Efficiently Protecting Virtualized Desktop Infrastructures Against Malware

Performance Comparison between Traditional- and Centralized Antivirus

Arris Huijgen
University of Twente

Graduation Committee

University of Twente
Dr. Pascal van Eck

Radboud University Nijmegen
Dr.ir. Erik Poll

Deloitte
Coen Steenbeek, MSc
Henri Hambartsumyan, MSc

June 18, 2013

Executive Summary

The cloud is getting increasingly popular and also desktops are migrated to the cloud which are called Hosted Virtual Desktops (HVDs). Because virtualization makes hardware resources very flexible, it is often used to build a cloud platform. These desktops also need to be protected against malware. Virtualization software provider VMware added capabilities to its corporate product to provide antivirus protection from outside the Virtual Machine (VM) using its vShield module. Several antivirus vendors including Trend Micro developed antivirus software making use of this module.

Because no comparisons have been done yet between traditional antivirus and antivirus software making making use of virtualization, research has been conducted comparing Trend Micro's traditional antivirus software Worry-Free Business Security (WFBS) with its vShield-compatible antivirus software called Deep Security (DS). This research showed that despite self-protection measures it is relatively easy to disable or remove the DS antivirus software inside the HVD without being detected. Moreover, it turned out that in this small environment simulating 10 HVDs, the performance of WFBS is much better compared to DS while DS also used much more resources. This is a remarkable result as DS is specifically aimed for virtualized environments and can therefore be expected to perform better than the traditional WFBS antivirus software. During the test it turned out that WFBS uses the full CPU of the VM while DS uses its dedicated antivirus VM to scan the files leaving the test VM in an idle state which has performance advantages for the processes running inside the VM. Furthermore, due to DS's usage of a dedicated VM and several additional VMs that are required to use this software, the memory load of DS is much higher compared to WFBS. It should however be taken into account that in a large-scale environment, DS might perform much better as it is aware of the virtualization.

Preface

In the process of writing my Master's Thesis I used various sources of knowledge and experience that pointed me into the direction needed to accomplish this project.

In September 2012 I started my graduation project in the Amstelveen Office of Deloitte. I would like to thank all professionals who were willing to discuss my topic, particularly my supervisors Coen Steenbeek and Henri Hambartsumyan for their intellectual opinion on the content of my graduation thesis. I would also like to thank Daan Muller who provided me with his knowledge on the topic of virtualization and feedback on my thesis.

In the period of November 2012 until February 2013, I worked on my thesis at the Deloitte office in Tel Aviv. I would like to thank the people who made it possible for me to go there, specifically Angelique van Houten who put a lot of effort into it. I am also very grateful to Sharon Cohen for providing me all resources in the Tel Aviv office to work on my project.

Finally, I would like to thank Pascal van Eck from the University of Twente and Erik Poll from the Radboud University for all support and feedback throughout the thesis project and their flexibility in providing supervision, even during my stay in Israel.

Thank you so much, all of you.

Arris Huijgen, June 2013

Contents

1. Introduction

Lately many services have been gradually migrated to the cloud and expectations are that in the future even more software we currently run locally will be moved to the cloud.[1] The cloud has many advantages such as the global availability, cost efficiency, flexible scalability, solid data storage and backup.[2]

Besides webmail, online storage and browser-based office software, desktops in the cloud, also known as HVDs, are getting increasingly popular. HVDs are workstations that have been moved to the cloud requiring the user to only have a thin client to connect to its personal virtual desktop. A more extended explanation of HVDs will be provided in Chapter 3. This report will primarily focus on the malware protection of HVDs, and more specifically on HVDs making use of VMware's corporate virtualization software vSphere combined with antivirus product Deep Security from Trend Micro which is aimed at virtualized environments.

The first part of this report will start with looking at the cloud, its possibilities and why virtualization is useful to build the cloud. Next, the focus will shift to a more specific usage of the cloud, namely HVDs. Software available to protect HVDs against malware is compared and DS is chosen to be further researched.

After looking at the cloud, how the cloud relates to HVDs and the possibilities of securing these HVDs, a performance test will be conducted with vSphere in combination with DS in the second part of this report. This performance test starts by carefully examining the hardware required and a methodology for testing. Based on this methodology the tests are conducted, results are aggregated and statistics are derived. Finally, results of the tests are listed and a conclusion regarding antivirus software in HVD Infrastructures is drawn.

1.1. Objectives

Many companies have heard about the cloud and the possibilities of migrating local desktops to the cloud (HVDs). One of the reasons that withholds them from migrating however, is the protection of their business data. As indicated in Chapter 1.4, various papers have already been written on how to protect private data in the cloud from falling into the wrong hands. Yet, less research has been done on how to protect virtual desktops in the cloud (HVDs) against malware. In addition, no research has been done yet regarding possible combinations between virtualization- and antivirus (AV) software to implement malware protection in an HVD environment and the security of these products.

The following topics will be dealt with in this report:

- Defining the different types of cloud computing and their relation with malware protection;

- Explaining the differences between the various types of desktop virtualization;
- Describing the range of virtualization products available including a comparison of centralized antivirus software available for these products;
- Providing insight in the vSphere product of VMware, in terms of use and relations among the various VMware products and vSphere components;
- Researching the robustness in security of Trend Micro's DS software for HVD environments which makes use of the VMware vShield security module.
- Differentiating the performance of three types of antivirus configurations using benchmarking. Tested configurations are: No antivirus and Trend Micro's DS and WFBS.

In the next paragraph, the scope of these topics will be further defined.

1.2. Structure and Scope

This report will start with explaining the concept of cloud computing and enumerate the different levels of cloud computing. To explain the different types of cloud computing, an enumeration of the types of cloud computing will be provided in Chapter 2. For each type of cloud computing a description will be given and examples of popular real-life services will be provided. Moreover, an example of a security capability which can be provided in addition to the service is explained. This is all explained at a high level and does not contain technical details.

Next, the different types HVDs will be discussed in Chapter 3 and a schematic overview of the various components in a HVD architecture will be illustrated. Following the research regarding the different virtualization architectures, vendors of virtualization software are listed and compared in Chapter 4.

Moving from virtualization software to malware protection, in Chapter 5 a short introduction to malware detection methods is provided, different architectures for centralized antivirus software are listed and finally the advantages and disadvantages of centralized antivirus software are enumerated.

Focusing more on protecting against malware in virtual environments in Chapter 6, this report provides a list of centralized antivirus products and compares them based on possibilities and integration with the virtualization solution. This information is gathered from each of the vendor's websites. During this research not all software has been tested to verify the vendor's claims as this would take too much time compared to the time available to write the thesis.

After providing general information about virtualization software and centralized antivirus software, the focus is shifted to the virtualization software of VMware in Chapter

7. This report provides a description of VMware's big and confusing product portfolio including an overview of the relations between the various products. This overview includes all of the corporate software related to VMware ESX. Virtualization software aimed for single user usage like VMware Player or Workstation is not included in this overview. Also any additional tools provided by VMware are not included.

In Chapter 8 the integration between DS and VMware vSphere is researched and demonstrated schematically. This is done by researching the binaries and drivers that are part of the software and by examining links between the various software components.

As no access to the security Application Programming Interface (API) of the VMware virtualization software was granted (see Appendix A), the possibilities and inner working of the API could only be determined by reverse engineering. Files that should be reverse engineered are the binaries that take care of the communication between the VM and the antivirus software outside of the virtual machine. Because reverse engineering is a totally different area inside the field of computer security compared to looking at antivirus software in virtualized environments, this research is limited to examining the relations between the various components on a higher level instead of defining the internal working of the API.

Using the insight gained in the architecture and workings of VMware vSphere and DS, the DS software is researched to see if there are any flaws in the functional security of the product. As the main purpose of the product is to provide protection against malware, this research is focused at the possibility disabling or removing the protection and the detection of the unprotected VM in the antivirus management interface.

After examining the inner workings and self-protection of VMware vSphere in combination with Trend Micro Deep Security (DS), Trend Micro's traditional antivirus product Worry-Free Business Security (WFBS) is benchmarked against DS in Chapter 9. This is done in order to determine what performance-wise the advantages and disadvantages are of using DS compared to WFBS. Because of the limited amount of hardware resources available, the test has been conducted representing an environment of about 10 workstations. Finally a conclusion will be drawn on the use of Trend Micro's centralized antivirus software compared to its traditional antivirus software.

This report will not consider the protection of the (thin) clients that connect to the HVD via some communication channel. One has to keep in mind however, that also the endpoints that are used to connect to an HVD, no matter how limited in functionality they are, might need some kind of protection to prevent malicious people from hijacking these devices and via these thin clients getting unauthorized access to the HVDs.

1.3. Approach

The research started with the broad topic of virtualization security. Over time this topic narrowed down to a specific research area which has been formulated into a clear set of

research questions and targets. For this report, mapping study approach[3] by Budgen et al. which is based on the Systematic Literature Review (SLR) method has been used to find and aggregate all relevant information to answer the research questions. In accordance to this method, first studies that are likely to be useful or related are collected. After additional examination the irrelevant studies are excluded. Finally, the relevant studies are investigated and assessed on quality and correctness and the information is used in the report.

To research the performance of centralized antivirus, benchmarks will be conducted to compare centralized virus protection supported by the virtualization software with traditional per-host antivirus software. This benchmark compares both solutions in matters of speed as well as usage of the various hardware components and virus detection rate. For both the centralized and traditional setup, antivirus products from Trend Micro will be used to limit the number variables involved in the test. More extensive information about the approach for the benchmark will be provided in Chapter 9.

1.4. Related Work

Various virtualization software comparisons have been performed to compare the most popular virtualization products for corporates available on the market. [[4],[5],[6]] These reports compare the harddisk and memory footprint of VMware ESX, Microsoft Hyper-V, Citrix XenServer and Red Hat Enterprise Virtualization (RHEV), benchmark the performance of each of the products and state the costs. However, no benchmarks have been conducted yet to compare the real-time protection of traditional antivirus software in a virtual environment with the centralized antivirus protection in a virtual enviroment.

In the area of malware protection in virtualized environments, research has been done by Chiueh et al. to inject kernel agents into the VM without the need of installing any piece of software into the VM.[7]

"AV-Test Independent IT-Security Institute" is an organization which on a regular basis tests antivirus products for the Windows operating system.[8] These tests compare the product's performance in realtime protection and while executing a full system scan. Moreover, the effectiveness in protecting against malware and removing malware of the antivirus products is compared. In addition to protecting against malware, antivirus software itself should be resistant against malware which tries to hide itself for the antivirus software or to remove the antivirus software. Anti-Malware Test Lab performed tests on the protection of antivirus software against malware that tries to manipulate, kill and remove the antivirus software.[9] In these tests Trend Micro's DS antivirus software has not been tested so in this report a self-protection test of this software will be performed.

2. The Cloud and Security

An increasing number of services is being moved to online infrastructures.[1] In the online infrastructure, three kinds of layers can be distinguished: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[1][10]. These layers are illustrated in Table 1 including examples of applications or components.

SaaS
E-mail, CRM, Games, Online Text Editor, $\cdots$
PaaS
Webserver, Database Host, Online Backup Service, $\cdots$
IaaS
Virtual Machine, Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), $\cdots$

Table 1: Cloud Computing Layers with applications and usage

Because services in the cloud are flexible and require high availability, a matching underlying platform is needed to provide in these needs. Running these services on bare hardware requires a great amount of hardware whereas in case of hardware failure, availability of the services is not guaranteed. However, when using virtualization, a dynamic platform is provided such that in case of a high load additional hardware can be added easily and removed whenever possible. Furthermore in case hardware fails, other hardware takes over its load and the defective hardware can easily be replaced without downtime of the system.

This chapter will explain the need for virtualization for these kind of cloud services, list the differences for each of the services and explain whether the delivered service includes security capabilities. Examples of various popular cloud services illustrate the importance of the cloud and the necessity of scalability and robustness to which users trust their private data.

2.1. Defining Virtualization

Before discussing the relation between the cloud and virtualization, first virtualization and related technology has to be explained. The following paragraphs will introduce virtualization and desktop virtualization and explain the distinction between the two.

[1] Sometimes also called IsaaS

Virtualization

Virtualization is used to host one or multiple virtual machines on one physical machine and share the hardware resources among the virtual machines. The division of these resources is managed by the hypervisor.[2]

The concept of virtualization can be viewed as adding an additional level of abstraction to an existing architecture. For example, ordinary applications within an operating system are also consolidated to an environment in a higher level of abstraction. In this environment it seems from the application's perspective it has access to to all memory space while in fact all physical resources are shared among the operating system and various processes running on the system. A second example of virtualization is Oracle's Java platform[3] which has been developed to provide a generic layer on top of any supported operating system or hardware platform to run applications. This enables applications developed in Java to run on any platform on which the Java Virtual Machine (JVM) runs. The last example of virtualization is user-space sandboxing applications that hook and emulate system calls to not limit the application, but in the meanwhile protect the underlying system. In this report however, virtualization only refers to the virtualization of complete operating systems on top of other operating systems or on bare hardware.

Desktop Virtualization

Desktop virtualization is the technology of separating the desktop environment and application software from the physical client device that is used to accessed it. This can be done by either connecting to a remote host, by using virtualization, or a combination of the two. This concept will be extensively explained in the next chapter.

2.2. Need for Virtualization

Because the number of active users on cloud services varies every minute, lots of capacity is needed to avoid any availability issues for the users. However, at off-peak moments, a great amount of unused capacity is available and resources are wasted. To solve this problem, virtualization is used to provide a dynamically scalable cloud, using different servers that can reside on different geographical locations, transparently delivering the amount of resources the clients request. These resources consist of computing power, memory and storage. All of these resources have to make sure that none of them cause data leaks, possibilities for unauthorized data modification or Denial of Services (DoSs). Depending on the service, antivirus software may or may not be included to protect the

[2] Although the term 'Hypervisor' and 'Virtual Machine Manager/Monitor (VMM)' are often used interchangeably, this document makes the distinction between Hypervisor which enables to run multiple guests concurrently on one host computer, and the VMM which allows a user to manage and monitor the virtual machines.

[3] http://www.oracle.com/java/

client against attacks by hackers and malware. This topic will be extensively discussed in the next chapter.

2.3. The Cloud

This paragraph will explain the different types of cloud services and includes examples of popular services and a discussion whether antivirus software is part of the service that is provided.

Cloud Architecture

The Cloud Security Alliance (CSA)[4] is a member-driven organization which promotes the use of best practices for providing security assurance within the area of cloud computing. CSA has compiled a security guidance for critical areas in cloud computing with the purpose to give insight in the different layers of the cloud architecture and the security challenges connected to each of the layers.[11] The model that is used by this guide to distinguish the various types of services is illustrated in Figure 1. In this figure the APIs layer provides virtualized hardware to the user whereas the "Integration & Middleware" layer is the operating system (OS). Finally, the Presentation layer delivers the data actually to the client. Each of these layers will be discussed more extensively in the following paragraphs.

IaaS, PaaS and SaaS

IaaS is the most basic layer provided by infrastructure providers and assigns resources to clients, usually by making use of virtualization. Examples of IaaS providers are Amazon Elastic Computing Cloud (EC2)[5] and GoGrid Private Cloud[6]. IaaS is only an abstraction layer of the hardware and provides processing resources which include CPU power, memory, storage space, connectivity and optionally a management API. Usually the user can choose which OS he or she wants to use after which the cloud provider will provide a bare installation of that OS on top of the IaaS infrastructure. The user then has to take care of the security of the system. In case workstations are moved to the cloud, the workstations are called HVDs. This phenomenon, which is also known as Desktop as a Service (DaaS)[7] or Virtual Desktop Infrastructure (VDI), will be explained more thoroughly in the next chapters.

The layer on top of IaaS is PaaS. PaaS does provide the software platform on which systems run while the underlying hardware resources are transparent to this platform. This includes integration with application development frameworks and middleware which

[4] https://cloudsecurityalliance.org/
[5] https://aws.amazon.com/ec2/
[6] http://www.gogrid.com/
[7] DaaS is sometimes also used to refer to Data as a Service, Datawarehousing as a Service or Datacenter as a Service but will in this report not be used as such.

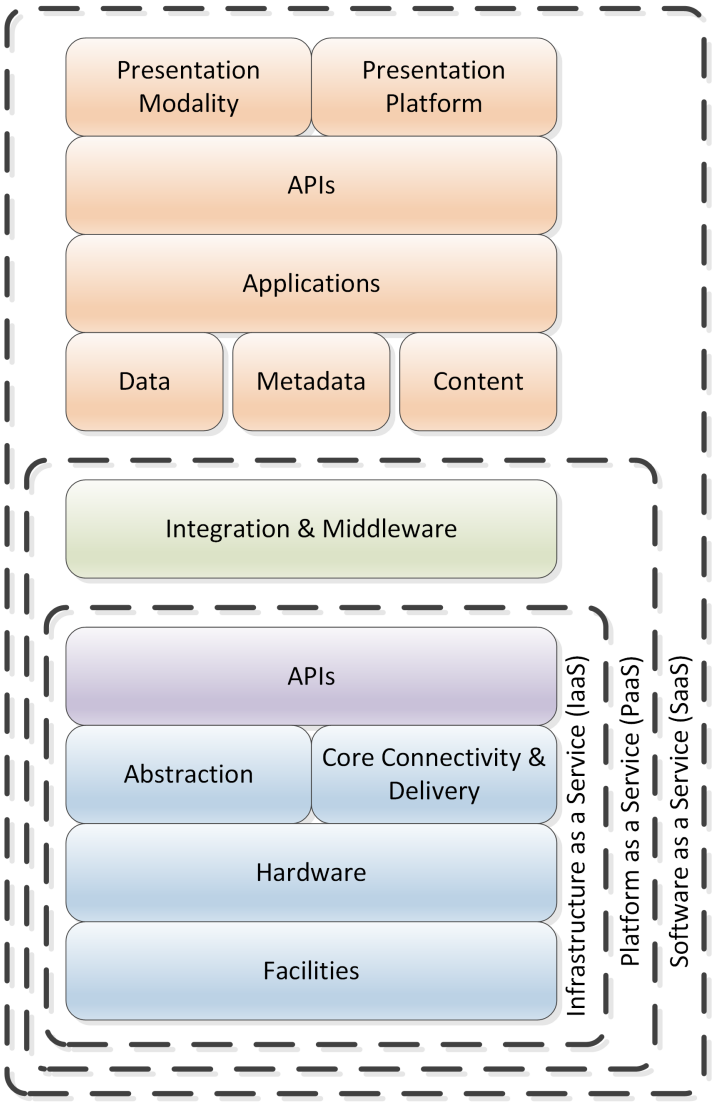


Figure 1: Cloud Architecture by The Cloud Security Alliance[11]

provides services to software applications beyond those available from the operating system. Examples of this type of service are Google App Engine[8] and Windows Azure[9]. On these services, webservers, database software and backup services can be run to have a fast platform for data storage and retrieval. For this type of service, hosting providers could provide security measures like antivirus software or malicious request filtering.

The highest level of cloud services is SaaS, also known as Software on Demand, which

[8]https://appengine.google.com/
[9]https://www.windowsazure.com/

is built on top of the underlying PaaS and IaaS layers. This level of service is used to deliver the fully abstracted service which includes user experience, content, presentation and management capabilities and can replace local software solutions. Examples are Google Docs[10] as alternative to the Microsoft Office Suite[11] and Windows Azure Online Backup[12] or iCloud[13] as alternative to the local backup. For this type of service, cloud providers can transparently provide additional security measures like antivirus software to make sure no harmful files are processed and stored by the service.

2.4. IaaS, PaaS and Centralized Antivirus Software

Depending on the infrastructure of the IaaS environment, customers will or will not be provided with the possibility to have centralized antivirus software. For example, imagine when the hosting company shares the underlying hardware to multiple customers who want to have freedom, flexibility and scalability. If that is the case, centralized antivirus software provided by the hosting company is limiting these customer's requirements and more freedom is provided when customers take care of the antivirus software on their systems themselves.

Another possibility are clients which do not want to have anything to do with the protection of their VMs. In that case providing protection against malware within the DaaS service can be delegated to the PaaS provider. The PaaS provider is then delivering the platform without the client having to worry about anything related to the OS making the OS a transparent platform.

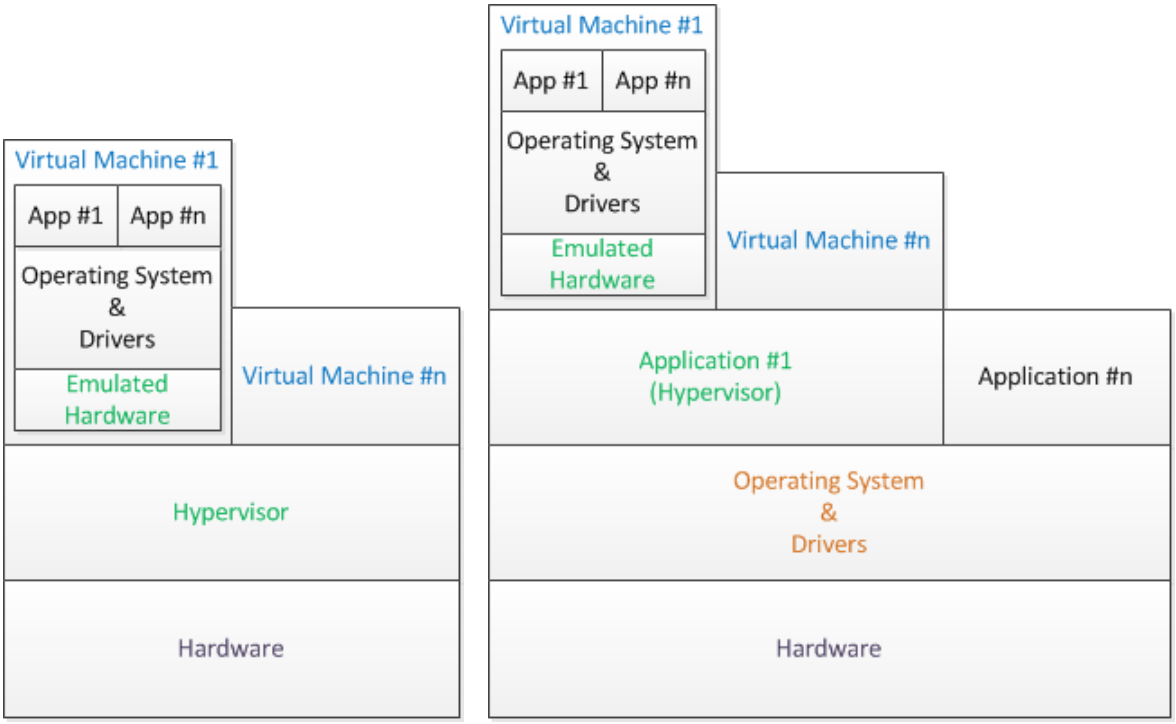
2.5. Conclusion

This chapter distinguished between the layers of cloud computing and its relation with virtualization and antivirus software. Next chapter will explore which possibilities are available to virtualize desktops and will then zoom into one specific type of virtual desktop.

[10] https://docs.google.com/
[11] https://office.microsoft.com/
[12] http://www.windowsazure.com/en-us/home/features/online-backup/
[13] https://www.icloud.com/

3. Desktop Virtualization

Desktop virtualization separates the desktop environment and associated applications from the physical client device that is used to access it. It is a way to delegate the execution of software to a confined environment. This environment can be a remote server but it is also possible to host this environment locally. Desktop virtualization should not be confused with traditional meaning of virtualization which differentiates between running the hypervisor on the bare hardware (classic virtualization) and running the hypervisor on top of another OS (hosted virtualization). Both possibilities are illustrated in Figure 2. This chapter will look into the various possibilities of desktop virtualization and describe the differences.



(a) Classic System VM

(b) Hosted VM

Figure 2: Virtualization Architectures

3.1. Types

Desktop virtualization can be distinguished in five types from which two are only client-side and three of them are server-hosted with a client component.[6] A schematic overview of all of the desktop virtualization types is shown in Figure 3. In this overview the hosted client-side virtualization and server-hosted HVD are both virtualized on the bare hardware (classic virtualization). The classic client-side virtualization is running on top of an OS (hosted virtualization) and the others are not virtualized in the architectural sense of the definition of virtualization. In the figure the types of desktop virtualization making use of classic virtualization are indicated with the green color. The one making use of hosted virtualization is indicated with the red color, while the other types of desktop virtualization not making use of the architectural sense of virtualization are indicated by the purple color.

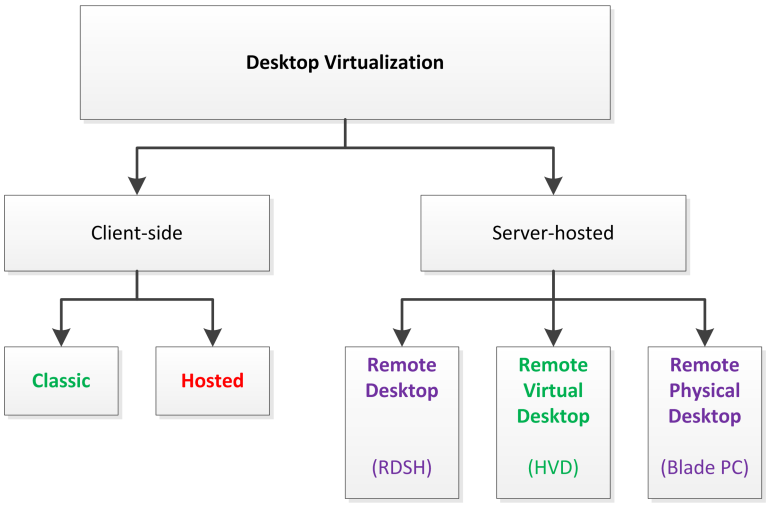


Figure 3: Types of Desktop Virtualization

The client-side possibilities of virtualization are either using classic or hosted virtualization. An advantage of using client-side virtualization over the traditional workstation configuration is that virtualized workstations are very portable an can easily be managed and replaced for example in case of a malware infection or software updates.

On the other hand there is the server-side desktop virtualization which requires the client only to have a thin-client to connect. This thin client presents the screen that is being sent from the server to the user while transferring user input from the keyboard and mouse to the server. Server-side desktop virtualization can be split up into 3 types. The first type is Remote Desktop Session Host (RDSH) which means that each user has its own desktop session but shares the computer platform with other users. An example of this type is the Terminal Server capability of Windows Server where many remote desktop sessions can be opened to the same host such that many users work simultaneously on the same server. The second type of server-hosted desktop virtualization is HVD and

provides a dedicated virtual desktop to every individual user. The difference between RDSH and HVD is that with a RDSH infrastructure all users use the same instance of the OS while with HVD every user connects to a dedicated VM instance at the HVD server infrastructure. For example, since Microsoft introduced Hyper-V in its Windows Server OS, it is possible to configure Windows Server as a HVD server. Compared to RDSH which allows multiple users to login and simultaneously work on one instance of the server OS, HVD at the moment a user connects boots up a new Hyper-V VM. This VM for example runs the Windows 7 Enterprise OS. After starting the VM, Hyper-V directs the control to the connecting user. This way the user does not interact with the host OS on the server but instead is routed through the HVD server to the confined VM. Finally, besides RDSH and HVD possibilities of the server-hosted category, there is the possibility to have a dedicated physical desktop which one can connect to and use.

3.2. Hosted Virtual Desktops

The popularity of HVDs is expected to grow drastically in the coming years. [[12],[13]] This paragraph will zoom in on the architecture of HVDs and look at the various components.

The HVD architecture consists of both a server and a client part. The server part is built on hardware such as CPU, memory and storage such as internal storage, Network Attached Storage (NAS) or Storage Area Network (SAN). As classic virtualization is much faster compared to hosted virtualization, classic virtualization is usually used to host HVDs. For authentication and assigning of a VM to a user, a so called broker component is present and is located between the client and the VM endpoint. As described in the previous chapters, HVDs can be distributed over several physical servers which are not bound to a geographical location.

3.3. Conclusion

In this chapter the five types of desktop virtualization have been explained and the HVD type of virtualization has been highlighted. From this point the focus will be shifted from the general cloud infrastructure to the IaaS type of service and more specifically HVDs. Using virtualization HVDs run multiple virtual machines on one or more physical servers, and users use (thin) clients to connect to and work on these machines.

The next chapter will look at the virtualization software available to build the cloud infrastructure. In the chapters following, the most popular virtualization software will be listed and antivirus software solutions developed for these platforms will be investigated.

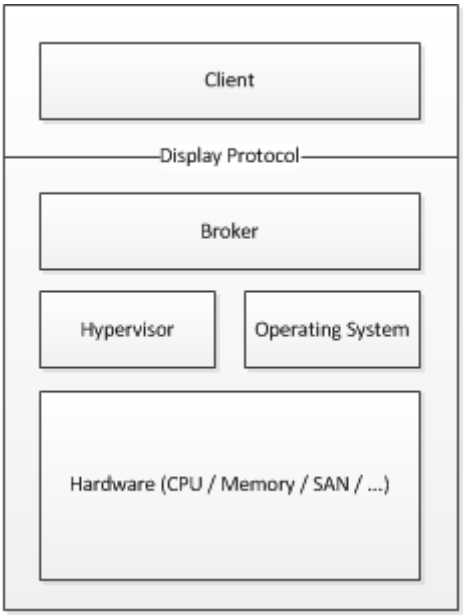


Figure 4: Architecture of Hosted Virtual Desktops [14]

4. Virtualization Products

Because nowadays virtualization is very popular, many vendors and open source projects have developed virtualization software. The software listed in this chapter has been compiled by searching virtualization software on the Internet and is targeted at classic and hosted client-side desktop virtualization and server-hosted HVD desktop virtualization as illustrated in Figure 3 of the previous chapter. After looking into the software available to virtualize, statistics about usage of virtualization software in corporates will be used to determine the market leaders in the area of corporate virtualization software.

4.1. Virtualization Software per Vendor

The following list groups the virtualization products per vendor and contains only the software that has been updated after January 2011. For every software package it is stated which kind of Desktop Virtualization (DV) it is targeted at and whether it is a classic system VM (*C*) which runs on the bare hardware or if it is a hosted VM (*H*) which runs on top of another operating system, as indicated by respectively the green and red color in Figure 3 in the previous chapter.

Product Name	Website	Aimed for	Type
Citrix			
XenClient	https://www.citrix.com/xenclient/	Classic client-side DV	*C*
XenServer	https://www.citrix.com/xenserver/	HVDs	*C*
Microsoft			
Hyper-V Server Virtualization	https://www.microsoft.com/hyper-v/	HVDs	*C*
Windows 8 Client Hyper-V	http://windows.microsoft.com/windows-8/	Classic client-side DV	*C*
Virtual PC	https://www.microsoft.com/virtual-pc/	Hosted client-side DV	*H*
Oracle			
VM Server	https://www.oracle.com/oraclevm/	HVDs	*C*
VM VirtualBox	https://www.virtualbox.org/	Hosted client-side DV	*H*
Parallels			
Cloud Server	http://www.parallels.com/products/pcs/	HVDs	*C*
Desktop	http://www.parallels.com/products/desktop/	Hosted client-side DV	*H*[14]

[14] For Mac

Server Bare Metal	http://www.parallels.com/products/server/baremetal/	HVDs	*C*
Server for Mac	http://www.parallels.com/products/server/mac/	HVDs	*C*
Workstation	http://www.parallels.com/products/workstation/	Hosted client-side DV	*H*[15]
VMware			
ESX Server	https://www.vmware.com/esx/	HVDs	*C*
Fusion	https://www.vmware.com/fusion/	Hosted client-side DV	*H*
Workstation	https://www.vmware.com/workstation/	Hosted client-side DV	*H*
Miscellaneous			
Bochs	http://bochs.sourceforge.net/	Hosted client-side DV	*H*
KVM	http://www.linux-kvm.org/	Hosted client-side DV	*H*
Linux Virtual Server	http://www.linuxvirtualserver.org/	HVDs	*C*
Linux-VServer	http://www.linux-vserver.org/	Hosted client-side DV	*H*
NOVA Hypervisor	http://hypervisor.org/	HVDs	*C*
QEMU	http://qemu.org/	Hosted client-side DV	*H*
Qubes OS	http://qubes-os.org/	Hosted client-side DV	*H*[16]
VMLite Workstation	http://www.vmlite.com/	Hosted client-side DV	*H*
Xen	http://www.xen.org/	HVDs	*C*

Table 2: Virtualization Software

Although there are many virtualization products, only a few of them have a big market share in business environments. The following paragraph will use the statistics available regarding the use of virtualization software in corporates to determine nowadays biggest players in this market.

[15] For PC
[16] VM launched for every application

4.2. Market Leaders in Corporate Virtualization

Classic system VM virtualization runs directly on the hardware and hence is the most efficient way of virtualizing. Therefore it is the most popular type of virtualization used in corporates. From the various products that use the classic system VM type of virtualization, Technology Researching company Gartner compiled a list of the most prominent corporates in this area.[15] "Magic Quadrant for x86 Server Virtualization Infrastructure" by Bittman et al. illustrated in Figure 5 shows that the leaders of the current virtualization market are VMware with its vSphere product range, Microsoft with its Hyper-V product and as small player Citrix with its Xen product.

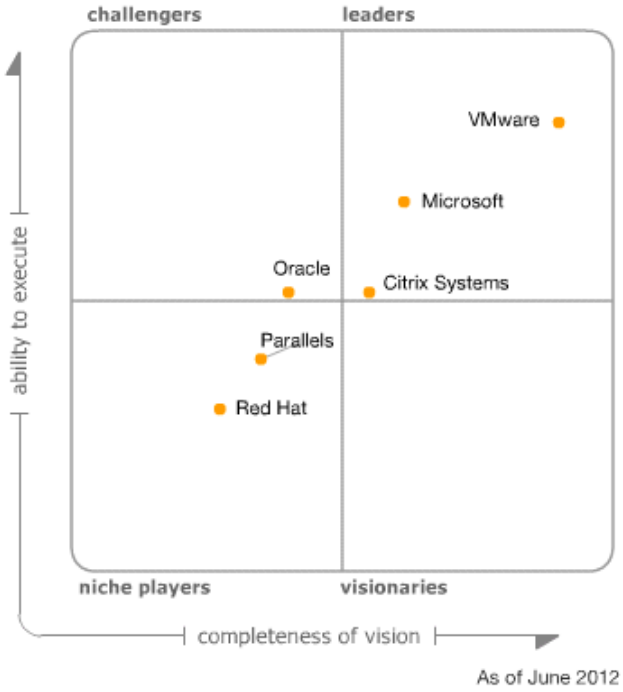


Figure 5: Magic Quadrant for x86 Server Virtualization Infrastructure [15]

VMware has been the main manufacturer of corporate virtualization software for years. Starting mid 2006 however, Microsoft started shipping its virtualization solution called Hyper-V with Windows Server 2008. Since then it has been getting increasingly popular and is, although VMware is still the main vendor of corporate virtualization software, now getting a real competitor of VMware.

Although Citrix is a small player when looking at the full market of virtualization software, Ctrix is still the biggest party in the world of HVDs. Moreover, popular cloud

services like Amazon EC2 and Rackspace still make use of Citrix's Xen product. [[16], [17]] As illustrated in Figure 6, Citrix is followed at a relatively big distance by VMware and Microsoft. However by improving their software and adding new features all the time, VMware and Microsoft are slowly getting more hold on the area of HVDs which is shown in Figure 7.

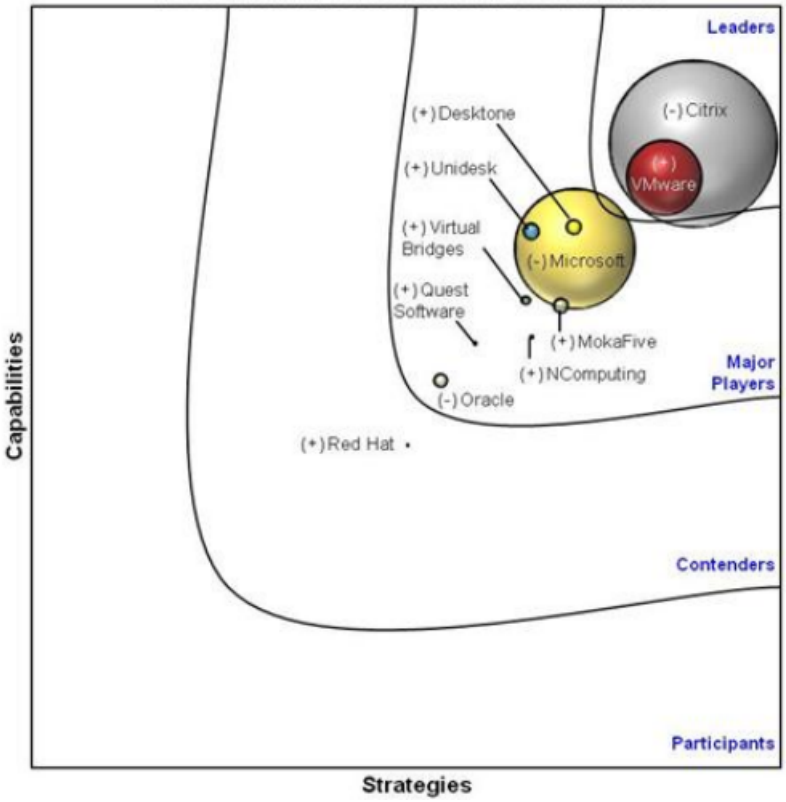
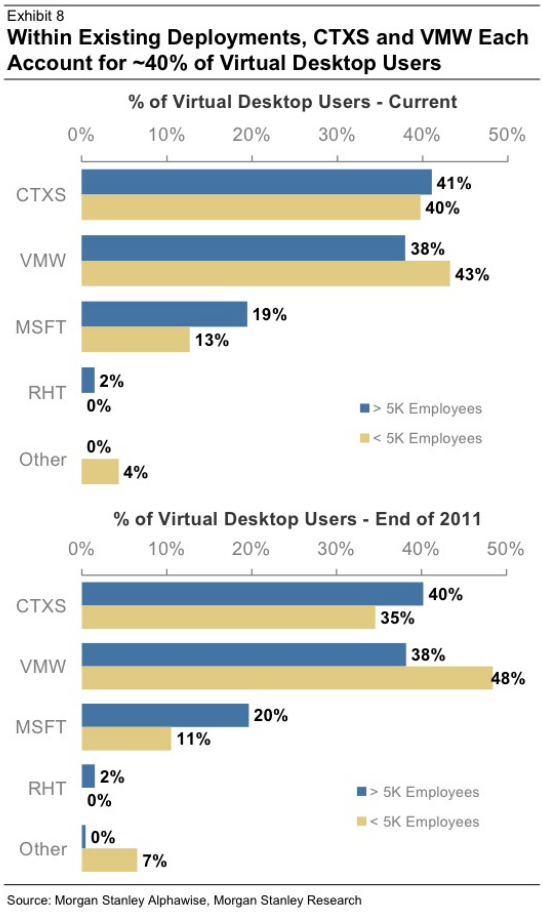


Figure 6: IDC MarketScape 2012: Worldwide Client Virtualization Vendor Assessment [18]



Citrix Systems (CTXS)
VMware (VMW)
Microsoft (MSFT)
Red Hat (RHT)

Figure 7: Comparison of percentage of Virtual Desktop Users in 2011 [19]

4.3. Conclusion

Although a lot of virtualization solutions are available, only VMware and Microsoft have a serious share in the corporate virtualization market with Citrix following at a distance. However, when specifically looking at the HVD environments, Citrix still is the main supplier of software with VMware following at a short distance. The tricky thing with comparing these vendors is to overlook this crucial difference: important vendors for virtualization software in general can differ from vendors that specifically aim their products at market of HVDs.

With every update of the virtualization software, new features and improvements are added to rival with the competitors and get a bigger share in the market. This might gradually lead to the situation in which the market adopts VMware or Microsoft products for their HVD environment and by doing that abandon and decrease the market share of Citrix in HVDs.

The next chapter will look at how antivirus software works and, the ways antivirus software can be centralized and the advantages and disadvantages of using centralized antivirus software.

5. Centralizing Antivirus Software

For HVD environments, centralized antivirus software can be implemented in different ways. Before going into the implementations of antivirus software in a virtualized environment, the various ways of detecting malware will be explained to get some additional insight into malware and how antivirus software works. Finally the capabilities that can be delegated from the clients to the centralized antivirus software are discussed.

5.1. Antivirus Detection Methods

Many new pieces of malware are detected every day and there is a continuous battle between the malware writers applying various techniques to avoid detection and the antivirus companies trying to detect these tricks while preserving a low rate of false positives. Generally antivirus software is plugged into the disk access mechanism of the OS and triggers the scan each time a file is written or accessed. This paragraph distinguishes the different types of malware and then looks into the methods of detecting them.

Malware Types

Malware can be distinguished in various different types which are listed below.[20]

- **Logic Bomb**: Uses a trigger to execute a certain payload. The condition of the trigger is only limited by the malware writers' imagination.
- **Backdoor**: Allows an attacker to bypass a security check or grants access to certain resources that were otherwise unreachable, such as a commandline shell.
- **Virus**: Malware that, when executed, tries to replicate itself.
- **Worm**: Similar to a virus but is standalone and spread from machine to machine across networks.
- **Rabbit**: Similar to a worm, but deletes the original copy of itself after replication.
- **Spyware**: Collects information from a computer and transmits it to someone else. Information can be usernames and passwords, e-mail addresses or creditcard numbers.
- **Adware**: Similar to spyware but more focused on the user and their habits.

A piece of malware can also be a combination of above types of malware. For example malware that is used to create a botnet of zombies includes both the worm and backdoor features in order to both replicate itself over the network and in the meanwhile provide access to the infected host to the administrator of the botnet.

Detection Types

Antivirus software uses various methods to identify and remove malware. These methods can be distinguished into the first-generation simple scanning methods and the second-generation scanning methods which are more advanced.[21] These methods are used on executable files, but also on scripts downloaded from websites and macro viruses.

The simplest approach of detecting malware is string scanning. These methods simply looks for a sequence of bytes that is inside the malware but will likely not appear in legitimate files. In addition to just looking for an exact sequence of bytes, wildcards can be used to skip bytes or byte ranges and allow more variations in defining potentially malicious sequences. Another way of checking whether a certain file is malicious is by counting the number of mismatches of a certain sequence when comparing it with the malware signature in the antivirus signature database. The lower the number of mismatches, the more likely the scanned file is malware.

The second generation of scanning methods try to refine the detection of malware. Because an increasing number of malware was mutated by inserting junk instructions in order to prevent detection, smart scanning was introduced which skips these parts of the malware and does not store it in the malware signature either. In addition to removing the junk instructions, also the nonessential statements can be dropped. This results in the skeleton of the code which enhances detection of files belonging to the same family of malware. This method is most useful for macro viruses, which are viruses embedded in for example a Word document. Instead of matching only one sequence of the file to a signature, also two or more sequences throughout the file can be checked. This can be done by only checking the constant bits of the virus body and matching these against the sequences in the malware signature. Nowadays scanners also use code emulation in addition to these mentioned 'offline' detection methods.

With this knowledge, the next paragraphs will look into the advantages and disadvantages of centralized antivirus architectures.

5.2. Types of Architectures

The classic way of protecting virtual machines is installing an antivirus solution on each of the VMs, just as if they are physical machines. This implementation uses more memory than when similar resources are in memory only once, assuming that the hypervisor naively assigns memory to the VMs. The implementation is illustrated in Figure 8(a) .

The first possibility to unburden the VMs is to install an agent in every VM which outsources tasks to the software that is configured for centralized malware protection. A schematic overview of this implementation is shown in Figure 8(b) .

The easiest solution from a management perspective is to have a single VM which takes care of protecting the other VMs without having to install agent software. An schematic

overview of this possibility is shown in Figure 8(c).Chiueh et al. have achieved this by injecting antivirus software into the VMs.[7] Later in this document a commercial product will be examined which also provides this feature.

In the latter two architectures, there are multiple steps involved in delegating the scanning to centralized antivirus software. These steps will be discussed more extensively in Chapter 8.5.

5.3. Centralized Antivirus Software

This paragraph will list the pros and cons of using a antivirus solution in a centralized setting using a hypervisor and verify the possible advantages of virtualizing the antivirus software could have over running dedicated antivirus software in every individual VM.[22]

Manageability

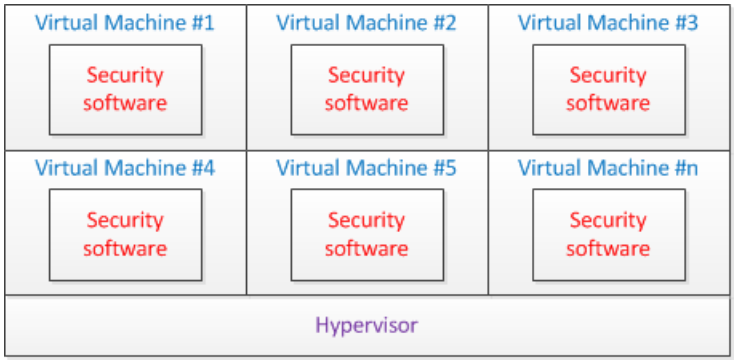
First of all the manageability of the antivirus software in the various VMs greatly increases. To see the status of the antivirus software, system administrators only have to login into the management console to get an overview of all detection statistics and anomalies. In case an antivirus instance seems to have problems, the system administrator can pinpoint the machine and either use the management software or a remote desktop connection to fix the software. Furthermore, VMs can be automatically isolated from the network in case the antivirus or firewall software stops working or if the system is infected with malware. This severely reduces the risk for other systems to get infected.

Resources

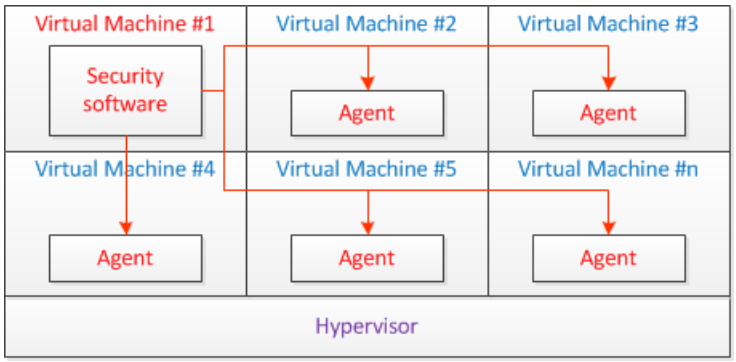
Another advantage of using centralized antivirus software is the reduced use of resources which can be split up into various types of resources.

A decreased usage of Internet traffic is the advantage in the scope of networking resources. Instead of having every computer download its own antivirus software updates like antivirus or firewall signatures and program updates, the manager software takes care of updating both the software itself as well as the signatures included in the software. Furthermore, VMs do not need Internet access to download updates which improves the security of the computer. Also when due to a policy computers are not allowed to be connected to the Internet, they can still be provided with up-to-date antivirus software using the centralized antivirus management software.

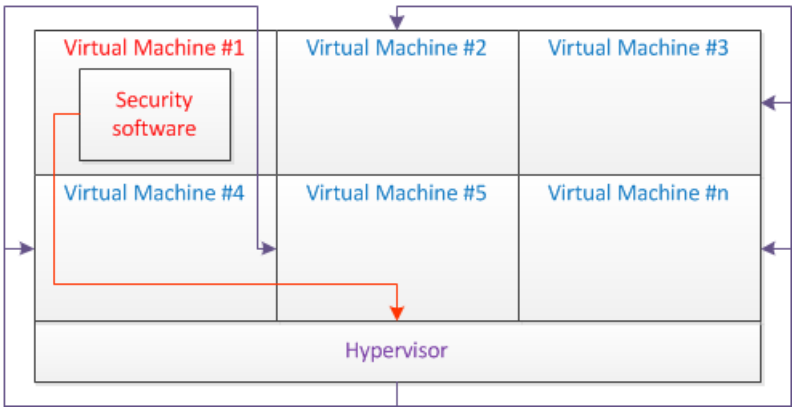
Furthermore, depending on the architecture of the software, the antivirus software has to exist only once in the system's memory. This avoids duplicated memory with the scan engine and signatures in each of the running VMs.



(a) Antivirus Software per Individual VM



(b) Centralized Antivirus Software with in-guest Agents



(c) Agentless Centralized Antivirus Software

Figure 8: Types of Antivirus Software Architectures in Virtualized Environments

Scanning

In case of antivirus software, the engine is also able to scan virtual harddisks (VHDs) offline. This is useful to remove malware which hide and protect themselves when the

virtual machine is running. Furthermore, when virtual machines are turned off while running the periodical full system scan, these machines will not be excluded from the scan. Furthermore, centralized antivirus software can avoid so-called antivirus storms.[23] An antivirus storm is the phenomenon that a large number of VMs execute a virus scan at the same time. This uses much more resources from the hardware compared to normal usage of the VMs and can slow down the performance dramatically. Centralized antivirus software can regulate the scans based on the load of the hardware.

Security

Because monitoring is done outside the system, it can quickly be detected when malware nested itself into the system or in case the malware has managed to disable the antivirus software. In contrast to traditional antivirus software that only runs and reports locally, this is a big improvement to the security of the system as not only the system protects itself, but also a 3rd party system is involved in protecting the system's security.

Partnered with this advantage is also a big disadvantage. In case an attacker manages to exploit the central monitoring software, he or she has access to the antivirus software of all VMs connected. Using these privileges the monitoring might be disabled and even removed from the system or even worse, depending on the architecture of the antivirus software, the attacker can get access to the harddisk and memory of every system. Therefore centralized antivirus also leads to a Single Point of Failure (SPOF).

Complexity

By introducing centralization in antivirus software via the hypervisor, also a bigger complexity of the environment is introduced. Whereas the hypervisor was previously only responsible for adding an abstraction layer to the hardware, now also features to access and have control over the VM are added to the virtualization software. Furthermore, more software is added and therefore the people that manage the environment need more knowledge to also configure and monitor the additional software that has been added by centralizing the malware protection.

5.4. Conclusion

In this chapter the methods of detecting malware by antivirus software have been explained to be able to see how antivirus software can be centralized. Next a distinction has been made between the different types of implementing antivirus software in a virtual intfrastructure and finally the advantages and disadvantage of the centralized antivirus solution are listed. This showed that although there are many advantages in centralizing the antivirus software, it comes also with some disadvantages which have to be seriously considered prior to implementation in the environment.

The next chapter look into the antivirus software available for VMware vSphere, Microsoft Hyper-V and Citrix XenServer and compare the capabilities of each of the virtualization platforms.

6. Antivirus Software for Virtualized Environments

Many types of antivirus software packages that are usually installed within the virtual machine could be migrated to the hypervisor. The coming paragraph enumerates the different types security capabilities together with the threats they protect against. This list of capabilities is compiled based on the capabilities the vendor says their product offers, merging similar and overlapping capabilities among the various vendors. The capabilities in this list are used in Table 3 to compare the capabilities of available centralized antivirus software. This table contains both agentless antivirus software[17] as well as only centralized antivirus software. The difference between the two is that agentless software is supported by the hypervisor which provides access to the resources inside the VM while the other type makes use of an agent in order to communicate and get access to the resources in the VM.

6.1. Compared Security Capabilities

Antivirus

Antivirus software is used to prevent malware infections. Malware can get onto the system via for example file sharing, e-mail, websites or peer-to-peer networks. Methods antivirus applications use to detect malware are scanning of files written to the disk, monitoring the activity of applications to discover malicious activity, and periodically run a system scan to detect malware using the most recent malware signatures. When a piece of malware is found, the antivirus software tries to unload the malware from memory and remove its executable payload from disk. A specific type of malware is a rootkit. Rootkits are stealthy malware that have full control over the system, including the software that can be used to protect the rootkit. In this document, rootkits are also considered as a type of malware.

Firewall

A firewall is used to regulate incoming traffic from the network and outgoing traffic to the network. Using rules, applications and ports by default are blocked from making connections. If a firewall is configured to allow certain traffic, the traffic can flow to the designated hosts and IP ranges.

Integrity Monitor

An integrity monitor blocks unauthorized applications and changes on a system. Policies can be set to provide which changes to the system are allowed and which are explicitly not.

[17] Also known as in-hypervisor antivirus software

Log Inspection

Collects log files and correlates events to determine their importance. Suspicious events can be highlighted by for example notifying the system administrator.

IDS and IPS

IDS and IPS systems make it possible to monitor the network for attacker payloads and other malicious activity. The difference between an IDS and IPS is that an IDS only inspects network traffic and alerts when something malicious is found while an IPS additionally also prevents the traffic from going through. The mechanism of detection and prevention of malicious web application traffic is also called Web Filtering by some antivirus software vendors.

6.2. Available Agentless Antivirus Software

Based on the security capabilities distinguished in the previous paragraph, this table has been compiled and compares antivirus software available on the market which is aimed at virtualized environments. The software is compared in possibilities as well as in supported virtualization platforms. Moreover, the table marks software which does not need the installation of an agent in the virtualized OS.

	Antivirus	**Firewall**	**IDS/IPS**	**Integrity Monitor**	**Log Inspection**
5nine Security Manager for Hyper-V Data Center	m	m			
Bitdefender Security for Virtualized Environments	c, m, v[1]				
Checkpoint Security Gateway Virtual Edition	v	v	v		
IBM Security Virtual Server Protection	v[2]	v			
Juniper Virtual Gateway (vGW) Series	v	v	v		
Kaspersky Security for Virtualization	v[1]				
McAfee MOVE AntiVirus	c, m, v[1]				
Reflex Systems vTrust	v	v			
Trend Micro Deep Security (DS) [24]	c, m, v[1]	c, m, v[1]	c, m, v[1]	c, m, v[1]	c, m, v

Table 3: Hypervisor-supported Antivirus Software with Supported Virtualization Platforms

Symbols

Symbol	**Meaning**
c	Citrix XenServer
m	Microsoft Hyper-V
v	VMware vSphere

[1] This is an agentless solution.
[2] Protection specifically against rootkits.

6.3. Conclusion

Various vendors are providing antivirus software for virtualized environments that are cooperating with the hypervisor to accomplish the best performance. Many of the provided solutions are still relying on agents within the virtual machines to protect the system. However since VMware introduced its security API in 2009, an increasing number of antivirus software vendors are developing agentless solutions that make use of the API provided by VMware.

Table 3 shows that DS is the most extensive agentless antivirus software currently available and implements most of the security capabilities that will be enumerated in Chapter 8.5. Trend Micro was the first one with its DS product to make use of this API [25] and kept their products updated as the VMware API featureset extended. After Trend Micro using this API, other antivirus software vendors followed.

Because VMware is currently the main vendor of virtualization software and because VMware is the first and so far the only virtualization software company which provides an API to protect VMs without the need of agents, from now on the focus will be on VMware. In the next chapter, VMware's portfolio of cloud-related products will be reviewed and relations between the products will be revealed. Furthermore, the capabilities of the products will be enumerated to provide a better insight in its capabilities.

7. VMware Virtualization

VMware is an American company that provides cloud and virtualization software and services. As shown in Chapter 4.2, VMware currently is the market leader in corporate virtualization software and has over 13.000 employees.[26] VMware has a broad range of products including several of them related to the cloud and HVDs.

7.1. Product Hierarchy

For Server Hosted desktop virtualization making use of classic system virtualization, VMware provides the ESX and ESX Integrated (ESXi) hypervisors, also known as vSphere hypervisor. At the moment VMware is phasing out the ESX hypervisor and replacing it by the ESXi hypervisor which has a smaller footprint as management capabilities are moved to the vSphere Suite. The vSphere Client can be installed on any system connected to the ESXi server. Using the vSphere Client, capabilities additional to the free bare vSphere hypervisor can be activated at the vSphere host depending on which one of the three editions (Standard, Enterprise, Enterprise Plus) is licensed.[27] Capabilities of VMware vSphere can be distinguished into 6 categories that will be enumerated in the next paragraph.

A vSphere hypervisor can also be managed by the vCenter software. VMware vCenter provides capabilities for load-balancing, hardware monitoring and central management of multiple servers running the vSphere hypervisor. The vCenter Server Appliance can be downloaded to manage the vCenter Server and indirectly all underlying vSphere hosts.[28]

In addition to VMware vCenter, VMware vCloud is used to deliver IaaS, guaranteeing uptime by providing real-time migration of the infrastructure to other vCenter environments in case of a failure of one environment. To extend vCloud, vCloud Director delivers tools to easily build and manage an infrastructure of vCloud configurations. Preconfigured virtual machines can be placed into the infrastructure and network connections between the virtual machines can be set up. An overview of the relations between all cloud-related VMware products is illustrated in Figure 9. In this figure, the solid lines mean that the software is steadily connected while the dotted line indicates that the vSphere Client is not required to be connected all the time in order to have a well-functioning virtualization infrastructure.

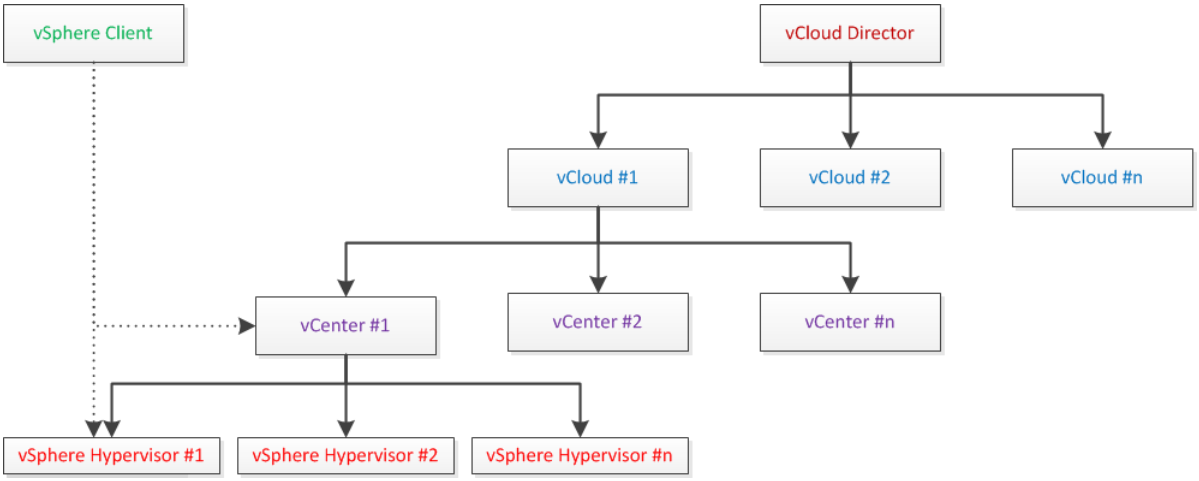


Figure 9: Relations among VMware products

7.2. vSphere

VMware vSphere is the main component in VMware's virtualization architecture. The capabilities of vSphere can be distinguished into six categories which collectively provide the dynamic cloud feature set.[29]

The first category is aimed at *computation* and includes the vSphere ESXi Hypervisor which abstracts the hardware resources and allow their sharing by multiple VMs. It also provides possibilities of balancing the VMs across multiple physical hosts and migrating them in case hardware maintenance of a server is planned.

The next category of capabilities deal with the *storage* of data. Mechanisms are provided that place VMs based on I/O latency and storage capacity. Storage is automatically moved non-disruptively to eliminate I/O bottlenecks and can be prioritized based importance of availability. Using vSphere Virtual Machine File System (VMFS) a high performance cluster file system can be set up to provide fast and concurrent access to storage by the virtualized servers.

Networking services are the third category of capabilities of vSphere. These capabilities deal with isolating traffic, sharing network capacity, enforcing bandwidth limits and load balancing. Furthermore, the network runtime state of VMs is maintained as they move across multiple hosts using the computation and storage capabilities. This enables in-line monitoring and centralized firewall services.

Another category assures *availability* of the system which implies minimizing downtime by monitoring operating system and hardware failures, automatically restarting VMs on other physical servers in the resource pool when server failure is detected and restarting VMs when an operating system failure is detected.

Automation is a category which aims for easy deployment and administration of vSphere hosts. This includes command line tools that can be used in automated scripts which can automatically install and configure new hosts or roll out patches.

Finally, the vShield *security* capabilities provide various capabilities that relate to scanning and blocking network traffic offloading antivirus and anti-malware agent processing to a dedicated Virtual Appliance (VA). The next chapter will extensively go into this category of capabilities.

7.3. Conclusion

VMware has a big range of products, with many different capabilities. These products are frequently also related to each other, either as a required component or as an extension. The capabilities that are included all have unique names that are used to refer to technology used. To make it even more complex, options have been added, removed and merged over time and new names are given to these aggregated capabilities.

The main part of VMware vSphere is the ESXi hypervisor which takes care of the actual virtualization. In addition to ESXi there are various modules that take care of storage, networking, availability, deployment, administration and security. The security module of the VMware vSphere software will be covered in detail in the next chapter.

8. Agentless Protection

As the products and services of VMware are now clear, this chapter will zoom into the options regarding protection of the VMs running in a virtual environment. VMware's VMsafe product which is the module that makes agentless antivirus possible is the base of this chapter. This module has already been renamed several times which will be explained in the first paragraph. The paragraphs following will go into the communication between VMware and the modules of Trend Micro within the VM.

8.1. VMware Security Capabilities

Since the first quarter of 2008 VMware provides the possibility to offload antivirus software to the hypervisor without the need of agents inside the VM using its VMware VMsafe software.[30] In the next release of VMware vSphere, the capabilities of VMsafe were migrated to the VMware vShield Endpoint Security (EPSEC) Suite [31] and additional capabilities were added. At that moment, VMware vShield consisted of the following components:

- **vShield Edge:** Provides security at the perimeter of the virtual network [32];
- **vShield App:** Application-aware firewall [33];
- **vShield App with Data Security:** Application-aware firewall with feature which using Deep Packet Inspection (DPI) can monitor sensitive data being transferred over the virtual network [34];
- **vShield Endpoint:** Provides the possibility to offload antivirus software to a dedicated VA delivered by a VMware partner [35];
- **vShield Edge for vCloud Director:** Virtualization-aware security for VMware vCloud IaaS software [36].

Since VMware vShield 5.1, the functionality has been divided over VMware vSphere and the additional module called VMware vCloud Network and Security (vNaS). The following changes have been carried out [37]:

- vShield Edge and vShield App with Data Security have been merged into VMware vCloud Networking and Security Advanced;
- vShield App has been renamed to VMware vCloud Networking and Security Standard;
- vShield Endpoint is now included in vSphere 5.1, except for the Essentials Edition of vSphere;
- vShield Edge for vCloud Director is left unchanged.

A schematically illustrated summary of the changes made to the product structure over time is shown in Figure 10.

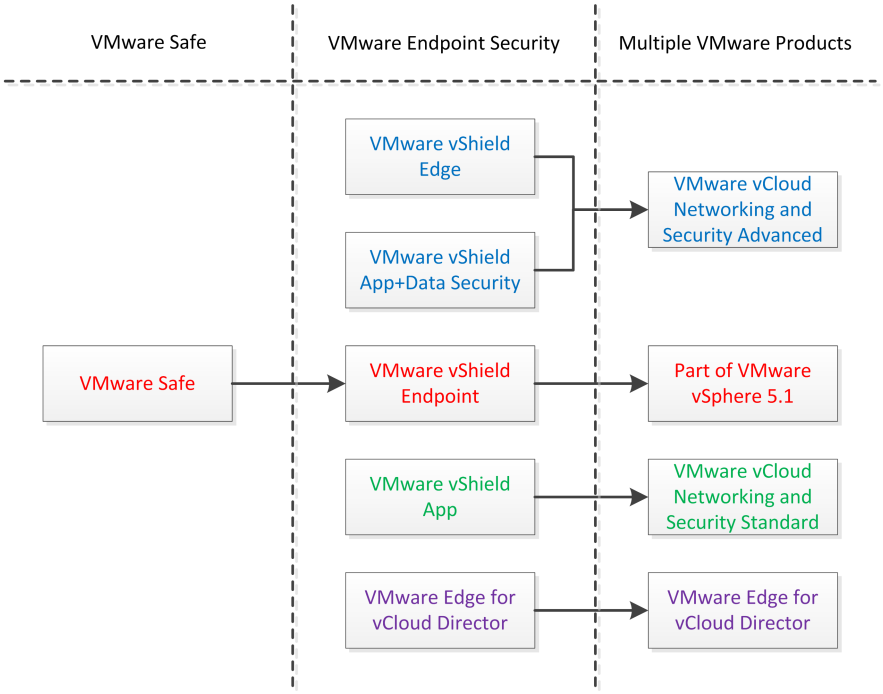


Figure 10: Changes of the VMware product structure over time

Two editions of the vNaS Suite are available: a Standard and Advanced edition whose feature comparison is listed in Table 4.[38]

The Standard edition consists of multiple components targeted at different areas in the field of security.[39] vNaS includes a hypervisor-based Firewall which protects applications in the virtual datacenter from network-based attacks. DHCP, NAT, VPN and VXLAN take care of interdomain connectivity and secure communication channels.[40] In addition to the these connectivity capabilities, the vCloud Ecosystem Framework provides service insertion at the Virtual Network Interface Controller (VNIC) and the edge of the virtual network. In all cases even when moving virtual machines among different ESX hosts in a cluster, the policies and protection will still hold. Compared to the Standard Edition of the vNaS Suite, the Advanced Edition adds support for HA which minimizes downtime by monitoring virtual machines to detect OS and hardware failures and takes action in case a failure occurs.[41]

	Standard	Advanced
Firewall	•	•
Virtual Private Network (VPN)	•	•
Virtual Extensible LAN (VXLAN)	•	•
vCloud Ecosystem Framework	•	•
Network Address Translation (NAT)	•	•
Dynamic Host Configuration Protocol (DHCP)	•	•
High Availability (HA)		•
Load Balancing		•
Data Security		•
Endpoint	(Bundeled in vSphere)	

Table 4: Feature Comparison between vNaS Standard and Advanced Edition [38]

The following paragraphs will first provide an overview of the general architecture of VMware vShield Endpoint. Next, the architecture of Trend Micro's agentless antivirus solution called DS will be explained and the integration of DS in EPSEC will be discussed.

8.2. vShield Endpoint

VMware vShield Endpoint, the module in VMware vSphere which provides the possibilities for agentless protection, consists of two parts. The first part are the Virtual Machine Communication Interface (VMCI) and vShield kernel modules in the hypervisor which allow direct communication from the hypervisor with the VMs. The second part are the drivers within the VM which communicate via the virtualized hardware to the kernel modules.

VMware developed VMCI to facilitate fast and efficient communication between guest VMs and their host. The API of VMCI is similar to that of the Berkeley UNIX and Windows socket interface. The VMCI socket library supports both connection-oriented stream sockets and connectionless datagram sockets like respectively Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and can also be used for Inter-Process Communication (IPC), transferring data among processes on the same system. VMCI, in contrast to TCP/UDP, can however only have two endpoints.[42]

Complementary to the modules in the hypervisor are the VMCI and vShield drivers in the VMs which allow the virtual machine to efficiently and directly communicate with the hypervisor. As will be illustrated in Figure 11, the VMware vShield Endpoint Thin Agent which is required for agentless antivirus is also dependent on this library. Because drivers reside deep inside the OS, they provide an interface for the hypervisor to intercept system calls and execute certain actions before continuing to execute the original

system call. For example in case a system call is made to read a file from disk, the vShield driver can intercept this call, scan the file first by providing access to the VM via VMCI and then allow the system call to continue execution. A visualization of this example will be illustrated later in this chapter in Figure 13.

The tables in this and the following paragraph list the drivers, services that are added to Windows after installing the DS Agent. This information has been gathered using the Monitoring Tool of the Microsoft Certification Toolkit [43], the Windows Device Manager (`devmgmt.msc`), Sysinternals Autoruns [44], and the `HKLM\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder` registry key [[45],[46]]. As OS, the 64bit version of Windows 7 and 8 is used as an increasing number of users are moving to Windows 7 and 8 and specifically to the x64 architecture of Windows because of the memory limitations that exist in the 32bit (x86) version.[18]

In Table 5, drivers installed by the VMware Tools wizard are listed. These drivers greatly improve the performance of the VM by slightly modifying the guest, while not altering the OS kernel.[47] In paragraph 8.4 the drivers used by VMware vShield will be explained more extensively.

Driver Description	**Filename**
VMware SVGA 3D	`%SystemRoot%\System32\Drivers\vm3dmp.sys`
VMware PCI Virtual Machine Communication Interface Bus Device	`%SystemRoot%\System32\Drivers\vmci.sys`
VMware Host-Guest File System Driver	`%SystemRoot%\System32\Drivers\vmhgfs.sys`
VMware Server Memory Controller	`%CommonProgramFiles%\VMware\Drivers\memctl\vmmemctl.sys`
VMware Pointing PS/2 Device Driver	`%SystemRoot%\System32\Drivers\vmmouse.sys`
VMware Raw Disk Helper Driver	`%ProgramFiles%\Vmware\VMware Tools\vmrawdsk.sys`
VMware vShield Endpoint Thin Agent	`%SystemRoot%\System32\Drivers\vsepflt.sys`
VMware vSockets Service	`%SystemRoot%\System32\Drivers\vsock.sys`

Table 5: VMware Driver Files in Windows 7 x64

[18] Statcounter Global OS Statistics 2011-2013: http://gs.statcounter.com/#os-ww-monthly-201101-201301

In addition to the drivers to improve the communication with virtual hardware components, additional socket libraries are installed which can be used to be able to easily and quickly connect from the VM via the hypervisor to a hardware component or socket.[48] Libraries used by these sockets are listed in Table 6.

Socket Library Description	**Filename**
VMCI vSockets DGRAM	`%SystemRoot%\System32\vsocklib.dll`
VMCI vSockets STREAM	`%SystemRoot%\System32\vsocklib.dll`

Table 6: VMware Socket Libraries

8.3. Trend Micro Deep Security

Trend Micro's DS which is aimed at protecting HVD infrastructures is one of the first products that started to make use of the EPSEC API. Furthermore, as illustrated in Table 3 of Chapter 6, DS makes use of the whole feature set that EPSEC provides in order to keep track of the system's security.

DS can provide protection in two ways: either agentless or using an agent. When using agentless protection, the VMware vShield Endpoint driver has to be installed in the guest OS and the VMware ESX host has to be prepared to establish the connection between the VMware vShield Endpoint driver in the guest OS and the driver in the hypervisor. After this driver has been installed, as shown in Table 3 of paragraph 6.2, most capabilities are available without installing any agent in the VM. The only feature that is currently not available via the VMware vShield Endpoint API is the Log Inspection. The agentless and agent solution can run simultaneously without any problems such that the Log Inspection feature of the agent is complementing the malware protection capabilities of the agentless solution. Table 7 shows the drivers by DS after installing the Trend Micro Agent in addition to the agentless protection.

Driver Description	**Filename**
Trend Micro Instant Message Deep Security Agent Driver (Trend Micro LightWeight Filter Driver)	`%SystemRoot%\System32\Drivers\tbimdsa.sys`
Trend Micro Activity Monitor Module	`%SystemRoot%\System32\Drivers\tmactmon.sys`
Trend Micro Common Module	`%SystemRoot%\System32\Drivers\tmcomm.sys`
Trend Micro Event Management Module	`%SystemRoot%\System32\Drivers\tmevtmgr.sys`

Table 7: Trend Micro Drivers

Via the Trend Micro Agent, the user using the VM can also be notified about malware events and about the status of the antivirus software. The services in the Table 8 take care of this.

Service Description	**Filename**
Trend Micro Security Modules Manager	`%ProgramFiles%\Trend Micro\AMSP\coreServiceShell.exe`
Deep Security Manager Agent	`%ProgramFiles%\Trend Micro\Deep Security Agent\ds_agent.exe`
Deep Security Notifier	`%ProgramFiles%\Trend Micro\Deep Security Agent\Notifier.exe`

Table 8: Trend Micro Services

When installing the DS Agent, the `ds_agent.exe` process starts listening on port 4118/TCP. This port is used to transfer data from the DS Manager to the Agent.[49] Furthermore the `coreServiceShell.exe` service connects to a remote host which turns out to be the cloud-based Smart Scan service of Trend Micro[19] which, if the local client cannot determine the risk of the file, connects to the local Smart Scan Server. If the local Smart Scan Server is not available, the client will attempt to use the Global Smart Smart Scan Server.[50] Ports used by the agent are listed in Table 9.

Process	**L. Port**	**Status**	**R. Host**	**R. Port**	**Description**
`ds_agent.exe`	4118/ TCP	LISTENING	-	-	Manager to Agent communication
`coreServiceShell.exe`	[rand]	ESTABLISHED	`2.22.84.42`	443/ TCP	Trend Micro Smart Scan service

Table 9: Open Trend Micro Ports

[19]The WHOIS information does not show who is controlling the server. However by connecting to the https port of the IP address, the certificate reveals the certificate is created for `*.icrc.trendmicro.com`. A quick search disclosed that this connection is used for the Trend Micro Smart Scan.

8.4. VMware Tools and Deep Security Agent

Figure 11 shows the relations between both the DS Agent drivers and VMware vShield Endpoint drivers with the native Microsoft drivers. As explained in the previous paragraph, the DS Agent drivers are not dependent of the VMware vShield Endpoint drivers as both the agentless and agent solution can be running simultaneously. The schematic overview shows that various Trend Micro components are dependent on each other and also VMware vShield Endpoint components have mutual dependencies. The arrows in the figure demonstrate the dependency hierarchy and show that all components except the VMware vSockets Service are in the end dependent of the native Microsoft OS drivers. The dotted lines provide a description for each of the modules shown in the overview.

The relations between the various drivers has been compiled using the Dependency Walker tool[20] and Hex-Rays IDA Pro[21]. The Dependency Walker utility is able to scan scan Windows binaries to show a hierarchical list of the binaries' dependencies whereas IDA Pro is an extensive tool for the reverse engineering and debugging of binaries.

[20] http://www.dependencywalker.com/
[21] http://www.hex-rays.com/products/ida/

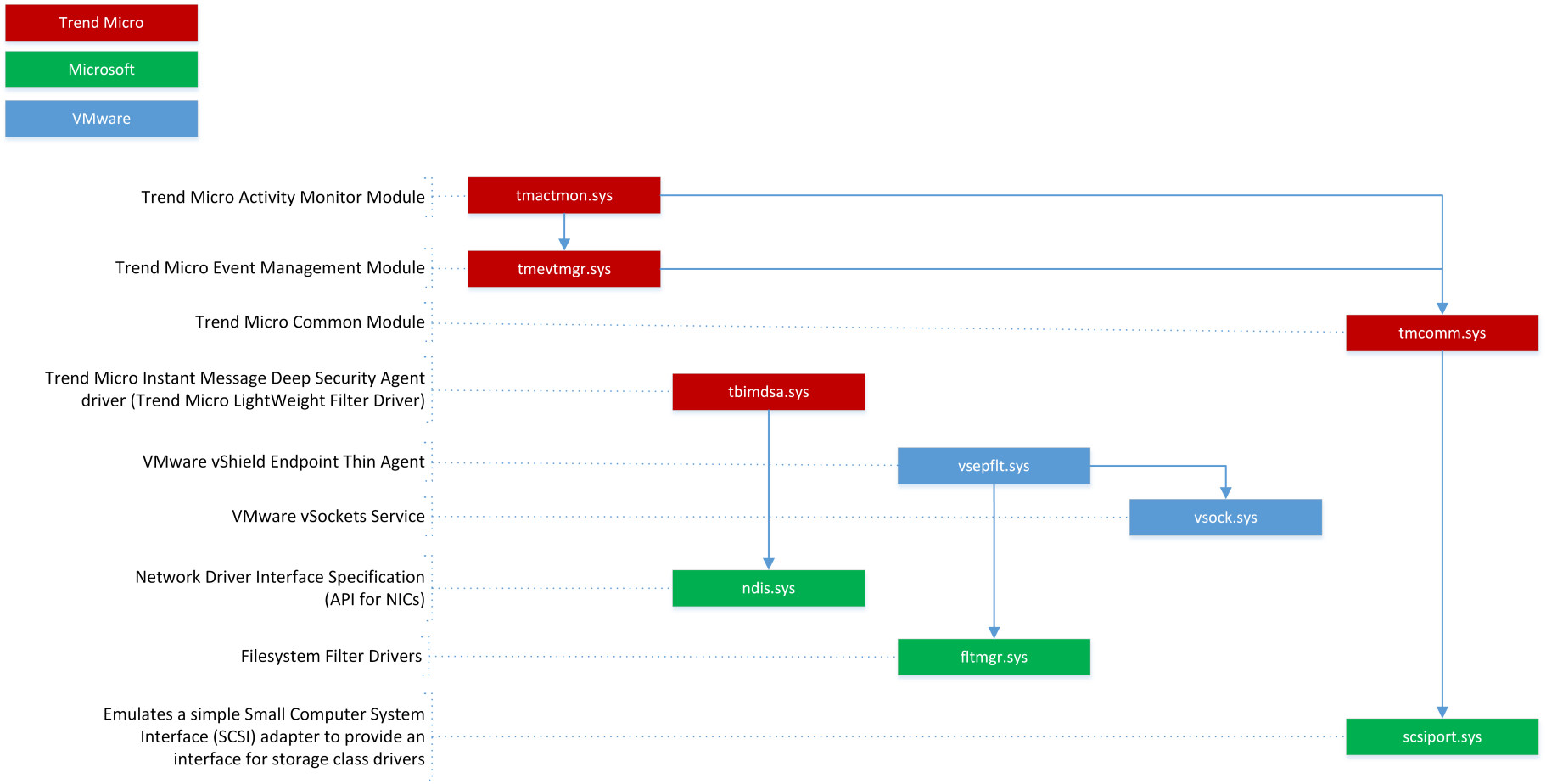


Figure 11: Relations between Microsoft Windows, VMware vShield Endpoint and Trend Micro Deep Security Components

8.5. Agentless Protection

Infrastructure

To provide agentless protection, various components have to be put in place. As shown in Figure 12, there are different types of components. An appliance is a standalone virtual machine which has a certain OS and runs certain software. It consists usually of one big file which can be loaded into VMware vSphere using the VMware vSphere Client. A new VM will be configured and the appliance VM will boot.[51]

vSphere Installation Bundles (VIBs) are software packages that may contain drivers, Common Information Model (CIM) providers [52], VMkernel modules, or other software.[53] From these types of software, CIM provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. An example of a popular implementation of CIM is Simple Network Management Protocol (SNMP).[54]

Installation

First of all a VMware vCenter has to be configured with at least one VMware vSphere Hypervisor (ESXi) host. To provide possibilities to offload security capabilities from a virtual machine, the VMware vShield Manager appliance has to be deployed on an ESXi host. Next, the DS Appliance has to be deployed on every ESXi host on which VMs are running that have to be protected by DS agentless security. After the appliances have been put in place, the DS Manager and DS Relay software can be installed on a Windows Server VM.

The DS Manager is used to manage the configuration of DS and the VMs that have to be protected by DS while the DS Relay is used to download updates from the Trend Micro update server and serves them to the clients in the local network. Now all appliances and software have been installed, the VMs that have to be protected need to have a security profile assigned, which is done via the web interface of the DS Manager. The full overview of the infrastructure of VMware vShield Endpoint in combination with DS is explained in the schematic of Figure 12. In this figure the straight lines are connections between the required components while the dotted line is an optional connection from the vShield Client to manage the setup.

As mentioned in paragraph 8.3 , VMware vShield Endpoint does not support Log Inspection. In case Log Inspection is wanted, the DS Agent has to be installed into the VMs which can be done by either deploying the DS Agent Microsoft Installer (.msi) via Active Directory or by manually installing the agent into the VM.

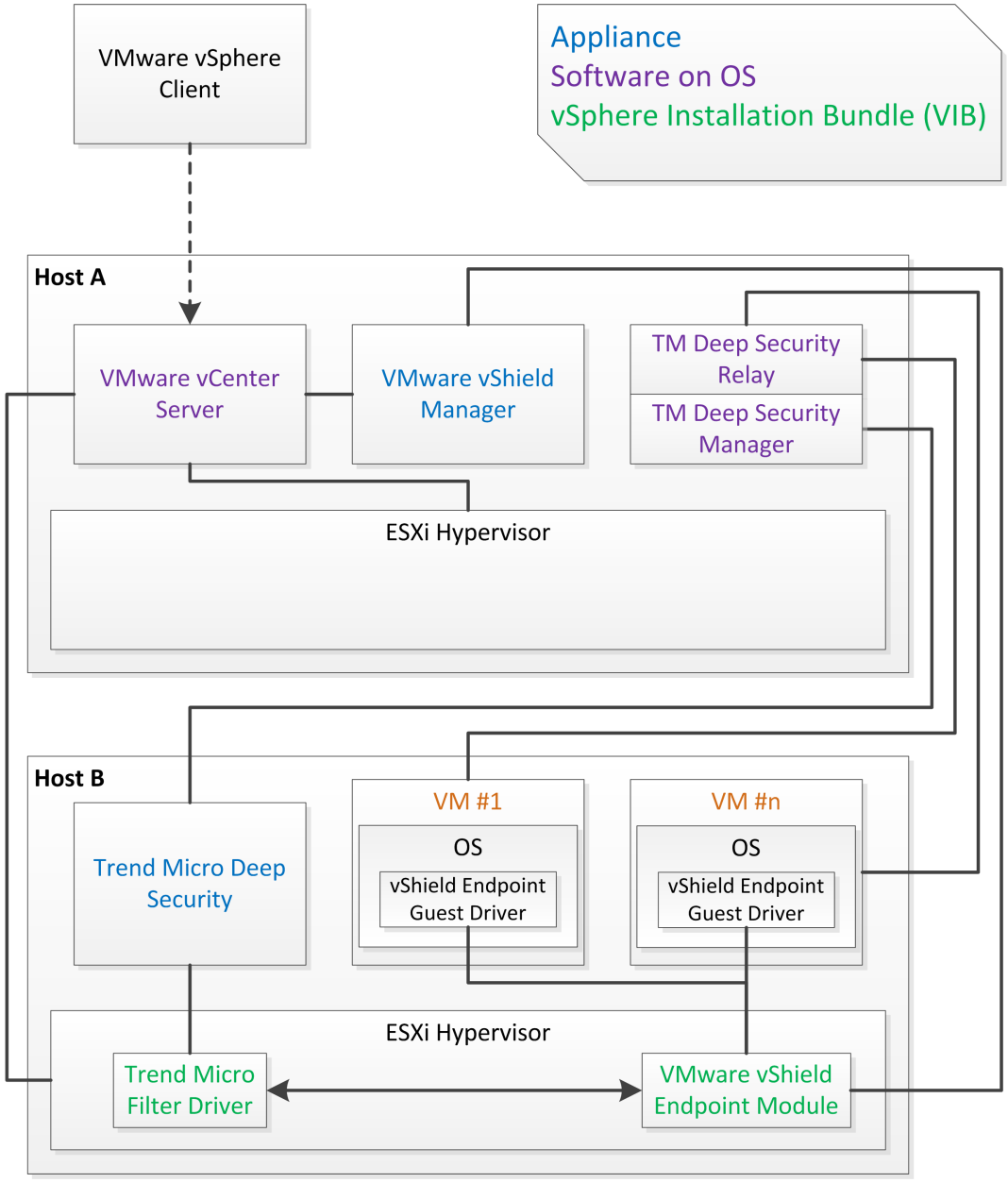


Figure 12: DS Infrastructure [[55], [56], [57]]

Workings

When a file is accessed, first the agent will calculate the checksum of the file and send it to the antivirus software which checks the hash against a list of known malware. In case the checksum is found, it sends back the result of the scan. In case the checksum is not found, the file or a pointer to the file is sent to the antivirus software for analysis

and the result is reported back to the guest VM. Results of scans can be cached on both the guest VM and in the centralized antivirus software in order to speed up the process of checking the system for malicious files. A schematic overview of this process is illustrated in Figure 13 .

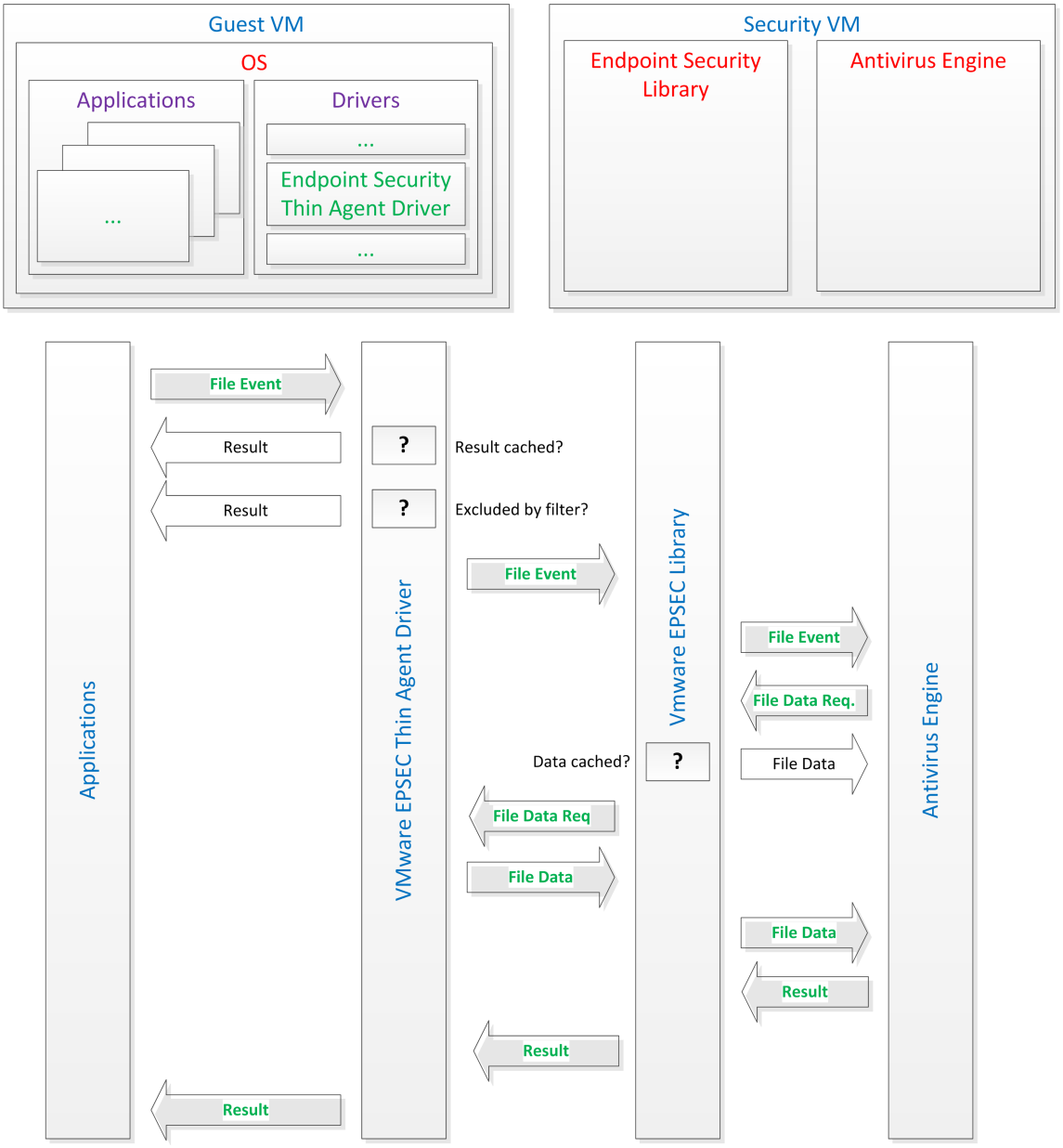


Figure 13: Trend Micro Deep Security File Scan [58]

8.6. Weaknesses

Disable Agentless Protection

As shown in the previous paragraphs, the DS Agentless protection completely relies on the VMware vShield Endpoint drivers which are included in the VMware Tools software. The advantage of this is that no additional drivers from antivirus software companies are needed for the antivirus software to work. The main disadvantage however is that if one can disable the vShield Endpoint driver in the guest OS, the antivirus software will also stop working and the VM is susceptible for malware.

The VMware vShield Endpoint driver in a Windows guest OS can be disabled using the Windows built-in sc.exe (Service Control) tool. This can be done by executing the following command in a elevated command prompt: `sc stop vsepflt`. After stopping the VMware vShield Endpoint driver, the VM cannot communicate any file accessing activities anymore to the centralized antivirus software and will thus stop protecting the machine.

In addition to stopping the VMware vShield Endpoint driver, it is also possible to completely remove the driver so even when rebooting the VM, the driver will not start again and the machine will not be protected against malware. The easiest way to remove the driver is by just using the VMware Tools uninstaller to either selectively remove the VMware vShield Endpoint driver, or removing the whole VMware tools software package.

As many users are using the local administrator account, one has sufficient permissions to disable the malware protection and execute his or her malicious tools. When only disabling the protection temporarily, it might also be possible to remain undetected for the antivirus management interface. This possibility will be explained more extensively in the next paragraphs.

Disable and Remove Agent

DS has a feature which prevents end-users from uninstalling, stopping or modifying the Deep Security Agent. This feature can be enabled and disabled via the DS web interface in the System Settings under the System section.[59] Furthermore a password can be configured to allow users knowing the password to uninstall, stop or change the DS Agent.

After booting up Windows, three Trend Miro processes are started:

1. **coreServicesShell.exe**
2. **coreFrameworkHost.exe**
3. **ds_agent.exe** - Graphical User Interface (GUI) for the DS software providing both a icon in the System Tray and a window which displays the status of DS.

To stop the Trend Micro monitoring software, kill these processes using an Administrative account. After that the VM will be unprotected. When trying to fully uninstall the software via the DS Agent uninstaller, the following error message is shown: "Removal or modification of this application is prohibited by its security settings.". The cause of this message to be shown is when the value of the `Self Protect` DWORD in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Deep Security Agent` exists and is unequal to `0`. The system will however throw up an access denied error in case one tries to modify the value or delete the key.

To get around this problem, the three processes mentioned earlier have to be killed. After killing these processes, the registry key can be changed or removed after which the DS software can be uninstalled. A script to automate this process can be found in Appendix C .

Alert

The DS management interface provides an overview of information about all VMs protected by the software. This information includes notifications about activated clients, detected malware and client events. It also includes warnings about clients from which the antivirus software seemed to stop working.

The DS software checks this by requesting the list of running virtual machines from the VMware vCenter Server and every heartbeat comparing this list with the list of clients registered for antivirus software. In case the list of running VMs contains a VM that is not registered with the DS Manager, this problem will be noted. Depending on the configuration in the System Settings in the System node of the DS Manager, an alert will be generated and shown in both the list of error messages in the DS manager as well as in the VMware vSphere Client.

The Heartbeat Configuration in the System Settings of the DS Manager has 2 parameters related to timing alerts. These parameters are the interval i in minutes and the number of missed heartbeats m. In case using the methods described in the previous paragraphs, the antivirus software of a VM is disabled or removed, an alert will be generated in at most $i \cdot m$ minutes. With the default setting this will provide an attacker $10 \cdot 2 = 20$ minutes of time to do malicious things and re-enable the protection in order to stay undetected.

8.7. Conclusion

Similar to the confusing naming of the corporate products of VMware, VMware also rebranded its security API products. Because of this, thorough research has to be done to the licensing of products and capabilities prior to purchase. The extent of these products and capabilities related to security of both the network and the virtual clients is improving all the time and 3rd party vendors are adapting the improved capabilities to their products.

Using the drivers included in the VMware Tools package which is installed in the virtual guest OS, VMware vShield Endpoint provides an extensive API to allow interception of system functions. This can be efficiently used centrally to scan files and network traffic inside VMs for malicious behavior.

Using various VAs and software packages that provide scanning capabilities and management options, VMware together with Trend Micro offers a good working solution for offloading antivirus software from VMs.

The DS software however has some weaknesses which enable an attacker to temporarily disable the antivirus software to circumvent antivirus restrictions or to remove the DS Agent software, even though it is configured that users are denied the permission to remove the software in the DS Management software.

In addition to these vendor-specific problems, VMware vShield Endpoint might contain vulnerabilities that open the ability for an attacker to break out of the VM using the vShield Endpoint interface and get access to all VMs that use the vShield Endpoint API.

9. Benchmarking

To test whether hypervisor-supported antivirus products have any advantages in performance compared to traditional antivirus products, benchmarks have to be performed. In order to accomplish reliable and representative results, the software used for the hypervisor-supported and traditional malware protection has to be as similar as possible, only differing in whether it is centralized or not. The scanning engine and malware signatures have to be similar.

As DS has already been examined in the previous chapters of this report and because Trend Micro also provides traditional antivirus software, the products from Trend Micro are chosen to be used in the benchmark. Trend Micro provides several antivirus products. The first product is Trend Micro Titanium Antivirus Plus, which is intended for home users and provides malware protection.[22] In addition to only the antivirus software, it is also possible to buy antivirus software which also includes a firewall and protection against data leakage. Furthermore, Trend Micro provides 2 major types of malware protection software for businesses. The first type is Trend Micro WFBS which is aimed at small business up to 250 computers. The second type is Trend Micro OfficeScan which is developed to be used in large corporates having more than 250 computers.

For this benchmark the Trend Micro WFBS software will be used as this test will include only a few VMs. WFBS comes in 3 flavors: Standard, Services and Advanced from which this benchmark will use the Standard version as solely the antivirus capability has to be tested and no additional protection measures like loss of information via e-mail or protection of Android devices.[23]

[22] http://www.trendmicro.com/us/home/products/titanium/antivirus-plus/
[23] http://www.trendmicro.com/us/small-business/product-security/

9.1. Setup

Software

Various software packages from VMware, Trend Micro and Microsoft are used to build the test environment. These software packages are listed including each of its requirements in Table 10. In case both the minimum and recommended requirements were listed, the minimum requirements have been used. As all requirements specify that every computer needs 2 processor cores or more, this information is omitted from the table. A short description of every software package is provided in the following paragraphs.

Software	**Mem**	**HD**	**Requirements Source**
VMware vSphere Hypervisor 5.1	2 GB	80 GB	VMware vSphere Hypervisor Requirements for Free Virtualization [24]
VMware vCenter Server 5.1 Enterprise Plus	8 GB	85 GB	VMware Knowledge Base - Minimum system requirements for installing vCenter Server [25]
VMware vShield Manager 5.1.2	8 GB	60 GB	VMware Knowledge Base - Installing vCloud Networking and Security 5.1.x best practices [26]
Trend Micro Deep Security Virtual Appliance 9.0	1 GB	20 GB	Trend Micro - Deep Security 9: System Requirements [27]
Trend Micro Deep Security Manager 9.0 (DS)	4 GB	1.5 GB	
Trend Micro Deep Security Relay 9.0	0.5 GB	1 GB	
Trend Micro Worry-Free Business Security 5.1 (WFBS)	1 GB [28]	5 GB	Trend Micro - Worry-Free Business Security Standard System Requirements [29]
Microsoft Windows 7 Enterprise x64 SP1	2 GB	20 GB	Microsoft - Windows 7 System Requirements [30]
Microsoft Windows Server 2008 R2 SP1	0.5 GB	10 GB	Microsoft - Windows Server 2008 R2 System Requirements [31]
StressLinux 11.4 x64	0.25 GB	2 GB	Debian Minimum Hardware Requirements [32]

Table 10: Minimum System Requirements of Software Packages

VMware vSphere Hypervisor is responsible for virtualizing and dividing the hardware resources and providing an API to manage VMs. The vSphere Hypervisor is also known as ESX and since vSphere version 4 also known as ESXi.[60]

VMware vCenter Server is used to join the ESXi hosts and be able to manage them in a centralized way. Moreover, it delivers monitoring, resource management and optimization, and possibilities to automate tasks.

As mentioned in Chapter 8.5, VMware vShield Manager is a component of the VMware vCloud Networking and Security software. This software is an addition to VMware vCenter Server and manages the vShield module in the hypervisor while providing a web interface to configure the module.

Trend Micro's Deep Security (DS) VA takes care of the actual protection of the VMs via the vShield Endpoint module which resides in the ESXi Hypervisor. File accesses in protected VMs are intercepted and scanned by this VA. From now on, when referring to the DS VA, the abbreviation Deep Security Virtual Appliance (DSVA) will be used. The DS Manager provides a web interface for system administrators which provides both possibilities for configuration and screens to monitor the VMs protected by DS. As shown in Figure 12 of Chapter 8.5, the DS Manager is connected to the DSVA to keep track of the statistics of scanned files, found viruses and actively protected VMs.

Trend Micro Deep Security Relay is an application which is used to download antivirus signature updates and spread them over the DSVA on the network. This way, signatures only have to be downloaded once supplying them to all the VAs. Moreover, only the host on which the DS Relay resides needs access to the Internet while access to the Internet for the DSVA can be prohibited in the firewall.

As opposed to the DS centralized antivirus, WFBS is a traditional antivirus solution which has to be installed on top of a Windows machine. This software can be registered to a Trend Micro server after which it is possible to manage the software via the management website of Trend Micro.

Windows 7 Enterprise and Windows Server 2008 R2, both with Service Pack 1, are cur-

[24] https://www.vmware.com/products/datacenter-virtualization/vsphere-hypervisor/requirements.html
[25] http://kb.vmware.com/kb/1003882/
[26] http://kb.vmware.com/kb/2034173/
[27] http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/system-requirements-full-list/
[28] Using Smart Scan mode which cooperates with Trend Micro's online scan server in contrast to the traditional scan mode which only uses its local virus database.
[29] http://www.trendmicro.com/us/small-business/product-security/index.html#system-requirements
[30] http://windows.microsoft.com/en-us/windows7/products/system-requirements/
[31] http://technet.microsoft.com/windowsserver/bb414778.aspx
[32] According to the StressLinux FAQ at http://www.stresslinux.org/sl/wiki/FAQ, StressLinux is based on Debian whose System Requirements are listed at http://www.debian.org/releases/stable/i386/ch03s04.html.en

rently the second-last versions of respectively Microsoft's client and server OS and are widely used in corporates.[61]

Finally, StressLinux is a linux distribution which is aimed at stressing hardware resources such as CPU, Memory, Harddisk, Network and GPU. As explained more extensively in the next paragraph, StressLinux has been chosen as a light-weight alternative to Windows 7 in order to accurately simulate a real-life environment. StressLinux is based on Debian and uses much less harddisk resources compared to Windows 7.[62]

VMware vSphere Hypervisor 5.1, vCenter Server 5.1 and vShield Manager 5.1.2 are at the moment of writing (April 2013) the most recent versions of the VMware software. Also the Trend Micro Deep Security packages and Worry-Free Business antivirus software are the most recent at this time. Finally, Windows 7 Enterprise x64 with the most recent service pack and updates is installed in each of the VMs.

Hardware

The hardware used in the lab are two Lenovo Thinkpad T410 laptops and one HP 8200 Elite XL510AV PC. Detailed specifications are listed in Table 11 and Table 12. From this point on the hardware will be referred to as 'servers'.

	Type	**Specification**
CPU:	Intel Core i5 520M	Quad Core, 2.40 Ghz, 3 MB cache
Memory:		2x 4 GB, 1333 Mhz
Harddisk:	Hitachi Travelstar HTS725016A9A364	160 GB, 7200 RPM, 16MB cache
NIC:	Intel 82577LM Gigabit	1 Gbit

Table 11: Hardware specification of Lenovo Thinkpad T410 laptops

	Type	**Specification**
CPU:	Intel Core i5-2500	Quad Core, 3.30 Ghz, 6 MB cache
Memory:		4x 4 GB, 1333 Mhz
Harddisk:	Intel X25-M 80GB SSD 2.5' SSDSA2M080G2HP	80 GB, 250MB/s read, 70MB/s write, 16MB cache
NIC:	Intel 82574L Gigabit	1 Gbit

Table 12: Hardware specification of HP 8200 Elite XL510AV PC

Despite of the fast components like Solid State Drive (SSD), this hardware is not representative to hardware usually being used in data centers. Nevertheless, a comparison can be done with different types of malware protection products on the same kind of hardware, keeping in mind that the products will run faster on real server hardware.

Configuration

Based on this hardware and software the configuration for the tests is compiled taking into account the processing power, amount of memory and storage available.

In this lab, one server will be dedicated for management and coordination software. The other two servers will be used for running the client VMs, Trend Micro and vShield Manager Security VAs. The base for all three servers is the VMware vSphere Hypervisor which uses around 1 GB of memory on each server. On top of the VMware vSphere Hypervisor at the first server, the VMware vCenter Server VA has been installed. This VA takes care of the coordination between the vSphere Hypervisors, other connected VAs and allows management by the VMware vSphere Client management tool.

During the installation of DS, the decision has been taken to use an Embedded Database (Apache Derby database[33]) instead of using database software from Microsoft or Oracle.[63] Because this test environment consists of less than 10 PCs which is the amount of PCs the embedded database software is recommended to handle.[64] Moreover, the embedded database is automatically installed and therefore does not require a separate installation of Microsoft SQL Server or Oracle SQL.

Multiple instances of 64-bit Windows 7 Enterprise with the most recent service pack (SP1) and updates have been configured in the environment. To collect the most reliable results, the following configuration has been applied to the Windows 7 VMs:

- Latest version of VMware Tools;
- Windows Up-to-date with all patches until April 2013 to get the best experience of the OS;
- Windows Update Disabled to prevent benchmarks against being manipulated by Windows Update activity in the background;
- Windows Defender Disabled to not have other anti-malware software running and slowing down the VM;
- Configured fixed IP Address, Subnetmask, Gateway and DNS so no delays will be caused by the VM renewing its IP lease or looking up a host;
- The High Performance Power Plan has been selected to not allow energy saving measures to slow down the VM;
- Aero has been Disabled to not burden the hardware more by rendering transparency/3D graphics;
- The Screen Saver has been Disabled to prevent CPU usage by this process;

[33] Apache Derby is an open source relational database implemented entirely in Java. More information about Apache Derby can be found at https://db.apache.org/derby/

- VMware Tools Tray Icon has been Disabled;
- No Desktop Wallpaper;

None of the VM's harddisks is using snapshots as it might have a performance impact compared to using one VHD to which all changes in the filesystem are written directly. Snapshots can degrade performance because all changes made to the base disk are written to a separate file.[65] In that case for every read and write, a check has to be done whether the data is stored in the base disk or in (one of) the snapshot files.[66]

Moreover, as the harddisks of the two laptops are only 160 GB in size and the SSD of the PC is only 80 GB, the decision has been taken to configure the VHDs as dynamically expanding[34] harddisks instead of preallocated[35] harddisks. According to tests conducted by both VMware [67] and Venkat [68], it turns out there is a negligible performance loss when using dynamically expanding harddisks compared to preallocated harddisks. An additional workaround for the small harddisks was the use of StressLinux which is only 3GB in size compared to Windows 7 Enterprise which occupies almost 20 GB. During the benchmarks, StressLinux was used to simulate a live environment running multiple VMs by making use of harddisk, memory and CPU resources.

The next paragraph will explain the process of obtaining statistics in order to get a clear view on resource usage.

[34] Called 'thin provisioned' in VMware vSphere terminology
[35] Called 'thick provisioned' in VMware vSphere terminology

9.2. Statistics

VMware vCenter uses performance counters from the different ESX hosts to obtain and aggregate statistics about performance of the hosts and can be viewed and exported via the VMware vSphere Client. The following information is recorded by ESX for the ESX host itself, but also for every individual VM: CPU statistics, Memory statistics, Disk statistics, Network statistics and some other statistics related to cluster services and management agents. Samples are taken by the ESX hosts every 20 seconds. These samples are accrued over 20 seconds and represent the average load over these 20 seconds.[69] Information from these statistics can be used to effectively plot usage graphs of individual hardware components and the usage of the virtual hardware components for each VM.

CPU

CPU usage over time is something which can easily be obtained by looking at VMware's performance counters. Among various kinds of statistics including statistics about CPU locks and reservation of CPU capacity, the CPU performance counters provide information about the CPU usage in Mhz aggregated over all cores. This value is useful to determine both the CPU usage of the physical ESX host and the CPU usage of the individual VMs running on the system.

Memory

The VMware vCenter performance counters are also used to obtain the amount of memory used by the VMs and ESX system in total. The performance counters include information about swapping, the memory heap, shared memory, memory overhead and different types of memory usage. From these types of memory usage, the active memory usage and consumed memory usage provide a good view on the memory usage of the VM. Active memory shows the memory which has been used in the past small window of time while consumed memory is the amount of memory that is occupied by the VM.[70] Because the hypervisor is not aware of any caching algorithms within the guest OS, for Windows VMs, memory statistics are also obtained from the non-cached physical memory usage value in the Windows Task Manager. As the VAs are security hardened, it is difficult to get to a shell exposing this information and is therefore not taken into account.

Diskspace Usage

To determine the amount of disk space used by a certain VM, the harddisk space is obtained by looking at the size of the harddisk in the Summary tab of the VMware vSphere Client. By having the system booted up, also the additional space required for swap and other caching files is taken into account which provides a more accurate view on the disk usage statistics and actual disk space required to run the VM.

Disk Usage

From the statistics which include the amount of disk commands issued, read and write latencies and number of I/O operation, the read and write rate are used in the benchmark to get a good view on the disk performance.

Network

Using the performance counters, the data receive and data transmit rate in kilobytes per second (KB/s) of the VM and ESX are recorded. These values show the data transfer between the two ESX servers and can also be correlated with the disk usage statistics. Besides the transfer rate, the dropped packets, amount of network packets and several other statistics can be recorded, however the amount of KB/s is the most relevant counter in this benchmark as the test is aimed at measuring the transfer speed.

9.3. Methodology

Types of Tests

In order to be able to compare the differences between different types of antivirus protection, the following three types of environment benchmarks will be conducted:

1. Antivirus-less;
2. Trend Micro Deep Security (DS) malware protection;
3. Trend Micro Worry-Free Business Security (WFBS) malware protection.

To determine the influence on the different AV's performance of other VMs on the same server being busy, each benchmark has been conducted twice: the first time with the other machines in an idle state, and the second time using around 75 percent of both ESX its CPU power and memory.

Disk Space and Memory Usage

Disk space and memory used for each of the VMs is determined by measuring the VM's resources after installing and configuring the VM and performing a clean boot after which the system idles for 10 minutes. By having the system booted up, also the additional space required for temp, swap and other caching files are taken into account which provides a more accurate view on the disk usage statistics and actual disk space required to run the VM. Moreover, also the memory usage is acquired after 10 minutes of a clean boot of the VM. This value has been obtained from the Virtual Machines tab of VMware vSphere Client which lists all VMs on the ESX host including their sizes.

Boot Time

In addition to determining the space and memory used by the VM, also the boot time with the three different configurations has been measured. This will be done using tools included in Microsoft's Windows Performance Toolkit (WPT).[36] The WPT among other tools includes the `xbootmgr` and `xperf` utility. From these utilities, the first tool is aimed at recording performance information which includes information while booting Windows and several options can be configured to make the performance test as objective as possible and to run the test multiple times in a row. After recording performance information, the second tool is used to extract information about the time it takes to go through the different stages of the boot process and for each process the amount of resources used. These stages are illustrated in Figure 14. The output of the second tool is written to an xml file which among many other properties contains the value `bootDoneViaPostBoot`. The value of this property is the amount of milliseconds it took to boot to an idle desktop. The xperf utility samples the system every 100 ms during during the PostBoot phase. If the system is 80 percent or more idle at the time of the sample, xperf considers the system to be "idle" for that 100 ms interval. The phase persists until the system accumulates the `postBootRequiredIdleTime` property amount of seconds of idle time which by default is 10 seconds. Therefore, 10000 ms have to be subtracted from the `bootDoneViaPostBoot` property to get the actual boot time.[71] Because of the large amount of xml files that had to be processed, an EXtensible Stylesheet Language (XSL) script has been developed to quickly extract all the required values from the xml files. More information about extracting the values from the xml files can be found in Appendix D.

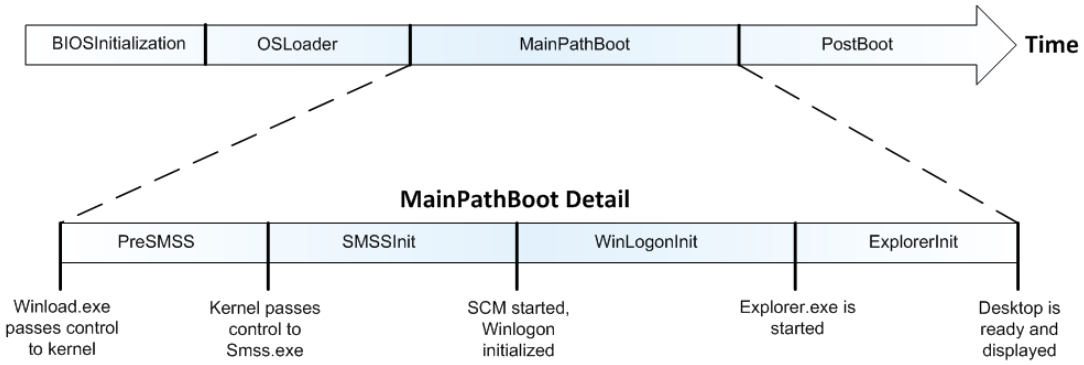


Figure 14: Stages in the Windows Boot process [71]

Benchmark

To test the performance of Trend Micro's DS and WFBS antivirus software, the software has to be triggered to scan files while monitoring its CPU and memory usage. Antivirus

[36] https://msdn.microsoft.com/performance/

software can be triggered by writing files to disk. Furthermore, a benchmark has to be done while not running any antivirus software. In order to avoid incorrect results because the disk is busy reading the files from its own filesystem which degrades performance and produces incorrect testing results, files will be copied over the network. The speed of the network is 1Gbit and other than sending some management and logging information between the vSphere Hypervisors and vSphere Server, vSphere Server and vShield manager, the DSVA and the DS Manager, the connection is only used for traffic between the VMs.

As a test 10 GB of data consisting of 1900 .zip files containing the files extracted from the Windows Installer 3.1 Redistributable[37] are used. The full file listing can be found in Appendix E. These files consist of a few executables, various dlls and some text files and are packed using the file compression tool 7-Zip[38]. The least compressing algorithm of 7-Zip has been chosen which only stores the files specified into a single file. This compressing algorithm is used to be able to quickly generate 10 GB of unique files. Because the least zip compression algorithm is used, the AV software also has to put less effort into decompressing and scanning the files. In order to prevent the antivirus software caching the result of a scan, a random text file is added to every zip to slightly modify the zip so the engine is not able to reuse a previous result. Moreover, for each test a new set of zips is generated to prevent incorrect results due to the caching mechanisms of VMware vShield/DS as shown in Figure 13 in Chapter 8. To test whether the AV software works, the eicar test virus has been inserted in one of each of the 1900 generated zips. The batch script that is used to generate the zips is available in Appendix G. In addition to this batch script, a script to measure the transfer time is used which is added to Appendix H. This script is a slightly modified version of the script provided at StackOverflow.[39]

The VMs participating in the test are booted and left idle for 10 minutes to allow them to fully start up and cache memory. During all of the tests, three StressLinux VMs are running, either in an idle state or being busy, depending on the test being conducted. Moreover, between benchmarks the StressLinux VMs are rebooted in order to free memory which has possibly been occupied during benchmarks and shows a biased view on the use of resources. Furthermore, VMs of VAs and Management servers that are not required during certain tests are shutdown. Examples are the DSVA Manager and vShield Manager VA which do not need to run while benchmarking WFBS or an environment without antivirus software. To prevent incorrect results due to delays in the authentication procedure, a network connection from the testing VM to the benchmark VM has been setup prior to starting the test.

[37] https://www.microsoft.com/download/details.aspx?id=25
[38] http://www.7-zip.org/
[39] http://stackoverflow.com/a/6209392/

Result Collection

The following steps are performed to develop the graphs:

1. File generation and copy is performed while timing the amount of seconds needed for the process of copying. Furthermore, statistics about the various hardware components involved are recorded.

2. Results of timing and statistics from the hardware components are correlated based on start time and duration of the copying process. Moreover, due to the generation of the new files which takes a while, from the statistics it can clearly be distinguished during which period of time the file transfer has occurred. Using statistics from both the Network Interface Controller (NIC) and from the CPU, the starting and end time of the transfer is determined and statistics from the different hardware components are correlated.

3. This process is repeated for each of the 3 test runs after which the results are put side by side and the average speed over these runs is calculated.

The next paragraph will go into the configuration of the servers including the hardware assigned to each of the VMs and the actual usage.

9.4. Server Configuration

Antivirus-less

The configuration of the three hosts without running any antivirus software is shown in Table 13. As no antivirus supporting VMs have to be running, only the hypervisor is running on every host. Furthermore, the first host is dedicated to vCenter Server, the second host used for generating and transferring files, and the third host running several clients. From these clients the Windows 7 VM is used as machine to transfer the files to. A schematic overview of this configuration is shown in Figure 15 .

		Memory				***Harddisk***	
				Usage			
Software	**Host**	**Required**	**Assigned**	**ESX**	**in-OS**	**Required**	**Usage**
VMware vSphere 5.1 Hypervisor	1	2 GB	n/a	1 GB	n/a	80 GB	1 GB
VMware vCenter Server 5.1	1	8 GB	8 GB	8 GB	n/a	85 GB	12 GB
VMware vSphere 5.1 Hypervisor	2	2 GB	n/a	1 GB	n/a	80 GB	1 GB
Windows 7 Enterprise SP1 x64	2	2 GB	1.5 GB	0.5 GB	0.5 GB	20 GB	18 GB
VMware vSphere 5.1 Hypervisor	3	2 GB	n/a	1 GB	n/a	80 GB	1 GB
Windows 7 Enterprise SP1 x64	3	2 GB	2 GB	0.5 GB	0.5 GB	20 GB	18 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB

Table 13: Configuration of the Testing Lab Without Antivirus Software

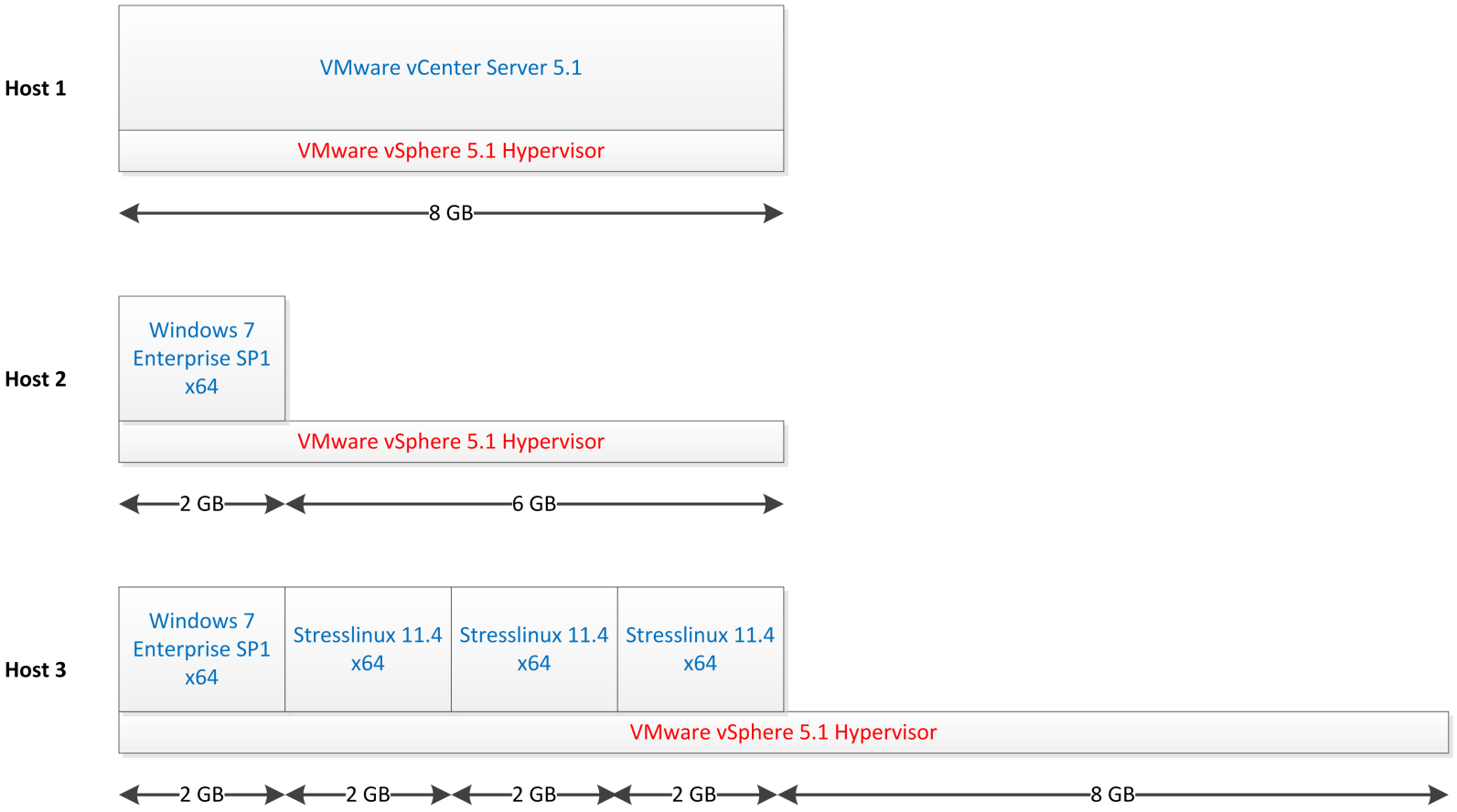


Figure 15: Schematic Overview of Hosts Running the AV-less Configuration

Trend Micro Deep Security (DS)

As described in Chapter 8.5, DS requires various components in order to be able to run. Similar to the benchmark without antivirus software, the first server runs the vCenter Server. The second server is running the DS manager which provides an interface to manage and configure the VMs running DS. Furthermore, it runs the DS Relay software which distributes updates over the hosts in the network. Finally, similar to the previous benchmark, this host runs an Windows 7 VM not protected by AV software which generates files and copies them over the network for benchmarking purposes.

Server three runs the DSVA, VMware vShield Manager and several clients including a Windows 7 VM having the DS Agent installed. The reason for this configuration has been explained in Chapter 8.3 . Moreover, more memory is assigned than the amount of memory available in the system. This is done to stay consistent with the other tests. Looking at the actual memory usage however, it is clear that the total amount of actually used memory does not exceed the amount of memory in the system. Therefore no memory swapping will occur and the VMs performance will not be degraded.

The configuration of the three hosts is shown in Table 14 while the schematic overview is shown in Figure 16 .

		Memory				*Harddisk*	
				Usage			
Software	**Host**	**Required**	**Assigned**	**ESX**	**in-OS**	**Required**	**Usage**
VMware vSphere 5.1 Hypervisor	1	2 GB	n/a	1 GB	n/a	80 GB	1 GB
VMware vCenter Server 5.1	1	8 GB	8 GB	8 GB	n/a	85 GB	12 GB
VMware vSphere 5.1 Hypervisor	2	2 GB	n/a	1 GB	n/a	80 GB	1 GB
Windows Server 2008 R2 SP1	2	0.5 GB	5 GB	4.5 GB	1.3 GB	10 GB	20 GB
+ Trend Micro Deep Security Manager 9.0	2	4 GB				1.5 GB	
+ Trend Micro Deep Security Relay 9.0	2	0.5 GB				1 GB	
Windows 7 Enterprise SP1 x64	2	2 GB	2 GB	0.5 GB	0.5 GB	20 GB	18 GB
VMware vSphere 5.1 Hypervisor	3	2 GB	n/a	1 GB	n/a	80 GB	1 GB
VMware vShield Manager 5.1	3	8 GB	8 GB	2.9 GB	n/a	60 GB	10 GB
Trend Micro Deep Security Virtual Appliance 9.0	3	2 GB	2 GB	0.5 GB	n/a	20 GB	2 GB
Windows 7 Enterprise SP1 x64	3	2 GB	2 GB	0.5 GB	0.5 GB	20 GB	18 GB
+ Trend Micro Deep Security Agent 9.0	3	0.5 GB				0.1 GB	
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB

Table 14: Configuration of the Testing Lab With the Trend Micro Deep Security Antivirus Software

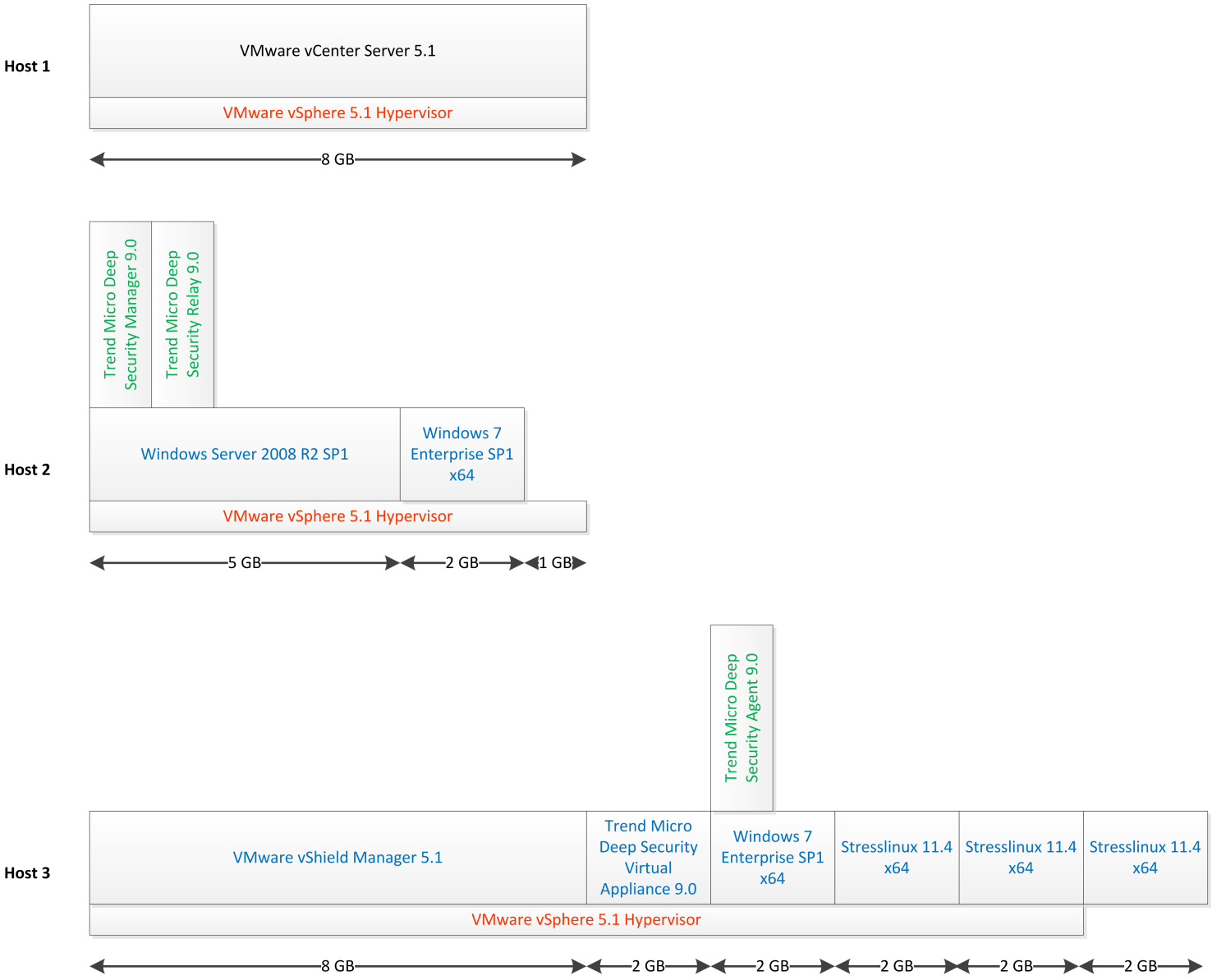


Figure 16: Schematic Overview of Hosts Running the DS Configuration

Trend Micro Worry-Free Business Security (WFBS)

As shown in Table 15 , WFBS does not need any additional VAs in order to run. Therefore, similar to the benchmark without antivirus software does not have any additional VMs running on the first two servers other than the VMware vCenter Server and Windows 7 VM used to generate and transfer files for benchmarking purposes. In addition to these two servers, the third server runs several clients which includes a Windows 7 VM running the WFBS antivirus software. A schematic overview of this configuration is illustrated in Figure 17 .

		Memory				***Harddisk***	
				Usage			
Software	**Host**	**Required**	**Assigned**	**ESX**	**in-OS**	**Required**	**Usage**
VMware vSphere 5.1 Hypervisor	1	2 GB	n/a	1 GB	n/a	80 GB	1 GB
VMware vCenter Server 5.1	1	8 GB	8 GB	8 GB	n/a	85 GB	12 GB
VMware vSphere 5.1 Hypervisor	2	2 GB	n/a	1 GB	n/a	80 GB	1 GB
Windows 7 Enterprise SP1 x64	2	2 GB	1.5 GB	0.5 GB	0.5 GB	20 GB	18 GB
VMware vSphere 5.1 Hypervisor	3	2 GB	n/a	1 GB	n/a	80 GB	1 GB
Windows 7 Enterprise SP1 x64	3	2 GB	2 GB	0.5 GB	0.5 GB	20 GB	18 GB
+ Trend Micro Worry-Free Business Security 5.1	3	0.25 GB				0.5 GB	
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB
StressLinux 11.4 x64	3	0.25 GB	2 GB	0.2 GB	n/a	1 GB	3 GB

Table 15: Configuration of the Testing Lab with the Trend Micro Worry-Free Business Antivirus Software

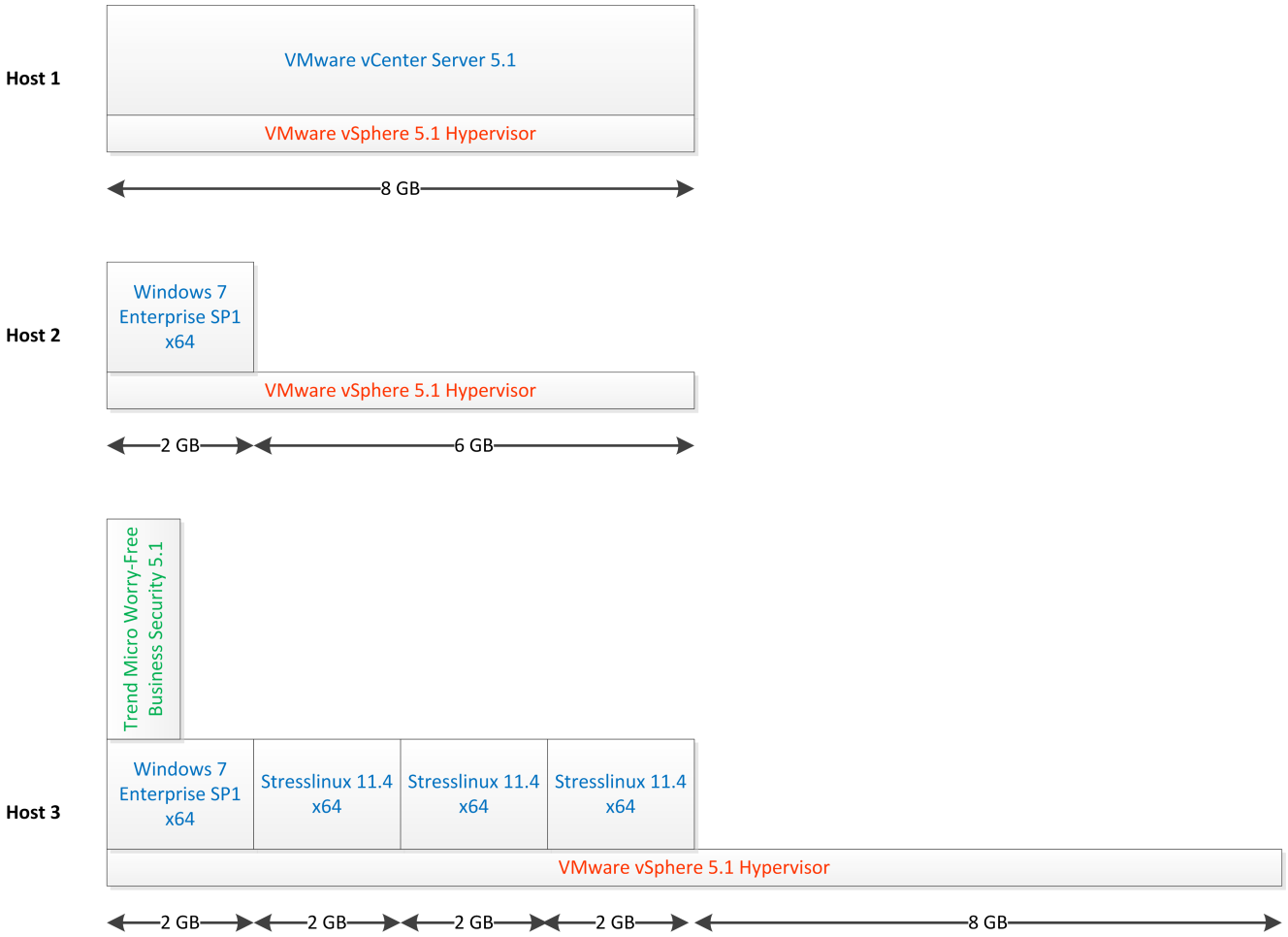


Figure 17: Schematic Overview of Hosts Running the WFBS Configuration

9.5. Benchmarks

This paragraph will list the results of the VM's startup time of the VM running different antivirus configurations. The three antivirus configurations that will be tested are:

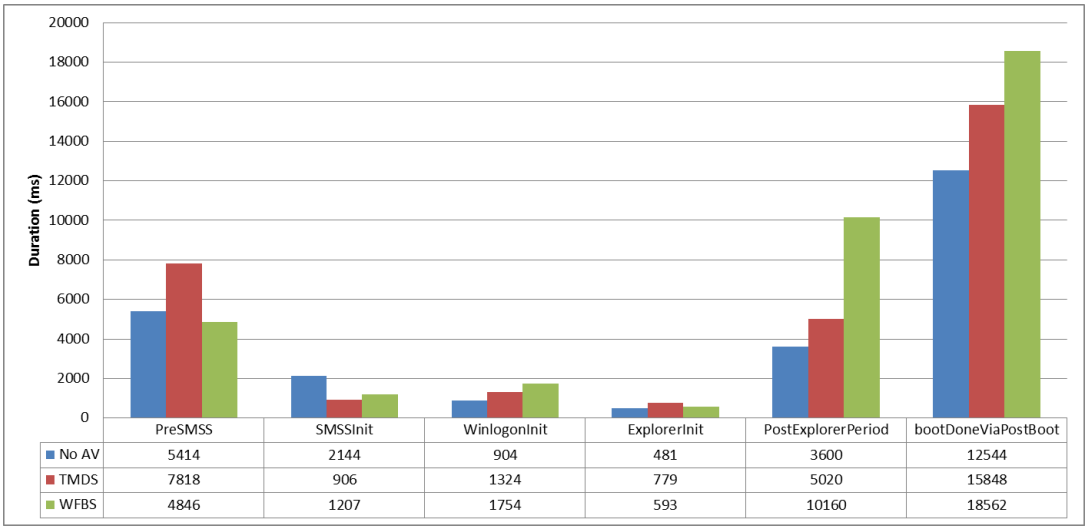
- Environment without using antivirus software which is being used as a baseline to compare the configurations that do run antivirus software
- Environment with Trend Micro's Deep Security (DS) centralized antivirus solution for virtualized environments.
- Environment with Trend Micro's Worry-Free Busines Security (WFBS) centralized antivirus solution which is not specifically aimed at virtualized environments.

Furthermore, for every antivirus configuration, its memory, CPU and load on the NIC are listed for the ESX server, VM running antivirus software and in the case of DS the additional DSVA. Finally, the total amount of resources used by each of the antivirus configurations is shown.

Boot Times

Five runs have been conducted measuring the amount of milliseconds (ms) it takes for each stage of the boot process to complete. By averaging and plotting these results, a clear overview of the impact of running AV software has been created and is displayed in Figure 18. The configurations used are respectively a PC without antivirus software, a VM using DS and a VM running WFBS. In this figure the last column is an addition of all columns to the left of it. The statistics on which this graph is based can be viewed under Boot Times in Appendix B.
This graph shows that overall the boot time increases for both DS and WFBS compared to not running antivirus software. DS mainly increases the duration of the `PreSMSS` phase of booting which is the initialization of the kernel. This phase includes loading drivers configured as `BOOT_START` which includes the VMware Tools drivers required for offloading AV software to a dedicated VA.[72] In contrast to DS, WFBS mainly increases the duration of the `PostExplorerPeriod` phase which is the phase in which the Windows GUI has already been initialized but programs are still starting up. This increased duration can be explained by the AV GUI having to load.

A remarkable result is the increased speed of the PreSMSS boot stage when comparing the configuration without antivirus with the configuration which runs WFBS. It does not make sense that a configuration running antivirus software is faster than a AV-less system. Therefore it can be concluded that these statistics might not be completely accurate.



	PreSMSS	SMSSInit	WinlogonInit	ExplorerInit	PostExplorerPeriod	bootDoneViaPostBoot
No AV	5414	2144	904	481	3600	12544
TMDS	7818	906	1324	779	5020	15848
WFBS	4846	1207	1754	593	10160	18562

Figure 18: Duration of Boot Stages for the Different Types of Antivirus Protection (lower is better)

Copying Performance

It is now clear what the influence of antivirus software on the boot time of the Windows 7 VM is. The next step is to test the VM's run-time performance which has be done by copying data to the VM. As explained in the methodology in paragraph 9.3, the environment has both been tested with other VMs being idle and other VMs in a busy state. Graphs of the different components of respectively the AV-less configuration, DS configuration and WFBS configuration are listed at the following pages.

Figure 19 shows the average transfer speeds over three tests with the three different antivirus configurations testing each configuration with both an idle state and with a high load.

By looking at this graph it is evident that both the configurations of running no antivirus and the configuration running WFBS have much faster transfer speeds compared to the configuration running DS. The following paragraphs will look at the details that lay behind the performance results of each of the antivirus configurations. For each configuration the performance statistics of every hardware component are shown.

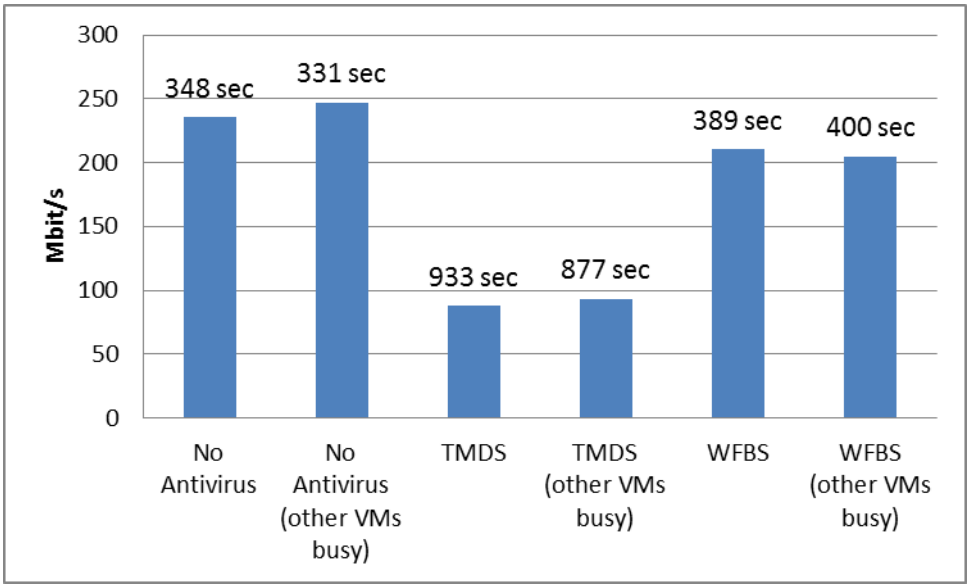
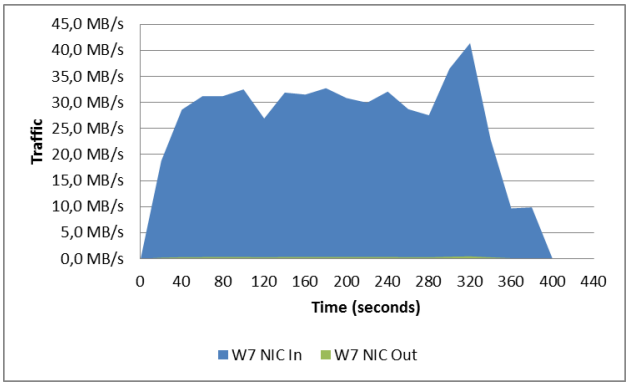


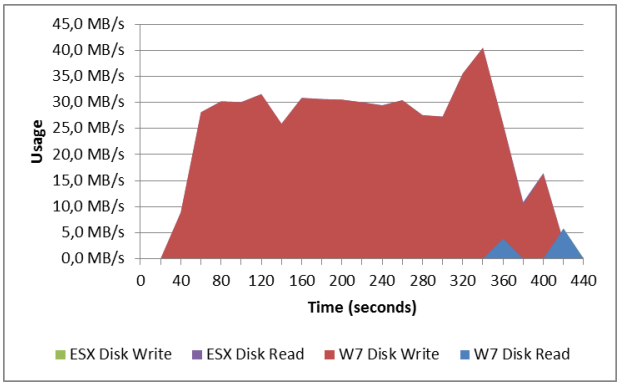
Figure 19: Average Transfer Speeds and Duration when Transferring 10 GB of Data. (higher is better)

Statistics per VM

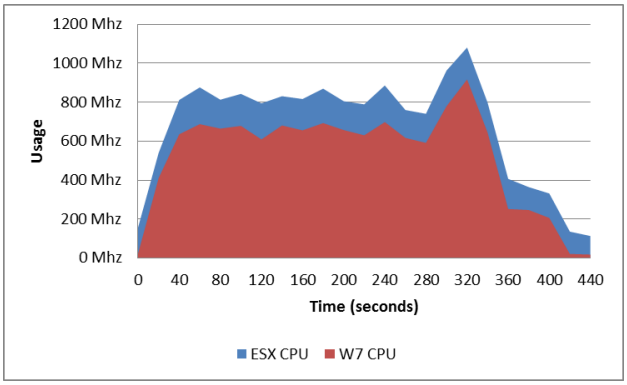
AV-less, other VMs Idle At the moment the data transfer starts, the input of the NIC as shown in Figure 20(a) increases from its idle state to around 30 MB/s which is approximately 240 Mbit. At the same time the harddisk of the VM starts writing at about the same speed without any overhead on the physical disk in ESX (Figure 20(b)). Furthermore, usage of the CPU in Figure 20(c) is similar to the usage of the NIC and disk. Observing the memory usage in Figure 20(d) shows that the 2 GB assigned by ESX to the VM has already been reserved during the whole measurement. During the transfer the amount of active memory gradually increases. Finally, a peak can be observed at the end of the transfer. Possible explanations for both of these observations will be listed later in this chapter.



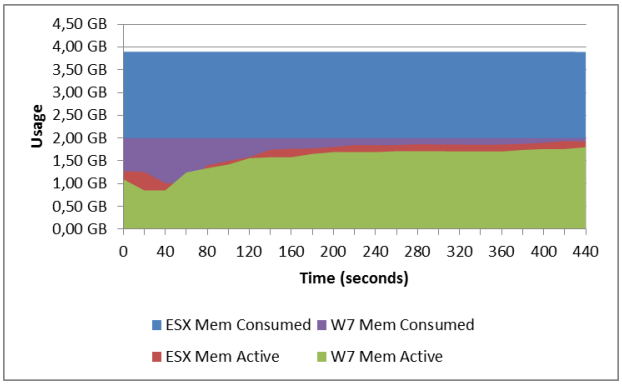
(a) Network



(b) Disk



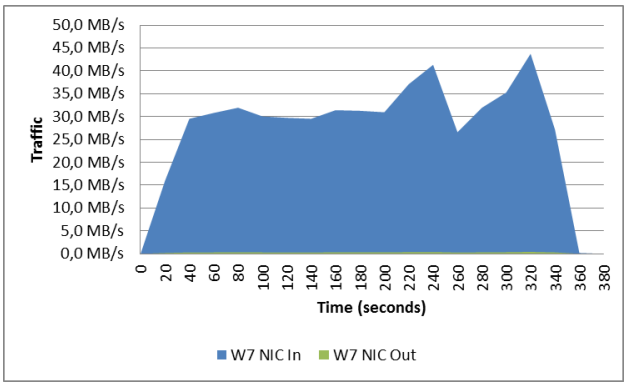
(c) CPU



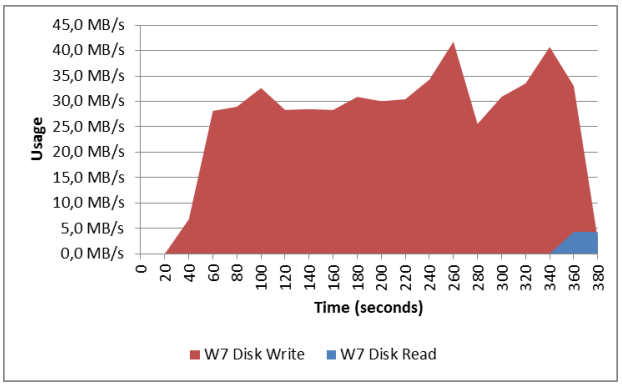
(d) Memory

Figure 20: AV-less Configuration while other VMs are Idle

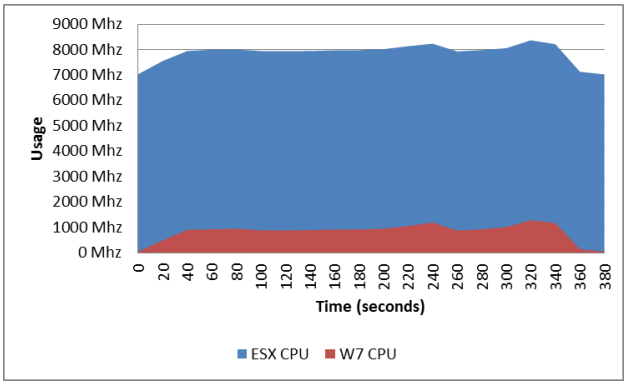
AV-less, other VMs Busy Comparing the AV-less configuration with both other VMs in an idle state and other VMs being busy shows that the transfer speed in Figure 21(a) is barely affected by the other busy VMs: both benchmarks show an average transfer speed of around 30 MB/s ($\sim$ 240 Mbit). Just like the first benchmark shown in Figure 20, the virtual harddisk in Figure 21(b) shows a similar graph as the NIC. Furthermore, although a large amount of CPU power is used for the other VMs, it barely has any influence on the transfer speed as shown in Figure 21(a). Finally, even though a vast amount of memory has been occupied by the other busy VMs, it does not degrade the memory usage of the Windows 7 VM as can be seen in the statistics in Appendix B.



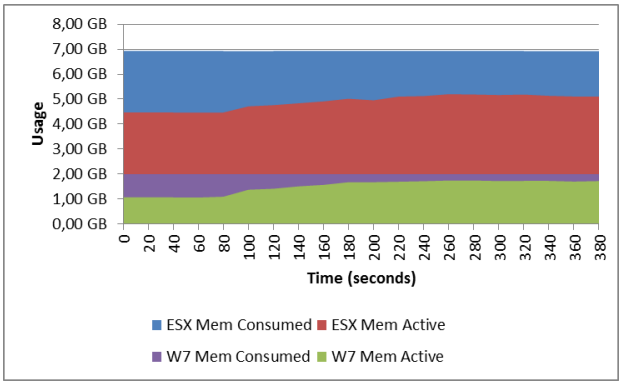
(a) Network



(b) Disk



(c) CPU

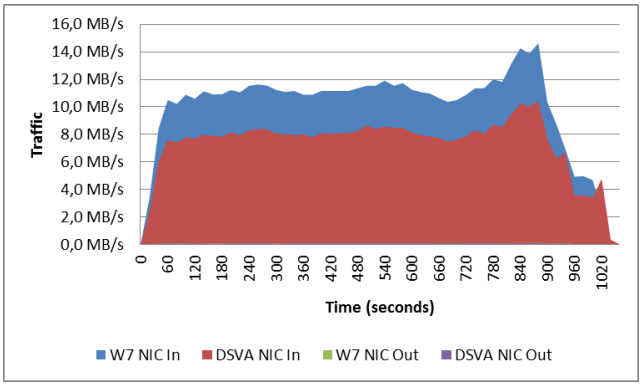


(d) Memory

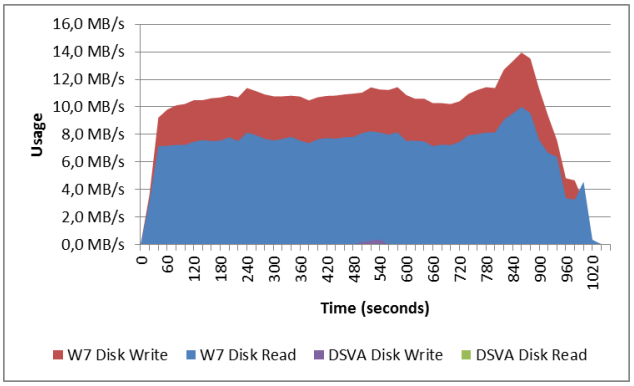
Figure 21: AV-less Configuration while other VMs are Busy

DS, other VMs Idle Measuring the network speed of the environment running DS results in an average transfer speed of around 11 MB/s for the NIC of the Windows 7 VM while the input for the DSVA is slightly more than 6 MB/s as shown in Figure 22(a). These speeds can be correlated with the usage of the VM's harddisk in Figure 22(b) which shows that the data from the network is written to disk while at the same time with a part of the writing speed, data is also being read from disk. This read speed can be correlated with the incoming NIC speed of the DSVA. An explanation is that the data read by the Windows 7 VM is transferred to the DSVA via the VMware VMCI driver. Because this driver does not utilize an actual NIC, this is however not visible in the benchmark. Within the DSVA the data is then scanned and via VMCI responses are reported back to the VM. In case a virus has been found, the vShield driver will then remove the file from the filesystem inside the VM and report to the DSVA whether the file has been removed successfully. The DSVA will then report the result to the DS Manager which can notify the system administrator based on its configuration. A further analysis of the fact that only part of the data written to disk is read again and transferred to the DSVA will be done in a later paragraph in this chapter.

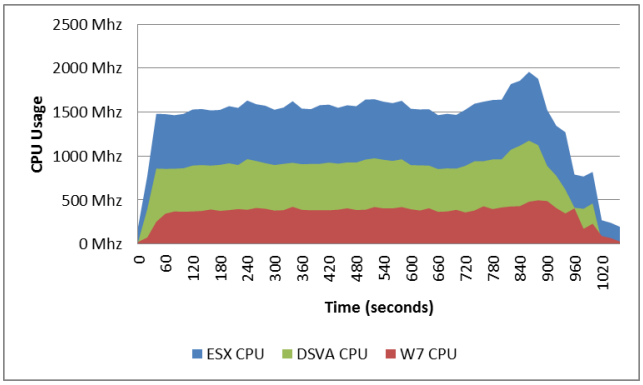
In Figure 22(c) it can be noticed that the DSVA almost uses 1 Ghz to process the incoming data and scan it for viruses. Using the peaks seen in the DSVA CPU usage, the graph can be correlated with the graphs of DSVA NIC input speed and VM's harddisk read rate. Finally, from the memory graph in Figure 22(d) it can be noticed that during most of the transfer the Windows 7 VM uses almost all of its memory. A possible reason for this will be explained later in this chapter. In contrast to the Windows 7 VM, the DSVA barely has any active memory.



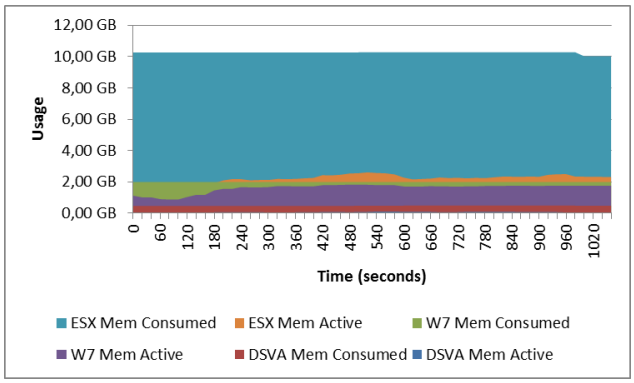
(a) Network



(b) Disk



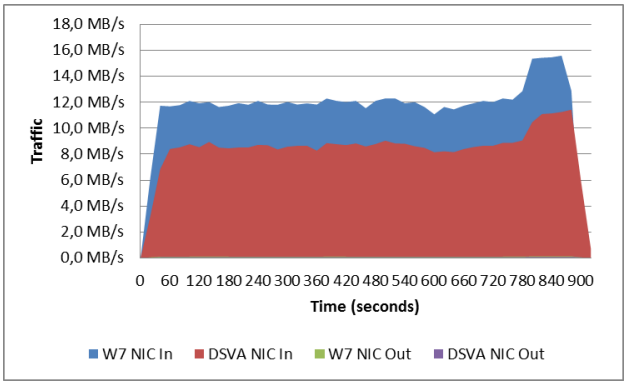
(c) CPU



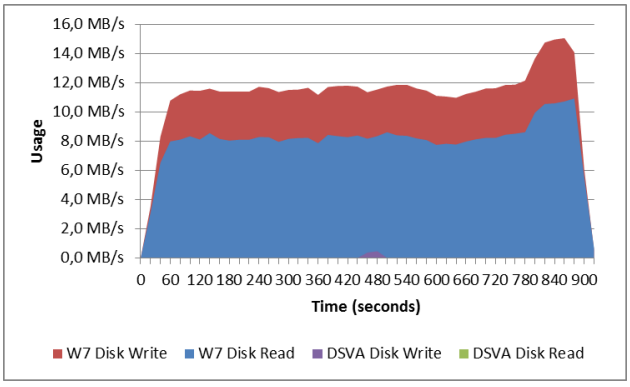
(d) Memory

Figure 22: DS Configuration while other VMs are Idle

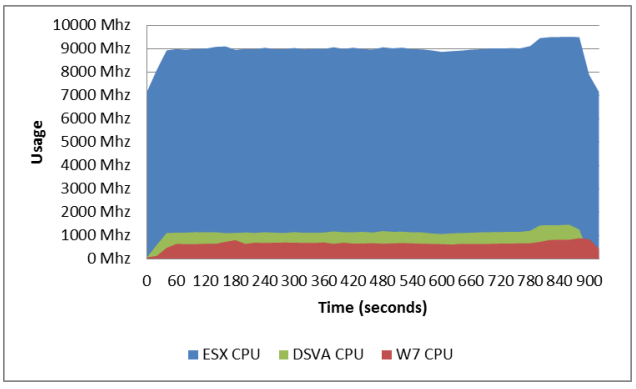
DS, other VMs Busy As shown in Figure 23(a) the VM's average network speed and NIC average speed of the DSVA are respectively 12 MB/s and 8 MB/s. This is remarkable as these speeds are slightly faster compared to the speeds of DS with other VMs idle. An possible explanation will be provided later in this chapter. The values of both the NICs of the Windows 7 VM and DSVA can again be directly correlated with the values of the disk write and read speed in Figure 23(b). Figure 23(c) shows that most of the CPU's power is used by ESX which mainly consists of the StressLinux VMs. These VMs are using a vast amount CPU and memory from which the increased memory usage compared to Figure 22(d) is shown in Figure 23(d). Due to the continuous read and write actions on the memory performed by the StressLinux VMs, a vast piece of ESX memory is also shown as active. Similar to the test with other VMs idle, this test also shows that the output from the Windows 7 VM to the DSVA is less than the total size of the file transfer to the Windows 7 VM. This shows that the remarkable result in the previous test was not an exceptional case. A possible explanation for this result will be provided in a later chapter.



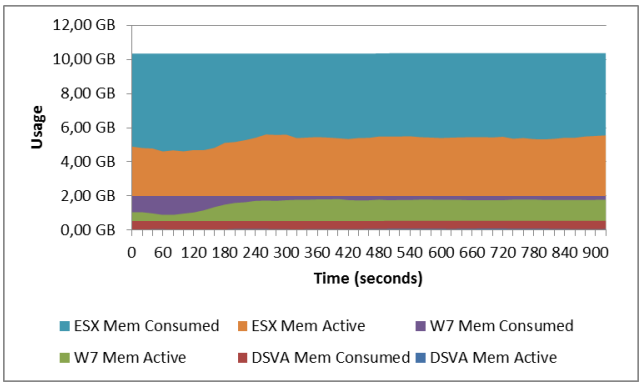
(a) Network



(b) Disk



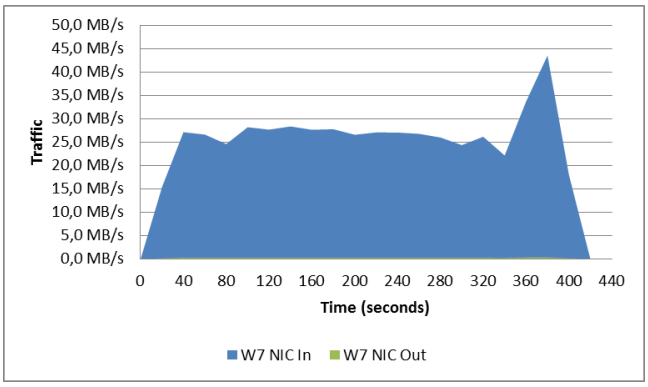
(c) CPU



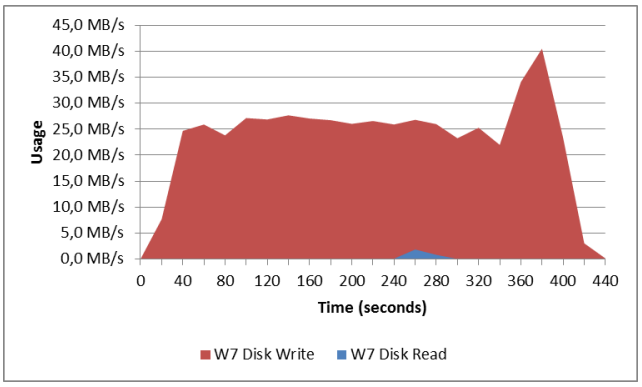
(d) Memory

Figure 23: DS Configuration while other VMs are Busy

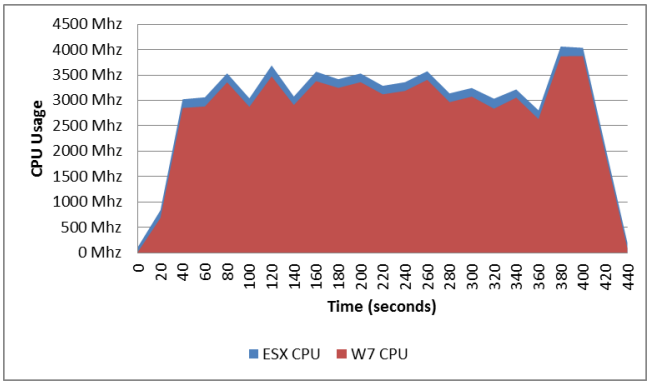
WFBS, other VMs Idle As displayed in Figure 24(a), WFBS brings an average network speed of more than 25 MB/s. Just like with the other antivirus configurations a peek in the file transfer can be observed at the end of the transfer. Similar behavior can be observed from the virtual harddisk statistics in Figure 24(b). Figure 24(c) shows that during the transfer the CPU is intensively used which makes sense as the VM itself scans the files that are being written to disk. From this graph it can furthermore be noticed that the CPU is still busy for a short period of time after the data transfer over the NIC has already finished. A possible explanation will be provided later in this chapter.



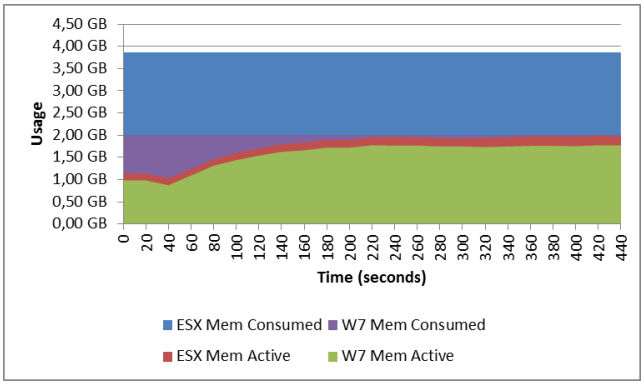
(a) Network



(b) Disk



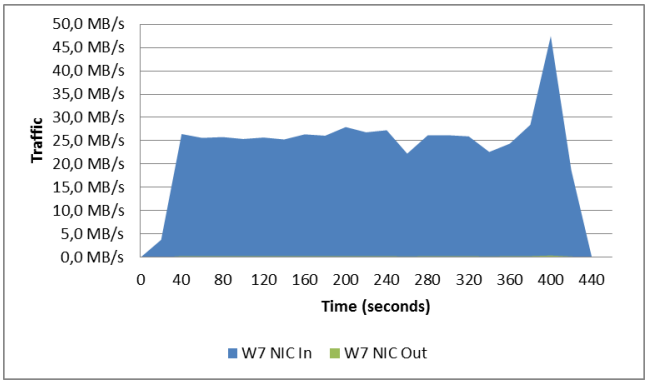
(c) CPU



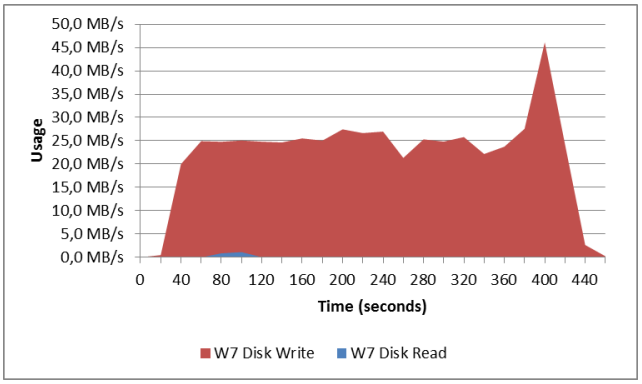
(d) Memory

Figure 24: WFBS Configuration while other VMs are Idle

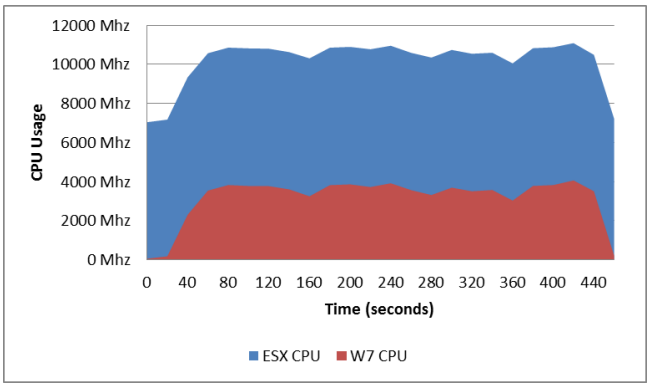
WFBS, other VMs Busy Similar to the test where other VM were idle instead of utilizing resources, the incoming NIC speed is also around 25 MB/s and also the virtual harddisk uses this speed writing the data (Figure 25(a) and 25(b)). Looking at the ESX CPU usage in Figure 25(c) it can be noticed that more than 10000 Mhz is used of which a little bit less than 4000 Mhz is used by the Windows 7 VM. This is quite similar to the benchmark results of WFBS with the other VMs being idle in 24(c). The memory graph in Figure 25(d) shows that just like when the other VMs are idle, a similar amount of memory of the Windows 7 VM is active. This is because the Windows 7 VM is able to use a similar amount of network and CPU resources despite of the higher burden on the hardware. Finally, also a large amount of ESX memory is active due to the continuous read and write actions of the simulated busy StressLinux VMs.



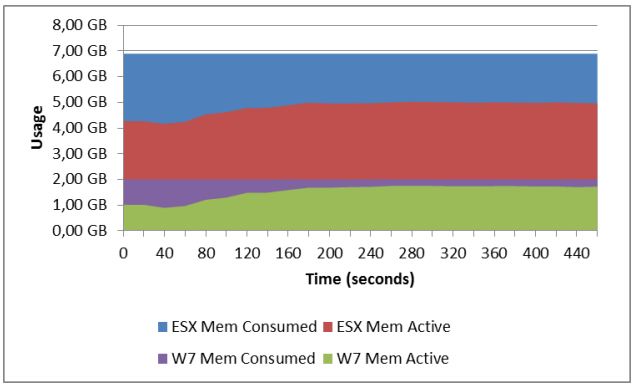
(a) Network



(b) Disk



(c) CPU



(d) Memory

Figure 25: WFBS Configuration while other VMs are Busy

Comparing AV Performance

After looking at the performance of the individual AV configurations with both the other VMs being idle and busy, this paragraph will make a direct comparison of all three configurations. As the state (busy or idle) of the other VMs did not have much influence on the performance of the Windows 7 VM, this paragraph will only compare the results of the Windows 7 VM with the other VMs being idle. Furthermore, as the previous paragraph already zoomed in on the usage of resources on the Windows 7 VM and the usage in ESX with its overhead, this paragraph will only look at the Windows 7 VM unless stated otherwise.

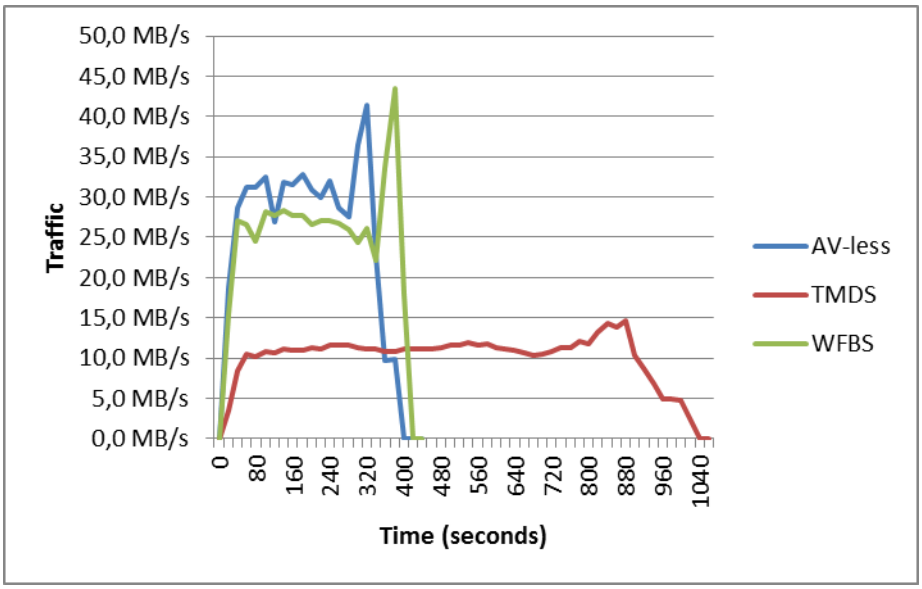
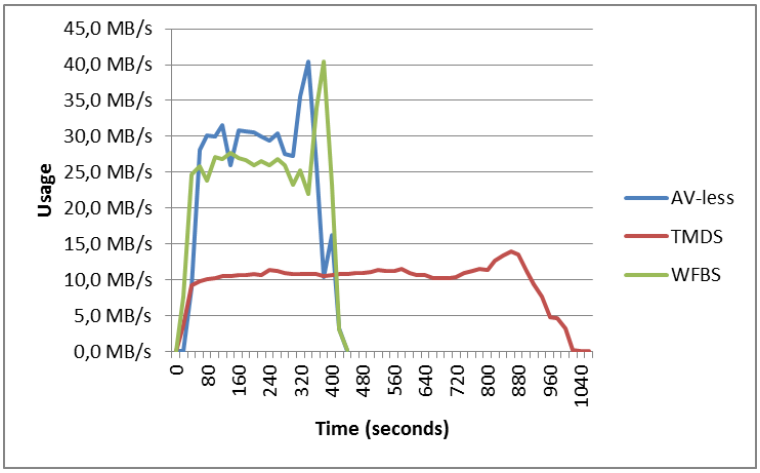
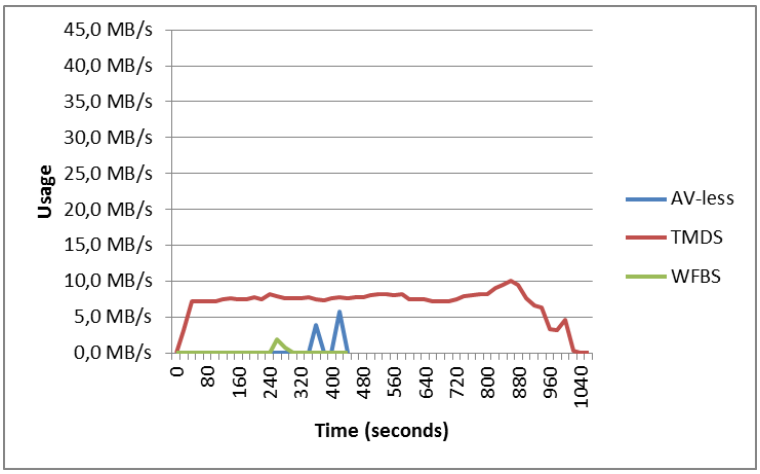


Figure 26: Comparison of NIC Transfer Speeds over Time

In addition to Figure 19 which is only showing the average transfer speed, Figure 26 shows the transfer speed of all three of the AV configurations over time. In this chart the peak at the end of each of the file transfers is again clearly visible.



(a) Write

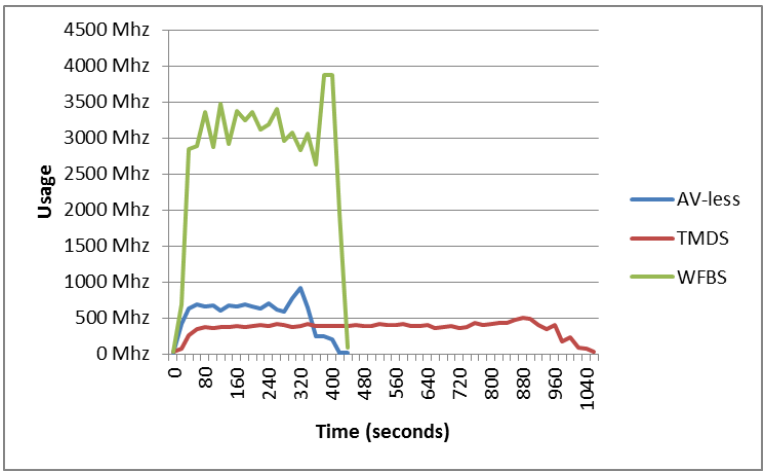


(b) Read

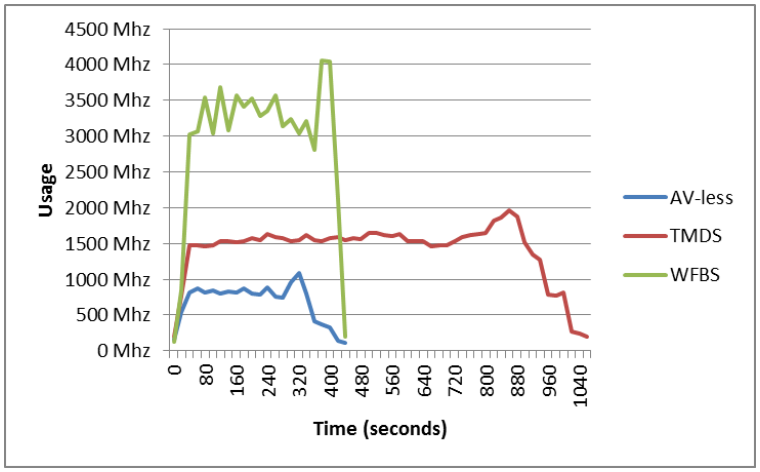
Figure 27: Comparison of Read Speeds From and Write Speeds To the VHD

The write speeds of the harddisk in 27(a) show a progress similar to the NIC speeds in Figure 26 including the peak at the end of each of the transfers. Looking at the disk read speed in 27(b) shows that only DS reads data from the Windows 7 VHD and - as concluded based on Figure 22(a) - sends it to the DSVA to scan it for viruses. The other two antivirus configurations barely read anything from disk which in case of WFBS can be concluded that all files are scanned prior to writing them to disk. It can furthermore be noticed that there are two small peaks in Windows 7 disk read speed during the benchmark of the AV-less configuration. Because no AV software is running which might need to read some data, it can be concluded this is caused by the Windows OS, possibly running a scheduled task after a certain idle time or periodically performing

some action. Moreover a small peak in of disk reading during the benchmark of WFBS might indicate some antivirus signature update being downloaded or similar to DS a Windows action being performed.



(a) Windows 7 VM



(b) ESX

Figure 28: Comparison of CPU Usage over Time

As can be noticed from Figure 28(a), WFBS uses by far most of the CPU power of the Windows 7 VM. However, when putting the CPU usage in perspective with DS using the DSVA to scan for viruses, the usage graph changes to Figure 28(b) which shows the actual CPU usage of DS is three times the usage of the Windows 7 VM, although its usage is still under WFBS's usage. A possible reason for the fact that the AV-less configuration uses more CPU than DS in Figure 28(a) is that the former of the two has a much higher transfer speed.

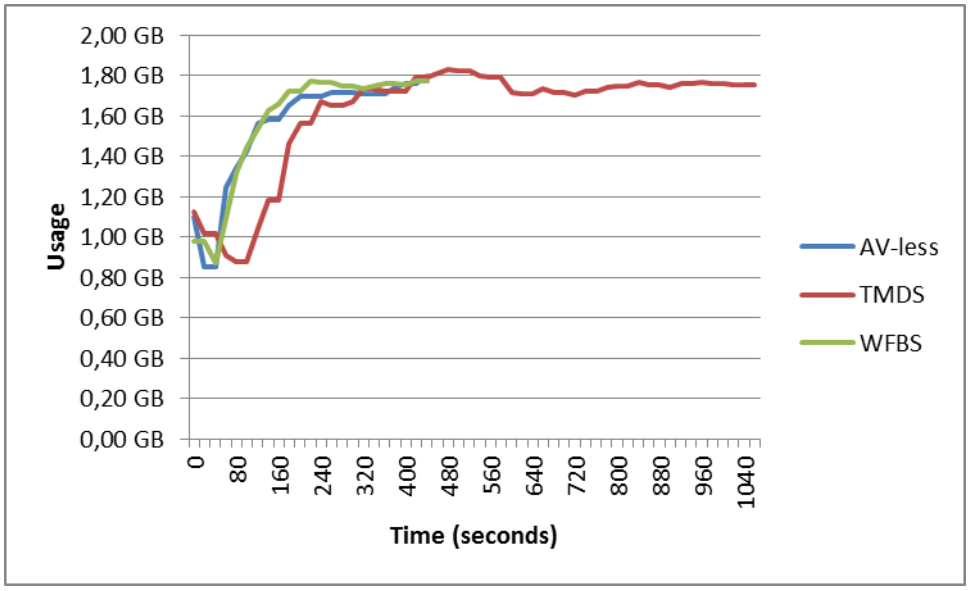
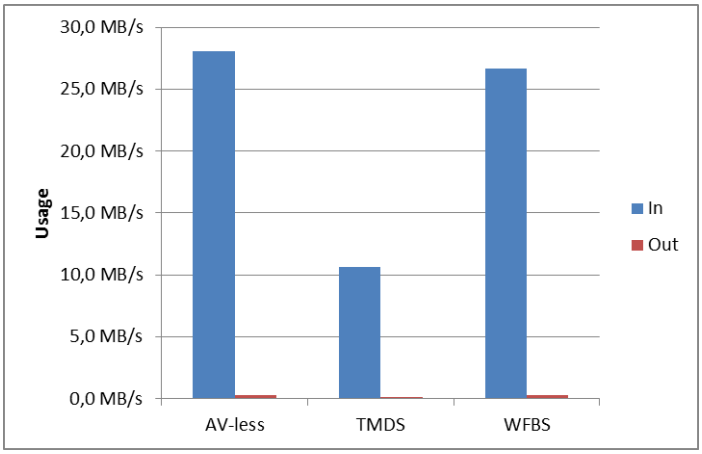
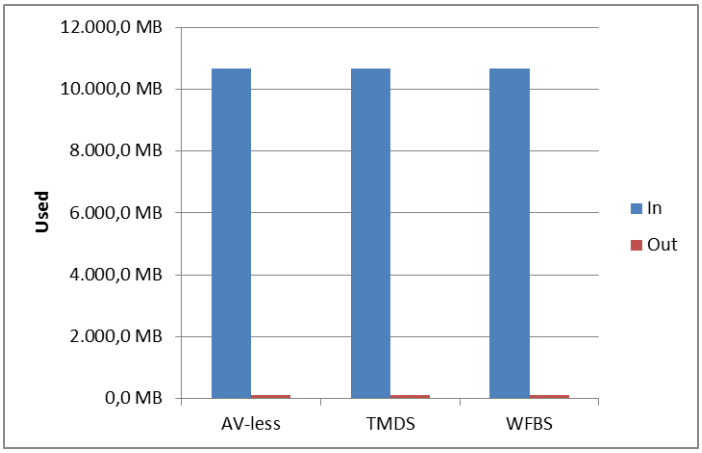


Figure 29: Comparison of Active Memory over Time

Figure 29 shows that the active memory of each of the configurations at the start of the file transfer increases from 1 GB to around 1.8 GB. For both the AV-less configuration and WFBS the process of increasing active memory usage happens earlier. This can be caused by the faster transfer speed for which the memory is used as a buffer between the NIC and harddisk. Later also DS shows an increase of active memory of the Windows 7 VM.



(a) Average

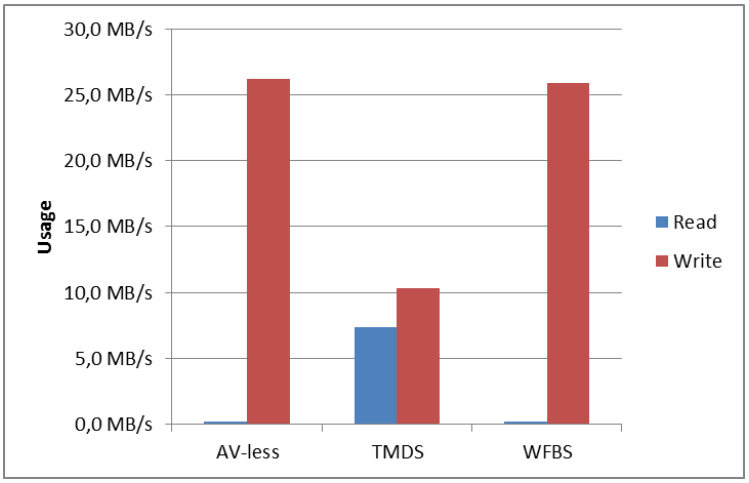


(b) Commutative

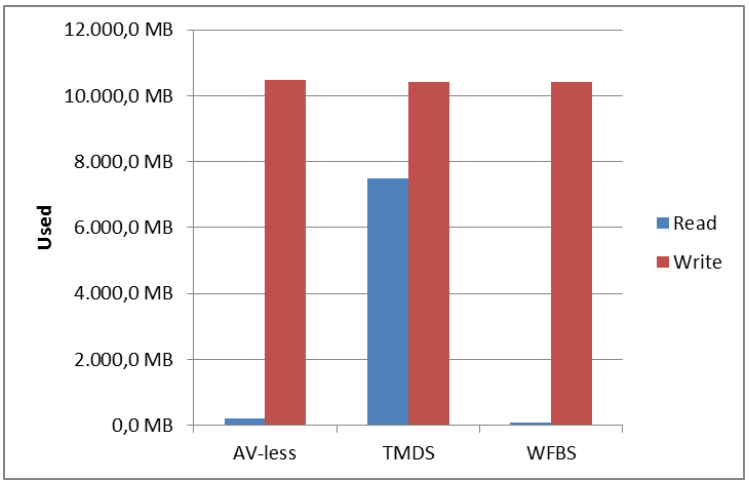
Figure 30: Comparison of Average and Commutative NIC Usage

Based on the time the NIC was actively sending or receiving data and the amount of data being sent during the active time, the average speed of of the NIC can be calculated which is shown in 30(a). The data in this chart slightly differs from the data in the chart of Figure 19 at the beginning of this chapter due to issues with ESX performance measuring as described in Appendix A.

Figure 30(b) shows the total amount of traffic used by ESX. Due to a little overhead of the TCP protocol the amount of incoming data totals to slightly more than 10 GB. As might be concluded based on the graphs of Figure 22, DS probably transfers its data to scan not via the NIC of the protected VM but via the vShield VMCI interface. For this reason it is also not visible in this graph.



(a) Average

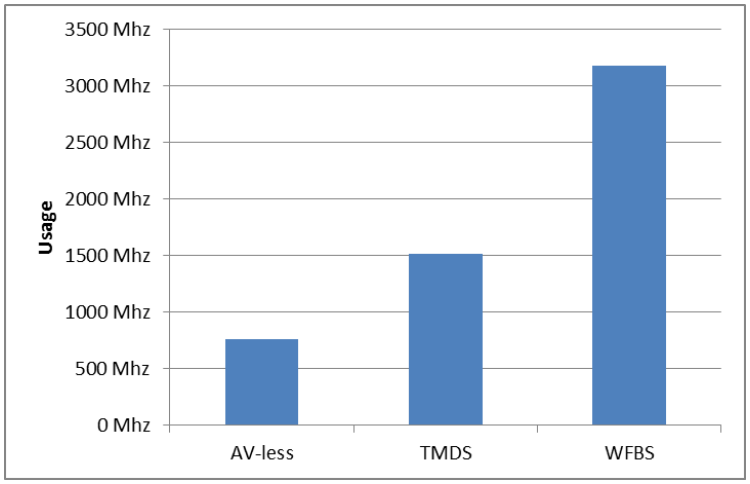


(b) Commutative

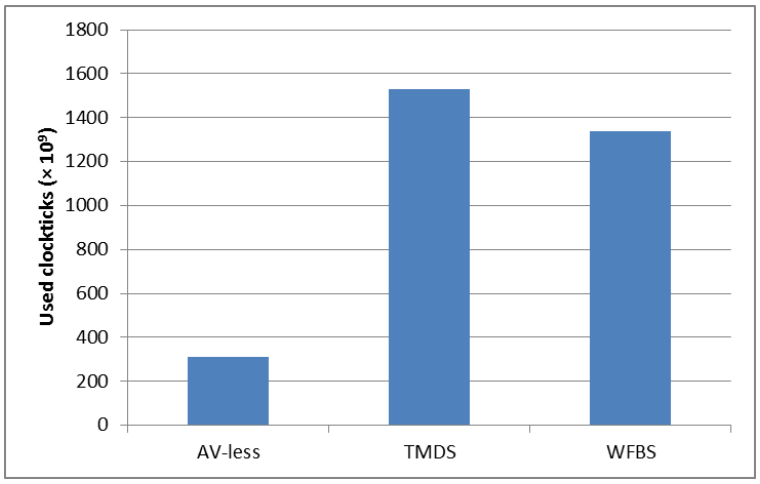
Figure 31: Comparison of Commutative and Average Disk Usage

Due to the lower incoming network speed, also the write speed to the VHD is slower compared to the speed of the AV-less configuration and WFBS. Furthermore, DS also has a significantly higher disk read rate compared to the two other configurations. Both the AV-less and WFBS configuration have a similar disk write rate and both of them barely read any data from the VHD because in the environment without antivirus there is no need to, and in case of WFBS its architecture appears to be designed to scan the files prior to writing them to disk. These statistics are visually shown in Figure 31(a).

Multiplying the duration of the disk read and write time with its respective speeds, the chart in Figure 31 is compiled. Similar to the commutative incoming network traffic shown in Figure 30, the amount of written data is around 10 GB while in case of DS the data read from disk is slightly more than 7 GB.



(a) Average



(b) Commutative

Figure 32: Comparison of Average and Commutative CPU Usage

Figure 32(a) shows the average CPU usage during the file transfer. Without antivirus software having to scan every file, the CPU is also busy to process the incoming network traffic and write it to disk. From this chart it is clear that WFBS uses the CPU to its maximum during the time the files are transferred while DS uses half of it. However,

when combining the usage with the time it took to finish the benchmark in Figure 32(b), DS uses about 10 percent more CPU power compared to WFBS to write the 10 GB data transfer to disk having scanned every file for viruses.

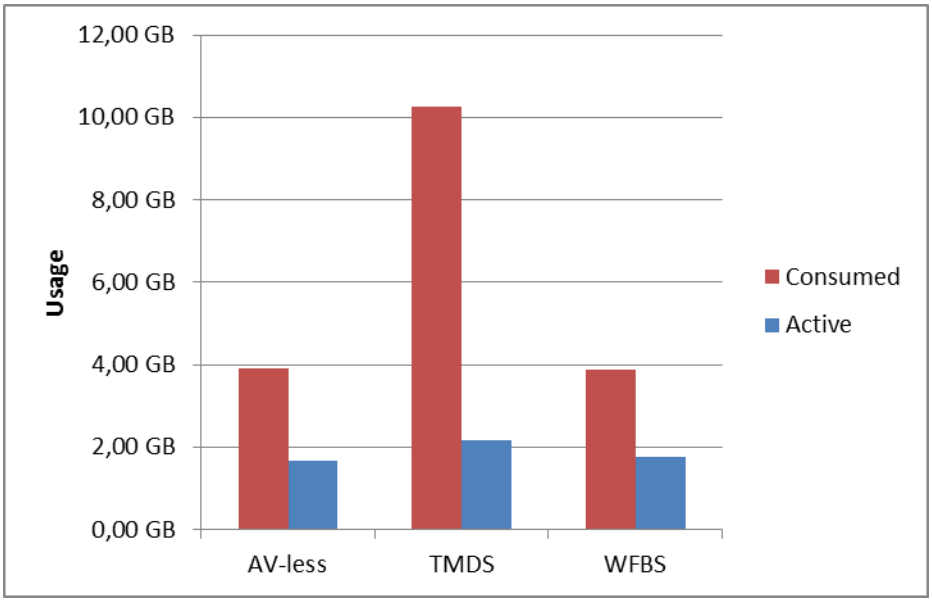


Figure 33: Comparison of Commutative Memory Usage

In the chart of Figure 33 is shown that both the AV-less and WFBS configuration have a similar memory usage. This is because in addition to the AV-less configuration, WFBS only adds the antivirus application to the Windows 7 VM. As shown in Table 14 in paragraph 9.3, DS however adds the DSVA VM and VMware vShield Manager VA to this server. In addition to that DS also requires the DS Manager running which in this case, due to limited harddisk space on the benchmark server, is running on a different server. Looking again at Table 14 shows this would add 4 GB of consumed and 0.5 GB of active memory to DS's column resulting in a total memory consumption of respectively 14.5 and 2.5 GB of memory. This amount of consumed memory is almost 4 times the amount of memory needed for the AV-less and WFBS configuration.

Summary of Remarkable Results

Test VM Memory Every graph shows that the Windows 7 VM's consumed memory has been at its maximum possible memory (See Table 10) during the whole benchmark. An explanation can be that due to the fact that the VM is first left idle for 10 minutes (See the Methodology in paragraph 9.3) during which Windows prefetches data into memory in order to perform faster. This leads to ESX reserving more memory for the VM until the moment it reached its assigned amount of memory. Furthermore, each graph shows that during the test, the amount of active memory of the Windows 7 VM increases. A possibility is that this memory is used as a buffer between the NIC and relatively slow harddisk. In case of configurations running AV software, memory can be used to perform an in-memory scan or copy the data to DSVA in case of respectively WFBS and DS.

Transfer Speeds Although transfer speeds barely differ when comparing configurations with other VMs either idle or busy, a remarkable result is that the transfer speed is sometimes even slightly faster when the other VMs are busy compared to the same test while other VMs are idle. An explanation for this could be that in this case the benchmarks with other VMs idle are conducted prior to the benchmarks with other VMs being busy. Looking at Table 20 in Appendix B shows that there is a trend that the transfer slightly decreases each subsequent test. This behavior can be caused by ESX or Windows 7 assigning more priority and consequently more resources to its transferring components because of the intensive usage of the network.

Transfer Peak In each of the configurations at the end of every transfer, a peak in transfer speed can be observed. Because this peak is clearly visible in each of the antivirus configurations it must have something to do with the ESX host. An explanation could be that this is caused by ESX fetching data from the NIC's buffer and regulating it to the correct VM. Moreover, at the end of the transfer a peak in network, disk and CPU usage can be noticed. The explanation of this can be that the source VM which resides on a different server buffered its files in memory and copied the last files from its memory to the destination host. As memory is much faster than a harddisk, this lead to a high peak at the end. Further research has to be done to give a clearer explanation for this. This has been added to Future Work in Chapter 11.

DSVA Datatransfer Another remarkable observation is the fact that both Figure 22 and Figure 23 show that the 10 GB of benchmark data is written to the Windows 7 VM's disk, however only 7 GB is read from the disk and sent to the DSVA. A possible explanation of this behavior could be that only filetypes that could be malicious are sent to the DSVA or chunks of files are sent to the DSVA after which more data is requested in case it could be malicious. Another possibility is that data from the Windows 7 VM is compressed when being sent to the DSVA. When manually testing compressing the files using the basic compression algorithm of 7-Zip, it results in a file with the size of

25 percent of the original file. However, for the data to be compressed the full 10 GB have to be read from disk after which it can be compressed resulting in less amount of data being inputted on the NIC of the DSVA. In this case however, only 7 GB is read from disk and also 7 GB is transferred over the DSVA NIC.

WFBS CPU usage An explanation for the fact that the CPU is still busy for a while after the NIC is already idle could be that instead of slowing down the NIC transfer speed, a queue of files that still have to be scanned is compiled which is still being processed at the moment the network transfer has already finished. If that is the case, the files not yet scanned are kept in memory and written to disk after being scanned which matches the amount of the VM's active memory in Figure 24(d). From the ESX statistics however, it is not possible to see by which process the active memory is being used. Therefore it cannot be concluded that WFBS is flushing its cache to disk while scanning it for malware.

9.6. Conclusion

Based on the benchmark results several conclusions can be drawn. Firstly, in this test environment, WFBS performance-wise matches the transfer speed of an AV-less environment while DS's transfer speed was less than half of it. The writing performance of the VHD is in all of the cases similar to the transfer speed over the network while in case of WFBS no data is being read from the disk. DS however also reads data from the VHD at a speed of about 70 percent of its writing speed. A clear reason for this behavior cannot be provided within the scope of this research.

When looking at CPU usage within the Windows 7 VM, DS uses the least CPU power while WFBS uses all of the VM's CPU power. However, when looking at ESX's CPU usage, DS has significantly more CPU usage although WFBS still uses twice this amount. Due to DS's increased transfer time compared to WFBS, both solutions still use a similar amount of accumulated processing power.

Comparing memory usage, DS uses the most memory by far. While the WFBS software barely increases the memory usage of the Windows 7 VM, the required DS VAs does increase the memory usage greatly. Although on a large scale HVD environment the memory usage might not increase drastically, many VMs can be running WFBS before it is more efficient in terms of memory to run DS instead of WFBS.

On the other hand looking at CPU usage, because all malware scanning is confined to a single VM, when on multiple VMs there is a lot of file activity, the server's CPU will not be overloaded by all the virus scanning processes running. Instead the DSVA will be very busy up to the limit of the hardware assigned to that VM while the virtualized workstations running on that server will be responsive. In case of WFBS this situation would lead to all VMs using their full CPU each resulting in an excessive amount of CPU usage on the physical hosts which slows down the system's overall responsiveness. A disadvantage of DSVA however is that the DSVA is likely to be a bottleneck in file transfers.

The conclusion based on the performance tests conducted in this test environment therefore is that WFBS performs more than three times faster than DS in data transfers, has less disk usage and uses one third of the memory being used by DS. On the other hand the performance-related advantage of DS is that the Windows 7 VM uses less than one-sixth of WFBS's CPU power and is therefore much more responsive to the end user.

A note can be made regarding the scalability of these results. Because the hardware used in this test environment is possibly not representative for hardware used in a real life environment, it was able to simulate the performance of both DS and WFBS only on a scale of around 10 PCs. A much brighter result could be accomplished for DS in case this test would have been conducted on an environment of hundreds of VMs running on top of several physical hosts. Based on the current results, this would probably result in excessive CPU usage of WFBS when executing multiple file transfers simultaneously

while DS preserves the host's stability due to the containment of the virusscan in the VA.

This benchmark did not include tests in manageability, security and system performance for periodic full system scans as explained in Chapter 5.3. A big advantage of DS is that no AV software has to be installed and newly created VMs are immediately protected with the latest antivirus updates. Furthermore, full system scans can be run which take into account that the VM because they are virtualized are running on one physical host and are therefore able to prevent antivirus storms. Finally, improved security is possible because only the DSVA needs access to the Internet download updates while the others can be blocked access to the Internet.

10. Conclusion

The conclusion of this report has been split into two parts from which the first part deals with the content of the report and conclusions that can be drawn from the benchmark while the second part evaluates the process of the research.

10.1. Report

In this report general information about cloud computing has been provided and the three architectural layers of cloud computing have been enumerated in Chapter 2. From these three layers, the focus shifted to IaaS to further research desktop virtualization in Chapter 3. The five types of desktop virtualization are enumerated and explained and from these types, HVDs are picked to further research as its popularity is expected to grow drastically in the coming years.

After explaining the infrastructure of HVDs, a list of popular virtualization software has been compiled and for each piece of software its type from the five types of desktop virtualization software is determined in Chapter 4. Furthermore from this list leaders in the different market segments of corporate virtualization are determined. Looking in the area of virtualization in general VMware is the leader followed by Microsoft. However, when looking at HVDs, Citrix is the main supplier. With their latest products, VMware and Microsoft are also conquering the area of HVDs and are gaining market share while Citrix is losing grounds.

Taking a sidestep, the various types of malware and methods of malware detection have been explained in paragraph 5.1. After that, in Chapter 5 the three types of architectures have been enumerated which include traditional antivirus, agent-supported antivirus with centralized management and centralized antivirus without the need of agents. From these types its advantages and disadvantages have been compared resulting in the conclusion that centralizing centralizing antivirus software comes with many advantages, however a few crucial disadvantages have to be considered prior to implementation.

After looking at the possible types of architectures of antivirus software, the centralized architecture has been picked to be further researched in Chapter 6. A list of products providing centralized antivirus software has been compiled listing the platforms it works on, comparing the product's features and stating whether an agent is required. From this list, Trend Micro Deep Security (DS) running on VMware's vShield technology appeared to be the most extended and mature solution currently available. Elaborating on this result, in Chapter 7 VMware's complex product portfolio has been explained and the VMware vSphere product hierarchy has been visualized and the interaction of DSVAs, VIBs, drivers and software between the VMware vShield Endpoint and DS has been schematized and the connections between the different components has been illustrated. This resulted into a clear overview of the interdependent relations between the components of VMware vSphere and DS.

Examining the DS software in Chapter 8, it turned out that DS despite of the anti-removal measures implemented in the DS software, the antivirus protection can be disabled from within the VM which, depending on the configured time between the heartbeats and alarm threshold, remains undetected for a while before the DS Interface will show a warning to the administrator. This opens up possibilities for attackers to temporarily disable the antivirus software to use hacking tools or install malicious software.

In addition to the predominant theoretical research in the first part, the second part written in Chapter 9 consisted of running benchmarks in order to determine the performance of DS compared to Trend Micro's traditional antivirus solution WFBS with an AV-less configuration as baseline. For the preparations of the actual benchmark, an overview of hardware requirements for each of the configurations have been listed and a methodology has been written to produce accurate and relevant results during the actual benchmark. Although recent hardware has been used, the hardware might not be representative for a real life environment. Using this hardware the benchmark resulted in the conclusion that performance-wise WFBS has three times higher transfer speeds and uses much less memory compared to DS. On the other side however, the performance of workstations using DS barely decreases even a bit when processing files while in case of WFBS, all of the VM's CPU resources are used. This stable performance can be a requirement of VMs in an HVD Infrastructure.

Depending on the scale of the organization, network speed requirements and level of security needed for the virtualized workstations, a decision can be made which type of antivirus solution to implement. Organizations should therefore not immediately go for the antivirus software that is specifically developed for virtualized environments, but instead look what the advantages and disadvantages of using a virtualization-aware antivirus product are compared to using a traditional antivirus product.

10.2. Process

Choosing Topic

The research started with determining a topic related to virtualization security. Although the scope of virtualization security seemed already very specific, it turned out that within this scope there are still many possibilities of topics to research. After writing a general document about virtualization, the focus of the research shifted to antivirus software in virtualized environments.

Getting Access to VMware API

Quickly after making the decision to focus on antivirus software in virtualized environments it was clear that at that moment VMware was the leader in virtualization software and was the only one who provided the possibility for antivirus software vendors to plug-in their software into the virtualization software in order to protect the VMs. For the research of the inner workings of the communication between the VMware virtualization software and the antivirus software, it was useful to gain access to the API which makes this possible.

To get access to this vShield API, a subscription to become a Technology Alliance Partner (TAP) of VMware is needed which costs 750 dollar annually. Gaining access to this API via either the University of Twente or Radboud University turned out to be not possible. Furthermore, although there is some partnership related to consulting between Deloitte and VMware, it was not the case that some Deloitte office was already a TAP of VMware which is the only partnership that allows access to the vShield API.

After concluding that paying for the subscription was the only option to gain access, Deloitte offered the budget to become a TAP. Shortly after subscribing it was possible to login into the TAP website. Exploring the website, it however turned out that even as a TAP it is not possible to get access to the vShield API. Some research turned out that the vShield API is only accessible for TAP partners that are invited by VMware.

The thing that can be learned from this process is that if you want to start an application for something which can take a while to gain access to, first explicitly ask for the confirmation that the objective you have by filing the application and paying the possible fees will be accomplished after the process is finished.

Testing Lab

The testing lab in Israel consisted of a single server with 8 GB of memory. During the installation of the various components that are required in order to run and test DS, it turned out that the amount of memory needed had been vastly underestimated. Moving some VMs to a laptop with also 8 GB of memory (from which around 3 GBs of memory were already occupied by Windows and other applications) provided just enough memory to run the test environment.

In the Netherlands a lab has been setup with 2 laptops having both 8 GB of memory. This amount of memory was sufficient to install and run the test environment, however it was not representative when benchmarking the software. This lead to adding another server having 16 GBs of memory, enough to build a small test environment running multiple VMs simultaneously.

Things that can be learned from the process of building a testing lab are that first there should be a clear overview of software that has to run in the lab and the hardware requirements of each of the components. Furthermore, the purpose of the lab has to be defined. For example, when just testing the functionality the testing environment does not have to run optimally nor requires a big number of running client VMs while in case the purpose is to benchmark the performance of centralized antivirus software in a virtualized environment, the software has to run without being limited by any hardware limitations and the number of VMs need to be representative to a a real environment.

Actual Benchmark

After installing and configuring the testing lab, scripts have been developed to generate unique data which is used to test the performance of the different antivirus configurations. No big problems were encountered while writing the scripts. Because transferring 1 GB of data seemed to be sufficient to determine the performance all tests had been conducted transferring 1 GB of data and results had been collected and transformed into graphs. Looking at the graphs however, it turned out that the statistics of running no AV and WFBS did not result in a sufficient amount of data for comparison and to draw conclusions from. This is because of the 20 seconds intervals between ESX's statistics as further explained in Appendix A. Because of this, all tests have been conducted for a second time using 10 GB of data instead of 1 GB. This resulted in longer transfer times which generated a sufficient amount of data to create graphs and perform statistical analysis. Comparing the transfer time with the ESX statistic intervals it would have been possible to detect this issue in an earlier stage.

Writing Report

Writing the report has been done throughout the whole period. This way no information and findings are left out of the report. During the preparations of the benchmark, small notes have been made regarding every decision taken. Afterwards these notes are written in the report in a more extended form.

11. Future Work

In addition to documenting the interaction between the various components of VMware vShield Endpoint and the connected antivirus VA, future research should be done to the possibilities to break out of the VM. One might be able to break out by exploiting the VMware vShield Endpoint interface which connects the VM via the hypervisor to the antivirus VA. Furthermore other virtualization software products like Microsoft's Hyper-V which is used increasingly often should in the future be researched for its possibilities to offload antivirus software. Finally, in this report we only looked at the server side of HVDs, however research should be done how to protect the (thin) client against attacks.

Some results of the benchmark lead to questions what the reason of that specific behavior is. Researching these reasons are not in the scope of this research which is also limited by time constraints.

11.1. Microsoft Hyper-V

While this report is mainly focused on VMware vSphere, Microsoft with its Hyper-V product is also a big player in the realm of corporate virtualization. The possibilities of Microsoft's Hyper-V product can also be researched and its security can be examined. Hyper-V already provides an API which allows the inspection of network traffic[40], but looking at the rapidly developing featureset of Hyper-V, it will in the future probably also support antivirus software outside of the VM.

11.2. VMware vShield Endpoint Breakout

Centralized antivirus software besides many advantages, also brings the disadvantage that the software might be exploited so an attacker may break out of the VM to the VMware vShield Endpoint driver in the hypervisor. This would open many possibilities to the attacker including getting access to other VMs that are also using the VMware vShield Endpoint API or even exploiting the hypervisor itself. Research could be done on how vulnerable the VMware vShield Endpoint API is for attacks.

11.3. Client Protection

As this report completely focused at the server side of HVDs, research could be done on how to secure the client endpoints of the HVD environment. One can look at the hardware, drivers and client software used in order to connect the client to the HVD and interact with it. These implementations might be vulnerable to attacks too by which an attacker via the client might get access to HVD.

[40] http://technet.microsoft.com/library/hh831452.aspx

11.4. DS Behavior

During the benchmark 10 GB of data was transferred over the network and written to the harddisk of the Windows 7 VM. However, during the transfer DS also appeared to be reading 7 GB from the harddisk which was possible to correlate with the input of the DSVA NIC while expected is that the full 10 GB is being sent to the DSVA. Based on the information about the internals of DSVA in this report, research can be done how DS works internally and what the reason is only 7 GB is read when transferring 10 GB of data.

12. References

[1] Robert P. Mahowald and Connor G Sullivan. *Worldwide SaaS and Cloud Software 20122016 Forecast and 2011 Vendor Shares*. Aug. 2012. URL: http://www.idc.com/getdoc.jsp?containerId=236184.

[2] (Unattributed). *Cloud Computing - Finding the right fit among constantly evolving cloud options*. Jan. 2013. URL: http://cdwg.com/cloudguide.

[3] David Budgen et al. "Using mapping studies in software engineering". In: *Proceedings of PPIG*. 2008, pp. 195–204.

[4] E. Scholten. *Enterprise Hypervisor Comparison*. Version 5.0. Dec. 2012. URL: http://www.vmguru.nl/wordpress/wp-content/uploads/2012/12/Hypervisor-comparison.pdf.

[5] Turvey S. and T from Enex TestLab Booth. *Virtualisation suites compared*. Aug. 2012. URL: http://www.zdnet.com/virtualisation-suites-compared-7000001456/.

[6] R. Spruijt. *VDI Smackdown!* Aug. 2012. URL: http://www.pqr.com/images/stories/Downloads/whitepapers/vdi%20smackdown.pdf.

[7] T. Chiueh et al. "Stealthy deployment and execution of in-guest kernel agents". In: *Proc. of The Black Hat, USA* (2009). URL: http://www.blackhat.com/presentations/bh-usa-09/CONOVER/BHUSA09-Conover-SADEintoVM-PAPER.pdf.

[8] AV-Test Independent IT-Security Institute. *Detailed Test Reports - Corporate*. Jan. 2013. URL: http://www.av-test.org/tests/corporate-user/.

[9] Anti-Malware Test Lab. *Antivirus Software Tests for Self-Protection*. Jan. 2013. URL: http://www.anti-malware-test.com/antivirus-tests/anti-virus-self-protection-tests.

[10] L.M. Vaquero et al. "A break in the clouds: towards a cloud definition". In: *ACM SIGCOMM Computer Communication Review* 39.1 (2008), pp. 50–55.

[11] J Archer et al. "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0". In: *Cloud Security Alliance* (2011), pp. 1–177. URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[12] Kiyomi Yamada and Jeffrey Hewitt. *Gartner Identifies Three Growth Opportunities in the Server Market Through 2015*. Oct. 2012. URL: https://www.gartner.com/newsroom/id/2186615.

[13] (Unattributed). *Forecast: Hosted Virtual Desktops, Worldwide, 2012-2016, 2012 Update*. June 2012. URL: http://www.slideshare.net/cknook/vdi-communicator-customer-presentation.

[14] HP. *Enterprise Reference Architecture for Client Virtualization for HP Virtual-System: Implementing the HP Architecture for Citrix XenDesktop on Microsoft Windows Server 2008 R2 Hyper-V*. Oct. 2011. URL: http://h30613.www3.hp.com/media/files/hp-20120525190329000000-CitrixXenDesktop.pdf.

[15] T.J. Bittman et al. "Magic Quadrant for x86 Server Virtualization Infrastructure". In: *Gartner Research Note G* 213635 (2012). URL: https://www.gartner.com/technology/reprints.do?id=1-1AWDKK7&ct=120613&st=sb.

[16] Jiang Dejun, Guillaume Pierre, and Chi-Hung Chi. "EC2 Performance Analysis for Resource Provisioning of Service-Oriented Applications". In: *Proceedings of the 3rd Workshop on Non-Functional Properties and SLA Management in Service-Oriented Computing*. Nov. 2009.

[17] Rackspace. *Rackspace - Frequently Asked Questions*. May 2013. URL: http://www.rackspace.com/cloud/cloud_hosting_faq/.

[18] Brett Waldman and Iris Feng. *IDC MarketScape: Worldwide Desktop Virtualization 2012 Vendor Analysis*. Nov. 2012. URL: http://www.citrix.com/content/dam/citrix/en_us/documents/oth/idc-marketScape-2012.pdf.

[19] Morgan Stanley Research. *Hard Field Data on Virtual Desktop ROI & Adoption*. May 2011. URL: http://mobilityjourney.com/2011/06/13/vdi-market-share-view-vmware/.

[20] John Aycock. *Computer viruses and malware*. Springer Publishing Company, Incorporated, 2010.

[21] Peter Szor. *The Art of Computer Virus Research and Defense*. Addison-Wesley Professional, 2005. ISBN: 0321304543.

[22] (Unattributed). *Antivirus Best Practices for VMware View 5*. Oct. 2012. URL: https://www.vmware.com/files/pdf/VMware-View-AntiVirusPractices-TN-EN.pdf.

[23] L. Garber. "The Challenges of Securing the Virtualized Environment". In: *Computer* (2012), pp. 17–20.

[24] (Unattributed). *Deep Security 8.0 - SP1 Getting Started & Installation Guide*. 2012. URL: ftp://ftp.antivirus.com/documentation/guides/Deep%20Security%208%20Getting%20Started%20and%20Installation%20Guide.pdf.

[25] (Unattributed). *Changing the Game with Agentless Security for the Virtual Data Center*. May 2012. URL: https://www.vmware.com/files/pdf/partners/trendmicro/vmware-trendmicro-anti-virus-virtual-datacenter-sb-en.pdf.

[26] (Unattributed). *VMware - LinkedIn*. Jan. 2013. URL: https://www.linkedin.com/company/vmware.

[27] (Unattributed). *VMware vSphere Architectures Compared*. Jan. 2013. URL: https://www.vmware.com/products/vsphere/esxi-and-esx/compare.html.

[28] (Unattributed). *VMware vCenter Server Features*. Jan. 2013. URL: https://www.vmware.com/products/vcenter-server/features.html.

[29] (Unattributed). *VMware vSphere: Enterprise Cloud Computing & Virtualization Features*. Jan. 2013. URL: https://www.vmware.com/products/datacenter-virtualization/vsphere/features.html.

[30] (Unattributed). *New VMware VMsafe Technology Allows the Virtual Datacenter to Be More Secure Than Physical Environments*. Feb. 2008. URL: https://www.vmware.com/technical-resources/security/vmsafe/faq.html.

[31] (Unattributed). *What is the EPSEC (Endpoint Security) API and how is it related to VMsafe?* Jan. 2013. URL: https://www.vmware.com/technical-resources/security/vmsafe/faq.html.

[32] VMware. *VMware vShield Edge - Secure the Edge of the Datacenter*. May 2011. URL: http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Edge-Datasheet.pdf.

[33] VMware. *VMware vShield App - Protect Applications from Network-Based Attacks*. May 2011. URL: http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-App-Datasheet.pdf.

[34] VMware. *VMware vShield App with Data Security - Protect Applications from Network-Based Attacks and Discover Sensitive Data*. May 2011. URL: http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-App-with-Data-Security-Datasheet.pdf.

[35] VMware. *VMware vShield Endpoint - Enhanced Endpoint Security and Performance for Virtual Datacenters*. May 2011. URL: http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Endpoint-Datasheet.pdf.

[36] VMware. *VMware vCloud Director - Build Secure Private Clouds to Deliver Infrastructure as a Service*. May 2011. URL: http://www.vmware.com/files/pdf/vmware-vcloud-director-DS-EN.pdf.

[37] (Unattributed). *VMware vShield End of Availability Information*. Jan. 2013. URL: https://www.vmware.com/products/vshield/overview.html.

[38] (Unattributed). *VMware vCloud Networking and Security Datasheet*. Version 5.1. Aug. 2012. URL: https://www.vmware.com/files/pdf/products/vcns/VMware-vCloud-Networking-and-Security-Datasheet.pdf.

[39] (Unattributed). *VMware vShield Quick Start Guide*. Version 5.1. Dec. 2012. URL: https://www.vmware.com/pdf/vshield_51_quickstart.pdf.

[40] (Unattributed). *VXLAN - VMware Software Defined Networking*. Jan. 2013. URL: https://www.vmware.com/solutions/datacenter/vxlan.html.

[41] (Unattributed). *VMware vSphere Features - High Availability (HA)*. Jan. 2013. URL: https://www.vmware.com/products/datacenter-virtualization/vsphere/high-availability.html.

[42] VMware. *VMCI Sockets Programming Guide*. Sept. 2012. URL: https://www.vmware.com/support/developer/vmci-sdk/.

[43] (Unattributed). *Windows Server 2008 R2 Logo Program for Software*. Jan. 2013. URL: http://msdn.microsoft.com/library/windows/desktop/dd744769(v=vs.85).aspx.

[44] Mark Russinovich and Bryce Cogswell. *Sysinternals Autoruns for Windows*. Jan. 2013. URL: http://technet.microsoft.com/sysinternals/bb963902.aspx.

[45] (Unattributed). *Windows Storage Driver Architecture*. Jan. 2013. URL: http://msdn.microsoft.com/library/windows/hardware/ff566978(v=vs.85).aspx.

[46] (Unattributed). *Load Order Groups for File System Filter Drivers*. Jan. 2013. URL: http://msdn.microsoft.com/library/windows/hardware/ff549694(v=vs.85).aspx.

[47] (Unattributed). "Understanding Full Virtualization, Paravirtualization, and Hardware Assist". In: *Technical report, VMWare, Inc.* (2007). URL: https://www.vmware.com/files/pdf/VMware_paravirtualization.pdf.

[48] (Unattributed). *VMCI Sockets Programming Guide*. Jan. 2013. URL: http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/ws8x_esx51_vmci_sockets.pdf.

[49] (Unattributed). *Communication ports used by Deep Security*. Sept. 2012. URL: http://esupport.trendmicro.com/solution/en-us/1060007.aspx.

[50] (Unattributed). *Difference between the Conventional Scan and Smart Scan functions of Worry-Free Business Security (WFBS)*. Jan. 2013. URL: https://esupport.trendmicro.com/solution/en-us/1053817.aspx.

[51] (Unattributed). *What are Virtual Appliances?* Jan. 2013. URL: https://www.vmware.com/nl/appliances/getting-started/overview/.

[52] (Unattributed). *vSphere Client Hardware Health Monitoring*. Nov. 2010. URL: https://www.vmware.com/files/pdf/techpaper/hwhm41_technote.pdf.

[53] (Unattributed). *Creating a vSphere Update Manager Depot*. Aug. 2011. URL: https://www.vmware.com/files/pdf/techpaper/vsphere-50-update-manager-depot.pdf.

[54] Inc. Distributed Management Task Force. *Common Information Model (CIM) Infrastructure Specification*. Version 2.3. Oct. 2005. URL: http://www.dmtf.org/sites/default/files/standards/documents/DSP0004V2.3_final.pdf.

[55] Rob Randell. *VMware Security Briefing*. Oct. 2010. URL: http://communities.vmware.com/servlet/JiveServlet/download/1633024-44565/VMUG_Presentation.pptx.

[56] Paul Arana. *Deep Security 8.0 Deployment Guide*. July 2012. URL: http://affinitypartner.trendmicro.com/media/559904/deep_security_8.0_deployment_guide.pdf.

[57] Vojtech Morvek. *VMware & McAfee - Efficient interconnection technology vShield and MOVE*. June 2012. URL: http://www.comguard.cz/fileadmin/user_upload/sbornik/Com_Sec_Brno_2012/McAfee_VMware_29052012.pdf.

[58] Andreas Diehl. *Trend Micro - Wirkungsvolle Sicherung virtueller Rechenzentren*. Nov. 2012. URL: http://www.user2000.de/index_htm_files/DDSS%20Deep%20Security.pdf.

[59] Trend Micro. *Trend Micro Technical Support - Uninstalling Deep Security Relay (DSR)*. Feb. 2013. URL: https://esupport.trendmicro.com/solution/en-us/1060378.aspx.

[60] VMware. *VMware ESXi/ESX 4.1 and ESXi 5.0 Comparison*. June 2012. URL: http://kb.vmware.com/kb/2005377/.

[61] J.P. Gownder, Christopher Voce, and Thayer Frechette. "Navigating Diversity In Operating Systems And Browsers". In: *Forrester Research* (2013).

[62] (Unattributed). *Stresslinux FAQ*. Mar. 2011. URL: http://www.stresslinux.org/sl/wiki/FAQ/.

[63] Trend Micro. *Trend Micro - Deep Security System Requirements*. Apr. 2013. URL: http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html#system-requirements.

[64] Trend Micro. *Trend Micro Technical Support - Information about the embedded database option in Deep Security*. Feb. 2013. URL: https://esupport.trendmicro.com/solution/en-us/1055083.aspx.

[65] VMware. *VMware Knowledge Base - Best practices for virtual machine snapshots in the VMware environment*. Oct. 2012. URL: http://kb.vmware.com/kb/1025279/.

[66] VMware. *VMware Knowledge Base - Understanding virtual machine snapshots in VMware ESXi and ESX*. Aug. 2012. URL: http://kb.vmware.com/kb/1015180/.

[67] VMware. *Performance study of VMware vStorage thin provisioning*. Nov. 2009. URL: https://www.vmware.com/pdf/vsp_4_thinprov_perf.pdf.

[68] Ravi Venkat. *VM Performance on Flash Part 2: Thin vs. Thick Provisioning Does it Matter?* Feb. 2012. URL: http://www.purestorage.com/blog/vm-performance-on-flash-part-2-thin-vs-thick-provisioning-does-it-matter/.

[69] VMware. *VMware Communities - vCenter Performance Counters*. Jan. 2011. URL: http://communities.vmware.com/docs/DOC-5600/.

[70] VMware. *Understanding Memory Resource Management in VMware ESX Server*. Aug. 2009. URL: https://www.vmware.com/files/pdf/perf-vsphere-memory_management.pdf.

[71] Microsoft. *Windows On/Off Transition Performance Analysis*. Apr. 2011. URL: http://msdn.microsoft.com/library/windows/hardware/gg463386.aspx.

[72] Claus Witjes and Arne Stremlau. *The Windows 7 Boot Process (sbsl)*. Oct. 2012. URL: https://social.technet.microsoft.com/wiki/contents/articles/11341.the-windows-7-boot-process-sbsl.aspx#OS_Initialization.

[73] Matt Conover and Tzi cker Chiueh. *Code Injection From the Hypervisor: Removing the need for in-guest agents*. 2009. URL: https://www.blackhat.com/presentations/bh-usa-09/CONOVER/BHUSA09-Conover-SADEintoVM-SLIDES.pdf.

[74] Chirag Modi et al. "A survey of intrusion detection techniques in Cloud". In: *Journal of Network and Computer Applications* 0 (2012), pp. –. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2012.05.003. URL: http://www.sciencedirect.com/science/article/pii/S1084804512001178.

[75] K. Scarfone. *Guide to Security for Full Virtualization Technologies*. DIANE Publishing, 2001, Chapter 3.1.

[76] AMD. *AMD64 Virtualization Codenamed "Pacifica" Technology - Secure Virtual Machine Architecture Reference Manual*. May 2005. URL: http://support.amd.com/us/Embedded_TechDocs/24593.pdf.

[77] L. van Doorn. "Hardware virtualization trends". In: *ACM/Usenix International Conference On Virtual Execution Environments: Proceedings of the 2 nd international conference on Virtual execution environments*. Vol. 14. 16. 2006, pp. 12–13.

[78] Intel. "Intel 64 and IA-32 Architectures Software Developer's Manual". In: *Volume-3C: System Programming Guide, Part 3* (Aug. 2012). URL: http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html.

[79] Daniel J. Sanok Jr. "An analysis of how antivirus methodologies are utilized in protecting computers from malicious code". In: *Proceedings of the 2nd annual conference on Information security curriculum development*. InfoSecCD '05. New York, NY, USA: ACM, 2005, pp. 142–144. ISBN: 1-59593-261-5. DOI: 10.1145/1107622.1107655. URL: http://doi.acm.org/10.1145/1107622.1107655.

[80] (Unattributed). *VMware Technology Alliance Partner(TAP) Program Guide*. Version 3.0. May 2012. URL: https://www.vmware.com/files/pdf/partners/TAP-Program-Guide.pdf.

[81] (Unattributed). *Intel Delivers New Era For Virtualization*. Nov. 2005. URL: http://web.archive.org/web/20051124123850/http://www.intel.com/pressroom/archive/releases/20051114comp.htm.

[82] (Unattributed). *AMD Delivers Desktop Product Powerhouse While Reducing Costs For Ecosystem Partners*. May 2006. URL: http://www.amd.com/us/press-releases/Pages/Press_Release_108605.aspx.

[83] Trend Micro. *VMware vShield Endpoint + Trend Micro Deep Security*. Jan. 2013. URL: http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/sb_vmware-agentless-security.pdf.

[84] A.W. Huijgen. "A Glance at the Virtualization Landscape". In: 2012.

13. Appendices

A. Problems Encountered

This appendix will describe the problems encountered during the research and the discoveries that became clear.

Difference between Intel and AMD Virtualization Instructions

While it initially seemed that Intel VT-x and AMD-V implemented a similar instruction set, it turned out that virtualization instructions differ.[77] Furthermore, the Intel instructionset contains more virtualization-related instructions than the AMD instructionset.[84]

Leaked VMware ESX Source Code

Recently hackers published the source code they supposedly some years ago stole from VMware.[41] This leak could have been useful for researching how VMware ESX/vSphere works internally, however, the source dates from between 1998 and 2004. At the end of November 2005, Intel released its first processors that include the VT-x virtualization extension.[81] Furthermore, AMD released its first processors that support virtualization in the second quarter of 2006.[82] As the most recent change of the leaked VMware ESX source dates to 2004, this means the source does not include support for the virtualization instructions of either of the processor vendors.

Trend Micro Deep Security Installation/Configuration

Because of the limited amount of memory available in the server and the unexpected large amount of VAs and VMs that are required to be able to use centralized antivirus software, an additional computer had to be configured to also run a few of the VMs. Furthermore, as VMware vShield and DS are complex products with lots of configuration settings, it took some time to figure out the correct settings. Settings that had to be configured are the various servers, services and ports, DNS configuration and IP configuration. Furthermore, a few times some appliances and services were not able to communicate with each other. One time this problem could only be solved by reinstalling and reconfiguring the various servers.

Different APIs

VMware provides a variety of public APIs (VIX API, CIM API, SRM API and more[42]) and in addition to that, private APIs which include an API which can be used to do introspection. It took a while before it was clear which API from the variety of VMware APIs was required for introspection.

[41] https://twitter.com/57UN/status/265000884159774720
[42] https://www.vmware.com/support/pubs/sdk_pubs.html

VMware vSphere Hypervisor Reset

The VMware vSphere Hypervisor provides a feature to reset all settings of the Hypervisor to its defaults. For the research after messing the environment up, it was needed to have a clean start to perform the installation of VMware vShield and DS and compare the list of kernel modules, processes, VIBs and document the steps executed. It turned out however, that even after executing the factory reset of the VMware vSphere Hypervisor, installed kernel modules and VIBs are still there! This thus required another installation, completely removing from the harddisk and reinstalling the VMware vSphere Hypervisor from the original installation media.

Access to VMware vShield API

After paying and registering for the VMware TAP program, you need to register for an additional program to get access to the specific API programs which includes the VMware vShield API.[43]

To be able to access the VMware vShield API, it stated on the website that one has to be a VMware TAP at at least the Access Level.[80] After going through the process of subscribing for this program and paying for the subscription, it however turned out that in order to get access to the VMware vShield API, even only the documentation, you have to be invited by the TAP program manager. After sending lots of e-mails back and forth to VMware we got a reply from a member of the TAP team stating that the VMware vShield API is only available to members of the VMware Elite TAP program and in addition to that members have to be invited to get access. This mail unfortunately ended the repeated attempts to get access to the VMware vShield API as it appears only well-known antivirus companies are allowed access to this API.

Getting Windows up-to-date

While building the test environment, Windows 7 x64 Professional has been downloaded from the Microsoft Developer Network (MSDN) Academic Alliance (MSDNAA) library of the University of Twente. After downloading this DVD was used to install Windows assuming that it was the most recent version. After the installation while running the updates however, it turned out that Windows Updated wanted to install Service Pack (SP) 1 for Windows 7 x64. Because it is not clear whether installing SP 1 afterwards has any implications on the performance of the OS compared to having SP 1 integrated in the installation DVD and because the Internet connection is not very fast to download SP 1, the decision was taken to install a new VM with Windows 7 x64 Enterprise. The installation went fast and although there were quite a lot of updates, SP 1 did not have to be installed so the updates did not take very long to finish.

[43] http://www.vmware.com/partners/programs/alliances/co-dev/api.html

StressLinux

StressLinux can be downloaded as both a VMware image and a bootable CD. As it had to be placed on VMware ESX, the decision was made to download the VMware image. However, after importing the image into VMware ESX using VMware vSphere Client, problems were reported by ESX when trying to boot the VM which had as result that the VM was not started. Finally the solution appeared to be to use the VMware Converter application[44] using the downloaded VMware image as source and the ESX server as destination. After the import finished it was possible to successfully boot the VM.

StressLinux was used to add some additional load on the hardware in order to test how the antivirus software would perform. Three StressLinux instances were placed on the ESX server running the tests and were aimed to all use one core of their virtual dual core processor and in the meanwhile use 1,5 GB of memory. However, when running the stress tool in StressLinux instructing it to emulate this load, it turned out it was using both of the cores which exhausted the full physical CPU. The solution for this problem appeared to be to only instruct the stress tool to fill up the 1,5GB of memory which apparently uses one full core of CPU power to perform operations on the reserved memory in order to keep it active.

Benchmarking using ESX #1

Due to the fact that ESX statistics are taken in intervals of 20 seconds, in the case of DS and WFBS the transfer time of 1 GB of data was too short to be able to use it as input for comparison. When using the 1 GB benchmark in Figure 34 as an example: the average time over 3 runs was 18 seconds for 1024 MB of data resulting in an average speed of almost 57 MB/s. However, the graph shows that maximum transfer speed has been a little bit more than 35 MB/s at its peak while the next 20 seconds its speed is slowing down to a little bit more than 15 MB/s after which the speed gradually drops to 0 MB/s. The following is happening: after 20 seconds ESX calculates an average of the first 20 seconds which in this case looking at Table 16 is 36.8 MB/s. After again recording for 20 seconds, the average speed is 16.9 MB/s. Finally the average transfer speed is 0 again. When calculating the amount of MBs transferred during these moments in time, the numbers turn out to be correct: $20 \cdot 36.8 + 20 \cdot 16.9 = 1074$, however the graphs are not clear. Therefore all tests had to be executed again, but this case with 10 GB of data instead of 1 GB in order to collect enough data to be able to plot a useful graph.

Benchmarking using ESX #2

In some cases, the statistics saved from VMware ESX had to be slightly adjusted. The problem in these cases was that the harddisk had already been writing at full speed in

[44] http://www.vmware.com/products/converter/

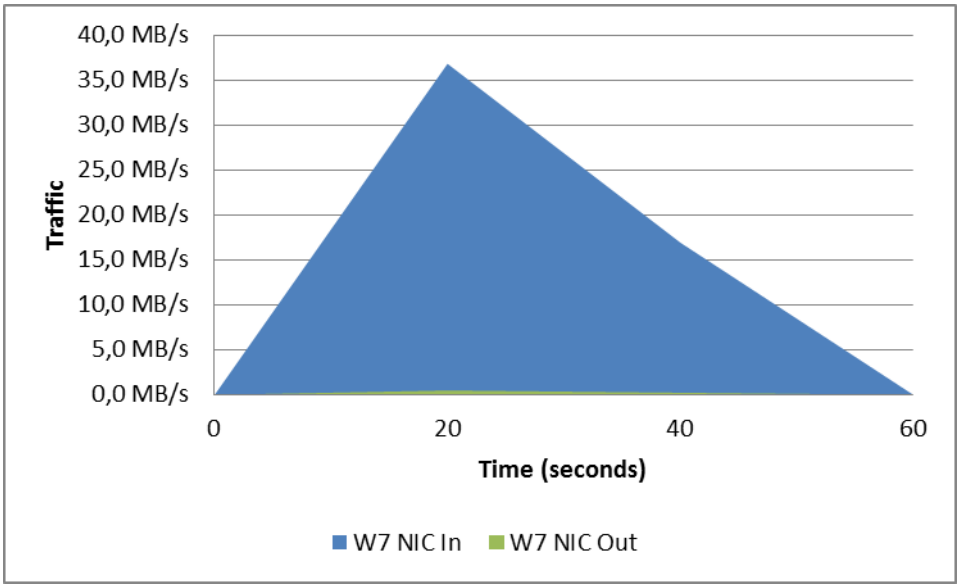


Figure 34: NIC speed of AV-less configuration while transferring 1 GB of data and other VMs are idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	00,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	26 Mhz	1,50 GB	0,87 GB
20	36,8 MB/s	0,5 MB/s	0,1 MB/s	27,9 MB/s	897 Mhz	1,50 GB	0,87 GB
40	16,9 MB/s	0,2 MB/s	14,2 MB/s	22,3 MB/s	783 Mhz	1,50 GB	0,87 GB
60	0,0 MB/s	0,0 MB/s	0,9 MB/s	0,0 MB/s	27 Mhz	1,50 GB	1,15 GB

Table 16: AV-lessWindows 7 VM while transferring 1 GB of data and other VMs are idle

while looking at the NIC no data had been transferred yet at all. Because ESX measures the average over 20 seconds, it is also not possible that sending an allocation request (assuming these exist in the Server Message Block (SMB) protocol) makes the disk write at full speed prior to receiving the actual data. This behavior has also not been observed while looking at the xcopy command[45] used in the benchmarking script of Appendix G. The adjustments have been carried out by shifting all values of either the network or the disk column up by one, synchronizing it with the values in the other columns.

[45] technet.microsoft.com/library/cc771254(v=ws.10).aspx

B. Benchmark Results

Boot Times

	Run 1	Run 2	Run 3	Run 4	Run 5	Average
PreSMSS:	5458	5348	5639	5342	5282	**5414**
SMSSInit:	1961	1989	1782	2253	2733	**2144**
WinlogonInit:	1213	1053	748	755	752	**904**
ExplorerInit:	405	659	428	500	411	**481**
PostExplorerPeriod:	3800	3200	3400	3800	3800	**3600**
bootDoneViaPostBoot:	**12839**	**12251**	**11999**	**12650**	**12979**	**12544**

Table 17: Timings in Milliseconds for Boot Stages of VM without AV software

	Run 1	Run 2	Run 3	Run 4	Run 5	Average
PreSMSS:	6861	7899	8047	8177	8108	**7818**
SMSSInit:	1079	857	868	856	868	**906**
WinlogonInit:	1848	1346	1285	910	1229	**1324**
ExplorerInit:	847	701	650	1160	535	**779**
PostExplorerPeriod:	5200	5100	5000	4700	5100	**5020**
bootDoneViaPostBoot:	**15836**	**15905**	**15852**	**15805**	**15842**	**15848**

Table 18: Timings in Milliseconds for Boot Stages of VM running DS

	Run 1	Run 2	Run 3	Run 4	Run 5	Average
PreSMSS:	4868	4824	4837	4854	4845	**4846**
SMSSInit:	1363	1052	1054	1503	1065	**1207**
WinlogonInit:	1799	1783	1959	1941	1289	**1754**
ExplorerInit:	697	523	555	687	503	**593**
PostExplorerPeriod:	9200	10100	10300	10700	10500	**10160**
bootDoneViaPostBoot:	**17929**	**18284**	**18707**	**19687**	**18204**	**18562**

Table 19: Timings in Milliseconds for Boot Stages of VM running WFBS

Transfer Speeds

	Run 1	**Run 2**	**Run 3**	**Avg**	**Mbit**
No Antivirus	382	329	334	**348**	**235**
No Antivirus (other VMs busy)	328	330	336	**331**	**247**
DS	985	925	889	**933**	**88**
DS (other VMs busy)	871	876	883	**877**	**93**
WFBS	394	388	386	**389**	**210**
WFBS (other VMs busy)	401	401	398	**400**	**205**

Table 20: Transfer Times in Seconds and Transfer Speed in Mbits when Transferring 10GB of Data

Performance: AV-less, other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	158 Mhz	3,89 GB	1,28 GB
20	18,7 MB/s	0,2 MB/s	0,0 MB/s	0,0 MB/s	540 Mhz	3,89 GB	1,26 GB
40	28,6 MB/s	0,3 MB/s	0,0 MB/s	8,9 MB/s	811 Mhz	3,90 GB	1,01 GB
60	31,1 MB/s	0,3 MB/s	0,0 MB/s	28,1 MB/s	876 Mhz	3,89 GB	1,00 GB
80	31,2 MB/s	0,3 MB/s	0,0 MB/s	30,2 MB/s	813 Mhz	3,89 GB	1,40 GB
100	32,4 MB/s	0,3 MB/s	0,0 MB/s	30,1 MB/s	842 Mhz	3,89 GB	1,50 GB
120	26,8 MB/s	0,3 MB/s	0,0 MB/s	31,6 MB/s	794 Mhz	3,89 GB	1,59 GB
140	31,8 MB/s	0,3 MB/s	0,0 MB/s	25,9 MB/s	831 Mhz	3,89 GB	1,75 GB
160	31,5 MB/s	0,3 MB/s	0,0 MB/s	30,9 MB/s	816 Mhz	3,90 GB	1,77 GB
180	32,6 MB/s	0,3 MB/s	0,0 MB/s	30,7 MB/s	869 Mhz	3,90 GB	1,77 GB
200	30,8 MB/s	0,3 MB/s	0,0 MB/s	30,5 MB/s	805 Mhz	3,90 GB	1,81 GB
220	29,8 MB/s	0,3 MB/s	0,0 MB/s	30,0 MB/s	789 Mhz	3,90 GB	1,85 GB
240	32,0 MB/s	0,3 MB/s	0,0 MB/s	29,5 MB/s	886 Mhz	3,90 GB	1,85 GB
260	28,6 MB/s	0,3 MB/s	0,0 MB/s	30,4 MB/s	760 Mhz	3,90 GB	1,85 GB
280	27,5 MB/s	0,3 MB/s	0,0 MB/s	27,6 MB/s	740 Mhz	3,90 GB	1,87 GB
300	36,4 MB/s	0,4 MB/s	0,0 MB/s	27,3 MB/s	962 Mhz	3,90 GB	1,86 GB
320	41,3 MB/s	0,5 MB/s	0,0 MB/s	35,6 MB/s	1081 Mhz	3,90 GB	1,86 GB
340	22,8 MB/s	0,3 MB/s	0,0 MB/s	40,5 MB/s	797 Mhz	3,90 GB	1,85 GB
360	9,6 MB/s	0,1 MB/s	3,9 MB/s	25,9 MB/s	407 Mhz	3,90 GB	1,86 GB
380	9,8 MB/s	0,1 MB/s	0,0 MB/s	10,9 MB/s	364 Mhz	3,90 GB	1,87 GB
400	0,0 MB/s	0,0 MB/s	0,1 MB/s	16,4 MB/s	332 Mhz	3,90 GB	1,90 GB
420	0,0 MB/s	0,0 MB/s	5,8 MB/s	3,3 MB/s	136 Mhz	3,89 GB	1,94 GB
440	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	113 Mhz	3,89 GB	1,93 GB

Table 21: ESX without AV software while other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	23 Mhz	2,00 GB	1,10 GB
20	18,8 MB/s	0,2 MB/s	0,0 MB/s	0,0 MB/s	411 Mhz	2,00 GB	0,85 GB
40	28,6 MB/s	0,3 MB/s	0,0 MB/s	8,9 MB/s	635 Mhz	2,00 GB	0,85 GB
60	31,2 MB/s	0,3 MB/s	0,0 MB/s	28,1 MB/s	687 Mhz	2,00 GB	1,25 GB
80	31,2 MB/s	0,3 MB/s	0,0 MB/s	30,2 MB/s	664 Mhz	2,00 GB	1,34 GB
100	32,5 MB/s	0,3 MB/s	0,0 MB/s	30,0 MB/s	678 Mhz	2,00 GB	1,42 GB
120	26,9 MB/s	0,3 MB/s	0,0 MB/s	31,6 MB/s	609 Mhz	2,00 GB	1,56 GB
140	31,9 MB/s	0,3 MB/s	0,0 MB/s	25,9 MB/s	681 Mhz	2,00 GB	1,58 GB
160	31,5 MB/s	0,3 MB/s	0,0 MB/s	30,8 MB/s	655 Mhz	2,00 GB	1,58 GB
180	32,7 MB/s	0,3 MB/s	0,0 MB/s	30,6 MB/s	693 Mhz	2,00 GB	1,65 GB
200	30,8 MB/s	0,3 MB/s	0,0 MB/s	30,5 MB/s	657 Mhz	2,00 GB	1,69 GB
220	29,9 MB/s	0,3 MB/s	0,0 MB/s	30,0 MB/s	630 Mhz	2,00 GB	1,69 GB
240	32,1 MB/s	0,3 MB/s	0,0 MB/s	29,4 MB/s	698 Mhz	2,00 GB	1,69 GB
260	28,7 MB/s	0,3 MB/s	0,0 MB/s	30,4 MB/s	617 Mhz	2,00 GB	1,71 GB
280	27,5 MB/s	0,3 MB/s	0,0 MB/s	27,5 MB/s	591 Mhz	2,00 GB	1,71 GB
300	36,5 MB/s	0,4 MB/s	0,0 MB/s	27,3 MB/s	779 Mhz	2,00 GB	1,71 GB
320	41,4 MB/s	0,5 MB/s	0,0 MB/s	35,5 MB/s	917 Mhz	2,00 GB	1,71 GB
340	22,8 MB/s	0,3 MB/s	0,0 MB/s	40,5 MB/s	644 Mhz	2,00 GB	1,71 GB
360	9,7 MB/s	0,1 MB/s	3,9 MB/s	25,8 MB/s	252 Mhz	2,00 GB	1,71 GB
380	9,8 MB/s	0,1 MB/s	0,0 MB/s	10,4 MB/s	247 Mhz	2,00 GB	1,74 GB
400	0,0 MB/s	0,0 MB/s	0,0 MB/s	16,2 MB/s	206 Mhz	2,00 GB	1,76 GB
420	0,0 MB/s	0,0 MB/s	5,8 MB/s	3,2 MB/s	21 Mhz	2,00 GB	1,76 GB
440	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	18 Mhz	2,00 GB	1,80 GB

Table 22: Windows 7 VM without AV Software while other VMs idle

Performance: AV-less, other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	7035 Mhz	6,93 GB	4,47 GB
20	15,9 MB/s	0,2 MB/s	0,0 MB/s	6,8 MB/s	7555 Mhz	6,93 GB	4,47 GB
40	29,5 MB/s	0,3 MB/s	0,0 MB/s	28,2 MB/s	7947 Mhz	6,93 GB	4,47 GB
60	30,8 MB/s	0,3 MB/s	0,0 MB/s	29,0 MB/s	8000 Mhz	6,93 GB	4,46 GB
80	31,9 MB/s	0,3 MB/s	0,0 MB/s	32,6 MB/s	8005 Mhz	6,93 GB	4,46 GB
100	30,0 MB/s	0,3 MB/s	0,0 MB/s	28,4 MB/s	7947 Mhz	6,93 GB	4,71 GB
120	29,6 MB/s	0,3 MB/s	0,0 MB/s	28,5 MB/s	7939 Mhz	6,93 GB	4,76 GB
140	29,5 MB/s	0,3 MB/s	0,0 MB/s	28,3 MB/s	7947 Mhz	6,93 GB	4,83 GB
160	31,3 MB/s	0,3 MB/s	0,0 MB/s	30,9 MB/s	7970 Mhz	6,93 GB	4,91 GB
180	31,2 MB/s	0,3 MB/s	0,0 MB/s	30,1 MB/s	7980 Mhz	6,93 GB	5,02 GB
200	30,9 MB/s	0,3 MB/s	0,0 MB/s	30,5 MB/s	8021 Mhz	6,93 GB	4,95 GB
220	37,0 MB/s	0,4 MB/s	0,0 MB/s	34,3 MB/s	8134 Mhz	6,93 GB	5,10 GB
240	41,2 MB/s	0,4 MB/s	0,0 MB/s	41,8 MB/s	8233 Mhz	6,93 GB	5,12 GB
260	26,6 MB/s	0,3 MB/s	0,0 MB/s	25,6 MB/s	7930 Mhz	6,93 GB	5,20 GB
280	31,8 MB/s	0,3 MB/s	0,0 MB/s	30,9 MB/s	7980 Mhz	6,93 GB	5,18 GB
300	35,2 MB/s	0,4 MB/s	0,0 MB/s	33,6 MB/s	8058 Mhz	6,93 GB	5,16 GB
320	43,6 MB/s	0,4 MB/s	0,0 MB/s	40,7 MB/s	8367 Mhz	6,93 GB	5,18 GB
340	27,1 MB/s	0,3 MB/s	4,4 MB/s	33,1 MB/s	8215 Mhz	6,93 GB	5,13 GB
360	0,2 MB/s	0,0 MB/s	4,3 MB/s	2,9 MB/s	7130 Mhz	6,93 GB	5,11 GB
380	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,2 MB/s	7025 Mhz	6,93 GB	5,11 GB

Table 23: ESX without AV software while other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	48 Mhz	2,00 GB	1,07 GB
20	16,0 MB/s	0,2 MB/s	0,0 MB/s	0,0 MB/s	494 Mhz	2,00 GB	1,07 GB
40	29,5 MB/s	0,3 MB/s	0,0 MB/s	6,8 MB/s	902 Mhz	2,00 GB	1,07 GB
60	30,8 MB/s	0,3 MB/s	0,0 MB/s	28,1 MB/s	922 Mhz	2,00 GB	1,06 GB
80	32,0 MB/s	0,3 MB/s	0,0 MB/s	29,0 MB/s	950 Mhz	2,00 GB	1,09 GB
100	30,1 MB/s	0,3 MB/s	0,0 MB/s	32,6 MB/s	885 Mhz	2,00 GB	1,37 GB
120	29,7 MB/s	0,3 MB/s	0,0 MB/s	28,3 MB/s	878 Mhz	2,00 GB	1,41 GB
140	29,5 MB/s	0,3 MB/s	0,0 MB/s	28,5 MB/s	896 Mhz	2,00 GB	1,51 GB
160	31,4 MB/s	0,3 MB/s	0,0 MB/s	28,3 MB/s	914 Mhz	2,00 GB	1,57 GB
180	31,3 MB/s	0,3 MB/s	0,0 MB/s	30,9 MB/s	920 Mhz	2,00 GB	1,67 GB
200	31,0 MB/s	0,3 MB/s	0,0 MB/s	30,0 MB/s	947 Mhz	2,00 GB	1,67 GB
220	37,1 MB/s	0,4 MB/s	0,0 MB/s	30,4 MB/s	1058 Mhz	2,00 GB	1,69 GB
240	41,3 MB/s	0,4 MB/s	0,0 MB/s	34,3 MB/s	1193 Mhz	2,00 GB	1,71 GB
260	26,6 MB/s	0,3 MB/s	0,0 MB/s	41,8 MB/s	875 Mhz	2,00 GB	1,74 GB
280	31,9 MB/s	0,3 MB/s	0,0 MB/s	25,6 MB/s	922 Mhz	2,00 GB	1,74 GB
300	35,3 MB/s	0,4 MB/s	0,0 MB/s	30,9 MB/s	1012 Mhz	2,00 GB	1,72 GB
320	43,8 MB/s	0,4 MB/s	0,0 MB/s	33,5 MB/s	1279 Mhz	2,00 GB	1,73 GB
340	27,2 MB/s	0,3 MB/s	0,0 MB/s	40,7 MB/s	1178 Mhz	2,00 GB	1,73 GB
360	0,2 MB/s	0,0 MB/s	4,3 MB/s	33,0 MB/s	142 Mhz	2,00 GB	1,70 GB
380	0,0 MB/s	0,0 MB/s	4,3 MB/s	2,8 MB/s	51 Mhz	2,00 GB	1,72 GB

Table 24: Windows 7 VM without AV software while other VMs busy

Performance: DS, other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	197 Mhz	10,26 GB	1,59 GB
20	4,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	770 Mhz	10,26 GB	1,49 GB
40	10,3 MB/s	0,1 MB/s	3,2 MB/s	3,7 MB/s	1481 Mhz	10,26 GB	1,44 GB
60	10,4 MB/s	0,1 MB/s	7,2 MB/s	9,3 MB/s	1478 Mhz	10,26 GB	1,39 GB
80	10,4 MB/s	0,1 MB/s	7,2 MB/s	9,9 MB/s	1466 Mhz	10,26 GB	1,38 GB
100	10,7 MB/s	0,1 MB/s	7,3 MB/s	10,2 MB/s	1481 Mhz	10,26 GB	1,40 GB
120	10,9 MB/s	0,1 MB/s	7,3 MB/s	10,3 MB/s	1530 Mhz	10,26 GB	1,51 GB
140	10,9 MB/s	0,1 MB/s	7,5 MB/s	10,5 MB/s	1535 Mhz	10,26 GB	1,63 GB
160	11,0 MB/s	0,1 MB/s	7,6 MB/s	10,5 MB/s	1520 Mhz	10,26 GB	1,79 GB
180	11,0 MB/s	0,1 MB/s	7,6 MB/s	10,7 MB/s	1525 Mhz	10,26 GB	1,92 GB
200	11,3 MB/s	0,1 MB/s	7,6 MB/s	10,7 MB/s	1568 Mhz	10,26 GB	2,10 GB
220	10,9 MB/s	0,1 MB/s	7,8 MB/s	10,9 MB/s	1549 Mhz	10,26 GB	2,19 GB
240	12,0 MB/s	0,1 MB/s	7,5 MB/s	10,7 MB/s	1632 Mhz	10,26 GB	2,18 GB
260	11,5 MB/s	0,1 MB/s	8,2 MB/s	11,4 MB/s	1590 Mhz	10,26 GB	2,11 GB
280	11,1 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	1573 Mhz	10,26 GB	2,13 GB
300	11,0 MB/s	0,1 MB/s	7,7 MB/s	11,0 MB/s	1527 Mhz	10,26 GB	2,13 GB
320	11,1 MB/s	0,1 MB/s	7,6 MB/s	10,8 MB/s	1553 Mhz	10,26 GB	2,19 GB
340	11,2 MB/s	0,1 MB/s	7,7 MB/s	10,8 MB/s	1624 Mhz	10,26 GB	2,19 GB
360	11,0 MB/s	0,1 MB/s	7,9 MB/s	10,9 MB/s	1541 Mhz	10,26 GB	2,19 GB
380	10,7 MB/s	0,1 MB/s	7,6 MB/s	10,8 MB/s	1534 Mhz	10,26 GB	2,23 GB
400	11,0 MB/s	0,1 MB/s	7,4 MB/s	10,5 MB/s	1579 Mhz	10,26 GB	2,26 GB
420	11,3 MB/s	0,1 MB/s	7,7 MB/s	10,7 MB/s	1585 Mhz	10,26 GB	2,43 GB
440	11,0 MB/s	0,1 MB/s	7,8 MB/s	10,9 MB/s	1550 Mhz	10,26 GB	2,42 GB
460	11,4 MB/s	0,1 MB/s	7,7 MB/s	10,9 MB/s	1578 Mhz	10,26 GB	2,46 GB
480	11,1 MB/s	0,1 MB/s	7,8 MB/s	11,0 MB/s	1568 Mhz	10,26 GB	2,54 GB
500	11,4 MB/s	0,1 MB/s	7,8 MB/s	11,2 MB/s	1643 Mhz	10,27 GB	2,56 GB
520	11,8 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	1647 Mhz	10,27 GB	2,61 GB
540	11,7 MB/s	0,1 MB/s	8,3 MB/s	11,6 MB/s	1619 Mhz	10,28 GB	2,57 GB
560	11,6 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	1603 Mhz	10,28 GB	2,55 GB
580	11,8 MB/s	0,1 MB/s	8,0 MB/s	11,3 MB/s	1629 Mhz	10,28 GB	2,48 GB
600	10,9 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	1538 Mhz	10,28 GB	2,28 GB
620	11,1 MB/s	0,1 MB/s	7,6 MB/s	10,9 MB/s	1531 Mhz	10,28 GB	2,17 GB
640	10,8 MB/s	0,1 MB/s	7,6 MB/s	10,7 MB/s	1534 Mhz	10,28 GB	2,19 GB
660	10,4 MB/s	0,1 MB/s	7,5 MB/s	10,7 MB/s	1466 Mhz	10,28 GB	2,22 GB
680	10,5 MB/s	0,1 MB/s	7,2 MB/s	10,3 MB/s	1481 Mhz	10,28 GB	2,29 GB
700	10,4 MB/s	0,1 MB/s	7,3 MB/s	10,3 MB/s	1469 Mhz	10,28 GB	2,25 GB
720	10,9 MB/s	0,1 MB/s	7,2 MB/s	10,3 MB/s	1528 Mhz	10,28 GB	2,27 GB
740	11,5 MB/s	0,1 MB/s	7,5 MB/s	10,5 MB/s	1596 Mhz	10,28 GB	2,23 GB

760	11,7 MB/s	0,1 MB/s	8,0 MB/s	11,0 MB/s	1619 Mhz	10,28 GB	2,27 GB
780	11,7 MB/s	0,1 MB/s	8,0 MB/s	11,3 MB/s	1638 Mhz	10,28 GB	2,25 GB
800	11,9 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	1643 Mhz	10,28 GB	2,30 GB
820	13,2 MB/s	0,1 MB/s	8,2 MB/s	11,4 MB/s	1819 Mhz	10,28 GB	2,35 GB
840	13,9 MB/s	0,1 MB/s	9,1 MB/s	12,8 MB/s	1858 Mhz	10,28 GB	2,34 GB
860	14,5 MB/s	0,1 MB/s	9,6 MB/s	13,4 MB/s	1958 Mhz	10,28 GB	2,33 GB
880	13,9 MB/s	0,1 MB/s	10,0 MB/s	14,0 MB/s	1879 Mhz	10,28 GB	2,35 GB
900	10,9 MB/s	0,1 MB/s	9,6 MB/s	13,6 MB/s	1525 Mhz	10,28 GB	2,33 GB
920	9,3 MB/s	0,1 MB/s	7,6 MB/s	11,3 MB/s	1345 Mhz	10,28 GB	2,45 GB
940	7,2 MB/s	0,1 MB/s	6,7 MB/s	9,4 MB/s	1272 Mhz	10,28 GB	2,49 GB
960	5,0 MB/s	0,1 MB/s	6,4 MB/s	7,6 MB/s	790 Mhz	10,28 GB	2,50 GB
980	4,7 MB/s	0,0 MB/s	3,4 MB/s	4,9 MB/s	768 Mhz	10,28 GB	2,35 GB
1000	2,4 MB/s	0,0 MB/s	3,3 MB/s	4,7 MB/s	820 Mhz	10,02 GB	2,34 GB
1020	0,0 MB/s	0,0 MB/s	4,6 MB/s	3,2 MB/s	271 Mhz	10,02 GB	2,33 GB
1040	0,0 MB/s	0,0 MB/s	0,4 MB/s	0,2 MB/s	241 Mhz	10,02 GB	2,33 GB
1060	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	196 Mhz	10,02 GB	2,32 GB

Table 25: ESX with DS while other VMs idle

Time	**NIC In**	**NIC Out**	**Disk Read**	**Disk Write**	**CPU**	**Mem Consumed**	**Mem Active**
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	24 Mhz	2,00 GB	1,13 GB
20	3,5 MB/s	0,0 MB/s	3,2 MB/s	3,6 MB/s	73 Mhz	2,00 GB	1,02 GB
40	8,4 MB/s	0,1 MB/s	7,1 MB/s	9,2 MB/s	253 Mhz	2,00 GB	1,02 GB
60	10,5 MB/s	0,1 MB/s	7,2 MB/s	9,8 MB/s	345 Mhz	2,00 GB	0,91 GB
80	10,2 MB/s	0,1 MB/s	7,2 MB/s	10,1 MB/s	371 Mhz	2,00 GB	0,88 GB
100	10,9 MB/s	0,1 MB/s	7,2 MB/s	10,2 MB/s	367 Mhz	2,00 GB	0,88 GB
120	10,6 MB/s	0,1 MB/s	7,5 MB/s	10,5 MB/s	370 Mhz	2,00 GB	1,04 GB
140	11,1 MB/s	0,1 MB/s	7,6 MB/s	10,5 MB/s	376 Mhz	2,00 GB	1,18 GB
160	10,9 MB/s	0,1 MB/s	7,5 MB/s	10,6 MB/s	393 Mhz	2,00 GB	1,18 GB
180	10,9 MB/s	0,1 MB/s	7,6 MB/s	10,7 MB/s	377 Mhz	2,00 GB	1,46 GB
200	11,2 MB/s	0,1 MB/s	7,8 MB/s	10,8 MB/s	385 Mhz	2,00 GB	1,56 GB
220	11,1 MB/s	0,1 MB/s	7,5 MB/s	10,7 MB/s	398 Mhz	2,00 GB	1,56 GB
240	11,5 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	389 Mhz	2,00 GB	1,67 GB
260	11,6 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	410 Mhz	2,00 GB	1,65 GB
280	11,5 MB/s	0,1 MB/s	7,7 MB/s	10,9 MB/s	401 Mhz	2,00 GB	1,65 GB
300	11,2 MB/s	0,1 MB/s	7,6 MB/s	10,8 MB/s	381 Mhz	2,00 GB	1,67 GB
320	11,1 MB/s	0,1 MB/s	7,7 MB/s	10,8 MB/s	385 Mhz	2,00 GB	1,73 GB
340	11,2 MB/s	0,1 MB/s	7,8 MB/s	10,8 MB/s	423 Mhz	2,00 GB	1,73 GB
360	10,9 MB/s	0,1 MB/s	7,6 MB/s	10,8 MB/s	389 Mhz	2,00 GB	1,72 GB
380	10,9 MB/s	0,1 MB/s	7,4 MB/s	10,5 MB/s	384 Mhz	2,00 GB	1,72 GB

400	11,2 MB/s	0,1 MB/s	7,6 MB/s	10,7 MB/s	384 Mhz	2,00 GB	1,72 GB
420	11,2 MB/s	0,1 MB/s	7,7 MB/s	10,8 MB/s	383 Mhz	2,00 GB	1,79 GB
440	11,2 MB/s	0,1 MB/s	7,7 MB/s	10,8 MB/s	391 Mhz	2,00 GB	1,79 GB
460	11,2 MB/s	0,1 MB/s	7,8 MB/s	10,9 MB/s	406 Mhz	2,00 GB	1,81 GB
480	11,3 MB/s	0,1 MB/s	7,8 MB/s	11,0 MB/s	387 Mhz	2,00 GB	1,83 GB
500	11,5 MB/s	0,1 MB/s	8,1 MB/s	11,0 MB/s	389 Mhz	2,00 GB	1,82 GB
520	11,5 MB/s	0,1 MB/s	8,2 MB/s	11,4 MB/s	421 Mhz	2,00 GB	1,82 GB
540	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,3 MB/s	405 Mhz	2,00 GB	1,80 GB
560	11,5 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	406 Mhz	2,00 GB	1,79 GB
580	11,7 MB/s	0,1 MB/s	8,2 MB/s	11,4 MB/s	420 Mhz	2,00 GB	1,79 GB
600	11,3 MB/s	0,1 MB/s	7,5 MB/s	10,9 MB/s	395 Mhz	2,00 GB	1,71 GB
620	11,1 MB/s	0,1 MB/s	7,5 MB/s	10,6 MB/s	381 Mhz	2,00 GB	1,71 GB
640	11,0 MB/s	0,1 MB/s	7,5 MB/s	10,6 MB/s	407 Mhz	2,00 GB	1,71 GB
660	10,6 MB/s	0,1 MB/s	7,2 MB/s	10,3 MB/s	366 Mhz	2,00 GB	1,73 GB
680	10,4 MB/s	0,1 MB/s	7,3 MB/s	10,3 MB/s	370 Mhz	2,00 GB	1,71 GB
700	10,5 MB/s	0,1 MB/s	7,2 MB/s	10,2 MB/s	389 Mhz	2,00 GB	1,71 GB
720	10,9 MB/s	0,1 MB/s	7,5 MB/s	10,4 MB/s	359 Mhz	2,00 GB	1,70 GB
740	11,3 MB/s	0,1 MB/s	7,9 MB/s	10,9 MB/s	381 Mhz	2,00 GB	1,72 GB
760	11,3 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	429 Mhz	2,00 GB	1,72 GB
780	12,0 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	397 Mhz	2,00 GB	1,74 GB
800	11,8 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	416 Mhz	2,00 GB	1,75 GB
820	13,1 MB/s	0,1 MB/s	9,1 MB/s	12,7 MB/s	427 Mhz	2,00 GB	1,75 GB
840	14,3 MB/s	0,1 MB/s	9,5 MB/s	13,3 MB/s	430 Mhz	2,00 GB	1,77 GB
860	13,9 MB/s	0,1 MB/s	10,0 MB/s	13,9 MB/s	481 Mhz	2,00 GB	1,75 GB
880	14,6 MB/s	0,1 MB/s	9,5 MB/s	13,5 MB/s	497 Mhz	2,00 GB	1,75 GB
900	10,3 MB/s	0,1 MB/s	7,6 MB/s	11,3 MB/s	489 Mhz	2,00 GB	1,74 GB
920	8,7 MB/s	0,1 MB/s	6,7 MB/s	9,3 MB/s	409 Mhz	2,00 GB	1,76 GB
940	6,9 MB/s	0,1 MB/s	6,4 MB/s	7,6 MB/s	347 Mhz	2,00 GB	1,76 GB
960	4,9 MB/s	0,0 MB/s	3,4 MB/s	4,8 MB/s	406 Mhz	2,00 GB	1,77 GB
980	5,0 MB/s	0,0 MB/s	3,3 MB/s	4,7 MB/s	172 Mhz	2,00 GB	1,76 GB
1000	4,7 MB/s	0,0 MB/s	4,6 MB/s	3,1 MB/s	231 Mhz	2,00 GB	1,76 GB
1020	2,5 MB/s	0,0 MB/s	0,4 MB/s	0,2 MB/s	92 Mhz	2,00 GB	1,75 GB
1040	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	67 Mhz	2,00 GB	1,75 GB
1060	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	29 Mhz	2,00 GB	1,75 GB

Table 26: Windows 7 VM with DS while other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	25 Mhz	0,47 GB	0,05 GB
20	2,5 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	395 Mhz	0,47 GB	0,06 GB
40	6,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	859 Mhz	0,47 GB	0,06 GB
60	7,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	855 Mhz	0,47 GB	0,05 GB
80	7,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	856 Mhz	0,47 GB	0,05 GB
100	7,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	862 Mhz	0,47 GB	0,05 GB
120	7,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	893 Mhz	0,47 GB	0,04 GB
140	8,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	898 Mhz	0,47 GB	0,04 GB
160	7,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	892 Mhz	0,47 GB	0,04 GB
180	7,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	900 Mhz	0,47 GB	0,07 GB
200	8,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	918 Mhz	0,47 GB	0,07 GB
220	7,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	899 Mhz	0,47 GB	0,07 GB
240	8,3 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	966 Mhz	0,47 GB	0,07 GB
260	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	945 Mhz	0,47 GB	0,07 GB
280	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	920 Mhz	0,47 GB	0,07 GB
300	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	899 Mhz	0,47 GB	0,06 GB
320	8,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	912 Mhz	0,47 GB	0,06 GB
340	8,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	924 Mhz	0,47 GB	0,06 GB
360	8,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	908 Mhz	0,47 GB	0,07 GB
380	7,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	910 Mhz	0,47 GB	0,07 GB
400	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	912 Mhz	0,47 GB	0,07 GB
420	8,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	926 Mhz	0,47 GB	0,09 GB
440	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	914 Mhz	0,47 GB	0,09 GB
460	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	929 Mhz	0,47 GB	0,09 GB
480	8,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	927 Mhz	0,47 GB	0,07 GB
500	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,2 MB/s	960 Mhz	0,48 GB	0,09 GB
520	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,3 MB/s	975 Mhz	0,48 GB	0,09 GB
540	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,4 MB/s	958 Mhz	0,48 GB	0,11 GB
560	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	946 Mhz	0,48 GB	0,11 GB
580	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	964 Mhz	0,49 GB	0,12 GB
600	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	897 Mhz	0,49 GB	0,09 GB
620	7,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	895 Mhz	0,49 GB	0,09 GB
640	7,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	892 Mhz	0,49 GB	0,09 GB
660	7,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	852 Mhz	0,49 GB	0,09 GB
680	7,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	861 Mhz	0,49 GB	0,07 GB
700	7,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	858 Mhz	0,49 GB	0,07 GB
720	7,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	890 Mhz	0,49 GB	0,08 GB
740	8,3 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	942 Mhz	0,49 GB	0,10 GB
760	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	942 Mhz	0,49 GB	0,10 GB
780	8,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	963 Mhz	0,49 GB	0,09 GB

800	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	965 Mhz	0,49 GB	0,09 GB
820	9,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1073 Mhz	0,49 GB	0,09 GB
840	10,3 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1119 Mhz	0,49 GB	0,10 GB
860	10,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1176 Mhz	0,49 GB	0,08 GB
880	10,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1125 Mhz	0,49 GB	0,08 GB
900	7,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	889 Mhz	0,49 GB	0,09 GB
920	6,3 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	776 Mhz	0,49 GB	0,08 GB
940	6,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	619 Mhz	0,49 GB	0,08 GB
960	3,6 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	413 Mhz	0,49 GB	0,06 GB
980	3,5 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	401 Mhz	0,49 GB	0,06 GB
1000	3,4 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	462 Mhz	0,48 GB	0,06 GB
1020	4,8 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	28 Mhz	0,48 GB	0,05 GB
1040	0,4 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	26 Mhz	0,48 GB	0,05 GB
1060	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	26 Mhz	0,48 GB	0,05 GB

Table 27: DSVA while other VMs idle

Performance: DS, other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	7161 Mhz	10,34 GB	4,90 GB
20	6,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	8096 Mhz	10,34 GB	4,81 GB
40	11,7 MB/s	0,1 MB/s	4,2 MB/s	4,7 MB/s	8925 Mhz	10,34 GB	4,78 GB
60	11,7 MB/s	0,1 MB/s	8,0 MB/s	10,5 MB/s	8983 Mhz	10,34 GB	4,61 GB
80	11,7 MB/s	0,1 MB/s	8,1 MB/s	11,2 MB/s	8954 Mhz	10,34 GB	4,68 GB
100	12,1 MB/s	0,1 MB/s	8,2 MB/s	11,3 MB/s	8993 Mhz	10,34 GB	4,62 GB
120	11,9 MB/s	0,1 MB/s	8,3 MB/s	11,6 MB/s	8999 Mhz	10,34 GB	4,70 GB
140	12,0 MB/s	0,2 MB/s	8,2 MB/s	11,6 MB/s	9076 Mhz	10,34 GB	4,69 GB
160	11,6 MB/s	0,2 MB/s	8,6 MB/s	11,7 MB/s	9094 Mhz	10,34 GB	4,82 GB
180	11,7 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	8947 Mhz	10,34 GB	5,11 GB
200	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,5 MB/s	8988 Mhz	10,34 GB	5,16 GB
220	11,7 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	8975 Mhz	10,34 GB	5,28 GB
240	12,1 MB/s	0,1 MB/s	8,1 MB/s	11,5 MB/s	9037 Mhz	10,34 GB	5,41 GB
260	11,8 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	8978 Mhz	10,34 GB	5,61 GB
280	11,8 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	8980 Mhz	10,34 GB	5,58 GB
300	12,0 MB/s	0,1 MB/s	8,0 MB/s	11,4 MB/s	9027 Mhz	10,34 GB	5,59 GB
320	11,8 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	8969 Mhz	10,34 GB	5,39 GB
340	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,6 MB/s	8999 Mhz	10,34 GB	5,43 GB
360	11,8 MB/s	0,1 MB/s	8,1 MB/s	11,5 MB/s	8985 Mhz	10,34 GB	5,45 GB
380	12,3 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	9059 Mhz	10,34 GB	5,43 GB

400	12,1 MB/s	0,1 MB/s	8,5 MB/s	11,9 MB/s	8988 Mhz	10,34 GB	5,39 GB
420	12,0 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	9039 Mhz	10,34 GB	5,34 GB
440	12,1 MB/s	0,1 MB/s	8,3 MB/s	11,8 MB/s	8981 Mhz	10,34 GB	5,40 GB
460	11,5 MB/s	0,1 MB/s	8,4 MB/s	11,7 MB/s	8962 Mhz	10,34 GB	5,41 GB
480	12,1 MB/s	0,1 MB/s	8,2 MB/s	11,9 MB/s	9056 Mhz	10,35 GB	5,49 GB
500	12,3 MB/s	0,1 MB/s	8,7 MB/s	12,1 MB/s	9014 Mhz	10,36 GB	5,48 GB
520	12,3 MB/s	0,1 MB/s	8,5 MB/s	11,8 MB/s	9040 Mhz	10,36 GB	5,49 GB
540	11,9 MB/s	0,1 MB/s	8,4 MB/s	12,0 MB/s	8976 Mhz	10,36 GB	5,50 GB
560	12,0 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	8969 Mhz	10,36 GB	5,45 GB
580	11,6 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	8921 Mhz	10,36 GB	5,43 GB
600	11,0 MB/s	0,1 MB/s	7,9 MB/s	11,4 MB/s	8859 Mhz	10,36 GB	5,40 GB
620	11,6 MB/s	0,1 MB/s	7,7 MB/s	11,0 MB/s	8891 Mhz	10,36 GB	5,42 GB
640	11,4 MB/s	0,1 MB/s	7,9 MB/s	11,2 MB/s	8916 Mhz	10,36 GB	5,44 GB
660	11,7 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	8956 Mhz	10,36 GB	5,45 GB
680	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	8977 Mhz	10,36 GB	5,45 GB
700	12,1 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	9008 Mhz	10,36 GB	5,43 GB
720	11,9 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	9006 Mhz	10,36 GB	5,47 GB
740	12,3 MB/s	0,1 MB/s	8,3 MB/s	11,8 MB/s	9017 Mhz	10,36 GB	5,36 GB
760	12,2 MB/s	0,1 MB/s	8,5 MB/s	11,9 MB/s	9014 Mhz	10,36 GB	5,40 GB
780	12,8 MB/s	0,1 MB/s	8,4 MB/s	11,9 MB/s	9107 Mhz	10,36 GB	5,33 GB
800	15,3 MB/s	0,1 MB/s	8,8 MB/s	12,3 MB/s	9450 Mhz	10,36 GB	5,32 GB
820	15,3 MB/s	0,1 MB/s	10,5 MB/s	14,4 MB/s	9489 Mhz	10,36 GB	5,35 GB
840	15,4 MB/s	0,1 MB/s	10,6 MB/s	15,0 MB/s	9497 Mhz	10,36 GB	5,41 GB
860	15,6 MB/s	0,1 MB/s	10,6 MB/s	14,9 MB/s	9505 Mhz	10,36 GB	5,41 GB
880	12,8 MB/s	0,1 MB/s	10,8 MB/s	15,1 MB/s	9493 Mhz	10,36 GB	5,49 GB
900	0,8 MB/s	0,1 MB/s	11,0 MB/s	13,5 MB/s	7882 Mhz	10,36 GB	5,52 GB
920	0,0 MB/s	0,0 MB/s	2,6 MB/s	2,2 MB/s	7149 Mhz	10,36 GB	5,55 GB

Table 28: ESX with DS while other VMs busy

Time	**NIC In**	**NIC Out**	**Disk Read**	**Disk Write**	**CPU**	**Mem Consumed**	**Mem Active**
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	64 Mhz	2,00 GB	1,05 GB
20	6,2 MB/s	0,1 MB/s	3,1 MB/s	3,5 MB/s	140 Mhz	2,00 GB	1,05 GB
40	11,7 MB/s	0,1 MB/s	6,5 MB/s	8,3 MB/s	478 Mhz	2,00 GB	0,99 GB
60	11,7 MB/s	0,1 MB/s	8,0 MB/s	10,8 MB/s	648 Mhz	2,00 GB	0,90 GB
80	11,8 MB/s	0,1 MB/s	8,1 MB/s	11,2 MB/s	636 Mhz	2,00 GB	0,90 GB
100	12,1 MB/s	0,1 MB/s	8,3 MB/s	11,5 MB/s	640 Mhz	2,00 GB	0,97 GB
120	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	655 Mhz	2,00 GB	1,04 GB
140	12,0 MB/s	0,1 MB/s	8,6 MB/s	11,6 MB/s	650 Mhz	2,00 GB	1,17 GB
160	11,6 MB/s	0,1 MB/s	8,2 MB/s	11,4 MB/s	738 Mhz	2,00 GB	1,35 GB

180	11,7 MB/s	0,1 MB/s	8,0 MB/s	11,4 MB/s	810 Mhz	2,00 GB	1,50 GB
200	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	649 Mhz	2,00 GB	1,60 GB
220	11,8 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	700 Mhz	2,00 GB	1,64 GB
240	12,1 MB/s	0,1 MB/s	8,3 MB/s	11,7 MB/s	688 Mhz	2,00 GB	1,72 GB
260	11,8 MB/s	0,1 MB/s	8,3 MB/s	11,6 MB/s	697 Mhz	2,00 GB	1,74 GB
280	11,8 MB/s	0,1 MB/s	8,0 MB/s	11,4 MB/s	706 Mhz	2,00 GB	1,72 GB
300	12,0 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	699 Mhz	2,00 GB	1,76 GB
320	11,8 MB/s	0,1 MB/s	8,2 MB/s	11,5 MB/s	688 Mhz	2,00 GB	1,79 GB
340	11,9 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	686 Mhz	2,00 GB	1,79 GB
360	11,8 MB/s	0,1 MB/s	7,9 MB/s	11,2 MB/s	710 Mhz	2,00 GB	1,81 GB
380	12,3 MB/s	0,1 MB/s	8,4 MB/s	11,7 MB/s	651 Mhz	2,00 GB	1,81 GB
400	12,1 MB/s	0,1 MB/s	8,3 MB/s	11,8 MB/s	700 Mhz	2,00 GB	1,83 GB
420	12,0 MB/s	0,1 MB/s	8,3 MB/s	11,8 MB/s	660 Mhz	2,00 GB	1,77 GB
440	12,1 MB/s	0,1 MB/s	8,4 MB/s	11,7 MB/s	661 Mhz	2,00 GB	1,75 GB
460	11,5 MB/s	0,1 MB/s	8,2 MB/s	11,3 MB/s	679 Mhz	2,00 GB	1,75 GB
480	12,1 MB/s	0,1 MB/s	8,3 MB/s	11,5 MB/s	655 Mhz	2,00 GB	1,79 GB
500	12,3 MB/s	0,1 MB/s	8,6 MB/s	11,7 MB/s	673 Mhz	2,00 GB	1,75 GB
520	12,3 MB/s	0,1 MB/s	8,4 MB/s	11,9 MB/s	681 Mhz	2,00 GB	1,77 GB
540	11,9 MB/s	0,1 MB/s	8,4 MB/s	11,9 MB/s	671 Mhz	2,00 GB	1,77 GB
560	12,0 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	655 Mhz	2,00 GB	1,79 GB
580	11,6 MB/s	0,1 MB/s	8,1 MB/s	11,5 MB/s	649 Mhz	2,00 GB	1,79 GB
600	11,1 MB/s	0,1 MB/s	7,7 MB/s	11,1 MB/s	640 Mhz	2,00 GB	1,78 GB
620	11,6 MB/s	0,1 MB/s	7,8 MB/s	11,1 MB/s	619 Mhz	2,00 GB	1,78 GB
640	11,4 MB/s	0,1 MB/s	7,8 MB/s	11,0 MB/s	647 Mhz	2,00 GB	1,78 GB
660	11,7 MB/s	0,1 MB/s	8,0 MB/s	11,2 MB/s	642 Mhz	2,00 GB	1,75 GB
680	11,9 MB/s	0,1 MB/s	8,1 MB/s	11,4 MB/s	642 Mhz	2,00 GB	1,75 GB
700	12,1 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	652 Mhz	2,00 GB	1,75 GB
720	12,0 MB/s	0,1 MB/s	8,2 MB/s	11,6 MB/s	661 Mhz	2,00 GB	1,76 GB
740	12,3 MB/s	0,1 MB/s	8,4 MB/s	11,8 MB/s	665 Mhz	2,00 GB	1,79 GB
760	12,2 MB/s	0,1 MB/s	8,5 MB/s	11,9 MB/s	672 Mhz	2,00 GB	1,79 GB
780	12,8 MB/s	0,1 MB/s	8,6 MB/s	12,1 MB/s	675 Mhz	2,00 GB	1,80 GB
800	15,3 MB/s	0,1 MB/s	9,9 MB/s	13,7 MB/s	736 Mhz	2,00 GB	1,77 GB
820	15,4 MB/s	0,1 MB/s	10,5 MB/s	14,7 MB/s	815 Mhz	2,00 GB	1,77 GB
840	15,5 MB/s	0,1 MB/s	10,6 MB/s	15,0 MB/s	826 Mhz	2,00 GB	1,77 GB
860	15,6 MB/s	0,1 MB/s	10,7 MB/s	15,1 MB/s	827 Mhz	2,00 GB	1,77 GB
880	12,9 MB/s	0,1 MB/s	10,9 MB/s	14,1 MB/s	892 Mhz	2,00 GB	1,77 GB
900	0,8 MB/s	0,1 MB/s	5,6 MB/s	6,1 MB/s	855 Mhz	2,00 GB	1,78 GB
920	0,0 MB/s	0,0 MB/s	0,7 MB/s	0,6 MB/s	443 Mhz	2,00 GB	1,78 GB

Table 29: Windows 7 VM with DS while other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	73 Mhz	0,54 GB	0,05 GB
20	3,2 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	614 Mhz	0,54 GB	0,05 GB
40	6,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1113 Mhz	0,54 GB	0,06 GB
60	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1128 Mhz	0,54 GB	0,06 GB
80	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1131 Mhz	0,54 GB	0,05 GB
100	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1152 Mhz	0,54 GB	0,05 GB
120	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1142 Mhz	0,54 GB	0,05 GB
140	8,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1149 Mhz	0,54 GB	0,05 GB
160	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1111 Mhz	0,54 GB	0,05 GB
180	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1117 Mhz	0,54 GB	0,05 GB
200	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1136 Mhz	0,54 GB	0,07 GB
220	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1121 Mhz	0,54 GB	0,08 GB
240	8,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1148 Mhz	0,54 GB	0,08 GB
260	8,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1128 Mhz	0,54 GB	0,07 GB
280	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1114 Mhz	0,54 GB	0,06 GB
300	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1153 Mhz	0,54 GB	0,06 GB
320	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1122 Mhz	0,54 GB	0,05 GB
340	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1126 Mhz	0,54 GB	0,06 GB
360	8,3 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1135 Mhz	0,54 GB	0,06 GB
380	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1182 Mhz	0,54 GB	0,06 GB
400	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1148 Mhz	0,54 GB	0,06 GB
420	8,7 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1148 Mhz	0,54 GB	0,06 GB
440	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1163 Mhz	0,54 GB	0,07 GB
460	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,4 MB/s	1133 Mhz	0,54 GB	0,07 GB
480	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,5 MB/s	1197 Mhz	0,54 GB	0,07 GB
500	9,0 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1166 Mhz	0,55 GB	0,09 GB
520	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1170 Mhz	0,56 GB	0,09 GB
540	8,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1143 Mhz	0,56 GB	0,09 GB
560	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1140 Mhz	0,56 GB	0,09 GB
580	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1095 Mhz	0,56 GB	0,09 GB
600	8,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1071 Mhz	0,56 GB	0,09 GB
620	8,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1100 Mhz	0,56 GB	0,08 GB
640	8,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1112 Mhz	0,56 GB	0,09 GB
660	8,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1126 Mhz	0,56 GB	0,09 GB
680	8,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1146 Mhz	0,56 GB	0,11 GB
700	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1149 Mhz	0,56 GB	0,10 GB
720	8,6 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1155 Mhz	0,56 GB	0,10 GB
740	8,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1166 Mhz	0,56 GB	0,09 GB
760	8,9 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1164 Mhz	0,56 GB	0,09 GB
780	9,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1213 Mhz	0,56 GB	0,09 GB

800	10,5 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1441 Mhz	0,56 GB	0,09 GB
820	11,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1449 Mhz	0,56 GB	0,08 GB
840	11,1 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1454 Mhz	0,56 GB	0,08 GB
860	11,2 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1469 Mhz	0,56 GB	0,06 GB
880	11,4 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	1266 Mhz	0,56 GB	0,06 GB
900	5,8 MB/s	0,1 MB/s	0,0 MB/s	0,0 MB/s	188 Mhz	0,56 GB	0,06 GB
920	0,7 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	72 Mhz	0,56 GB	0,07 GB

Table 30: DSVA while other VMs busy

Performance: WFBS, other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	126 Mhz	3,87 GB	1,14 GB
20	15,4 MB/s	0,2 MB/s	0,1 MB/s	7,7 MB/s	839 Mhz	3,87 GB	1,14 GB
40	27,1 MB/s	0,3 MB/s	0,1 MB/s	24,7 MB/s	3023 Mhz	3,87 GB	1,03 GB
60	26,6 MB/s	0,3 MB/s	0,0 MB/s	25,9 MB/s	3062 Mhz	3,87 GB	1,24 GB
80	24,5 MB/s	0,3 MB/s	0,0 MB/s	23,8 MB/s	3534 Mhz	3,87 GB	1,46 GB
100	28,1 MB/s	0,3 MB/s	0,1 MB/s	27,2 MB/s	3042 Mhz	3,87 GB	1,60 GB
120	27,6 MB/s	0,3 MB/s	0,1 MB/s	26,9 MB/s	3689 Mhz	3,87 GB	1,71 GB
140	28,3 MB/s	0,3 MB/s	0,1 MB/s	27,7 MB/s	3078 Mhz	3,87 GB	1,80 GB
160	27,6 MB/s	0,3 MB/s	0,1 MB/s	27,1 MB/s	3566 Mhz	3,87 GB	1,83 GB
180	27,7 MB/s	0,3 MB/s	0,0 MB/s	26,7 MB/s	3418 Mhz	3,87 GB	1,89 GB
200	26,5 MB/s	0,3 MB/s	0,1 MB/s	26,1 MB/s	3531 Mhz	3,87 GB	1,89 GB
220	27,0 MB/s	0,3 MB/s	0,1 MB/s	26,6 MB/s	3288 Mhz	3,87 GB	1,96 GB
240	27,0 MB/s	0,3 MB/s	0,1 MB/s	25,9 MB/s	3359 Mhz	3,87 GB	1,96 GB
260	26,7 MB/s	0,3 MB/s	1,9 MB/s	26,8 MB/s	3575 Mhz	3,87 GB	1,95 GB
280	26,0 MB/s	0,3 MB/s	0,8 MB/s	26,0 MB/s	3139 Mhz	3,87 GB	1,93 GB
300	24,3 MB/s	0,3 MB/s	0,0 MB/s	23,3 MB/s	3244 Mhz	3,87 GB	1,93 GB
320	26,1 MB/s	0,3 MB/s	0,1 MB/s	25,3 MB/s	3034 Mhz	3,87 GB	1,94 GB
340	22,1 MB/s	0,3 MB/s	0,1 MB/s	22,0 MB/s	3217 Mhz	3,87 GB	1,95 GB
360	33,6 MB/s	0,4 MB/s	0,0 MB/s	34,1 MB/s	2806 Mhz	3,87 GB	1,98 GB
380	43,4 MB/s	0,4 MB/s	0,1 MB/s	40,5 MB/s	4061 Mhz	3,87 GB	1,98 GB
400	18,0 MB/s	0,2 MB/s	0,1 MB/s	23,4 MB/s	4036 Mhz	3,87 GB	1,97 GB
420	0,0 MB/s	0,0 MB/s	0,0 MB/s	3,3 MB/s	2103 Mhz	3,87 GB	1,99 GB
440	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,2 MB/s	194 Mhz	3,87 GB	1,98 GB

Table 31: ESX with WFBS while other VMs idle

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	27 Mhz	2,00 GB	0,98 GB
20	15,4 MB/s	0,2 MB/s	0,0 MB/s	7,7 MB/s	686 Mhz	2,00 GB	0,98 GB
40	27,1 MB/s	0,3 MB/s	0,0 MB/s	24,7 MB/s	2852 Mhz	2,00 GB	0,87 GB
60	26,6 MB/s	0,3 MB/s	0,0 MB/s	25,9 MB/s	2881 Mhz	2,00 GB	1,09 GB
80	24,6 MB/s	0,3 MB/s	0,0 MB/s	23,8 MB/s	3357 Mhz	2,00 GB	1,31 GB
100	28,2 MB/s	0,3 MB/s	0,0 MB/s	27,1 MB/s	2874 Mhz	2,00 GB	1,44 GB
120	27,7 MB/s	0,3 MB/s	0,0 MB/s	26,9 MB/s	3472 Mhz	2,00 GB	1,54 GB
140	28,4 MB/s	0,3 MB/s	0,1 MB/s	27,7 MB/s	2910 Mhz	2,00 GB	1,63 GB
160	27,6 MB/s	0,3 MB/s	0,0 MB/s	27,0 MB/s	3379 Mhz	2,00 GB	1,66 GB
180	27,8 MB/s	0,3 MB/s	0,0 MB/s	26,7 MB/s	3247 Mhz	2,00 GB	1,72 GB
200	26,6 MB/s	0,3 MB/s	0,0 MB/s	26,0 MB/s	3360 Mhz	2,00 GB	1,72 GB
220	27,1 MB/s	0,3 MB/s	0,1 MB/s	26,6 MB/s	3120 Mhz	2,00 GB	1,77 GB
240	27,1 MB/s	0,3 MB/s	0,1 MB/s	25,9 MB/s	3187 Mhz	2,00 GB	1,77 GB
260	26,8 MB/s	0,3 MB/s	1,8 MB/s	26,8 MB/s	3406 Mhz	2,00 GB	1,77 GB
280	26,0 MB/s	0,3 MB/s	0,8 MB/s	26,0 MB/s	2965 Mhz	2,00 GB	1,75 GB
300	24,4 MB/s	0,3 MB/s	0,0 MB/s	23,3 MB/s	3075 Mhz	2,00 GB	1,75 GB
320	26,1 MB/s	0,3 MB/s	0,0 MB/s	25,3 MB/s	2837 Mhz	2,00 GB	1,73 GB
340	22,2 MB/s	0,3 MB/s	0,1 MB/s	22,0 MB/s	3055 Mhz	2,00 GB	1,75 GB
360	33,7 MB/s	0,4 MB/s	0,0 MB/s	34,1 MB/s	2633 Mhz	2,00 GB	1,76 GB
380	43,5 MB/s	0,4 MB/s	0,1 MB/s	40,5 MB/s	3869 Mhz	2,00 GB	1,76 GB
400	18,0 MB/s	0,2 MB/s	0,0 MB/s	23,3 MB/s	3874 Mhz	2,00 GB	1,75 GB
420	0,0 MB/s	0,0 MB/s	0,0 MB/s	3,0 MB/s	1965 Mhz	2,00 GB	1,77 GB
440	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,1 MB/s	82 Mhz	2,00 GB	1,77 GB

Table 32: Windows 7 VM with WFBS while other VMs idle

Performance: WFBS, other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	7038 Mhz	6,89 GB	4,26 GB
20	3,8 MB/s	0,0 MB/s	0,1 MB/s	0,5 MB/s	7172 Mhz	6,89 GB	4,26 GB
40	26,4 MB/s	0,3 MB/s	0,0 MB/s	20,0 MB/s	9339 Mhz	6,89 GB	4,16 GB
60	25,6 MB/s	0,3 MB/s	0,0 MB/s	24,9 MB/s	10571 Mhz	6,89 GB	4,24 GB
80	25,7 MB/s	0,2 MB/s	0,9 MB/s	24,8 MB/s	10856 Mhz	6,89 GB	4,53 GB
100	25,4 MB/s	0,2 MB/s	1,2 MB/s	25,1 MB/s	10820 Mhz	6,89 GB	4,62 GB
120	25,6 MB/s	0,2 MB/s	0,1 MB/s	24,8 MB/s	10801 Mhz	6,89 GB	4,78 GB
140	25,2 MB/s	0,2 MB/s	0,1 MB/s	24,7 MB/s	10626 Mhz	6,89 GB	4,79 GB
160	26,3 MB/s	0,3 MB/s	0,1 MB/s	25,6 MB/s	10308 Mhz	6,89 GB	4,89 GB
180	26,0 MB/s	0,2 MB/s	0,1 MB/s	25,1 MB/s	10854 Mhz	6,89 GB	4,99 GB
200	27,9 MB/s	0,3 MB/s	0,0 MB/s	27,5 MB/s	10893 Mhz	6,89 GB	4,96 GB
220	26,8 MB/s	0,2 MB/s	0,1 MB/s	26,7 MB/s	10773 Mhz	6,89 GB	4,96 GB
240	27,2 MB/s	0,2 MB/s	0,2 MB/s	27,0 MB/s	10952 Mhz	6,89 GB	4,97 GB
260	22,2 MB/s	0,2 MB/s	0,2 MB/s	21,4 MB/s	10592 Mhz	6,89 GB	5,00 GB
280	26,1 MB/s	0,3 MB/s	0,1 MB/s	25,3 MB/s	10348 Mhz	6,89 GB	5,02 GB
300	26,2 MB/s	0,3 MB/s	0,1 MB/s	24,9 MB/s	10738 Mhz	6,89 GB	5,01 GB
320	25,9 MB/s	0,2 MB/s	0,1 MB/s	25,8 MB/s	10542 Mhz	6,89 GB	5,00 GB
340	22,6 MB/s	0,2 MB/s	0,1 MB/s	22,2 MB/s	10593 Mhz	6,89 GB	4,99 GB
360	24,3 MB/s	0,2 MB/s	0,0 MB/s	23,8 MB/s	10050 Mhz	6,89 GB	5,00 GB
380	28,4 MB/s	0,3 MB/s	0,1 MB/s	27,6 MB/s	10828 Mhz	6,89 GB	4,99 GB
400	47,4 MB/s	0,4 MB/s	0,1 MB/s	46,2 MB/s	10876 Mhz	6,89 GB	4,98 GB
420	18,6 MB/s	0,2 MB/s	0,1 MB/s	24,3 MB/s	11085 Mhz	6,89 GB	5,00 GB
440	0,0 MB/s	0,0 MB/s	0,1 MB/s	3,2 MB/s	10488 Mhz	6,89 GB	4,98 GB
460	0,0 MB/s	0,0 MB/s	0,1 MB/s	0,4 MB/s	7203 Mhz	6,89 GB	4,96 GB

Table 33: ESX with WFBS while other VMs busy

Time	NIC In	NIC Out	Disk Read	Disk Write	CPU	Mem Consumed	Mem Active
0	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,0 MB/s	52 Mhz	2,00 GB	1,01 GB
20	3,8 MB/s	0,0 MB/s	0,1 MB/s	0,5 MB/s	175 Mhz	2,00 GB	1,01 GB
40	26,4 MB/s	0,3 MB/s	0,0 MB/s	20,0 MB/s	2302 Mhz	2,00 GB	0,89 GB
60	25,6 MB/s	0,2 MB/s	0,0 MB/s	24,9 MB/s	3539 Mhz	2,00 GB	0,97 GB
80	25,8 MB/s	0,2 MB/s	0,9 MB/s	24,8 MB/s	3822 Mhz	2,00 GB	1,21 GB
100	25,4 MB/s	0,2 MB/s	1,1 MB/s	25,1 MB/s	3775 Mhz	2,00 GB	1,29 GB
120	25,7 MB/s	0,2 MB/s	0,0 MB/s	24,8 MB/s	3768 Mhz	2,00 GB	1,48 GB
140	25,3 MB/s	0,2 MB/s	0,1 MB/s	24,7 MB/s	3600 Mhz	2,00 GB	1,49 GB
160	26,4 MB/s	0,3 MB/s	0,0 MB/s	25,5 MB/s	3247 Mhz	2,00 GB	1,59 GB
180	26,1 MB/s	0,2 MB/s	0,0 MB/s	25,0 MB/s	3817 Mhz	2,00 GB	1,68 GB
200	27,9 MB/s	0,3 MB/s	0,0 MB/s	27,5 MB/s	3858 Mhz	2,00 GB	1,68 GB
220	26,8 MB/s	0,2 MB/s	0,0 MB/s	26,6 MB/s	3720 Mhz	2,00 GB	1,70 GB
240	27,3 MB/s	0,2 MB/s	0,2 MB/s	27,0 MB/s	3913 Mhz	2,00 GB	1,71 GB
260	22,2 MB/s	0,2 MB/s	0,1 MB/s	21,3 MB/s	3564 Mhz	2,00 GB	1,75 GB
280	26,2 MB/s	0,2 MB/s	0,1 MB/s	25,3 MB/s	3312 Mhz	2,00 GB	1,75 GB
300	26,2 MB/s	0,2 MB/s	0,0 MB/s	24,8 MB/s	3688 Mhz	2,00 GB	1,75 GB
320	26,0 MB/s	0,2 MB/s	0,0 MB/s	25,8 MB/s	3505 Mhz	2,00 GB	1,73 GB
340	22,6 MB/s	0,2 MB/s	0,1 MB/s	22,2 MB/s	3569 Mhz	2,00 GB	1,73 GB
360	24,4 MB/s	0,2 MB/s	0,0 MB/s	23,7 MB/s	3027 Mhz	2,00 GB	1,74 GB
380	28,4 MB/s	0,3 MB/s	0,1 MB/s	27,6 MB/s	3776 Mhz	2,00 GB	1,74 GB
400	47,5 MB/s	0,4 MB/s	0,0 MB/s	46,1 MB/s	3822 Mhz	2,00 GB	1,73 GB
420	18,7 MB/s	0,2 MB/s	0,1 MB/s	24,3 MB/s	4059 Mhz	2,00 GB	1,73 GB
440	0,0 MB/s	0,0 MB/s	0,0 MB/s	2,7 MB/s	3504 Mhz	2,00 GB	1,70 GB
460	0,0 MB/s	0,0 MB/s	0,0 MB/s	0,2 MB/s	194 Mhz	2,00 GB	1,72 GB

Table 34: Windows 7 VM with WFBS while other VMs busy

C. Source of tmkill.vbs

Listing 1: Script to kill and remove the DS Agent.

```
'Determine Windows version
Set w = GetObject("winmgmts:{impersonationLevel=impersonate,(Debug)}!\\.\root\cimv2")
Set os = w.ExecQuery("Select * from Win32_OperatingSystem")
Dim build
For Each o in os
    build = o.BuildNumber
Next

'Elevate UAC if Vista+
If build>=5000 and WScript.Arguments.length=0 Then
    Set e = CreateObject("Shell.Application")
    e.ShellExecute "wscript.exe", """" & WScript.ScriptFullName & """ uac","","runas",1
Else
    'Kill Processes
    Set pl = w.ExecQuery("Select * from Win32_Process Where Name = 'coreServiceShell.exe' or " _
                                                                & "Name = 'coreFrameworkHost.exe' or " _
                                                                & "Name = 'ds_agent.exe'")
    For Each p in pl
        p.Terminate()
    Next

    'Disable Agent Self Protection
    Set reg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv")
    reg.SetDWORDValue &H80000002,"SOFTWARE\TrendMicro\Deep Security Agent","Self Protect",0

    'Determine Installer GUID using System Architecture information
    w = GetObject("winmgmts:root\cimv2:Win32_Processor='cpu0'").AddressWidth
    Dim g
    If w=32 Then
        g = "{10CC7E08-C4A3-4F8D-A49C-4BE90B1693B2}"
    Else
```

```
32          g = "{4E02FA4C-5238-454C-BBEB-61E314F8EC9A}"
33      End If
34
35      'Uninstall Agent
36      Set s = WScript.CreateObject("WScript.Shell")
37      r = s.Run("msiexec /x " & g,0,True)
38
39      'Report Back
40      If r=0 Then
41          MsgBox "Trend Micro Deep Security Agent killed and removed succesfully!",64,"Succesful"
42      Else
43          MsgBox "Something went wrong...",16,"Failed"
44      End If
45  End If
```

D. Extracting Values from Boottime xml

For each type of AV configuration, the following commandline has been run inside the folder in which the .xml files resided where the source of `iterate.xsl` is shown below:
`del ..\output.txt && for /F %i in ('dir /b *.xml') do @msxsl "%i" "..\iterate.xsl" >>..\output.txt`

Listing 2: xsl file to extract relevant boot values from the xml files.

```
1  <xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/
       Transform" xmlns:xs="http://www.w3.org/2001/XMLSchema">
2          <xsl:output omit-xml-declaration="yes" indent="yes"/>
3          <xsl:strip-space elements="*" />
4          <xsl:variable name='nl'><xsl:text>&#xa;</xsl:text></
               xsl:variable>
5          <xsl:template match="/results/boot/timing">
6                  <xsl:for-each select="interval">
7                          <!--<xsl:value-of select="concat(@name, ': ',
                               @duration, $nl)" />-->
8                          <xsl:value-of select="concat('&amp;amp; ',
                               @duration, $nl)" disable-output-escaping="
                               yes" />
9                  </xsl:for-each>
10                 <!--<xsl:value-of select="concat('Boot time: ',((
                       @bootDoneViaPostBoot)-(@postBootRequiredIdleTime))
                       , $nl)" />-->
11                 <xsl:value-of select="concat('&amp;amp; ',((
                       @bootDoneViaPostBoot)-(@postBootRequiredIdleTime))
                       , $nl)" disable-output-escaping="yes" />
12                 <xsl:value-of select="concat($nl,$nl,$nl)" />
13         </xsl:template>
14 </xsl:stylesheet>
```

E. File Listing of Benchmark zip

The following listing shows the files packed in the zip file including the additional file called 'random' containing a sequence number. Furthermore, once every test a zip is injected with the eicar.com test virus to determine whether the antivirus software works correctly.

Listing 3: Listing of files contained in WindowsInstaller-KB893803-v2-x86.exe.

```
\
  eicar.com              68
  empty.cat           6.566
  msi.dll         2.890.240
  msiexec.exe        78.848
  msihnd.dll        271.360
  msimsg.dll        884.736
  msisip.dll         15.360
  random                  6
  spmsg.dll          13.536
  spuninst.exe      209.632

  update\             <dir>
    eula.txt              4.092
    kb893803v2_net.cat   29.493
    kb893803v2_w2k.cat   29.493
    kb893803v2_wxp.cat   29.493
    spcustom.dll         22.240
    update.exe          718.048
    update.ver              365
    updatebr.inf            287
    update_w2k3.inf      27.016
    update_win2k.inf     27.017
    update_wxp.inf       27.011
    updspapi.dll        371.936
```

F. StressLinux Commandline

StressLinux has various options in order to benchmark different components. For this benchmark the `stress` command[46] is used to generate workload. The following options are available:

Listing 4: Available parameters for stress tool.

```
'stress' imposes certain types of compute stress on your system

Usage: stress [OPTION [ARG]] ...
 -?, --help         show this help statement
     --version      show version statement
 -v, --verbose      be verbose
 -q, --quiet        be quiet
 -n, --dry-run      show what would have been done
 -t, --timeout N    timeout after N seconds
     --backoff N    wait factor of N microseconds before work starts
 -c, --cpu N        spawn N workers spinning on sqrt()
 -i, --io N         spawn N workers spinning on sync()
 -m, --vm N         spawn N workers spinning on malloc()/free()
     --vm-bytes B   malloc B bytes per vm worker (default is 256MB)
     --vm-stride B  touch a byte every B bytes (default is 4096)
     --vm-hang N    sleep N secs before free (default is none, 0 is
         inf)
     --vm-keep      redirty memory instead of freeing and
         reallocating
 -d, --hdd N        spawn N workers spinning on write()/unlink()
     --hdd-bytes B  write B bytes per hdd worker (default is 1GB)

Example: stress --cpu 8 --io 4 --vm 2 --vm-bytes 128M --timeout 10s

Note: Numbers may be suffixed with s,m,h,d,y (time) or B,K,M,G (size)
    .
```

From the various options available, the following commandline has been used: `stress --vm 1 --vm-bytes 1536M`. This stresses the computer using one worker and makes the VM use 1.5 GB of memory.

[46] http://weather.ou.edu/~apw/projects/stress/

G. Source of CreateAndTransfer.cmd

Listing 5: cmd.exe batch script to generate unique zip files and transfer them while measuring the time it takes.

```
@echo off
setlocal EnableDelayedExpansion
if [%1] EQU [] echo Provide the last octet of the IP address or "reset" to reset the number. 192.168.254.[input] && goto :eof
if %1 EQU reset echo 0 > startnr.txt && goto :eof

for /F %%i in (startnr.txt) do set startnr=%%i
set /A endnr=%startnr% + 550
set /A startnr=%startnr% + 1
set /A virusnr=%startnr% + ((%endnr% - %startnr%) / 2)

echo Cleaning up...
del /Q .\Zips\WindowsInstaller-KB893803-v2-x86_*.zip > nul 2>&1
del /Q \\192.168.254.106\Users\Public\Downloads\WindowsInstaller-KB893803-v2-x86_*.zip > nul 2>&1

echo Creating zips %startnr% - %endnr%
pushd WindowsInstaller-KB893803-v2-x86
set count=%startnr%
for /L %%i in (%startnr%,1,%endnr%) do (
        echo !count!>random
        "C:\Program Files\7-Zip\7z.exe" a -wx0 -r -bd ..\Zips\WindowsInstaller-KB893803-v2-x86_!count!.zip *>nul
        if !count! EQU !virusnr! (
                "C:\Program Files\7-Zip\7z.exe" a ..\Zips\WindowsInstaller-KB893803-v2-x86_!count!.zip ..\eicar.com>nul
                echo Eicar testvirus inserted in WindowsInstaller-KB893803-v2-x86_!count!.zip
        )
        set /a count += 1
)
popd

echo Benchmarking...
call timeit.cmd xcopy /Y /E "Zips" "\\192.168.254.%1\Users\Public\Downloads"

echo %endnr%>startnr.txt
endlocal
```

H. Source of timeit.cmd

Listing 6: cmd.exe batch script to calculate the amount of time used to execute a command.

```
1  @echo off
2  @setlocal
3  :: Source: http://stackoverflow.com/a/6209392
4
5  set start=%time%
6
7  :: runs your command
8  cmd /c %*
9
10 set end=%time%
11 set options="tokens=1-4 delims=:."
12 for /f %options% %%a in ("%start%") do set start_h=%%a&set /a start_m
       =100%%b %% 100&set /a start_s=100%%c %% 100&set /a start_ms=100%%d
       %% 100
13 for /f %options% %%a in ("%end%") do set end_h=%%a&set /a end_m=100%%
       b %% 100&set /a end_s=100%%c %% 100&set /a end_ms=100%%d %% 100
14
15 set /a hours=%end_h%-%start_h%
16 set /a mins=%end_m%-%start_m%
17 set /a secs=%end_s%-%start_s%
18 set /a ms=%end_ms%-%start_ms%
19 if %hours% lss 0 set /a hours = 24%hours%
20 if %mins% lss 0 set /a hours = %hours% - 1 & set /a mins = 60%mins%
21 if %secs% lss 0 set /a mins = %mins% - 1 & set /a secs = 60%secs%
22 if %ms% lss 0 set /a secs = %secs% - 1 & set /a ms = 100%ms%
23 if 1%ms% lss 100 set ms=0%ms%
24
25 :: mission accomplished
26 set /a totalsecs = %hours%*3600 + %mins%*60 + %secs%
27 rem echo Command took %hours%:%mins%:%secs%.%ms% (%totalsecs%.%ms%s
       total)
28 echo.
29 echo %start_h%:%start_m%:%start_s%.%start_ms% -- %end_h%:%end_m%:%
       end_s%.%end_ms% (%totalsecs%.%ms%s total)
```

I. Glossary

.msi Microsoft Installer

API Application Programming Interface

Appliance Fully installed/configured virtual machine that can directly be run in a virtualization environment.

AV antivirus

CIM Common Information Model

CSA Cloud Security Alliance

CTXS Citrix Systems

DaaS Desktop as a Service

DHCP Dynamic Host Configuration Protocol

DoS Denial of Service

DPI Deep Packet Inspection

DS Deep Security

DSVA Deep Security Virtual Appliance

DV Desktop Virtualization

EC2 Elastic Computing Cloud

EPSEC VMware vShield Endpoint Security

ESX Elastic Sky X (VMware ESX)

ESXi ESX Integrated

GUI Graphical User Interface

HA High Availability

HVD Hosted Virtual Desktop

IaaS Infrastructure as a Service

ICS Internet Connection Sharing

IDS Intrusion Detection System

IPC Inter-Process Communication

IPS Intrusion Prevention System

JVM Java Virtual Machine

ms milliseconds

MSDN Microsoft Developer Network

MSDNAA MSDN Academic Alliance

MSFT Microsoft

NAS Network Attached Storage

NAT Network Address Translation

NIC Network Interface Controller

OS operating system

PaaS Platform as a Service

PPTP Point-to-Point Tunneling Protocol

RDSH Remote Desktop Session Host

RHEV Red Hat Enterprise Virtualization

RHT Red Hat

SaaS Software as a Service

SAN Storage Area Network

SLR Systematic Literature Review

SMB Server Message Block

SNMP Simple Network Management Protocol

SP Service Pack

SPOF Single Point of Failure

SSD Solid State Drive

SSTP Secure Socket Tunneling Protocol

TAP Technology Alliance Partner

TCP Transmission Control Protocol

UDP User Datagram Protocol

VA Virtual Appliance

VDI Virtual Desktop Infrastructure

vGW Virtual Gateway

VHD virtual harddisk

VIB vSphere Installation Bundle

VM Virtual Machine

VMCI Virtual Machine Communication Interface

VMFS Virtual Machine File System

VMM Virtual Machine Manager/Monitor

VMW VMware

vNaS VMware vCloud Network and Security

VNIC Virtual Network Interface Controller

VPN Virtual Private Network

VXLAN Virtual Extensible LAN

WFBS Worry-Free Business Security

WPT Windows Performance Toolkit

XSL EXtensible Stylesheet Language