ISSN: 2516-6190 (Print) 2516-7219 (Online) http://sevenbridges.ncl-coll.ac.uk

Advantages and Disadvantages of Virtualisation

Heather Broadley

Seven Bridges, Vol. 6 (2018)

Published on: 05/07/2018

Seven Bridges is published by:
Newcastle College
Rye Hill Campus
Scotswood Road
NE4 7SA

Advantages and Disadvantages of Virtualisation

Heather Broadley
FdSc Networking and Security
Newcastle College

ABSTRACT

Literature indicates that there are many advantages of virtualization, from the roles of network applications, to the controls and security. Network users must be compliant with ISO 27000 using all or some of the recommendations set out in ISO 27002. This is a major consideration for any companies but especially those dealing with sensitive customer information. Having tight control over staff is just as important as having a secure network. Research shows that there are a variety of good practices that can be considered when setting up a network for a new or existing company. For example, tools, reports and latest server configurations can used to assist when setting up domains, policies and security. Documentation of a network is one of the most important things any organisation must do for its staff, or they will have no records of how things are configured.

KEYWORDS: Compliancy, LAN Server, Security, Virtualisation.

INTRODUCTION

This research is going to discuss the advantages and disadvantages of virtualisation and use critical analysis for the purpose of supporting a conclusion. The paper will also: incorporate the role of network applications and the use of controls to improve information security and the network itself define the role and purpose of ISO 27000 and 27002 compliancy and recommendations, and how this can help improve information security; identify best practices, security considerations and tools for setting up a new windows server, as well as the configuration and operational help these tools give. For critical evaluation purposes documentation for an example network has been included for future replication and to explain why it has been done.

ADVANTAGES AND DISADVANTAGES OF VIRTUALISATION

An advantage to virtualisation is that it can help by reducing costs and outgoings for the company. This is done by reducing the carbon footprint and avoiding hefty costs from governments. Lower energy consumption for cooling and electricity results in smaller monthly bills, as well as reducing the hardware costs for servers and related resources. However, the cost of transferring a network from non-virtual to virtual can be expensive due to server costs and software licenses. (Rivera, 2017)

Isolated testing as a development environment allows testing of different OSs (operating systems) and fault prevention as well as protection against viruses. This can also include security advantages as each VM (virtual machine) can be independent of each other which reduces the vulnerability over all. On the other hand, VMs are a resource hog and require a lot of processing power and RAM (random access memory) as well as a lot of disk storage space (Ganore, 2005).

VMs are incredibly lightweight and portable due to them being stored on HDDs (hard disk drives). This in turn means there are no bulky and heavy servers to move around should the company relocate or have their facilities updated. They are also very easy to maintain. On the other hand, this does mean that a facility that lacks proper security and theft prevention could have all their data walk out the door due to the compact nature of HDDs. A VM can also be copied across onto a removable storage device.

Disaster recovery for virtualisation can be very quickly implemented should something go wrong, and the time taken to do this is usually hours instead of days. This, of course, depends on the size of the company and how much data is to be recovered (Kirvan, 2009). Redundancy for servers is always a fantastic idea as having multiple physical servers, running the same software can limit any service interruption; should one server go down, another can just take its place, and everything will continue to run (Strickland, 2008). Unfortunately running multiple physical servers can be expensive to purchase and monthly electrical bills can go up.

Virtualisation is easily scalable and more machines can be added very quickly and easily to the network that is already there. This makes expansion very quick, cost effective and can reduce the need to purchase additional hardware. This gives flexibility to add, remove and backup with minimal disruption. However, it takes a certain level of expertise and knowledge to maintain a virtual network. Without the required knowledge VMs can easily be broken and bad habits, such as laziness and complacency, develop in those using them.

In conclusion virtualisation has many fantastic benefits including cost effectiveness, ease of use, ease of maintenance, disaster recovery and the reduction of physical space required. Other benefits include the up time of systems and ease of information sharing across a vast secured network, as well as keeping access to sensitive data restricted, ease of migration when upgrading servers or simply moving from legacy to virtualisation. Over all the advantages of virtualisation outweigh the disadvantages of virtualisation (Ganore, 2005).

NETWORK APPLICATIONS, SOFTWARE, CONTROLS AND ISO 27000/2 SECURITY

Network applications, software security and controls are incredibly important for any network as they can provide a secure base and help eliminate threats both externally and internally to the network. Network applications provide useful and functional data transfer from one point to another across a network.

An example of software for a server would be to use SSH (secure socket shell) on the server such as PuTTY, Tectia and WinSCP. This software provides a pair of cryptographic keys which can be used for user authentication as an alternative to password-based logins. This can be done in two ways - private keys and public keys. The private key is kept secret by the user and the public key can be given out freely. This type of authentication is completely encrypted but it is possible to allow password-based logins. However, should a password-based login be allowed it is recommended to have a solution like fail2ban in place which will limit the amount of password guesses and greatly reduces the risk of a hacker using a brute force or rainbow table attack to gain access (Ellingwood, 2015). SSH is incredibly easy and quick to set up and is a great way to ensure remote access is secure.

If the network is to connect externally to the internet the best way to do that would be to use SSL/TLS (secure socket layer/transport layer security) encryption. This is particularly useful at preventing 'man in the middle' attacks on a network. Preventing an outsider from imitating a server within the network means that network traffic won't get intercepted, captured and then used maliciously at a later date. Each server within the network can be configured to recognise certain certificates of authenticity. This is a way of keeping the network safe without using a VPN (virtual private network) to encrypt the data (Ellingwood, 2015).

Firewalls are one of the most basic ways to help ensure the network is secure. They stop both incoming and outgoing threats and are usually the first line of defense. It is also possible to exclude traffic sent to and from specific ports and protocols or aimed at specific ports and protocols. Application-level gateway is more commonly known as a proxy server which sits between the internal network perimeter and external server to help clean up external communications as well as monitor them. Unfortunately, some applications may be unable to run fully when a proxy server is enabled and need special configuration. Stateful-inspection combines all the above-mentioned aspects and more. This helps prevent DOS (denial of service) attacks but it can require custom and often complicated configurations. The higher up the OSI model the firewall can sit, the better chance it has to prevent unwanted attacks or intrusions and provides the best security (Bittlingmeier and King, 2013).

Antivirus and antimalware software are also very good ways to stay protected from both external and internal threats. Antivirus software uses a heuristic method to track viruses and examine behaviour; this means that a virus can be detected well before it becomes a threat and as long as the antivirus software is up to date (Cobb, 2002). Antiviral software such as AVG and Norton are most commonly used. Antimalware is just as important as antivirus software as malware cannot always be detected by antiviral software. If a network is not properly protected then malicious software can sneak onto a network and steal sensitive information such as passwords, bank details, user accounts and more. Antimalware software such as MalwareBytes and SpyBot Search & Destroy are popular and effective programmes (DuPaul, 2012).

Controls for a virtual network include: secure configurations for hardware and software, controlled access to information on a need to know basis, data loss prevention, limitation and control of services and applications, and controlled use of administrative privileges (Jackson, 2013). All controls can be implemented before user's log in and can be set to either individuals, groups of people or whole departments as well as the network itself. Secure configurations for hardware can be something as simple as keeping the room with the servers and switches in locked, either with a key, pin code entry or swipe card. Securely configuring software such as firewalls, antivirus, antimalware and OSs (operating systems) can be done by keeping them up to date with patches and updates as they become available from the organisation.

Limitations for services, applications and administrative privileges can be set via the server using UAC (user account control) and policies to govern certain people or groups of people. This can limit certain files, folders, access to the control panel, command prompt and even when they can be logged into the system. Data loss prevention gives the option to prevent people from using plug and play devices such as memory sticks, as they can contain viruses which may not be picked up via the antiviral software or harmful programs which can penetrate into a network and grant them access higher up than their security level currently allows, in turn allowing access to files and information which can then be copied off the network.

IDS (intrusion detection system) and IPS (intrusion prevention system) increase the security of the network as well as monitoring the traffic and scanning the packets of information that travel across the network. The main difference between the two is how they work when an attack is detected. (Panda Security, 2017) IDS provide preventative network security against suspicious activity, it sends out warnings to administrators, but it does not block incoming attacks. IPS controls the network access to protect it from attacks. Generally, IPS will have a set of rules and take action against the attack, blocking it before it succeeds in breaking in.

The purpose and role of ISO 27000 is a series of standards for information security for businesses. It is a means of performance analysis (ISO 27000, 2013). ISO 27002 is ‘a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.’ (ISO 27000, 2013). It is not a requirement to be ISO 27000/27002 compliant for a company but if they are, it can help with any problems that could potentially arise in the future if the company deals with particularly sensitive information such as: bank details, national insurance numbers, addresses, dates of birth, *etc*. Controls from ISO 27002 that can be applied to the network include things like password policies, access controls, physical and environmental security. If the company wishes to be certified for ISO 27002 compliance it can be done via an external auditing company which will then issue a certificate and seal. The controls to a network are similar in regards to the standard controls that can be applied. Password policies could require anything from a certain length, the inclusion of numbers or special characters and how often the password will expire. Physical and environmental security can include on site security personnel, biometric, keypad entry or swipe card access to certain areas, and whether the room housing your servers has a window. This can all help in not getting the business sued: by keeping audit logs and being audited regularly it helps keep things as secure as possible. Always using encryption makes life very difficult and unpleasant for anyone attempting to access the network or the information. The current standard for internet encryption utilises a 2048bit key. (Security.stackexchange.com, 2012)

WINDOWS SERVER COMPLIANCY

Best practices for setting up a new Windows server include: documenting the server setup, user controls and group policies, strong password policies, controlling administrators and test settings. Documenting the topology, forest and domain configurations are good practice because it is possible to see who has access to what, what the configuration settings are and group policies. A tool for the group policies is Microsoft GPMC (group policy management console) this unifies management of group policies across the network. (Deuby, 2006). The use of strong password policies makes it harder for an outsider to gain access to the network. This can include a specific length, numeric value and special characters. Controlling or limiting the administrators of a domain helps in the prevention of data loss and things going wrong. This stops people administering maintenance or performing tasks when they do not know what they are doing. Testing settings for group policies on a virtual duplicate of a forest can mean the difference between rolling out an updated group policy and having no problems, versus rolling it out live and finding lots of problems. MBSA (Microsoft baseline security analyser) determines the security state and assesses for any missing updates to the server. Reports from this can help with updates, firewalls and password checking. This makes sure things are as secure as possible. (Technet.microsoft.com, 2013) The server manager provides an overall view of the server and helps guide administrators through the process of installing, configuring and managing the roles and features of the server. (Technet.microsoft.com, 2007) Reports from the server manager can help identify what services are currently not running and why, a list of who has permissions and what for. These tools help in the configuration and operations of the server by making life a lot easier for the administrators working on it. It also helps to point out what needs fixing if something has gone wrong.

NETWORK DOCUMENTATION

This is an example of documentation for a small business network, the features and security considerations cover: file sharing, credential management, restricted access, DNS (domain name system), DHCP (dynamic host configuration protocol), group policies, static wallpapers, access control, application deployment, functional client machine(s), roaming profiles, home drives and folder redirection, antiviral and antimalware software, firewalls, whether or not the server is ISO 27000 compliant or just follows some of the ISO 27002 recommendations, password policies, IDS/IPS, encryption, UAC, physical and virtual security, backup domain controller.

IP (internet protocol) addressing scheme has been set so that certain IP addresses are unavailable from the pool of dynamically assigned addresses, but manually configured to the servers as a static IP, this is to ensure the servers always have the same address and can be accessed easily. This also works for any peripherals within the office, a printer for example. It has been set to a ‘Class C’ network with no subnetting.

User groups and configurations were set out according to the network share structure documented in the module guide. IT Services have full access to all the folders, the rest of the staff have read only access to ITSShared Resources$ UserResources$, Backgrounds$, Scripts$, TicketTracking$, Projects and their own Human Resources folder. HR (human resources) has full access to all of the HR folders. Project managers have full access to all the projects folders, the programmers have access to a specific project within the main projects folder. Administrators are also set to have no access to the control panel, command prompt, install applications or to access restricted information. The ‘$’ denotes that the folder is a specially hidden administrative share folder used to manage the network. They are not visible when browsing files using Windows explorer, also those folders have been hidden as an extra security measure. Groups within the domain have been created for each project with the relevant staff members for ease of control. Groups for each level have also been created for control and security so all project managers are within one group, all IT are within one group, HR are all within one group, programmers are all within one group and the admins are all within one group. This helps when new members of staff join the company or a person is promoted, all of the roles are already there and it saves time applying several new roles and removing old roles. Home drives, folder redirection and roaming profiles have also been added to the server. This is to ensure any work can be accessed from any client machine and is easily backup up. There is also a fully functioning application deployment policy in place. This makes installing software or rolling out new software, updates or applications incredibly quick and easy. A fully functioning backup domain controller is also available which has DHCP, DNS, DFSR (distributed file system replication) and some folders as an example. The reason for the backup domain controller is in the case of a ‘never event’ happening. The main server should never go down or offline but if maintenance was required, the server broke or something went wrong the backup controller would function instead of the main controller, thus allowing work to continue and limit the amount of downtime a company would have. This is all to ensure any change of staff within the IT or networking side are fully up to speed with what is already in place. Also helping to set up a new network there is a base to work off.

The network has been set up using Microsoft Windows Server 2012 R2 with the backup controller also running Microsoft Windows Server 2012 R2. I have chosen this because I already have a working knowledge and experience of Microsoft Windows as a client and that can be transferred onto server much easier and is a lot less time consuming than learning a whole new operating system and server like Linux for example. The client machines are Microsoft Windows 7 Professional and Microsoft Windows 8.1. These have been chosen again as I have a working knowledge of both of these systems from past experience and it is much easier to trouble shoot and problem solve on a system you already have knowledge on than a brand-new system. Also, it cannot be guaranteed that the person or people replicating the network would have any knowledge in any Linux systems, but it can be safely assumed most people will have a background in a Microsoft Windows client base at least.

REFERENCES

Bittlingmeier, D. and King, T. (2013). Understanding the Basic Security Concepts of Network and System Devices | CompTIA Security+ Exam: Devices, Media, and Topology Security | Pearson IT Certification. [online] Pearsonitcertification.com. Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=31562&seqNum=2 [Accessed 1 November 2017].

Cobb, C. (2002). Network Security: Anti-Virus Do's and Don'ts - dummies. [online] dummies. Available at: http://www.dummies.com/programming/networking/network-security-anti-virus-dos-and-donts/ [Accessed 2 November 2017].

Deuby, S. (2006). Security: 19 Smart Tips for Securing Active Directory. [online] Technet.microsoft.com. Available at: https://technet.microsoft.com/en-us/library/2006.05.smarttips.aspx [Accessed 10 November 2017].

DuPaul, N. (2012). Common Malware Types: Cybersecurity 101. [online] Veracode. Available at: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 [Accessed 2 November 2017].

Ellingwood, J. (2015). 7 Security Measures to Protect Your Servers | DigitalOcean. [online] Digitalocean.com. Available at: https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers [Accessed 2 November 2017].

Ganore, P. (2017). Advantages and Disadvantages of Virtual Server. [online] ESDS Official Knowledgebase. Available at: https://www.esds.co.in/kb/advantages-and-disadvantages-of-virtual-server/ [Accessed 23 October 2017].

ISO 27000, I. (2013). ISO 27000 - ISO 27001 and ISO 27002 Standards. [online] 27000.org. Available at: http://www.27000.org/ [Accessed 8 November 2017].

Jackson, W. (2013). 20 critical controls do improve cybersecurity, but are you using them? -- GCN. [online] GCN. Available at: https://gcn.com/articles/2013/07/08/20-critical-security-controls-implementation-lags.aspx [Accessed 8 November 2017].

Kirvan, P. (2009). How server virtualization benefits disaster recovery. [online] SearchDisasterRecovery. Available at: http://searchdisasterrecovery.techtarget.com/feature/How-server-virtualization-benefits-disaster-recovery [Accessed 23 October 2017].

Panda Security, P. (2017). What is the difference between an IDS and an IPS? - Technical Support - Panda Security. [online] Pandasecurity.com. Available at: https://www.pandasecurity.com/uk/support/card?id=31463# [Accessed 10 November 2017].

Rivera, A. (2017). The Pros and Cons of Virtualization. [online] Business News Daily. Available at: https://www.businessnewsdaily.com/6014-pros-cons-virtualization.html [Accessed 23 October 2017].

Security.stackexchange.com. (2012). Understanding 2048 bit SSL and 256 bit encryption. [online] Available at: https://security.stackexchange.com/questions/19473/understanding-2048-bit-ssl-and-256-bit-encryption [Accessed 8 November 2017].

Strickland, J. (2008). How Server Virtualization Works. [online] HowStuffWorks. Available at: https://computer.howstuffworks.com/server-virtualization.htm [Accessed 23 October 2017].

Technet.microsoft.com. (2013). Baseline Security Analyzer Frequently Asked Questions. [online] Available at: https://technet.microsoft.com/en-us/security/cc184922 [Accessed 15 November 2017].

Technet.microsoft.com. (2007). Server Manager Technical Overview. [online] Available at: https://technet.microsoft.com/en-us/library/cc753319(v=ws.10).aspx [Accessed 16 November 2017].