

5. Potential Pitfalls:

As with any technological endeavor there are several issues that can surface, especially when trying to implement a technology that requires users to give out information of their own home computers. Most of the other issues are security and support costs.

Common Compatibility & Performance Limitations

There are several compatibility and performance issues that apply to both light-weight and full virtualization, the most obvious one is the host OS support of the VM client as both software technologies rely on an underlying OS to run on. This limitation can prevent users with

[4] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011828

© SANS Institute 2008, Author retains full rights.

non-Windows OSs from being able to utilize the VM. Another issue they both share is the hardware resources of the host system; despite light-weight virtualization requires far fewer system resources than full, they are still at the mercy of the end-user's hardware. Some systems may not even have USB ports and other may not even meet the minimum processor and/or RAM requirements.

Security

*S*ecurity can be an issue when using USB drives that do not have encryption and/or some form of access control, such as passwords, pin numbers, or biometrics to authenticate the user; without authentication of the user and encryption, any data that is stored on the drive could be easily compromised[5]. However, it is possible to utilize various encryption programs or buy USB drives with hardware based encryption to prevent unauthorized access to organizational data.

Another security issue is making sure that the PC that the virtual workstation would run on, has sufficient security software installed (dependent on VM software technology used). Some VM clients include the ability to scan host system for security software before launching; if none is found, then it would alert the user that the machine is lacking security software and refuse to launch.

VPN compatibility issues are the last major security hurtle; however, this issue only applies to light-weight virtualization

---

[5] http://labmice.techtarget.com/articles/usbflashdrives.htm

© SANS Institute 2008, Author retains full rights.

products due to their immaturity at the time of this writing. There are a couple of ways to overcome this shortcoming such as:

1. Have end-users install VPN client software on the host computer.
2. Create scripts to install and/or dynamically install and uninstall the VPN client from the host computer.
3. Use VPN client technology that does not require kernel mode drivers (e.g. some SSL VPNs and SSH tunneling).

User Acceptance

Gathering end-user system information could be a potential problem as end-users may not be technologically inclined to know whether or not their system is capable of running the virtual workstation. This can be overcome by using simple instructions and check boxes that will allow the user to verify their system requirements quite easily.

The major issue that could be brought by end-users is the possible requirement of installing software on their home computers; this could lead to resistance as some people may not be comfortable having their employer's software on their computer. User education could be the one possible way to overcome this fear, such as the fact that Full VMs only require a player to be installed and therefore need not to worry about their employer spying on them, or in the case of Light-weight VMs the software will only need to be installed temporarily dependent on the vendor or script used for VPN and mapping network drives.

© SANS Institute 2008, Author retains full rights.

6. Cost Savings:

There are several monetary benefits towards using USB drives with a VM client and image stored on it. The two most obvious benefits are the cost of hardware and loss prevention. The hardware costs are generally the price differential between per unit cost of laptops versus per unit cost of a USB drive. At the time of this writing a 4GB USB drive costs around $20 USD and 8GB roughly $30 USD[6], plus the cost of software licenses; whereas laptops can range from $300 and up (April 22, 2008)[7]. If a laptop is lost or stolen the replacement costs can be staggering compared to a USB drive.

Licensing Costs

The cost of licensing will vary from product to product as of April 22nd, 2008 there is currently only one vendor offering light-weight virtualization that will work on USB drives called MojoPac by RingCube. This particular product does not require the licensing cost of an OS, as it borrows the host OS system files to create a virtual workspace; therefore the licensing costs are only associated to the software that is installed within the virtual workspace and that of the MojoPac (or MojoDrive), which as of July 30, 2007 the cost is $99 per a license[8]. As

---

[6] http://www.newegg.com/Store/SubCategory.aspx?SubCategory=522&name=USB-Flash-Drives

[7] http://www.newegg.com/Product/ProductList.aspx?Submit=ENE&N=2030260032&bop=And&Order=PRICE

[8] http://www.mojopac.com/enterprise/news/Press_release/2007730_channel_insider.pdf

© SANS Institute 2008, Author retains full rights.

for the Full VM products, they do require a license for each guest OS, along with the cost of additional applications, and the cost of the VM software itself. Currently, there are two Full VM products being offered:

1. **VMware ACE** – licensing costs can range from $1,250 USD for 10 licenses up to $26,200 USD for 200 licenses, including the software to create the VM images and technical support[9].

2. **Moka5** – licensing varies dependent on the number of licenses needed and 18% of the overall licensing cost is added for technical support[10].

Faster Recovery Time

In the event of a disaster organizational downtime can have a significant impact in regards to productivity and/or revenue. By having a business continuity plan in place and USB drives deployed to all employees who need access to IT resources in order to perform their job duties, an organization would be able to have continued operations during and after a disaster.

For example: ABC Inc. has 200 users with a primary data center in New Jersey and a hot-site back up data center in Nevada; a disaster

---

[9] http://store.vmware.com/servlet/ControllerServlet?Action=DisplayPage&Env=BASE&Locale=en_US&SiteID=vmware&id=ProductDetailsPage&productID=82426300

[10] Information was obtained from the Moka5 sales team.

© SANS Institute 2008, Author retains full rights.

happened in which the company's employees had to go home for safety reasons. Once the employees are home they, could turn on their home computers, plug in the USB drive and launch the virtual workstation, and finally connect to the backup data center via VPN. This would allow ABC Inc to continue operating while the disaster is taking place and even if the disaster was sustained for several months, ABC Inc employees would still be able to perform their duties over the long haul.

The intangible cost savings that comes with faster recovery is the fact that an organization can get backup and running, and be productive within a matter hours. This becomes more beneficial in private industry, in which availability is the key to business success in preventing lost revenue. As for public industry, availability could mean the success or failure of being able to serve the public and future voters[11].

7. Feasibility:

At the time of this writing there have only been a few case studies that prove a working concept for using USB drives with VMs stored on them that have been implemented; such as: Moka5 being implemented within Panasonic's disaster recovery plan[12]. The case study focuses on the cost of replacing lost laptops that contain sensitive corporate

[11] http://en.wikipedia.org/wiki/Business_continuity_planning#Impact_analysis

[12] http://www.moka5.com/solutions/casestudy_Panasonic.pdf

© SANS Institute 2008, Author retains full rights.

information and the potential for a security breach, if those laptops security mechanisms have been compromised. By using VM clients on encrypted USB drives for DR purposes, Panasonic has the ability reduce the cost of replacing lost or stolen laptops, while providing additional layers of security via license revocation that make the VM client inoperable to a would be criminal.

Remote access requirements can be the make or brake issue in regards to feasibility within any organization, especially in regards to IPSEC VPN access. Fortunately there are several alternatives that organizations requiring users to have remote access can take:

1. Secured Websites that use Secure Socket Layer (SSL) technology can provide remote access to company servers via web browser.

2. SSL-VPN, unlike its IPSEC VPN cousin, does not require kernel mode drivers and therefore can run within Light-weight VM software; however, there are some limitations to this technology. There are two types of SSL-VPNs[13]:

    a. Client Based, which uses a software program that connects to the corporate network. Dependent on vendor may or may not support advance protocol tunneling, such as protocols that allow the mapping of network drives or software that use Active Directory.

[13] http://www.windowsecurity.com/articles/VPN-Options.html

© SANS Institute 2008, Author retains full rights.

b. Clientless, which uses web browsers as a means of connecting to the corporate network; however, this technology is limited to web-based applications.

3. Thin client technology such as Citrix and Microsoft Remote Desktop can be used instead of having applications and/or data stored on the USB drive, as it would provide remote access to a remote desktop that would contain everything necessary for a user to perform his or her duties. The benefit of using this technology is that one could use smaller and less expensive usb drives; however, the costs could increase as remote desktop may require additional bandwidth and faster servers dependent on performance requirements.

As for organizations that do not require remote access for their users, they can easily get away with using Light-weight VM clients for disaster recovery purposes. The problem with offline mode implementation would be backing up data and/or making sure that the data stored on the drive is synchronized with the data stored on the corporate network. This can be overcome by using scripts or programs that automate or synchronize changes between the data on the network and the usb drive.

The feasibility of using usb drives with VM clients installed on them is dependent on organizational need and can only be determined by organization IT staff, management, and other stakeholders. Obtaining business requirements and performing a risk analysis is the only way to determine feasibility at this point in time. A checklist has been provided on the next page, as a means to gather business requirements.

© SANS Institute 2008, Author retains full rights.

8. Business Continuity On A Stick (BCOAS) Checklists:

The following checklists are to be used only as a guideline to the feasibility of using USB drives with VM clients on them for BCP/DR purposes, and therefore not a conclusive source for specific organizational needs. It is highly recommended that each organization to create its own checklist(s) to ensure that this technology will meet business needs.

Business Requirements:

1. Does your organization have a Business Continuity or Disaster Recovery Plan implemented?

2. List the bare minimum applications that end-users need in order to perform their job duties:

   1. _____

   2. _____

   3. _____

   4. _____

   5. _____

   6. _____

   7. _____

List others on back

© SANS Institute 2008, Author retains full rights.

Technical Requirements:

1. Do end-users need remote access in order to perform their job?

2. Vendor Dependent: Are end-users willing to install software on their computer?

3. What are the space requirements for the VM client and image?

4. What are the system requirements to run the image?

After answering all of the questions from both checklists, create a checklist with the necessary system requirements that your users need to verify that their systems are compatible with BCOAS USB drives. The end-user checklist should be the final determining factor on the feasibility of using the VMs on USB drives for your organization. Remember this technology is fairly new and therefore may become more feasible in the future.

© SANS Institute 2008, Author retains full rights.

9. References:

- Wikipedia, (May 8, 2008). Virtualization. Retrieved May 8, 2008, from Virtualization Web site: http://en.wikipedia.org/wiki/Virtualization
- Computer World, (March 05, 2007). Desktop Virtualization Success Stories. Retrieved May 8, 2008, from Desktop Virtualization Success Stories Web site: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011828
- Lab Mice, (May 8, 2008). USB Flash Drives: Useful Device or Security Threat?. Retrieved May 8, 2008, from USB Flash Drives: Useful Device or Security Threat? Web site: http://labmice.techtarget.com/articles/usbflashdrives.htm
- Wikipedia, (May 8, 2008). Business continuity planning. Retrieved May 8, 2008, from Business continuity planning Web site: http://en.wikipedia.org/wiki/Business_continuity_planning#Impact_analysis
- Moka5, (May 8, 2008). Disaster Recovery: Panasonic R&D. Retrieved May 8, 2008, from Disaster Recovery: Panasonic R&D Web site: http://www.mokafive.com/solutions/casestudy_Panasonic.pdf
- Shinder, DEBRA (Jun 10, 2004). Comparing VPN Options. Retrieved May 8, 2008, from DEBRA Web site: http://www.windowsecurity.com/articles/VPN-Options.html

© SANS Institute 2008, Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced